paloalto TECHDOCS

# Prisma Access – Verwaltung

4.00 and later



docs.paloaltonetworks.com

### Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

### About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

### Copyright

Palo Alto Networks, Inc.
www.paloaltonetworks.com

© 2022-2025 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

### Last Revised

April 11, 2025

# Table of Contents


**Prisma Access – Übersicht ..... 13**

Sicherer Internet-Verkehr mithilfe von Prisma Access ..... 17
- Die Bedeutung von Internetsicherheit ..... 17
- Prisma Access Secure Web Gateway (SWG) für die Cloud ..... 17
- Benutzer und Endpunkte mithilfe von Prisma Access schützen ..... 18

Wie Prisma Access verwaltet wird ..... 19

Sichtbarkeit und Überwachung von Prisma Access mit Strata Cloud Manager ..... 23

Prisma Access Standorte ..... 25
- Compute-Standorte, Stadt und Land ..... 26
- Schauplatz und Standortgruppe ..... 31
- Standorte nach Region ..... 35
- Standorte mit explizitem Proxy ..... 40
- Colo-Connect-Standort ..... 41
- Unterstützte Regionen des Strata Logging Service ..... 42
- Remote-Netzwerke – Standorte mit hoher Leistung, Replikation des Datenverkehrs und sicherem eingehenden Zugriff ..... 43
- Prisma Access-Standorte in China ..... 46
- Standorte des Typs „FedRAMP Moderate“ und „FedRAMP High“ ..... 46
- Karte der Standorte in Nordamerika ..... 46
- Standorte in lokalen Zonen ..... 47
- **Prisma Access und Verarbeitungsstandorte für zugehörige Dienste** ..... 48

Prisma Access-Infrastrukturverwaltung ..... 50

Prisma Access-APIs ..... 52
- APIs für Prisma Access (Managed by Strata Cloud Manager) ..... 52
- APIs für Prisma Access (Managed by Panorama) ..... 52
- Zugriff auf die Prisma Access (Managed by Panorama)-API über die Browser- und Webschnittstelle ..... 53
- curl-Befehle zum Abrufen der von Panorama verwalteten API-Befehle verwenden ..... 55
- CLI-Befehle mit Prisma Access (Managed by Panorama) verwenden ..... 56
- Prisma Access Insights-APIs ..... 56

Prisma Access von Panorama zu Strata Cloud Manager migrieren ..... 58
- Vorbereitung der Migration zu Prisma Access (Managed by Strata Cloud Manager) ..... 58
- Migration Ihrer Prisma Access (Managed by Panorama)-Bereitstellung zu Strata Cloud Manager ..... 59

**Prisma Access – Versionen und Upgrades ..... 73**

Prisma Access-Versionstypen ..... 74


 ©2025 Palo Alto Networks, Inc.

Dringend geplante Upgrades....75
Prisma Access Upgrade-Arten....76
Kadenz für Software- und Inhaltsaktualisierungen für Prisma Access....79
Prisma Access Dataplane-Upgrades....86
Upgrade-Benachrichtigungen und Updates erhalten....92
Anzeigen der Prisma Access-Softwareversionen....98
Prisma Access (Managed by Strata Cloud Manager)....98
Prisma Access (Managed by Panorama)....99
**Prisma Access-Einrichtung....103**
Prisma Access einrichten....105
Konfigurieren der Prisma Access-Serviceinfrastruktur....113
Mobile Benutzer: IP-Adresszuweisung....128
Beispiel: Beispiele für die Skalierung öffentlicher IP-Adressen (Mobile Benutzer)....129
Loopback-IP-Adresszuweisung (Mobile Benutzer)....131
Remote-Netzwerke: IPSec-Terminierungsknoten und Dienst-IP-Adressen....134
Remote-Netzwerke: Änderungen der IP-Adresse im Zusammenhang mit der Bandbreitenzuweisung....135
Remote-Netzwerke: Zuweisung von Dienst-IP-Adressen und Ausgangs-IP-Adressen....138
Abrufen der IP-Adressen für Prisma Access....139
IP-Optimierung für Bereitstellungen des Typs „Mobile Benutzer – GlobalProtect“ und....168
API-Beispiele zum Abrufen von Prisma Access-IP-Adressen....170
Benachrichtigungen erhalten, wenn IP-Adressen von Prisma Access sich ändern....173
Verwenden von Legacy-Skripten zum Abrufen von IP-Adressen....175
Abrufen von IP-Adressen mobiler Benutzer....178
Abrufen von öffentlichen IP-Adressen sowie Loopback- und Ausgangs-IP-Adressen....179
Prisma Access-Zonen....182
DNS für Prisma Access....184
Hochverfügbarkeit für Prisma Access....190
Vordefinierte Vorlagen: Dienstverbindung oder Remote-Netzwerk einbinden....193
Unterstützte IKE- und IPSec-Verschlüsselungsprofile für gängige SD-WAN-Geräte....198
**Prisma Access-Dienstverbindungen....201**
Dienstverbindung planen....203
Sammeln dieser Informationen zu Ihren Zentralen oder Rechenzentren....203
Konfigurieren einer Dienstverbindung in Prisma Access....205

 ©2025 Palo Alto Networks, Inc.

Aktivieren Sie den Zugriff zwischen mobilen Benutzern und Remote-Netzwerken mithilfe einer Dienstverbindung....235
Hinweise zu dynamischem Routing für Dienstverbindungen....237
Funktionsweise: Routing von Dienstverbindungsverkehr....237
Prisma Access-Standardrouting....238
Hot-Potato-Routing....242
**Prisma Access ZTNA-Connector....247**
ZTNA-Connector-Komponenten....249
Anwendungsfälle für ZTNA-Connector....250
Unterstützte Anwendungsfälle für Dienstverbindungen und ZTNA-Connector....254
Prinzipien von ZTNA-Connector 2.0....255
Anforderungen und Richtlinien für ZTNA-Connector....256
Unterstützte Versionen und Anforderungen von Prisma Access....256
App-Unterstützung....257
Einschränkungen bei Features und Funktionalität....258
Überlegungen zu Skalierung und Durchsatz....259
Unterstützte Umgebungen für das Anwendungshosting....259
Netzwerkanforderungen....260
Zuzulassende IP-Adressen und FQDNs für ZTNA-Connector....262
Zertifikatverwaltung....265
ZTNA-Connector aktivieren....267
ZTNA-Connector konfigurieren....274
Upgrade von ZTNA-Connectors....283
ZTNA-Connector-Diagnosetools....286
Connector-IP-Blöcke löschen....294
Automatische Erkennung von Anwendungen mit Cloud Identity Engine einrichten....299
Zielerkennung für private Anwendungen....300
Sicherheitsrichtlinie für Apps mit ZTNA-Connector-Aktivierung....307
ZTNA-Connector-VM in Ihr Rechenzentrum einbinden....325
Unterstützte ZTNA-Connector-Bereitstellungen....325
Microsoft Azure-Bereitstellungen, die von ZTNA-Connector unterstützt werden....329
Von ZTNA-Connector unterstützte Bereitstellungen der Google Cloud Platform....345
Von ZTNA-Connector unterstützte Amazon Web Services-Bereitstellungen....355
VMware ESXi-Bereitstellungen, unterstützt von Prisma Access ZTNA-Connector....362
KVM-Bereitstellungen, die von Prisma Access ZTNA-Connector unterstützt werden....373

 ©2025 Palo Alto Networks, Inc.

Hyper-V-Bereitstellungen, die von Prisma Access ZTNA-Connector unterstützt werden..... 378
ZTNA-Connector überwachen..... 392
Anzeigen von ZTNA-Connector-Protokollen..... 395
Beibehalten der Benutzer-ID-Zuordnung für ZTNA-Connector-Verbindungen mit Quell-NAT..... 398

**Einstellungen für Zugriff mit dynamischen Rechten konfigurieren..... 409**

Was bedeutet Zugriff mit dynamischen Rechten?..... 410
Zugriff mit dynamischen Rechten für Prisma Access über Common Services aktivieren..... 412
Autorisieren der Benutzergruppenzuordnung in Cloud Identity Engine für den Zugriff mit dynamischen Rechten..... 414
Zugriffsagenten aktivieren..... 422
Agent-Infrastruktur für den Zugriff mit dynamischen Rechten einrichten..... 423
Infrastruktureinstellungen konfigurieren..... 423
Prisma Access-Standorte auswählen..... 424
SC-NAT-Unterstützung für Zugriff mit dynamischen Rechten aktivieren..... 426
Routenzusammenfassung für Zugriff mit dynamischen Rechten aktivieren..... 428
Erstellen eines Snippets..... 430
Konfigurieren projektspezifischer Prisma Access Agent-Einstellungen..... 433
Konfigurieren von Weiterleitungsprofilen zum Verwalten des Agent-Datenverkehrs für Agenten für den Zugriff mit dynamischen Rechten..... 433
Konfigurieren der Einstellungen der Prisma Access Agent-App für den Zugriff mit dynamischen Rechten..... 441
Konfigurieren von DNS-Einstellungen für den Zugriff mit dynamischen Rechten..... 446
Konfigurieren der Einstellungen für HIP-Datenerfassung für den Zugriff mit dynamischen Rechten..... 447
Projekt erstellen..... 450
Datenverkehrslenkung für den Zugriff mit dynamischen Rechten..... 453
Prisma Access Agent für Zugriff mit dynamischen Rechten einrichten..... 455
Konfigurieren mehrstufiger Rollouts für den Prisma Access Agent..... 455
Konfigurieren allgemeiner globaler Einstellungen für Prisma Access Agents..... 458
Konfigurieren von HIP-Benachrichtigungen für den Zugriff mit dynamischen Rechten in Prisma Access Agent..... 461
Prisma Access Agent-Konfiguration per Push übertragen..... 467
Prisma Access Agent-Paket mit aktiviertem Zugriff mit dynamischen Rechten herunterladen..... 468
Mit dem Prisma Access Agent auf Ihre Projekte zugreifen..... 469

 ©2025 Palo Alto Networks, Inc.

Prisma Access Agent installieren....469
Anmeldung beim Prisma Access Agent, für den der Zugriff mit dynamischen Rechten aktiviert ist....473
Ändern der Vorgaben für den aktivierten Zugriff mit dynamischen Rechten Prisma Access Agent....475
Verbindung von Prisma Access Agent mit aktiviertem Zugriff mit dynamischen Rechten zu einem anderen Standort herstellen....476
Zu einem anderen Projekt wechseln....477
Verbindung von Prisma Access Agent mit aktiviertem Zugriff mit dynamischen Rechten zu einem anderen Server herstellen....477
Zwischen dem Prisma Access Agenten und der GlobalProtect-App wechseln....478
Anzeigen und Überwachen von Benutzern mit Zugriff mit dynamischen Rechten....480
Verbundene Benutzer....480
Anzeigen und Überwachen von Projekten mit Zugriff mit dynamischen Rechten....486
Projekte....486

**Prisma Access Colo-Connect....489**

Colo-Connect-Anwendungsfälle....491
Zugriff auf private Apps mit hoher Bandbreite....491
Private Konnektivität für private Anwendungen....491
Verwenden eines NaaS-Drittanbieters....491
Wie unterscheidet sich Colo-Connect von Dienstverbindungen und ZTNA-Connector?....493
Von Colo-Connect nicht unterstützte Produktmerkmale und Funktionalität....494
Anforderungen und Voraussetzungen für Prisma Access Colo-Connect....495
Konfigurieren von Prisma Access Colo-Connect....497

**App-Beschleunigung in Prisma Access....553**

Anforderungen und Richtlinien für die App-Beschleunigung....555
App-Beschleunigung konfigurieren....558

**Prisma Access Mobile Benutzer....581**

Mobile Benutzer: GlobalProtect....583
Planungscheckliste für GlobalProtect auf Prisma Access....584
GlobalProtect für mobile Benutzer einrichten....587
GlobalProtect — Tunneleinstellungen anpassen....623
GlobalProtect – Anpassen der App-Einstellungen....628
Ticketanforderung zur Deaktivierung von GlobalProtect....639
GlobalProtect-Voranmeldung....643
GlobalProtect – Clientloses VPN....660

 ©2025 Palo Alto Networks, Inc.

GlobalProtect für mobile Benutzer überwachen ..... 662
IP-Adresspools für eine GlobalProtect-Bereitstellung für mobile Benutzer ..... 668
Wie die GlobalProtect-App Prisma Access-Standorte für mobile Benutzer auswählt ..... 674
Zulassungslisten mobiler GlobalProtect-Benutzer erstellen ..... 676
GlobalProtect-App-Upgrades ..... 688
Prisma Access mit lokalen GlobalProtect-Gateways integrieren ..... 697
Mobile Benutzer: Expliziter Proxy ..... 708
Konfigurationsrichtlinien für den expliziten Proxy ..... 711
GlobalProtect im Proxy-Modus ..... 715
GlobalProtect im Tunnel- und Proxy-Modus ..... 730
Sichtbarkeit und Durchsetzung privater IP-Adressen für agentenbasierten Proxy-Verkehr ..... 754
SAML-Authentifizierung für expliziten Proxy ..... 756
„Expliziter Proxy“ einrichten ..... 759
Kerberos-Authentifizierung für Bereitstellungen des Typs „Expliziter Proxy“ ..... 784
Cloud Identity Engine-Authentifizierung für Bereitstellungen mit explizitem Proxy ..... 820
Proxy-Modus in Remote-Netzwerken ..... 825
Wie der explizite Proxy Benutzer identifiziert ..... 836
Weiterleitungsprofile des expliziten Proxys ..... 838
Richtlinien für PAC-Dateien ..... 847
Expliziter Proxy – Best Practices ..... 854
Expliziter Proxy – Überwachung und Fehlerbehebung ..... 855
Einstellungen für expliziten Proxy blockieren ..... 858
Expliziten Proxy-Internetverkehr mit speziellen Objekten auf bestimmte IP-Adressen beschränken ..... 860
Zugriff auf Ihr Rechenzentrum mit explizitem Proxy ..... 861
App-basierte Office 365-Integration mit explizitem Proxy ..... 865
Konfigurieren der Proxy-Verkettung mit Blue Coat Proxy ..... 869
Einen expliziten Proxy mit GlobalProtect (oder einem VPN eines Drittanbieters) verwenden ..... 874
IP-Adressoptimierung für Benutzer von explizitem Proxy – Proxy-Bereitstellungen ..... 889
DNS-Auflösung für Bereitstellungen für mobile Benutzer – Expliziter Proxy ..... 890
Anzeigen von Zuordnungen von Benutzern zu IP-Adressen oder Benutzergruppen ..... 892
Probleme beim Zugriff auf Websites von mobilen Benutzern melden ..... 898
Mobilen Benutzern die Authentifizierung bei Prisma Access ermöglichen ..... 900

 ©2025 Palo Alto Networks, Inc.

Authentifizierungsunterstützung und -funktionen ..... 902
Authentifizierung einrichten ..... 907
Mobilen Benutzern den Zugriff auf Unternehmensressourcen ermöglichen ..... 913

**Prisma Access-Remote-Netzwerke ..... 917**

Planungscheckliste für Remote-Netzwerke ..... 918
Remote-Netzwerkbandbreite zuweisen ..... 923
Migration zum neuen Modell planen ..... 939
Bandbreitenzuweisung für eine migrierte Bereitstellung mit aggregierter Bandbreite ..... 942
QoS-Migrationsrichtlinien ..... 944
Migration Ihrer Bandbreitenverwaltungseinstellungen ..... 949
Remote-Netzwerk einbinden ..... 956
Verbinden eines Remote-Netzwerkstandorts mit Prisma Access ..... 983
Hinzufügen primärer und sekundärer IPSec-VPN-Tunnel ..... 983
Weitere IKE Optionen ..... 984
Weitere IPSec-Optionen ..... 986
Routing für Ihr Remote-Netzwerk aktivieren ..... 987
Fehlerbehebung bei Standortverbindungen ..... 990
Mehrere Remote-Netzwerke einbinden ..... 992
Felder in der Remote-Netzwerk-Tabelle ..... 994
Verbindung des Remote-Netzwerks mit Prisma Access prüfen ..... 1005
Überprüfen des BGP-Status einer Remote-Verbindung ..... 1008
Konfigurieren eines über WAN-Link verbundenen Remote-Netzwerks und einer Serviceverbindung ..... 1009
QoS für Remote-Netzwerke ..... 1012
Garantierte Bandbreite ändern ..... 1031
Remote-Netzwerke – Hohe Leistung ..... 1034
Leistungsstarke Remote-Netzwerke – Funktionen und Richtlinien ..... 1034
Freigegebene Desktop-VDI mithilfe eines Terminalservers in Prisma Access integrieren ..... 1056

**Prisma Access – Überwachung und Transparenz ..... 1065**

Protokolle von Prisma Access ..... 1067
Externe Protokolle und andere Daten ..... 1069
Prisma Access Dashboards für Aktivitäten und Berichte ..... 1070
Prisma Access in Strata Cloud Manager anzeigen und überwachen ..... 1072
Erste Schritte bei der Prisma Access-Überwachung in Strata Cloud Manager ..... 1073
Anzeigen und Überwachen von Anwendungen ..... 1076
Anzeigen und Überwachen der App-Beschleunigung ..... 1079
Anzeigen mobiler Benutzer ..... 1081

 ©2025 Palo Alto Networks, Inc.

Anzeigen und Überwachen von IPv6 für mobile Benutzer....1081
Anzeigen und Überwachen von Zweigstellen....1083
Anzeigen und Überwachen von Rechenzentren....1090
Anzeigen und Überwachen von Netzwerkdiensten....1109
Anzeigen der Abonnementnutzung....1114
Anzeigen und Überwachen von Prisma Access-Standorten....1116
Anzeigen und Überwachen der IDs von Drittanbietergeräten....1118
Anzeigen und Überwachen der Remote-Browser-Isolation....1120
Prisma Access und Autonomous DEM....1122

**Benutzerbasierte Richtlinie in Prisma Access....1123**

Konfigurieren benutzerbasierter Richtlinien für Prisma Access....1124
Cloud Identity Engine in Prisma Access integrieren....1127
Abrufen von Benutzer-ID-Gruppenzuordnungen für Prisma Access....1134
Identitätsweitergabe....1144
Konfigurieren der Geräte-ID von Drittanbietern in Prisma Access....1160
APIs für Geräte-IDs von Drittanbietern....1167
Urteile aktualisieren....1167
**Alle Urteile löschen**....1170
Abfrageurteile....1171
**Abfrageurteile nach IP-Adresse**....1173
Abfrageurteil Statistiken....1174

**Mehrmandantenfähigkeit von Prisma Access....1177**

Konfiguration mit Mehrmandantenfähigkeit – Übersicht....1178
Mehrmandantenbereitstellung planen....1183
Von Grund auf neue Bereitstellung mit mehreren Mandanten erstellen....1186
Mehrmandantenfähigkeit aktivieren und den ersten Mandanten migrieren....1187
Mandanten zu Prisma Access hinzufügen....1195
Mandanten löschen....1201
Administrative Benutzer auf Mandantenebene erstellen....1206
Steuern des rollenbasierten Zugriffs für administrative Benutzer auf Mandantenebene....1210
Entfernen des Plug-in-Zugriffs für einen administrativen Benutzer auf Mandantenebene....1211
Protokolle nach Gerätegruppen-ID in einer Mehrmandantenbereitstellung sortieren....1216

**Prisma Access in einer FedRAMP-Umgebung....1219**

FedRAMP-Anforderungen für Prisma Access....1220
Installationsvorbereitung und Produktaktivierung – Anforderungen....1220
Erforderliche Panorama-, Plug-in- und PAN-OS-Dataplane-Versionen....1221

 ©2025 Palo Alto Networks, Inc.

Unterstützte Prisma Access-FedRAMP-Standorte ..... 1223
Unterstützte und nicht unterstützte Funktionen in einer FedRAMP-Bereitstellung von Prisma Access ..... 1223
Konfigurieren von Prisma Access in einer FedRAMP-Umgebung ..... 1225

**Prisma Access – Erweiterte Bereitstellungen ..... 1233**

Neuen Compute-Standort für einen bereitgestellten Prisma Access-Standort hinzufügen ..... 1235
IPv6-Unterstützung ..... 1237
Unterstützung von nativem IPv6 – Übersicht ..... 1239
IPv6-Networking und #IP-Pools in Ihrer Prisma Access-Infrastruktur aktivieren und konfigurieren ..... 1243
IPv6-Networking für die Bereitstellung für mobile Benutzer – GlobalProtect aktivieren ..... 1251
IPv6-Networking für Dienstverbindungen aktivieren ..... 1256
IPv6-Networking für Remote-Netzwerke aktivieren ..... 1263
DNS-Auflösung für Bereitstellungen für mobile Benutzer – GlobalProtect und Remote-Netzwerke ..... 1274
DNS-Auflösung für Bereitstellungen für mobile Benutzer – GlobalProtect und Remote-Netzwerke ..... 1276
DNS-Auflösung für Remote-Netzwerke ..... 1278
Wie BGP IP-Adresspools mobiler Benutzer für Dienstverbindungen und Remote-Netzwerkverbindungen ankündigt ..... 1280
Proxy-Unterstützung für Prisma Access und Strata Logging Service ..... 1282
Blockieren Sie eingehende Verbindungen aus bestimmten Ländern ..... 1283
Sicherer Internet-Verkehr aus AWS WorkSpace ..... 1284
Eine PAC-Datei auf AWS-WorkSpace-Clients konfigurieren ..... 1284
Konfigurieren eines Standort-zu-Standort-Tunnels zwischen AWS und Prisma Access ..... 1286
Prisma Access für Netzwerke ohne Standardroute ..... 1287
Was ist ein Netzwerk ohne Standardroute? ..... 1287
Überlegungen zu Netzwerken ohne Standardroute ..... 1287
Bereitstellungsempfehlungen zur Absicherung des Internetzugangs für Netzwerke ohne Standardroute ..... 1287
Wichtige Überlegungen ..... 1288
Prisma Access-Dienstverbindungen – Erweiterte Bereitstellungen ..... 1289
Multicloud-Redundanz für Dienstverbindungen ..... 1289
Internetgebundenen Datenverkehr mittels Datenverkehrslenkung an Dienstverbindungen weiterleiten ..... 1300
Routing für Dienstverbindungsverkehr ..... 1326
Netzwerk mit hoher Bandbreite mithilfe mehrerer Dienstverbindungen erstellen ..... 1339

 ©2025 Palo Alto Networks, Inc.

Benutzer-ID- und Geräte-ID-Zuordnung für Dienstverbindungen mit Quell-NAT beibehalten ..... 1353
Erweiterte Bereitstellungen von Prisma Access Mobile Benutzer – GlobalProtect ..... 1362
Mehrere Portale in Prisma Access konfigurieren ..... 1362
Dynamische DNS-Registrierungsunterstützung für Remote-Fehlerbehebung und Updates ..... 1373
Unterstützung der Registrierung von dynamischem DNS für „Mobile Benutzer – GlobalProtect“ ..... 1388
Kompromittierte Geräte in einer GlobalProtect-Bereitstellung von Prisma Access identifizieren und unter Quarantäne stellen ..... 1395
IPv6-Datenverkehr in Bereitstellungen von „Mobile Benutzer – GlobalProtect“ gezielt umleiten oder blockieren ..... 1404
HIP-Informationen mit Prisma Access weitergeben ..... 1409
Anzeigen von HIP-Berichten ..... 1419
Unterstützung für Gzip-Codierung in clientlosem VPN ..... 1421
Replikation des Datenverkehrs in Prisma Access ..... 1423
Erweiterte Bereitstellungen für Prisma Access-Remote-Netzwerke ..... 1436
Internes Gateway von Prisma Access ..... 1436
Sicheren eingehenden Zugriff auf Remote-Netzwerkstandorte gewähren ..... 1447

**Prisma Access für Clean Pipe ..... 1475**

Prisma Access für Clean Pipe – Übersicht ..... 1476
Clean Pipe-Anwendungsfälle ..... 1476
Beispiele für Clean Pipe ..... 1477
Clean Pipe- und Partner Interconnect-Anforderungen ..... 1478
Clean Pipe-Konfiguration abschließen ..... 1480
Mehrmandantenfähigkeit aktivieren und einen Mandanten erstellen ..... 1485

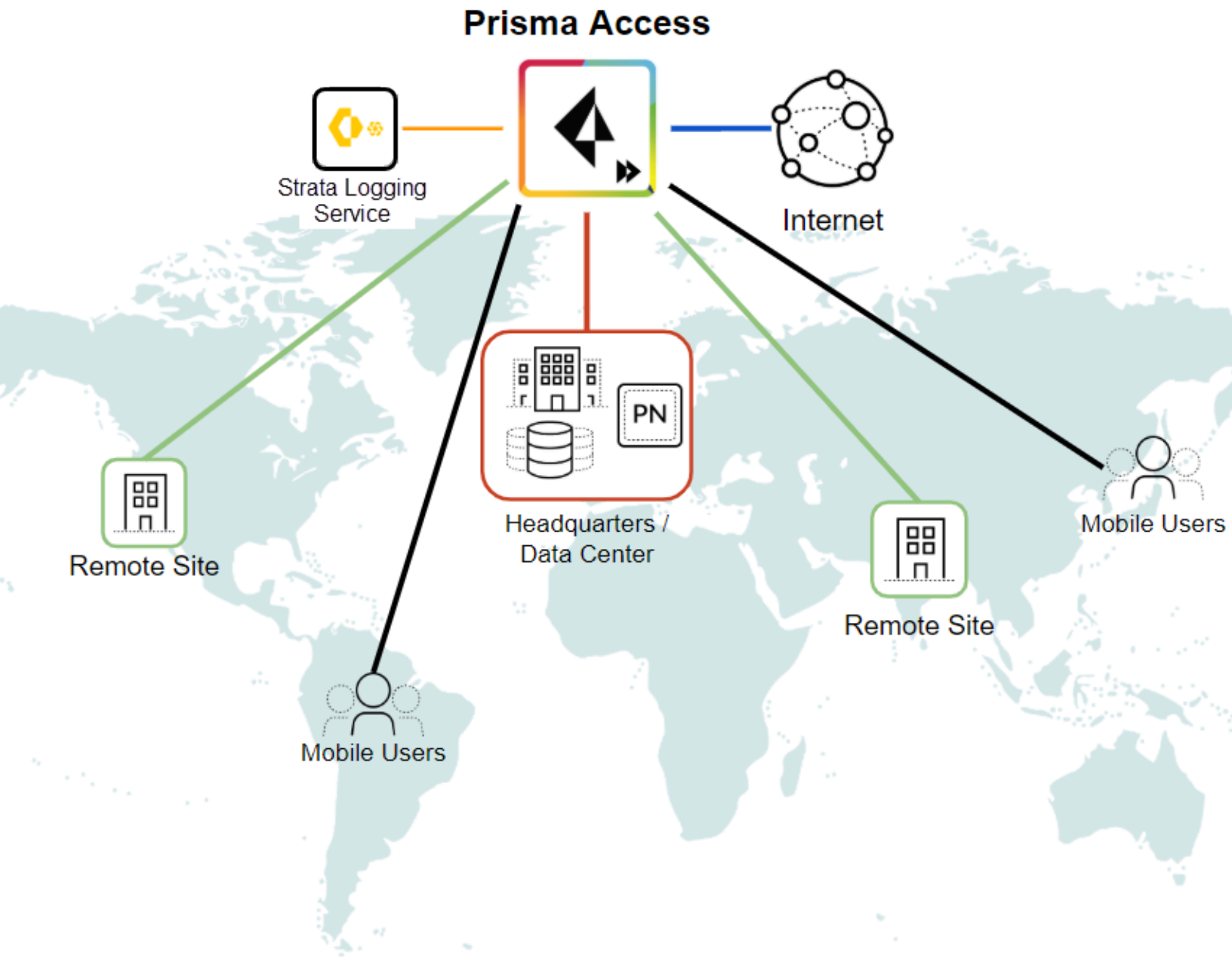
 ©2025 Palo Alto Networks, Inc.

# Prisma Access – Übersicht

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Sie müssen alle Benutzer an sämtlichen Standorten jederzeit schützen, um Ihre Anwendungen und Daten sicher zu halten. Aber wie geht das, wenn sich Ihr Fußabdruck global vergrößert, immer mehr Ihrer Benutzer mobil sind und Ihre Anwendungen und Daten aus Ihrem Netzwerk in die Cloud wandern? Prisma Access bietet diese konsistente Sicherheit, indem es Ihren Benutzern den sicheren Zugriff auf Cloud- und Rechenzentrumsanwendungen sowie das Internet ermöglicht, unabhängig davon, ob sie sich in Ihrer Zentrale oder Niederlassungen befinden oder ob sie unterwegs sind. Prisma Access überprüft konsequent den gesamten Datenverkehr über alle Ports hinweg und ermöglicht so einen sicheren Zugriff auf das Internet sowie auf Ihre sanktionierten SaaS-Anwendungen, Umgebungen in öffentlichen Clouds sowie Rechenzentren und Zentralen. Bedrohungsprävention, Malware-Prävention, URL-Filterung, SSL-Entschlüsselung und anwendungsbasierte Richtlinienfunktionen sind integriert, um Ihnen das gleiche Sicherheitsniveau zu bieten, unabhängig davon, wo sich Ihre Benutzer befinden oder auf welche Ressourcen sie zugreifen. Alle Prisma Access-Protokolle werden im Strata Logging Service gespeichert und bieten zentralisierte Analysen, Berichte und Forensik für alle Benutzer, Anwendungen und Standorte.

Prisma Access bietet umfassenden Schutz mit globaler Abdeckung, sodass Sie sich keine Sorgen um die Dimensionierung und Bereitstellung von Hardware-Firewalls in Ihren Niederlassungen oder den Aufbau und die Verwaltung von Appliances in Kollokationseinrichtungen machen müssen. Prisma Access bietet die Netzwerkinfrastruktur, um alle Ihre Remote-Niederlassungen, Ihre Zentralen, Rechenzentren und mobilen Benutzer zu verbinden, ohne dass Sie dafür eine eigene globale Sicherheitsinfrastruktur aufbauen und Ihre Betriebskapazität erweitern müssen.




Mit Prisma Access stellt Palo Alto Networks die Sicherheitsinfrastruktur weltweit bereit und verwaltet sie, um Ihre Remote-Netzwerke und mobilen Benutzer zu schützen. Prisma Access verschlüsselt die Daten durchgängig zwischen Mobile User Security Processing Nodes (MU-SPNs) und Remote Network Security Processing Nodes (RN-SPNs), zwischen SPNs und Service Connection Corporate Access Nodes (SC-CANs) sowie zwischen SC-CANs und dem Rechenzentrum.

- **Service Infrastructure** – Prisma Access sichert das Netzwerk Ihres Unternehmens mithilfe einer internen Serviceinfrastruktur. Sie stellen ein Subnetz für die Infrastruktur bereit, und Prisma Access baut mithilfe der IP-Adressen innerhalb dieses Subnetzes eine Netzwerkinfrastruktur zwischen Ihren Remote-Netzwerkstandorten und mobilen Benutzern auf und stellt

 ©2025 Palo Alto Networks, Inc.

Dienstverbindungen zu Ihren internen Netzwerkressourcen her (falls zutreffend). Die interne Kommunikation innerhalb der Cloud erfolgt über dynamisches Routing.

- **Dienstverbindungen** – Wenn Ihre Prisma Access-Lizenz diese enthält, haben Sie die Möglichkeit, IPSec-Tunnel einzurichten, um die Kommunikation zwischen internen Ressourcen in Ihrem Netzwerk und mobilen Benutzern und Benutzern an Ihren Remote-Netzwerkstandorten zu ermöglichen. Sie können beispielsweise eine Dienstverbindung zu einem Authentifizierungsserver in der Zentrale oder dem Rechenzentrum Ihres Unternehmens erstellen.

  Auch wenn Sie keine Dienstverbindung für Ihre Zentrale oder Ihr Rechenzentrum benötigen, empfehlen wir Ihnen, eine zu erstellen, um die Netzwerkkommunikation zwischen mobilen Benutzern und Remote-Netzwerkstandorten sowie zwischen mobilen Benutzern an verschiedenen geografischen Standorten zu ermöglichen.
- **Mobile Benutzer** – Bietet konsistente Sicherheit für Ihre mobilen Benutzer, unabhängig davon, ob sie auf Anwendungen in Ihrem Rechenzentrum zugreifen, SaaS-Anwendungen verwenden oder im Internet surfen. Sie können Ihren mobilen Benutzern ermöglichen, sich mit Prisma Access zu verbinden:
  - **GlobalProtect**

    Sie können die GlobalProtect-App für Ihre Benutzer bereitstellen (verfügbar für Smartphones, Tablets oder Laptops mit Microsoft Windows, Apple macOS und iOS, Android, Google Chrome OS und Linux), damit sie den Datenverkehr zur Durchsetzung von Richtlinien und zur Bedrohungsprävention an Prisma Access tunneln können. Die GlobalProtect-App stellt auch HIP-Berichte (Host Information Profile) bereit, damit Sie basierend auf dem Gerätestatus detaillierte Richtlinien erstellen können, um sicherzustellen, dass Endpunkte Ihre Sicherheitsstandards einhalten – beispielsweise bei den aktuellen Patches, Verschlüsselungs- und Virendefinitionen –, um auf Ihre sensibelsten Anwendungen zuzugreifen. Für den sicheren Zugriff auf Benutzer auf nicht verwalteten Geräten können Sie auch **Clientless VPN** aktivieren. Prisma Access wird je nach Region dynamisch ein- und ausgeschaltet, abhängig davon, wo sich Ihre Benutzer gerade befinden.
  - **Expliziter Proxy**

    Wenn das vorhandene Netzwerk Ihrer Organisation bereits explizite Proxys verwendet und PAC-Dateien auf Ihren Client-Endpunkten bereitstellt, können Sie problemlos zu Prisma Access migrieren, um den ausgehenden Internet-Verkehr mobiler Benutzer zu sichern.
- **Remote-Netzwerke** – Mit Remote-Netzwerken können Sie Remote-Netzwerkstandorte wie Zweigstellen und Benutzer in diesen Zweigstellen mit Cloud-basierten Firewalls der nächsten Generation schützen. Sie können den Zugriff auf die Subnetze an jedem Remote-Netzwerkstandort entweder über statische Routen, dynamisches Routing mit BGP oder eine Kombination aus statischen und dynamischen Routen aktivieren. Alle Remote-Netzwerkstandorte, die Sie einbinden, sind vollständig vermascht.
- **ZTNA-Connector** – Mit dem ZTNA-Connector (Zero Trust Network Access) können Sie sich einfach und sicher mit privaten Apps Ihres Unternehmens verbinden. Der ZTNA-Connector bietet mobilen Benutzern und Benutzern an Zweigstellen über einen automatisierten sicheren Tunnel Zugriff auf Ihre privaten Apps. Dadurch entfällt die Einrichtung von IPSec-Tunneln und Routing-Definitionen für den Zugriff auf die privaten Apps. Der ZTNA-Connector erfordert kein Routing von der Kundeninfrastruktur und kann Zugriff auf Anwendungen bieten, die überlappende IP-Adressen in Ihren Netzwerken verwenden.

 ©2025 Palo Alto Networks, Inc.

- **Strata Logging Service**–Prisma Access leitet alle Protokolle an den Strata-Protokollierungsdienst weiter. Im Rahmen der Aktivierung von Prisma Access geben Sie die Instanz des Strata Logging Servicees an, an die Sie Prisma Access-Protokolle weiterleiten möchten. Der Protokollverkehr verwendet nicht die lizenzierte Bandbreite, die Sie für Prisma Access erworben haben.

 ©2025 Palo Alto Networks, Inc.

# Sicherer Internet-Verkehr mithilfe von Prisma Access

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access | ❑ Prisma Access-Lizenz |

## Die Bedeutung von Internetsicherheit

Die Sicherung des Internetzugangs ist wichtiger als je zuvor und barg noch nie so viele Herausforderungen. Bestehende Altlösungen können ausweichende und gezielte Phishing- und andere webbasierte Angriffe nur schwer erkennen, während sie gleichzeitig neue Bedrohungen durch ungesicherten DNS-Datenverkehr vernachlässigen. Palo Alto Networks Prisma Access bietet Internetsicherheit dank einer branchenweit völlig neuen, ersten ML-basierten erweiterten URL-Filterung und mithilfe von DNS-Sicherheitsdiensten. Dank Prisma Access können Sie ausweichende und gezielte Phishing-Angriffe sowie dateilose Angriffe in Echtzeit verhindern und Schutz vor den neuesten hochentwickelten DNS-basierten Angriffen bieten.

## Prisma Access Secure Web Gateway (SWG) für die Cloud

Ein sicheres Web-Gateway ist aufgrund der zunehmenden Komplexität und Häufigkeit von Cyberbedrohungen ein entscheidendes Element in der heutigen digitalen Landschaft. Cyberkriminelle entwickeln ständig neue Taktiken und Techniken, um Sicherheitsmaßnahmen zu durchbrechen. Eine davon ist die Tarnung von bösartigem Code auf scheinbar seriösen Websites. Wenn Benutzer auf diese kompromittierten Websites zugreifen, geben sie unbeabsichtigt Anmeldeinformationen preis oder setzen Organisationen schädlichem Code aus, der – sofern er unbemerkt bleibt – verheerende Auswirkungen haben kann.

In einer derart risikoreichen Umgebung verstärkt das Fehlen eines robusten Sicherheits-Gateways das Risiko für die digitalen Assets einer Organisation erheblich. Ein solches Risiko könnte unbefugten Zugriff, Datendiebstahl und Störungen des Geschäftsbetriebs zur Folge haben, insbesondere angesichts der zunehmenden Verbreitung von Phishing- und Ransomware-Angriffen. Ohne die von SWG bereitgestellte Sicherheitsbarriere könnte ein Ransomware-Angriff eine Organisation effektiv erpressen, was zu finanziellen Verlusten und Reputationsschäden führen könnte.

Die Verwendung von verschlüsseltem Datenverkehr ist heute üblich, wobei HTTPS den Großteil des Web-Datenverkehrs ausmacht. Für eine Organisation besteht das Risiko von Sicherheitsbedrohungen, die in verschlüsselten Kanälen verborgen sind, wenn ihr ein SWG fehlt, das diesen Datenverkehr effektiv entschlüsseln und untersuchen kann.

Wenn jedoch nur Mehrpunktprodukte für SWG, Zugriff auf private Apps und CASB verwendet werden, kompliziert dies die Sache noch. Isolierte Produkte, die zu einem Angebot zusammengefügt werden, führen zu Paritätslücken und schlechten Sicherheitsergebnissen, sodass Sie anfällig für Angriffe werden. Diese Lösungen führen zu Sicherheitslücken bei Internet- und privaten Apps.

Um diese Herausforderungen zu bewältigen, bietet Prisma Access ein einheitliches Produkt an, das Management, Richtlinien und Daten für alle Benutzer und Apps über alle Funktionen hinweg konvergiert, einschließlich ZTNA, SWG, NG-CASB, FWaaS, DLP und mehr.

 ©2025 Palo Alto Networks, Inc.

Kunden können problemlos von älteren lokalen und cloudbasierten Proxy-Lösungen zu Prisma Access migrieren, um Inline-Sichtbarkeit zu erreichen und den Datenverkehr von Internet- und SaaS-Apps mithilfe branchenführender, KI-gestützter Sicherheitsschutzmaßnahmen zu kontrollieren.

## Benutzer und Endpunkte mithilfe von Prisma Access schützen

Prisma Access ist darauf ausgelegt, erfolgreiche Cyberangriffe zu verhindern. Daher bietet es mehr als nur die Absicherung des Webs. Um Cyberangriffe zu stoppen, muss der gesamte Datenverkehr untersucht werden. Alles ohne vollständige Inspektion des gesamten Datenverkehrs führt zu einer erheblichen Sicherheitslücke. Prisma Access schützt konsequent den gesamten Datenverkehr an allen Ports und vor allen Anwendungen. Dies ermöglicht Ihrem Unternehmen Folgendes:

- Verhindern erfolgreicher Cyberangriffe mit bewährten Sicherheitsphilosophien und Bedrohungsinformationen für umfassende Sichtbarkeit und präzise Kontrolle, die sich über das gesamte Unternehmen erstreckt.
- Vollständige bidirektionale Untersuchung des gesamten Anwendungsverkehrs – einschließlich Datenverkehr mit SSL- oder TLS-Verschlüsselung – an allen Ports, unabhängig davon, ob Sie mit dem Internet, mit der Cloud oder zwischen Zweigstellen kommunizieren.
- Profitieren von umfassenden Bedrohungsdaten, die auf automatisierten Bedrohungsdaten von Palo Alto Networks und Hunderten von Drittanbieterfeeds basieren.

Lesen Sie mehr über Prisma Access und die entsprechenden Lösungen.

 ©2025 Palo Alto Networks, Inc.

# Wie Prisma Access verwaltet wird

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Es gibt zwei Möglichkeiten zur Verwaltung von Prisma Access, aber Sie können nicht zwischen den Verwaltungsschnittstellen wechseln, nachdem Sie Ihre Prisma Access-Lizenz aktiviert haben (Ausnahme ist die Verwendung des Migrations-Workflows von einer Prisma Access (Managed by Panorama)- zu einer Prisma Access (Managed by Strata Cloud Manager)-Bereitstellung). Sie müssen also vor Beginn entscheiden, wie Sie Prisma Access verwalten möchten:

- **Prisma Access (Managed by Strata Cloud Manager)**

  Zur Verwaltung von Prisma Access aus der Cloud verwenden Sie Strata Cloud Manager. Mit der Cloud-Verwaltung können Sie Zweigstellen und mobile Benutzer schnell durch aufgabengesteuerte Workflows einbinden, mit denen Sie Ihre Umgebung in wenigen Minuten einrichten und testen können. Die Cloud-Verwaltung mit Strata Cloud Manager vereinfacht den Onboardingprozess durch die Bereitstellung vordefinierter Richtlinienregeln für den Internetzugang und die Entschlüsselung auf der Grundlage von Best Practices. Richten Sie schnell IPSec-Tunnel mit Standardeinstellungen ein, die für die gängigsten IPSec-fähigen Geräte geeignet sind, und aktivieren Sie die SSL-Entschlüsselung für empfohlene URL-Kategorien.

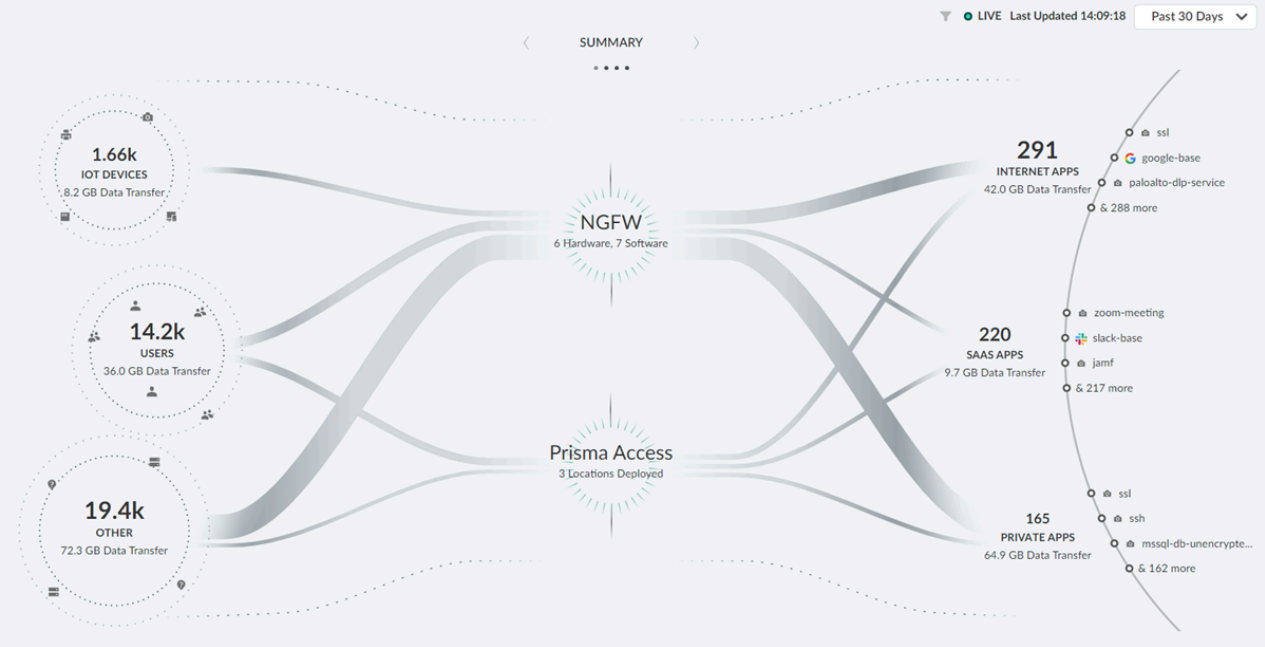
  **Strata Cloud Manager Command Center**

  Die Seite Strata Cloud Manager Command Center wird angezeigt, wenn Sie Ihren Strata Cloud Manager starten. Dieses Command Center hilft Ihnen bei der Bewertung des Zustands Ihres Netzwerks, verbessert die Transparenz und bietet eine Übersicht Ihrer Daten. Das Command Center verfügt über verschiedene Dashboards, um verschiedene Berichtstypen anzuzeigen.

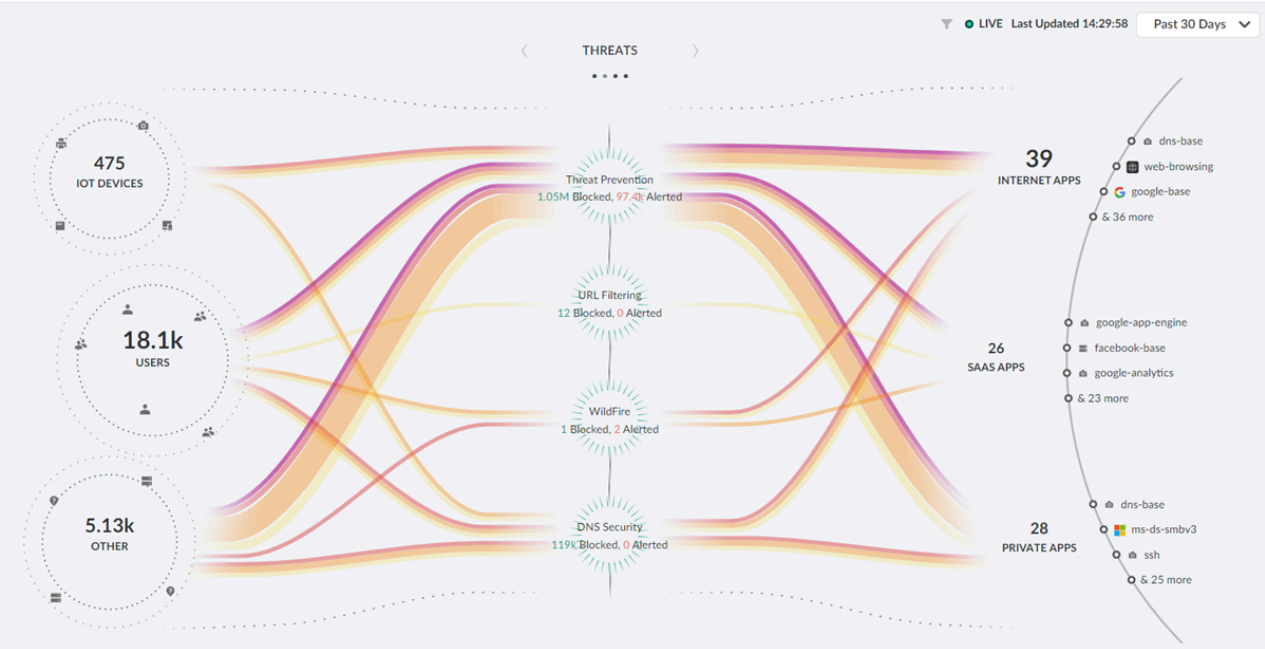
  - **Zusammenfassung**: Im Dashboard mit der Zusammenfassung können Sie die verschiedenen Datenquellen und Plattforminfrastrukturen wie NGFW oder Prisma Access anzeigen, über

 ©2025 Palo Alto Networks, Inc.

die die Daten von verschiedenen Datenquellen zu verschiedenen Anwendungen in Ihrem Netzwerk fließen.



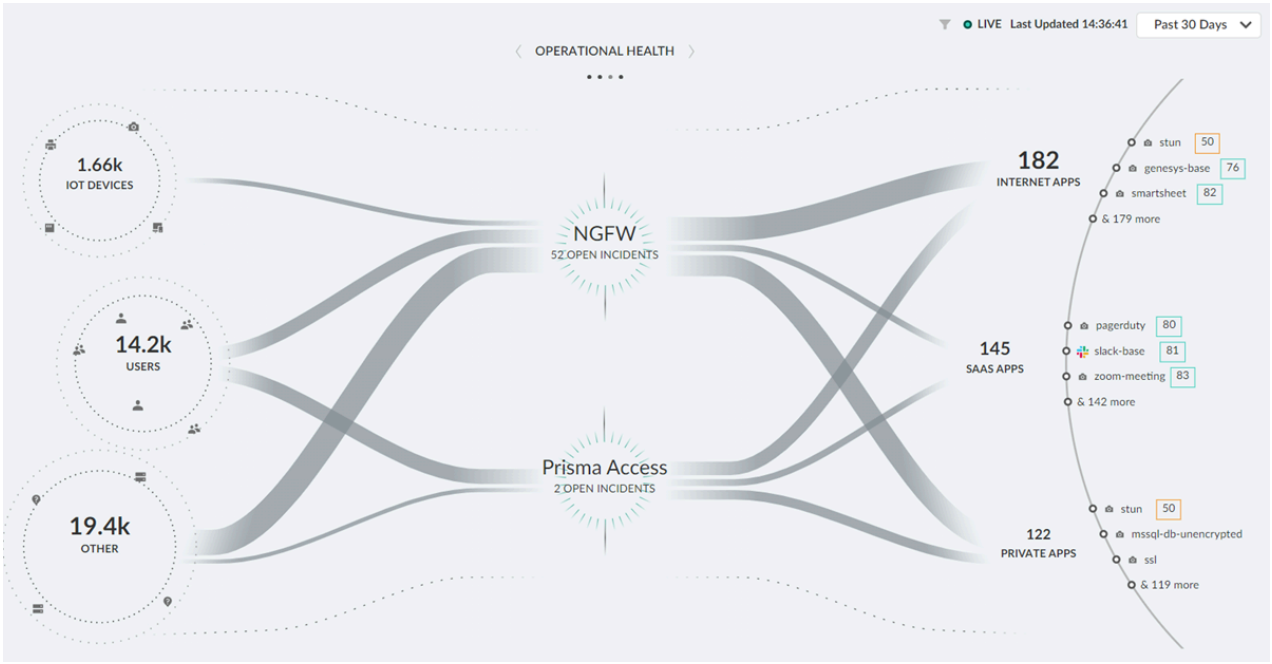

- **Bedrohungen**: In Ihrem Bedrohungs-Dashboard können Sie die Bedrohungen anzeigen, die von Ihren Sicherheitsanwendungen erkannt wurden. Sie können dieses Dashboard verwenden, um die blockierten und zugelassenen Bedrohungen in Ihrem Netzwerk zu überwachen oder Bereiche Ihres Netzwerks zu untersuchen, die möglicherweise einen geringen Prozentsatz des überprüften Datenverkehrs aufweisen.




- **Betriebszustand**: Zeigt den Zustand und die Benutzererfahrung in Ihrem Netzwerk an, wenn es von ADEM überwacht wird. Sie können diese Ansicht verwenden, um die

 ©2025 Palo Alto Networks, Inc.

Benutzererfahrung in Ihrem Netzwerk zu überwachen und den Schweregrad offener Vorfälle zu überprüfen.




- **Datensicherheit**: Zeigt den Datenverkehr innerhalb Ihres Netzwerks an, der laut den DLP- und SaaS-Sicherheitsabonnements vertrauliche Daten enthält und entsprechend gekennzeichnet wurde. Sie können diese Ansicht verwenden, um den Datenfluss durch Ihre Firewalls und verbundenen SaaS-Anwendungen sowie den Schweregrad aller Datenrisiken in Ihrem Netzwerk zu überwachen.




Klicken Sie in Ihren Dashboards auf eine dieser Kategorien, um die Ergebnisse entsprechend zu filtern.

 ©2025 Palo Alto Networks, Inc.

- **Prisma Access (Managed by Panorama)**

  Verwenden Sie das Plug-in „Cloud Services“ in Panorama, um Prisma Access einzurichten und zu verwalten. Diese Option ist empfehlenswert, wenn Sie Panorama bereits zum Verwalten von Firewalls der nächsten Generation verwenden und über eine gemeinsame Richtlinie verfügen, die Sie für den Zugriff auf Ihre Unternehmensanwendungen verwenden möchten.

  *Selbst wenn Sie Panorama zur Verwaltung von Prisma Access verwenden, können Sie Strata Cloud Manager weiterhin für viele Sichtbarkeits- und Überwachungsfunktionen in Prisma Access verwenden.* Weitere Informationen.

Nachdem Sie sich entschieden haben, welche Verwaltungsoption Sie verwenden möchten, befolgen Sie zunächst den Lizenzierungs- und Aktivierungsworkflow für die ausgewählte Option:

- Für die ersten Schritte mit Prisma Access (Managed by Panorama) Access führen Sie die Lizenzaktivierung über das Kunden-Support-Portal (CSP) durch und installieren Sie das Cloud Services-Plug-in auf Panorama.
- Für die ersten Schritte mit Cloud-verwaltetem Prisma Access führen Sie die Lizenzaktivierung über den Hub durch.

***Funktionsparität zwischen Panorama und Cloud Management***

*Es gibt einige Unterschiede zwischen dem, was auf Prisma Access (Managed by Panorama) Access und Prisma Access (Managed by Strata Cloud Manager) unterstützt wird. Eine Liste der unterstützten Funktionen in Prisma Access (Managed by Panorama) und Prisma Access (Managed by Strata Cloud Manager) finden Sie in der* Kompatibilitätsmatrix.

 ©2025 Palo Alto Networks, Inc.

# Sichtbarkeit und Überwachung von Prisma Access mit Strata Cloud Manager

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (von Panorama verwaltet) | • Prisma Access-Lizenz |

Es gibt zwei Möglichkeiten zur Verwaltung von Prisma Access:

- Für Prisma Access (Managed by Strata Cloud Manager) können Sie **Strata Cloud Manager** verwenden
- oder Sie können **Panorama** verwenden, um Prisma Access zu verwalten

Über diese beiden Verwaltungsschnittstellen können Sie Onboarding, Konfiguration und Durchsetzung von Sicherheitsrichtlinien für Ihre Prisma Access-Umgebung verwalten. Prisma Access ermöglicht jedoch auch umfassende Sichtbarkeit und Überwachung für Ihre Prisma Access-Umgebung und diese Funktionen werden in Strata Cloud Manager bereitgestellt.

**Wichtig:**

Unabhängig von der Verwaltungsschnittstelle, die Sie für Prisma Access verwenden (Strata Cloud Manager oder Panorama) können Sie Strata Cloud Manager für viele Ihrer Prisma Access-Sichtbarkeitsfunktionen und für die Interaktion mit Add-on-Abonnements wie KI-gestütztem Autonomous DEM verwenden.

| Prisma Access-Sichtbarkeits- und Überwachungsfunktionen in Strata Cloud Manager | |
|---|---|
| Autonomous DEM | Bietet native End-to-End-Sichtbarkeit und Einblicke in den gesamten Benutzerdatenverkehr in Ihrer Secure Access Service Edge(SASE)-Umgebung. Die ADEM-Funktionalität ist nativ in die GlobalProtect-App und in Prisma Access integriert. Daher müssen Sie keine zusätzlichen Appliances oder Agents bereitstellen. Sie können die Ursache von Problemen mit der digitalen Erfahrung schnell isolieren und die Problembehebung vereinfachen.<br><br>*Für diese Funktion ist die Add-on-Lizenz für Autonomous DEM zur Verwendung mit Prisma Access (Managed by Panorama) Access erforderlich.* |
| Dashboards und Berichte in Strata Cloud Manager | Durch die Sichtbarkeitsfunktionen in Strata Cloud Manager gewinnen Sie wichtige Erkenntnisse, die Sie nutzen können, um Ihre Richtlinienaktualisierungen anzupassen und Lücken in der Unternehmenssicherheit und Benutzerproduktivität zu schließen. |

 ©2025 Palo Alto Networks, Inc.

| Prisma Access-Sichtbarkeits- und Überwachungsfunktionen in Strata Cloud Manager | |
|---|---|
| | • **Interaktive Dashboards**<br>Erkunden Sie Daten zu Anwendungen, Bedrohungen, Benutzern und Sicherheitsabonnements in Ihrem Netzwerk<br>• **Berichte**<br>Viele Dashboards unterstützen Berichte, in denen Sie Daten offline freigeben und regelmäßige Aktualisierungen planen können |
| Strata Cloud Manager Command Center | Das Command Center ist eine interaktive, visuelle Zusammenfassung der IoT-Geräte, Benutzer, Hosts und des Datenverkehrs in Ihrem Netzwerk. Anhand der Daten Ihrer cloudbasierten Sicherheits- und ADEM-Abonnements zeigt das Command Center wichtige Informationen zu Bedrohungen, Benutzererfahrung und Sicherheit von Daten in Ihrem Netzwerk an.<br>Das Command Center ermöglicht Ihnen die Interaktion mit den Daten und die Visualisierung der Beziehungen zwischen Ereignissen im Netzwerk, sodass Sie Anomalien aufdecken oder Möglichkeiten zur Verbesserung Ihrer Netzwerksicherheit finden können. |

 ©2025 Palo Alto Networks, Inc.

# Prisma Access Standorte

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

Sie können Prisma Access an den Standorten Ihrer Wahl bereitstellen, basierend auf den Einstellungen für den Datenstandort und dem Ort, an dem bei Ihnen die meisten Benutzer arbeiten. Prisma Access steht an über 100 Standorten weltweit zur Verfügung, damit Ihre Benutzer mit einer auf ihre Gebietsschemata zugeschnittenen Benutzeroberfläche arbeiten können. Alle Prisma Access-Standorte werden basierend auf optimierter Leistung und Latenz einem Sicherheits-Compute-Standort zugeordnet. Dies bedeutet, dass der Datenverkehr in bestimmten Ländern an diesen definierten Compute-Standort geleitet wird.

*Wenn Sie Compute-Standorte auf bestimmte Länder beschränken müssen, finden Sie weitere Informationen in der Tabelle, in der das Land der Verarbeitung für Prisma Access und die damit verbundenen Dienstleistungen aufgeführt sind.*

Es gibt verschiedene Typen von Prisma Access-Standorten:

- **Standorte, sortiert nach Compute-Standort**: Wenn Sie Remote-Netzwerke konfigurieren, weisen Sie die Bandbreite nach Compute-Standort zu. Mindestens zwei (und häufig weitere) geografisch nahe beieinander liegende Prisma Access-Standorte werden zu Gruppen von *Compute-Standorten* zusammengefasst. Dies ist die Ebene, auf der Sie Bandbreite zuweisen, anstatt die Bandbreite für einzelne Prisma Access-Standorte oder für bestimmte Remote-Netzwerkstandorte zuzuweisen, wodurch Prisma Access Standorten an einem Compute-Standort basierend auf Last oder Bedarf dynamisch Bandbreite zuweisen kann.
- **Schauplatz- und Standortgruppe** – Wenn Sie in einer Bereitstellung des Typs „Mobile Benutzer – GlobalProtect“ IP-Adresspools zuweisen, können Sie IP-Pools nach Standortgruppe (eine Gruppe von Standorten, die kleiner als der Schauplatz ist), Schauplatz oder weltweit angeben. Verwenden Sie standortgruppenspezifische IP-Adresspools, wenn Sie über Dienste verfügen, die von der Quell-IP-Adresse des Benutzers abhängen, um die Details des Benutzers zu identifizieren (z. B. standortbasierte Dienste oder Dienste, die auf einer Benutzergruppe oder -funktion basieren), damit Sie Zugriffssteuerungsrichtlinien anwenden können oder um Routing- bzw. Richtlinienvorgänge für verschiedene Länder durchzuführen, wenn sich die Länder in unterschiedlichen Rechenregionen befinden.
- **Standorte nach Region** – Jeder Prisma Access-Standort verfügt über eine zugeordnete Region.
- **Standorte mit explizitem Proxy** – Expliziter Proxy verfügt über einen eigenen Satz von Standorten mit einer Teilmenge von Prisma Access-Standorten.
- **Colo-Connect-Standorte** – Colo-Connect verfügt über einen eigenen Satz von Standorten mit einer Teilmenge von Prisma Access-Standorten.
- **Regionen des Strata-Protokollierungsdienstes** – Prisma Access unterstützt eine Teilmenge von Regionen des Strata-Protokollierungsdienstes.

 ©2025 Palo Alto Networks, Inc.

- **Remote-Netzwerke – Standorte mit hoher Leistung, Replikation des Datenverkehrs und sicherem eingehenden Zugriff** – Bereitstellungen der Typen Leistungsstarke Remote-Netzwerke, Replikation des Datenverkehrs und Sicherer eingehender Zugriff verwenden eine Teilmenge von Prisma Access-Standorten.
- **Prisma Access-Standorte in China** – Bereitstellungen des Typs Prisma Access China verwenden Standorte in der VR China.
- **Standorte des Typs „FedRAMP Moderate“ und „FedRAMP High“** – Prisma Access Bereitstellungen des Typs „FedRAMP Moderate“ und „FedRAMP High“ verwenden eine Teilmenge von Prisma Access-Standorten.
- **Karte der Standorte in Nordamerika** – Verwenden Sie zur Orientierung bei der Auswahl von Standorten in Nordamerika diese Karte, auf der die geografische Abdeckung für Standorte in Nordamerika zu sehen ist.
- **Lokale Zonen** – Lokale Zonen platzieren Rechen-, Speicher-, Datenbank- und andere Dienste in der Nähe von großen Bevölkerungs- und Industriezentren. Diese Standorte verfügen über eigene Compute-Standorte.

  *Wenn Sie eine lokale Zone hinzufügen möchten, wenden Sie sich an Ihren Palo Alto Networks Vertreter.*

  Beachten Sie beim Bereitstellen lokaler Zonen die folgenden Richtlinien:

  - Standorte in lokalen Zonen unterstützen IPv6 nicht.
  - Standorte in lokalen Zonen verwenden keine bei Palo Alto Networks registrierten IP-Adressen.
  - Unterstützung von 1 Gbit/s für Remote-Netzwerke ist nicht verfügbar.
  - Die Redundanz von Remote-Netzwerk- und Dienstverbindungsknoten über Verfügbarkeitszonen hinweg ist nicht verfügbar, wenn Sie sie in derselben lokalen Zone bereitstellen, da beide Knoten in einer einzigen Zone bereitgestellt werden.
  - Diese lokalen Zonen verwenden keine bei Palo Alto Networks registrierten IP-Adressen. Wenn Sie Probleme beim Zugriff auf URLs haben, melden Sie das Problem mit der Website über https://reportasite.gpcloudservice.com/ oder wenden Sie sich an den Support von Palo Alto Networks.

*Das Datenblatt zum Datenschutz von Prisma Access enthält weitere Informationen zu Prisma Access-Standorten und wo Prisma Access Datenverkehr verarbeitet.*

## Compute-Standorte, Stadt und Land

Der erste Standort, der an jedem Compute-Standort aufgeführt ist (in Fettschrift), zeigt die Stadt und das Land des Compute-Standorts an.

Bei Standorten, die mit zwei Sternchen (**) gekennzeichnet sind, handelt es sich um *lokale Zonen*, die nicht alle Prisma Access-Funktionen unterstützen.

| Compute-Standort | Prisma Access Standort | Stadt und Land |
|---|---|---|
| Asien (Nordost) | **Japan (Mitte)** | **Tokio, Japan** |

 ©2025 Palo Alto Networks, Inc.

| Compute-Standort | Prisma Access Standort | Stadt und Land |
|---|---|---|
| Asien (Süd) | **Indien (West)** | **Mumbai, Indien** |
| | Bangladesch | Dhaka, Bangladesch |
| | Indien (Süd) | Chennai, Indien |
| | Pakistan (Süd) | Karatschi, Pakistan |
| | Pakistan (West) | Lahore, Pakistan |
| Asien (Südost) (Indonesien) | **Indonesien** | **Jakarta, Indonesien** |
| Asien (Südost) (Singapur) | **Singapur** | **Singapur** |
| | Kambodscha | Phnom Penh, Kambodscha |
| | Malaysia | Kuala Lumpur, Malaysia |
| | Myanmar | Yangon, Myanmar |
| | Pakistan (West) (II) | Islamabad, Pakistan |
| | Philippinen | Quezon City, Philippinen |
| | Sri Lanka | Colombo, Sri Lanka |
| | Thailand | Bangkok, Thailand |
| | Vietnam | Ho-Chi-Minh-Stadt, Vietnam |
| Australien (Süd) | **Australien (Süd)** | **Melbourne, Australien** |
| Australien (Südost) | **Australien (Südost)** | **Sydney, Australien** |
| | Australien (Ost) | Brisbane, Australien |
| | Neuseeland | Auckland, Neuseeland |
| | Papua-Neuguinea | Port Moresby, Papua-Neuguinea |
| Australien, West (Perth)** | **Australien, West (Perth)**** | **Perth, Australien** |
| Bahrain | **Bahrain** | **Manama, Bahrain** |
| Belgien | **Belgien** | **St. Ghislain, Belgien** |
| | Lettland | Riga, Lettland |
| | Senegal | Dakar, Senegal |
| Kanada, Mitte (Montreal) | **Kanada (Ost)** | **Quebec, Kanada** |
| Kanada, Mitte (Toronto) | **Kanada (Mitte)** | **Toronto, Kanada** |


©2025 Palo Alto Networks, Inc.

| Compute-Standort | Prisma Access Standort | Stadt und Land |
|---|---|---|
| Kanada, West (Calgary) | **Kanada (West)** | **Calgary, Kanada** |
| Europa (Mitte) | **Deutschland (Mitte)** | **Frankfurt, Deutschland** |
| | Österreich | Wien, Österreich |
| | Bulgarien | Sofia, Bulgarien |
| | Kroatien | Zagreb, Kroatien |
| | Tschechien | Prag, Tschechische Republik |
| | Ägypten | Kairo, Ägypten |
| | Deutschland (Nord) | Hamburg, Deutschland |
| | Deutschland (Süd) | München, Deutschland |
| | Griechenland | Athen, Griechenland |
| | Ungarn | Budapest, Ungarn |
| | Kuwait | Al Ahmadi, Kuwait |
| | Liechtenstein | Schaan, Liechtenstein |
| | Luxemburg | Luxemburg-Stadt, Luxemburg |
| | Republik Moldau | Chisinau, Moldawien |
| | Nigeria | Lagos, Nigeria |
| | Rumänien | Bukarest, Rumänien |
| | Slowakei | Bratislava, Slowakei |
| | Slowenien | Ljubljana, Slowenien |
| | Türkei | Istanbul, Türkei |
| | Ukraine | Kiew, Ukraine |
| | Usbekistan | Taschkent, Usbekistan |
| Europa, Mitte (Warschau) | **Polen** | **Warschau, Polen** |
| Europa (Nord) | **Finnland** | **Hamina, Finnland** |
| | Belarus | Minsk, Weißrussland |
| | Kasachstan | Astana, Kasachstan |
| | Litauen | Vilnius, Litauen |
| | Norwegen | Oslo, Norwegen |
| | Russland (Mitte) | Moskau, Russland |
| | Russland (Nordwest) | Sankt Petersburg, Russland |


©2025 Palo Alto Networks, Inc.

| Compute-Standort | Prisma Access Standort | Stadt und Land |
|---|---|---|
| Europa Nord (Stockholm) | **Schweden** | **Stockholm, Schweden** |
| Europa (Nordwest) | **Vereinigtes Königreich**<br>Ghana | **London, Vereinigtes Königreich**<br>Accra, Ghana |
| Europa (Nordwest), Paris | **Frankreich (Süd)** | **Paris, Frankreich** |
| Europa (Süd) | **Italien**<br>Jordanien<br>Kenia<br>Monaco | **Mailand, Italien**<br>Amman, Jordanien<br>Mombasa, Kenia<br>Monaco |
| Europa (Südwest) | **Spanien (Mitte)**<br>Andorra<br>Portugal<br>Spanien (Ost) | **Madrid, Spanien**<br>Andorra la Vella, Andorra<br>Lissabon, Portugal<br>Barcelona, Spanien |
| Europa (West) | **Niederlande (Mitte)**<br>Dänemark<br>Niederlande (Süd) | **Eemshaven, Niederlande**<br>Kopenhagen, Dänemark<br>Rotterdam, Niederlande |
| Frankreich (Nord) | **Frankreich (Nord)** | **Paris, Frankreich** |
| Hongkong | **Hongkong** | **Hongkong, China** |
| Indien (Nord) | **Indien (Nord)** | **Neu-Delhi, Indien** |
| Irland | **Irland** | **Dublin, Irland** |
| Japan (Süd) | **Japan (Süd)** | **Osaka, Japan** |
| Naher Osten (Mitte) (Katar) | **Katar** | **Doha, Katar** |
| Naher Osten (Mitte) (Saudi-Arabien) | **Saudi Arabien** | **Riad, Saudi-Arabien** |
| Naher Osten (Mitte) (VAE) | **Vereinigte Arabische Emirate** | **Dubai, Vereinigte Arabische Emirate** |
| Naher Osten (West) | **Israel** | **Tel Aviv, Israel** |


©2025 Palo Alto Networks, Inc.

| Compute-Standort | Prisma Access Standort | Stadt und Land |
|---|---|---|
| Nigeria (Lagos)** | **Nigeria (Lagos)**** | **Lagos, Nigeria** |
| Neuseeland (Auckland)** | **Neuseeland (Auckland)**** | **Auckland, Neuseeland** |
| Südafrika (Mitte) | **Südafrika (Mitte)** | **Johannesburg, Südafrika** |
| Südafrika (West) | **Südafrika (West)** | **Kapstadt, Südafrika** |
| Südamerika (Ost) | **Brasilien (Süd)**<br>Brasilien (Mitte)<br>Brasilien (Ost)<br>Paraguay<br>Venezuela | **São Paulo, Brasilien**<br>Brasília, Brasilien<br>Rio de Janeiro, Brasilien<br>Asunción, Paraguay<br>Caracas, Venezuela |
| Südamerika (West) | **Chile**<br>Argentinien<br>Bolivien<br>Peru<br>Uruguay | **Santiago, Chile**<br>Buenos Aires, Argentinien<br>Santa Cruz de la Sierra, Bolivien<br>Lima, Peru<br>Montevideo, Uruguay |
| Südamerika, West (Lima)** | **Südamerika, West (Lima)**** | **Lima, Peru** |
| Südkorea | **Südkorea** | **Seoul, Südkorea** |
| Schweiz | **Schweiz**<br>Uganda | **Zürich, Schweiz**<br>Kampala, Uganda |
| Taiwan | **Taiwan** | **ChangHua, Taiwan** |
| USA (Mitte) | **USA (Mitte)** | **Council Bluffs, USA** |
| USA (Mitte), Chicago** | **USA (Mitte), Chicago**** | **Chicago, USA** |
| USA (mittlerer Westen) | **USA (mittlerer Westen)** | **Salt Lake City, USA** |
| USA (Ost) | **USA (Ost)**<br>USA (Nordost)<br>Guatemala | **Ashburn, USA**<br>New York City, USA<br>Guatemala-Stadt, Guatemala |
| USA (Nordwest) | **USA (Nordwest)** | **The Dalles, USA** |


©2025 Palo Alto Networks, Inc.

| Compute-Standort | Prisma Access Standort | Stadt und Land |
|---|---|---|
| USA (Süd) | **USA (Süd)**<br>Mexiko (Mitte)<br>Mexiko (West) | **Dallas, USA**<br>Mexiko-Stadt, Mexiko<br>Guadalajara, Mexiko |
| USA (Südost) | **USA (Südost)**<br>Kolumbien<br>Costa Rica<br>Ecuador<br>Panama | **Moncks Corner, USA**<br>Bogotá, Kolumbien<br>San Jose, Costa Rica<br>Guayaquil, Ecuador<br>Panama-Stadt, Panama |
| USA, Südosten (Miami)** | **USA, Südosten (Miami)**** | **Miami, USA** |
| USA (Südwest) | **USA (Südwest)**<br>USA (West) | **Los Angeles, USA**<br>San Francisco, USA |

## Schauplatz und Standortgruppe

| Schauplatz/Standortgruppe | IP-Pool-Gruppen-ID |
|---|---|
| Kolumbien<br>Costa Rica<br>Ecuador<br>Guatemala<br>Mexiko (Mitte)<br>Panama<br>USA (Ost)<br>USA (Südost)<br>USA (Mitte)<br>Costa Rica<br>USA (Nord/Mitte)<br>USA (Nordost)<br>USA (Süd)<br>USA (Südost)<br>Venezuela | 1 |


©2025 Palo Alto Networks, Inc.

| Schauplatz/Standortgruppe | IP-Pool-Gruppen-ID |
|---|---|
| Kanada (Ost)<br>Kanada (Mitte) | 2 |
| Irland | 3 |
| Frankreich (Süd)<br>Ghana<br>GB | 4 |
| Frankreich (Nord) | 5 |
| Asien, Australien und Japan | 6 |
| Andorra<br>Österreich<br>Bulgarien<br>Kroatien<br>Tschechien<br>Ägypten<br>Deutschland (Mitte)<br>Deutschland (Nord)<br>Deutschland (Süd)<br>Griechenland<br>Ungarn<br>Israel<br>Italien<br>Jordanien<br>Kenia<br>Kuwait<br>Liechtenstein<br>Luxemburg<br>Republik Moldau<br>Monaco<br>Nigeria<br>Polen | 7 |


©2025 Palo Alto Networks, Inc.

| Schauplatz/Standortgruppe | IP-Pool-Gruppen-ID |
|---|---|
| Portugal<br>Rumänien<br>Slowakei<br>Slowenien<br>Saudi Arabien<br>Südafrika (Mitte)<br>Spanien (Mitte)<br>Spanien (Ost)<br>Türkei<br>Ukraine<br>Vereinigte Arabische Emirate<br>Usbekistan | |
| Belarus<br>Finnland<br>Kasachstan<br>Litauen<br>Norwegen<br>Russland (Mitte)<br>Russland (Nordwest)<br>Schweden | 8 |
| Dänemark<br>Niederlande (Mitte)<br>Niederlande (Süd) | 9 |
| Afrika, Europa und Naher Osten | 10 |
| Schweiz<br>Uganda | 11 |
| Belgien<br>Lettland<br>Senegal | 12 |
| Brasilien (Mitte) | 13 |


©2025 Palo Alto Networks, Inc.

| Schauplatz/Standortgruppe | IP-Pool-Gruppen-ID |
|---|---|
| Brasilien (Ost)<br>Brasilien (Süd)<br>Paraguay<br>Venezuela | |
| Australien (Ost)<br>Australien (Süd)<br>Australien (Südost)<br>Neuseeland<br>Papua-Neuguinea | 14 |
| Kambodscha<br>Indonesien<br>Malaysia<br>Myanmar<br>Philippinen<br>Singapur<br>Thailand<br>Vietnam | 15 |
| Hongkong | 16 |
| Taiwan | 17 |
| Südkorea | 18 |
| Bangladesch<br>Indien (Nord)<br>Indien (Süd)<br>Indien (West)<br>Pakistan (West)<br>Pakistan (Süd)<br>Katar | 19 |
| Südafrika (West)<br>Schweden<br>Südafrika (West) | 20 |


©2025 Palo Alto Networks, Inc.

| Schauplatz/Standortgruppe | IP-Pool-Gruppen-ID |
|---|---|
| Japan (Mitte)<br>Japan (Süd) | 21 |
| Bahrain | 22 |
| Kanada (West)<br>Mexiko (Mitte)<br>Mexiko (West)<br>USA (mittlerer Westen)<br>USA (Nordwest)<br>USA (Südwest)<br>USA (West) | 23 |
| Argentinien<br>Bolivien<br>Chile<br>Peru<br>Uruguay | 24 |

## Standorte nach Region

| Standorte |
|---|
| **Region Afrika** |
| Kenia |
| Nigeria |
| Senegal |
| Südafrika (Mitte) |
| Südafrika (West) |
| **Region Asien** |
| Bangladesch |
| Kambodscha |


©2025 Palo Alto Networks, Inc.

| Standorte |
| --- |
| Hongkong |
| Indien (Nord) |
| Indien (Süd) |
| Indien (West) |
| Indonesien |
| Kasachstan |
| Malaysia |
| Myanmar |
| Pakistan (Süd) |
| Pakistan (West) |
| Pakistan (West) (II) |
| Papua-Neuguinea |
| Philippinen |
| Singapur |
| Südkorea |
| Sri Lanka |
| Taiwan |
| Thailand |
| Vietnam |
| **Region ANZ** |
| Australien (Ost) |
| Australien (Süd) |
| Australien (Südost) |
| Neuseeland |
| **Region Europa** |

 ©2025 Palo Alto Networks, Inc.

| Standorte |
| --- |
| Andorra |
| Österreich |
| Belarus |
| Belgien |
| Bulgarien |
| Kroatien |
| Tschechien |
| Dänemark |
| Finnland |
| Frankreich (Nord) |
| Frankreich (Süd) |
| Deutschland (Mitte) |
| Deutschland (Nord) |
| Deutschland (Süd) |
| Ghana |
| Griechenland |
| Ungarn |
| Irland |
| Italien |
| Lettland |
| Liechtenstein |
| Litauen |
| Luxemburg |
| Republik Moldau |
| Monaco |

 ©2025 Palo Alto Networks, Inc.

| Standorte |
| --- |
| Niederlande (Mitte) |
| Niederlande (Süd) |
| Norwegen |
| Polen |
| Portugal |
| Rumänien |
| Russland (Mitte) |
| Russland (Nordwest) |
| Slowakei |
| Slowenien |
| Spanien (Mitte) |
| Spanien (Ost) |
| Schweden |
| Schweiz |
| Uganda |
| GB |
| Ukraine |
| Usbekistan |
| **Region Japan** |
| Japan (Mitte) |
| Japan (Süd) |
| **Region Naher Osten** |
| Bahrain |
| Ägypten |
| Israel |

 ©2025 Palo Alto Networks, Inc.

| Standorte |
| --- |
| Jordanien |
| Kuwait |
| Katar |
| Saudi Arabien |
| Türkei |
| Vereinigte Arabische Emirate |
| **Region Nordamerika** |
| Kanada (Mitte) |
| Kanada (Ost) |
| Kanada (West) |
| Costa Rica |
| Mexiko (Mitte) |
| Mexiko (West) |
| Panama |
| USA (Mitte) |
| USA (mittlerer Westen) |
| USA (Ost) |
| USA (Nordost) |
| USA (Nordwest) |
| USA (Süd) |
| USA (Südost) |
| USA (Südwest) |
| USA (West) |
| **Region Südamerika** |
| Argentinien |

 ©2025 Palo Alto Networks, Inc.

| Standorte |
| --- |
| Bolivien |
| Brasilien (Mitte) |
| Brasilien (Ost) |
| Brasilien (Süd) |
| Chile |
| Kolumbien |
| Ecuador |
| Paraguay |
| Peru |
| Uruguay |
| Venezuela |

## Standorte mit explizitem Proxy

Prisma Access unterstützt die folgenden Standorte mit explizitem Proxy. „Expliziter Proxy“ verwendet GeoDNS, um den mobilen Benutzer aufzulösen und mit dem nächstgelegenen Prisma Access-Benutzer zu verbinden.

- **Afrika, Europa und Naher Osten:**
  - Belgien
  - Finnland
  - Frankreich (Süd)
  - Deutschland (Mitte)
  - Israel
  - Italien
  - Niederlande (Mitte)
  - Polen
  - Katar
  - Saudi Arabien
  - Südafrika (Mitte)
  - Spanien (Mitte)
  - Schweiz
  - GB

 ©2025 Palo Alto Networks, Inc.

- **Asien, Australien und Japan:**
  - Australien (Süd)
  - Australien (Südost)
  - China
  - Hongkong
  - Japan (Mitte)
  - Japan (Süd)
  - Indien (Nord)
  - Indien (West)
  - Indonesien
  - Singapur
  - Südkorea
  - Taiwan
- **Nordamerika und Südamerika:**
  - Brasilien (Süd)
  - Chile
  - Kanada (Mitte)
  - Kanada (Ost)
  - USA (Mitte)
  - USA (Ost)
  - USA (Nordwest)
  - USA (Süd)
  - USA (Südost)
  - USA (Südwest)
  - USA (mittlerer Westen)

## Colo-Connect-Standort

Prisma Access Colo-Connect unterstützt folgende Prisma Access-Standorte. Wenn Sie Dienstverbindungen zur Unterstützung von Colo-Connect erstellen, achten Sie darauf, diese nur an den folgenden Standorten zu erstellen.



*Verwenden Sie für dedizierte Interconnect-Links die Option* GCP-Liste der Standorte *um dedizierte Interconnect-Verbindungen zu erstellen.*

- Australien (Süd)
- Australien (Südost)
- Belgien
- Brasilien (Süd)

 ©2025 Palo Alto Networks, Inc.

- Kanada (Mitte)
- Kanada (Ost)
- Chile
- Finnland
- Frankreich (Süd)
- Deutschland (Mitte)
- Hongkong
- Indien (Nord)
- Indien (West)
- Indonesien
- Italien
- Japan (Mitte)
- Japan (Süd)
- Niederlande (Mitte)
- Katar
- Saudi Arabien
- Singapur
- Südafrika (Mitte)
- Spanien (Mitte)
- Schweiz
- Taiwan
- GB
- USA (Mitte)
- USA (mittlerer Westen)
- USA (Ost)
- USA (Nordwest)
- USA (Süd)
- USA (Südost)
- USA (Südwest)

## Unterstützte Regionen des Strata Logging Service

Prisma Access unterstützt die folgenden Regionen des Strata-Protokollierungsdienstes:

- Australien
- Kanada
- Frankreich
- Deutschland


©2025 Palo Alto Networks, Inc.

- Japan
- Indien
- Indonesien
- Israel
- Niederlande – Europa
- Katar
- Saudi Arabien
- Singapur
- Schweiz
- Taiwan
- Vereinigtes Königreich
- Vereinigte Staaten – Amerika

## Remote-Netzwerke – Standorte mit hoher Leistung, Replikation des Datenverkehrs und sicherem eingehenden Zugriff

Mit Prisma Access werden die folgenden Remote-Netzwerk-Standorte mit hoher Leistung unterstützt:

- Andorra
- Argentinien
- Australien (Ost)
- Australien (Süd)
- Australien (Südost)
- Österreich
- Bangladesch
- Belarus
- Belgien
- Bolivien
- Brasilien (Mitte)
- Brasilien (Ost)
- Brasilien (Süd)
- Bulgarien
- Kambodscha
- Kanada (Mitte)
- Kanada (Ost)
- Chile
- Kolumbien

 ©2025 Palo Alto Networks, Inc.

- Costa Rica
- Kroatien
- Tschechien
- Dänemark
- Ecuador
- Ägypten
- Finnland
- Frankreich (Nord)
- Frankreich (Süd)
- Deutschland (Mitte)
- Deutschland (Nord)
- Deutschland (Süd)
- Ghana
- Griechenland
- Guatemala
- Hongkong
- Ungarn
- Indien (Nord)
- Indien (Süd)
- Indien (West)
- Indonesien
- Israel
- Italien
- Japan (Mitte)
- Japan (Süd)
- Jordanien
- Kasachstan
- Kenia
- Kuwait
- Lettland
- Liechtenstein
- Litauen
- Luxemburg
- Malaysia
- Mexiko (Mitte)
- Mexiko (West)

 ©2025 Palo Alto Networks, Inc.

- Republik Moldau
- Monaco
- Myanmar
- Niederlande (Mitte)
- Niederlande (Süd)
- Neuseeland
- Nigeria
- Norwegen
- Pakistan (Süd)
- Pakistan (West)
- Pakistan (West) (II)
- Panama
- Papua-Neuguinea
- Paraguay
- Peru
- Philippinen
- Polen
- Portugal
- Katar
- Rumänien
- Russland (Mitte)
- Russland (Nordwest)
- Saudi Arabien
- Senegal
- Singapur
- Slowakei
- Slowenien
- Südafrika (Mitte)
- Südkorea
- Spanien (Mitte)
- Spanien (Ost)
- Sri Lanka
- Schweiz
- Taiwan
- Thailand
- Türkei

 ©2025 Palo Alto Networks, Inc.

- Uganda
- GB
- Ukraine
- Uruguay
- USA (Mitte)
- USA (mittlerer Westen)
- USA (Ost)
- USA (Nordost)
- USA (Nordwest)
- USA (Süd)
- USA (Südost)
- USA (Südwest)
- USA (West)
- Usbekistan
- Venezuela
- Vietnam

## Prisma Access-Standorte in China

Prisma Access China unterstützt die folgenden Standorte in der VR China:

- China (Nord) – Peking (verwendet den Compute-Standort „China (Nord)“)
- China (Nordwest) – Ningxia (verwendet den Compute-Standort „China (Nordwest)“)

## Standorte des Typs „FedRAMP Moderate“ und „FedRAMP High“

Die Liste der FedRAMP-Standorte finden Sie in der Prisma SASE FedRAMP-Dokumentation.

## Karte der Standorte in Nordamerika

Verwenden Sie die folgende Karte als Referenz zur Orientierung bei der Auswahl von Prisma Access-Standorten in Nordamerika.

 ©2025 Palo Alto Networks, Inc.




## Standorte in lokalen Zonen

Die folgenden lokalen Zonen werden mit IPv4 in Prisma Access unterstützt:

- *Sie müssen gemeinsam mit Ihrem Palo Alto Networks Vertreter eine Anforderung für die Bereitstellung in einer der folgenden lokalen Zonen initiieren.*
- *IPv6 wird nicht unterstützt.*

- Australien (West), Perth
- Neuseeland (Auckland)
- Nigeria (Lagos)
- Südamerika (West), Lima
- USA (Mitte), Chicago
- USA (Südost), Miami


©2025 Palo Alto Networks, Inc.

# Prisma Access und Verarbeitungsstandorte für zugehörige Dienste

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

Prisma Access bietet eine lokale Erfahrung an mehr als 100 Standorten weltweit und ordnet jeden Standort basierend auf optimierter Leistung und Latenz einem Sicherheits-Compute-Standort zu.

Wenn Sie Compute-Standorte auf bestimmte Länder beschränken müssen, orientieren Sie sich an der Länderzuordnung für jeden Prisma Access-Standort und stellen Sie während der Konfiguration von Prisma Access nur die Standorte bereit, die diesen Ländern zugeordnet sind.

In der folgenden Tabelle finden Sie den Verarbeitungsstandort in den jeweiligen Ländern für Strata-Protokollierungsdienst-Regionen, Strata Cloud Manager (für Prisma Access (Managed by Strata Cloud Manager), Prisma Access Insights, Autonomous DEM und SaaS Security Inline).

| Strata Logging Service | Strata Cloud Manager – Konfiguration | Prisma Access Insights – Daten | Autonomous DEM | SaaS Security Inline |
|---|---|---|---|---|
| Vereinigtes Königreich | Vereinigtes Königreich | Vereinigtes Königreich | Vereinigtes Königreich | Vereinigtes Königreich |
| Niederlande | Deutschland | Niederlande | Niederlande | Deutschland (EU) |
| Deutschland | Deutschland | Deutschland | Deutschland | Deutschland (EU) |
| Schweiz | Schweiz | Schweiz | Schweiz | Deutschland (EU) |
| Frankreich | Deutschland | Frankreich | Frankreich | Deutschland (EU) |
| Singapur | Singapur | Singapur | Singapur | Singapur |
| Indien | Indien | Indien | Indien | Indien |
| Japan | Japan | Japan | Japan | Japan |
| Kanada | Kanada | Kanada | Kanada | Vereinigte Staaten |


©2025 Palo Alto Networks, Inc.

| Strata Logging Service | Strata Cloud Manager – Konfiguration | Prisma Access Insights – Daten | Autonomous DEM | SaaS Security Inline |
|---|---|---|---|---|
| Vereinigte Staaten | Vereinigte Staaten | Vereinigte Staaten | Vereinigte Staaten | Vereinigte Staaten |
| Australien | Australien | Australien | Australien | Australien |
| Israel | Deutschland | Israel | Israel | Deutschland (EU) |
| Katar | Katar | Katar | Katar | Deutschland (EU) |
| Saudi Arabien | Deutschland | Saudi Arabien | Saudi Arabien | Deutschland (EU) |
| Taiwan | Singapur | Taiwan | Taiwan | Singapur |
| Indonesien | Singapur | Indonesien | Indonesien | Singapur |


©2025 Palo Alto Networks, Inc.

# Prisma Access-Infrastrukturverwaltung

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (von Panorama verwaltet) | ❑ Prisma Access-Lizenz |

Prisma Access verwendet ein gemeinsam genutztes Eigentümermodell. Palo Alto Networks verwaltet die zugrunde liegende Sicherheitsinfrastruktur und stellt sicher, dass sie sicher, belastbar, aktuell und verfügbar ist, wenn Sie sie benötigen. Ihre Organisation ist dafür verantwortlich, Standorte und Benutzer einzubinden, Richtlinien per Push zu übertragen, sie zu aktualisieren, Protokolle abzufragen und Berichte zu erstellen.

Palo Alto Networks verwaltet die folgenden Teile der Sicherheitsinfrastruktur. Zusätzlich zur Sicherheitsinfrastruktur verwaltet Prisma Access Releases und Upgrades:

- **Prisma Access**
- **Strata Logging Service** – Wir verwalten den Zustellmechanismus für Protokolle.
- **Inhaltsaktualisierungen** – Wir verwalten Releases und Upgrades, einschließlich PAN-OS-Aktualisierungen. Für Ihre mobilen Benutzer hostet Prisma Access mehrere Versionen der GlobalProtect-App, und Sie können aus dieser Liste die aktive GlobalProtect-App-Version auswählen.
- **Fehlertoleranz** – Wir verwalten die Verfügbarkeit des Dienstes.
- **Automatische Skalierung** – Wir skalieren den Dienst automatisch, wenn Sie Dienstverbindungen oder Remote-Netzwerke hinzufügen oder wenn sich zusätzliche mobile Benutzer bei einem oder mehreren Gateways in einer Region anmelden.
- **Bereitstellung** – Wir stellen die Infrastruktur bereit (mit allem, was erforderlich ist).
- **Dienstüberwachung** – Wir überwachen den Dienststatus und sorgen dafür, dass er stets funktionsfähig ist.
- **Compute-Standort-Zuordnung** – Jeder Prisma Access-Standort wird basierend auf optimierter Leistung und Latenz dem Sicherheits-Compute-Standort zugeordnet. Dies bedeutet, dass der Datenverkehr in bestimmten Ländern an einen definierten Compute-Standort geleitet wird, sofern ein Systemadministrator nicht etwas anderes festlegt. Die Zuordnung zwischen Standort und Compute-Standort finden Sie im Prisma Access-Datenblatt zum Datenschutz.

Ihre Organisation verwaltet die folgenden Komponenten der Sicherheitsinfrastruktur.

- **Benutzer** – Sie verwalten das Onboarding mobiler Benutzer.
- **Authentifizierung** – Sie verwalten die Authentifizierung dieser Benutzer.
- **Mobilgeräteverwaltung (MDM)** – Sie können die mobilen Geräte Ihres Unternehmens, die mit Prisma Access geschützt werden, mit Ihrer eigenen MDM-Software steuern.
- (Nur Prisma Access (Managed by Panorama)) **Panorama und Cloud Services-Plug-in** – Sie stellen sicher, dass auf der Panorama-Instanz auf der das Cloud Service-Plug-in installiert ist, eine Panorama-Version ausgeführt wird, die das Cloud Services-Plug-in unterstützt. Darüber

 ©2025 Palo Alto Networks, Inc.

hinaus aktualisieren Sie das Cloud Services-Plug-in in Panorama, nachdem wir Sie darüber informiert haben, dass ein neues Plugin verfügbar ist.

- **Richtlinienerstellung und -verwaltung** – Sie planen und erstellen die Richtlinien in Panorama, die mit Prisma Access verwendet werden sollen.
- **Protokollanalyse und Forensik** – Prisma Access stellt die Protokolle bereit, Sie sorgen für die Analyse und Berichterstattung und verwenden dazu integrierte Tools, die von uns oder einem anderen Anbieter bereitgestellt werden.
- **Lokale Sicherheit** – Sie stellen die lokale Sicherheit zwischen Mikrosegmentierungen Ihres lokalen Netzwerks bereit. In einigen Bereitstellungen können Sie auch den gesamten Datenverkehr so leiten, dass er durch Prisma Access abgesichert wird.
- **Netzwerk** – Sie stellen die Netzwerkkonnektivität zu Prisma Access bereit.
- **Überwachung** – Sie überwachen den Status des lokalen Netzwerks.
- **Dienstkonnektivität** – Sie stellen die Konnektivität zum Prisma Access-Gateway für mobile Benutzer bereit (z. B. einen ISP). Sie stellen auch die lokalen Geräte bereit, die als Terminierungspunkte für die IPSec-Tunnel verwendet werden, die von den Dienstverbindungen und Remote-Netzwerkverbindungen verwendet werden.
- **Onboarding** – Sie binden mobile Benutzer, Standorte für Zentralen/Rechenzentren sowie Zweigstellen ein.
- (Nur Prisma Access (Managed by Panorama))**Backup** – Sie verwalten die Sicherung der Panorama-Konfiguration.

 ©2025 Palo Alto Networks, Inc.

# Prisma Access-APIs

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

## APIs für Prisma Access (Managed by Strata Cloud Manager)

Weitere Informationen zu den APIs für Prisma Access (Managed by Strata Cloud Manager) finden Sie auf pan.dev, der Website für Palo Alto Networks Entwicklerdokumente. Prisma Access (Managed by Strata Cloud Manager) verwendet diese APIs für die Einbindung, Konfiguration und den Betrieb von Diensten.

## APIs für Prisma Access (Managed by Panorama)

Zusätzlich zu den XML-APIs, die für die Konfiguration und Verwaltung in Panorama verfügbar sind, gibt es XML-APIs für das Cloud Services-Plugin, mit denen Sie Aufgaben für Prisma Access ausführen können. Verwenden Sie diese APIs über einen Dienst, eine Anwendung oder ein Skript von Drittanbietern, um Konfigurations- und Berichtsaufgaben für Prisma Access zu automatisieren.




 ©2025 Palo Alto Networks, Inc.

# Zugriff auf die Prisma Access (Managed by Panorama)-API über die Browser- und Webschnittstelle

Um über den Browser auf die API zuzugreifen, melden Sie sich bei der Panorama-Instanz an, die Prisma Access mit Administratorrechten verwaltet, und geben Sie dann am Ende der URL /api ein. Die URL wechselt zur XML-API-Browseroberfläche.

Die Prisma Access-APIs befinden sich in den folgenden XML Path Language(XPath)-Knoten in der XML-Baumstruktur:

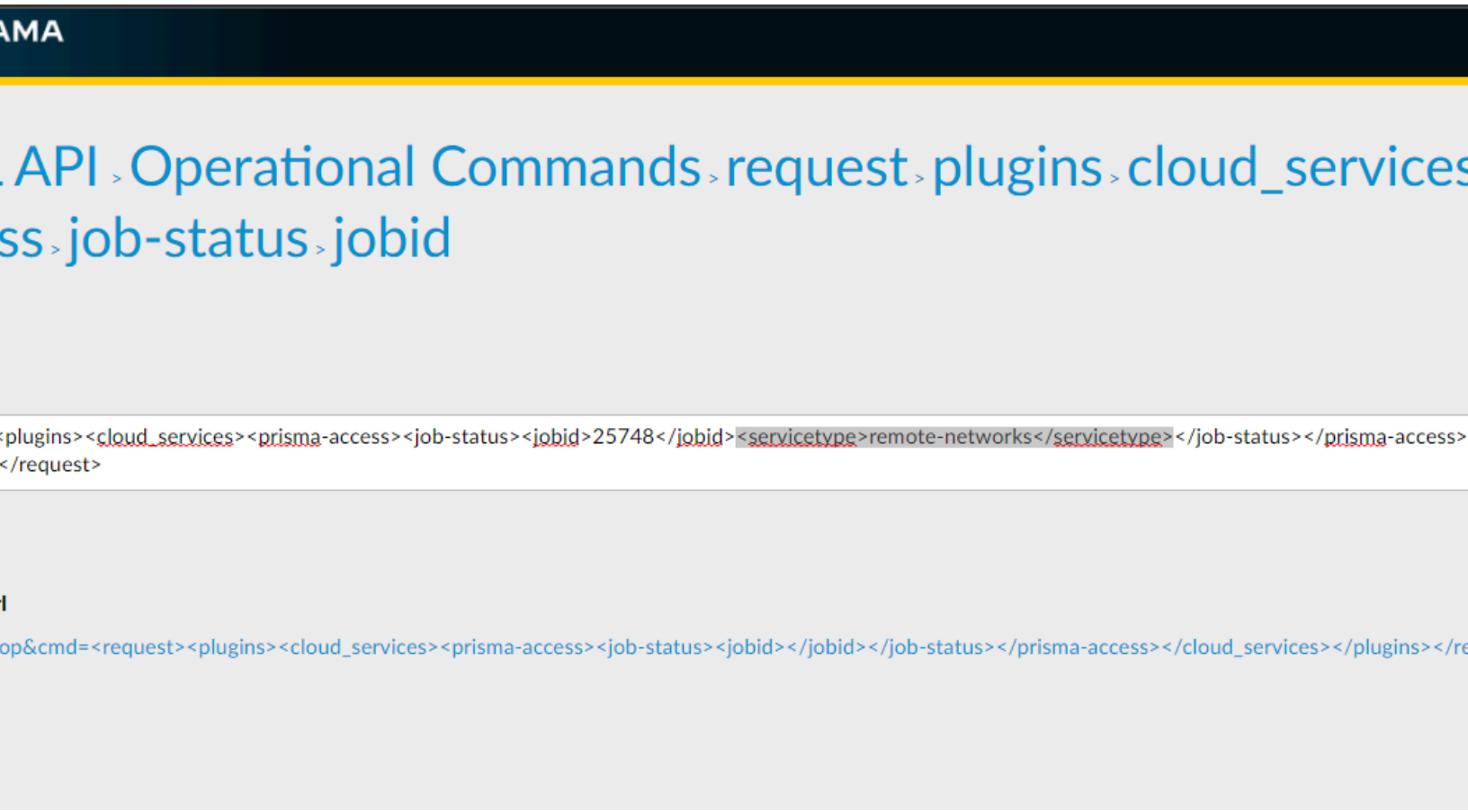
- Konfigurationsbefehle: **XML-API** > **Konfigurationsbefehle** > **devices** > **entry[@name='localhost.localdomain']** > **plugins** > **cloud_services**
- Betriebsbefehle: **XML-API** > **Betriebsbefehle** > **request** > **plugins** > **cloud_services** > **prisma-access**

Wenn Sie in der XML-Baumstruktur navigieren, füllt Prisma Access die Baumstruktur im Bereich **XML** aus. Sie können erforderliche Werte im Bereich **XML**eingeben und auf **Übermitteln** klicken, um eine XML-Anfrage zu bearbeiten. Um beispielsweise den Onboarding-Status eines Auftrags anzufordern, navigieren Sie zu **XML-API** > **Betriebsbefehle** > **request** > **plugins** > **cloud_services** > **prisma-access** > **job-status** > **jobid**, geben Sie die Job-ID in das Feld **jobid** und den Diensttyp in das Feld **servicetyp** ein und klicken Sie auf **Übermitteln**, um Ihre Anfrage zu senden.



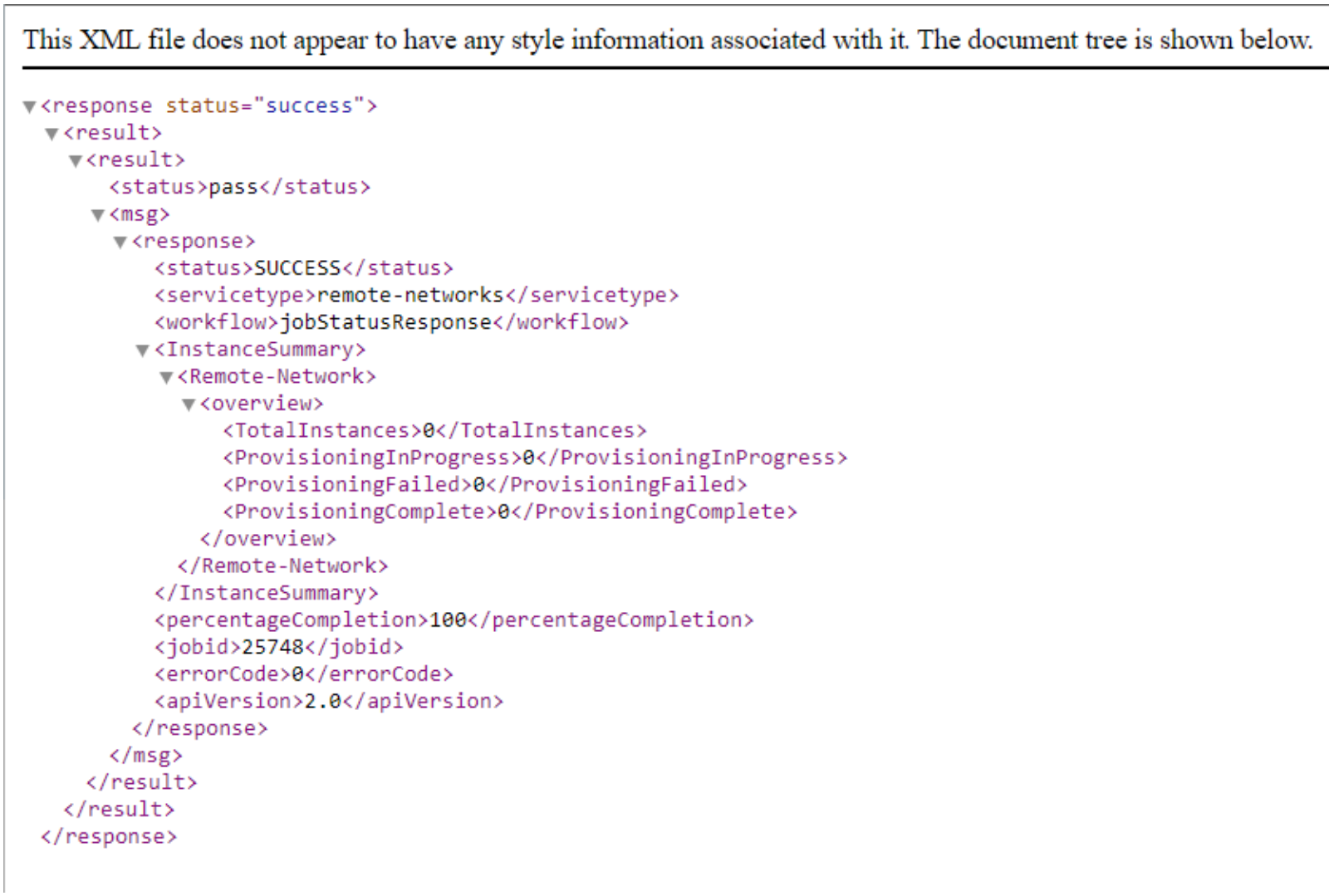
*Mit diesem XML-Code wird nur der Onboarding-Status eines Auftrags abgerufen. Um den Status aller Commit-Vorgänge abzurufen, verwenden Sie die Prisma Access-Benutzeroberfläche.*

 ©2025 Palo Alto Networks, Inc.




Prisma Access gibt die Ausgabe im XML-Format zurück.

 ©2025 Palo Alto Networks, Inc.



This XML file does not appear to have any style information associated with it. The document tree is shown below.


```
<response status="success">
  <result>
    <result>
      <status>pass</status>
      <msg>
        <response>
          <status>SUCCESS</status>
          <servicetype>remote-networks</servicetype>
          <workflow>jobStatusResponse</workflow>
          <InstanceSummary>
            <Remote-Network>
              <overview>
                <TotalInstances>0</TotalInstances>
                <ProvisioningInProgress>0</ProvisioningInProgress>
                <ProvisioningFailed>0</ProvisioningFailed>
                <ProvisioningComplete>0</ProvisioningComplete>
              </overview>
            </Remote-Network>
          </InstanceSummary>
          <percentageCompletion>100</percentageCompletion>
          <jobid>25748</jobid>
          <errorCode>0</errorCode>
          <apiVersion>2.0</apiVersion>
        </response>
      </msg>
    </result>
  </result>
</response>
```


Sie können auch die Weboberfläche verwenden, um in Panorama nach APIs zu suchen.

## curl-Befehle zum Abrufen der von Panorama verwalteten API-Befehle verwenden

Wenn Sie die CLI zum Abrufen von Ergebnissen der API-Befehle verwenden möchten, können Sie APIs in Verbindung mit der API verwenden, die Sie zum Abrufen von öffentlichen Adressen und Infrastruktur-IP-Adressen für Prisma Access verwenden. Verwenden Sie dazu den folgenden Befehl:

**Konfigurationsbefehle:**

`curl -k -X GET "https://`*<panorama-ip-address>*`/api/?key=`*<api-key>*`&type=config&cmd=`*<api-parameters></api-parameters>*

**Betriebsbefehle:**

`curl -k -X GET "https://`*<panorama-ip-address>*`/api/?key=`*<api-key>*`&type=op&cmd=`*<api-parameters></api-parameters>*

 ©2025 Palo Alto Networks, Inc.

Dabei gilt:

- *<panorama-ip-address>* ist die IP-Adresse der Panorama-Instanz, von der Prisma Access verwaltet wird.
- *<api-key>* ist der API-Schlüssel, der IP-Adressen für Prisma Access abruft (**Panorama** > **Cloud Services** > **Konfiguration** > **Diensteinrichtung** > **API-Schlüssel generieren**).
- *<api-parameters>* und *</api-parameters>* sind die API-Parameter, mit denen Sie die angeforderten Informationen aus der API abrufen.

Wenn eine Mehrmandantenbereitstellung vorliegt, fügen Sie der API den Namen des Mandanten hinzu, für den Sie API-Informationen abrufen möchten.

Beispiel für eine Prisma Access-Bereitstellung mit den folgenden Parametern:

- **Panorama-IP-Adresse:** 1.2.3.4
- **API-Schlüssel:** 12345abcde
- **Mandantenname:** tenant-1

Wenn Sie die Anzahl der aktiven mobilen Benutzer für diesen Mandanten abrufen möchten, geben Sie den folgenden curl-Befehl ein:

```
curl -k -X GET "https://1.2.3.4/api/?
key=12345abcde&type=op&cmd=<request><plugins><cloud_services><prisma-
access><multi-tenant><tenant-name><entry%20name='tenant-1'></entry></
tenant-name><remote-active-users-count/></multi-tenant></prisma-
access></cloud_services></plugins></request>"
```

## CLI-Befehle mit Prisma Access (Managed by Panorama) verwenden

Mit Prisma Access können Sie CLI-Befehle zum Abrufen von Prisma Access-Daten verwenden. Stellen Sie für den Zugriff auf die CLI eine SSH-Verbindung über die IP-Adresse der Panorama-Instanz her, mit der Prisma Access verwaltet wird.

Die CLI verwendet die gleichen Modi und weist das gleiche Verhalten auf wie die PAN-OS-Befehle. Anders ist lediglich die Eingabe des Mandantennamens für Mehrmandantenbereitstellungen. Sie geben den Mandantennamen mit dem Befehl `tenant-name` *Mandantenname* ein. Wenn beispielsweise der Mandantenname *tenant-1* lautet, geben Sie den folgenden Befehl ein, um die Anzahl der aktiven Benutzer in einer Mehrmandantenbereitstellung abzurufen:

```
admin-Panorama> request plugins cloud_services prisma-access multi-
tenant remote-active-users-count tenant-name tenant-1 pass Current
 User Count: 253
```

## Prisma Access Insights-APIs

Mit den Prisma Access Insights-APIs können Sie Ihre Prisma Access Insights-Mandanten nach Datenressourcen abfragen. Es gibt zwei Versionen der APIs. Die APIs Prisma Access Insights 2.0 und 1.0 ermöglichen es Ihnen, Ihren Prisma Access-Mandanten nach der Integrität Ihrer Prisma Access-Netzwerkbereitstellung abzufragen. Die API-Aufrufe sind für beide Versionen gleich.

 ©2025 Palo Alto Networks, Inc.

Allerdings verwendet jede Version andere Zugriffstoken und der Mechanismus, mit dem Sie ein Zugriffstoken erhalten, ist für jede Version anders.

Informationen zu den ersten Schritten mit Prisma Access Insights-APIs finden Sie im Entwicklerhandbuch unter Willkommen bei Prisma SASE.

Unter Prisma Access Insights-API finden Sie spezielle Inhalte für Prisma Access Insights-APIs, Informationen zu API-Version 2.0, API-Version 1.0, Beispiele für die Prisma Access Insights-API und FAQs zu PAI.

## Über 2.0-APIs

Prisma Access Insights 2.0-APIs sind für Prisma Access (Managed by Strata Cloud Manager)-Kunden gedacht, deren Mandanten von Palo Alto Networks mit einer TSG-Kennung (Tenant Service Group, Dienstgruppe für Mandanten) eingebunden wurden. Um herauszufinden, ob Ihr Mandant TSG-IDs verwendet, gehen Sie zum Prisma Access-Hub, klicken Sie auf den Anwendungsnamen **Prisma Access Insights** und lesen Sie die Informationen im Abschnitt **Apps verwalten**.

Die 2.0-APIs können auch von Prisma Access (Managed by Panorama)-Kunden genutzt werden. Handelt es sich in diesem Fall um eine Prisma Access (Managed by Panorama)-Bereitstellung mit mehreren Mandanten, verfügt nur der Supermandant über die TSG-ID und die Untermandanten werden mit der Strata Logging Service-Mandanten-ID in den Header aufgenommen.

**API 2.0-Fall**

Wenn nach der Migration des Supermandanten zur TSG-ID ein Untermandant abgefragt wird:

Der Header benötigt folgende Informationen: `Prisma-Mandant:tsg_id:Untermandant_id`

## Über 1.0-APIs

Prisma Access Insights 1.0-APIs sind für alle Prisma Access (Managed by Strata Cloud Manager)-Kunden mit einem Mandanten sowie Prisma Access (Managed by Panorama)-Kunden mit einem oder mehreren Mandanten gedacht.

**API 1.0-Fall**

Geben Sie vor der Migration des Supermandanten zur TSG-ID bei der Abfrage nach Untermandanteninformationen mithilfe der 1.0-APIs die Supermandanten-ID auf dem Endpunkt an:

`/api/sase/v1.0/resource/tenant/{Supermandanten-ID}/`

Fügen Sie den folgenden Header in den Aufruf ein: `Prisma-Tenant: {Mandanten-ID}: {Untermandanten-ID}`


©2025 Palo Alto Networks, Inc.

# Prisma Access von Panorama zu Strata Cloud Manager migrieren

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz<br><br>Um mit der Migration von Prisma Access (Managed by Panorama) zu Prisma Access (Managed by Strata Cloud Manager) zu beginnen, wenden Sie sich an Ihr Palo Alto Networks Account-Team. |

Wenn Sie mit einer bestehenden Prisma Access-Bereitstellung arbeiten, für die die Konfiguration von Panorama verwaltet wird, und für die Konfigurationsverwaltung zu Strata Cloud Manager migrieren möchten, bietet Palo Alto Networks einen Workflow im Produkt, mit dem Sie Ihre vorhandene Prisma Access-Konfiguration zu Strata Cloud Manager migrieren können.

Die Verwaltung Ihrer Prisma Access-Konfiguration mit Strata Cloud Manager anstelle von Panorama bietet Ihnen unter anderem folgende Vorteile:

- Kontinuierliche Best-Practice-Bewertungen
- Sichere Standardkonfigurationen
- Auf maschinellem Lernen (ML) basierende Konfigurationsoptimierung
- Optimierte Websicherheitsworkflows
- Eine interaktive visuelle Zusammenfassung (Command Center), die Ihnen hilft, Zustand, Sicherheit und Effizienz des Netzwerks zu bewerten
- Intuitive Workflows für komplexe Aufgaben
- Einfache und sichere Verwaltungs-APIs
- Cloudnative Architektur für Skalierbarkeit, Ausfallsicherheit und globale Reichweite
- Entfall der Hardwareverwaltung oder Softwarewartung

## Vorbereitung der Migration zu Prisma Access (Managed by Strata Cloud Manager)

Bevor Sie mit der Migration beginnen, sollten Sie sich über die Mindestanforderungen an die Software und die Prisma Access (Managed by Panorama)-Bereitstellungstypen, die Sie migrieren können, im Klaren sein.

- **Zeitpunkt der Migration** – Führen Sie Ihr Upgrade nicht während eines Dataplane- oder Infrastrukturupgrades durch. Überprüfen Sie Ihre Präferenzen für Upgrades, um zu sehen, ob ein Dataplane-Upgrade bevorsteht.
- **Unidirektionale Migration von Panorama zu Prisma Access (Managed by Strata Cloud Manager)** – Sie können nur von einer Prisma Access (Managed by Panorama)- zu einer Prisma Access (Managed by Strata Cloud Manager)-Bereitstellung migrieren. Nach der

 ©2025 Palo Alto Networks, Inc.

Migration zu Strata Cloud Manager können Sie nicht mehr zur Verwaltung Ihrer Prisma Access-Bereitstellung mit Panorama zurückkehren.

- **Mindestversion von Panorama** – Es ist mindestens Panorama 10.0 erforderlich.
- **Erforderliche Administratorrolle** – Sie müssen als Superuser in Strata Cloud Manager angemeldet sein, um mit der Migration zu beginnen.
- **Lizenzierungsanforderungen** – Es ist eine gültige Prisma Access-Lizenz erforderlich.
- **Cloud Identity Engine** – Sie müssen vor der Migration die Verzeichnissynchronisierungskomponente der Cloud Identity Engine in den aktuellen Prisma Access (Managed by Panorama)-Mandanten integriert haben.
- **Nicht unterstützte Funktionen** – Das Migrationsprogramm unterstützt die folgenden Prisma Access-Funktionen nicht:
  - Bereitstellungen mit mehreren Mandanten
  - IoT-Sicherheit
  - Datenfilterung (alternativ verwenden Sie Enterprise DLP)
  - SSH-Proxy
  - Separate Authentifizierung für GlobalProtect-Portale und -Gateways
- **Probleme aufgrund von Konfigurationsunterschieden** – Wenn Sie das Programm zum Auffinden von Konfigurationsunterschieden während der Migration ausführen, ignorieren Sie alle Unterschiede für die die folgenden Objektnamen aufgeführt sind, da sie sich nicht auf Ihre Konfiguration auswirken:
  - Clientless-vpn crypto-settings
  - Hip-profiles rename
  - Mobile-user-redundancy
  - Exclude-video-traffic

## Migration Ihrer Prisma Access (Managed by Panorama)-Bereitstellung zu Strata Cloud Manager

Führen Sie die folgenden Schritte aus, um Ihre Prisma Access (Managed by Panorama)-Bereitstellung zu einer Prisma Access (Managed by Strata Cloud Manager)-Bereitstellung zu migrieren.

Auf einer oberen Ebene haben Sie folgende Möglichkeiten:

1. Vergewissern Sie sich, dass Sie die neueste Konfiguration erfolgreich per Push an Prisma Access übertragen, die neueste Konfiguration gespeichert und eine XML-Konfigurationsdatei aus der Panorama-Instanz exportiert haben, von der Prisma Access verwaltet wird.
2. Starten Sie das Migrationsprogramm von Strata Cloud Manager aus.
3. Prüfen Sie die Konfigurationsunterschiede (Diffs) zwischen der Panorama-Konfiguration und der migrierten Strata Cloud Manager-Konfiguration.
4. Lösen Sie die Unterschiede auf und schließen Sie die Migration ab.

 ©2025 Palo Alto Networks, Inc.

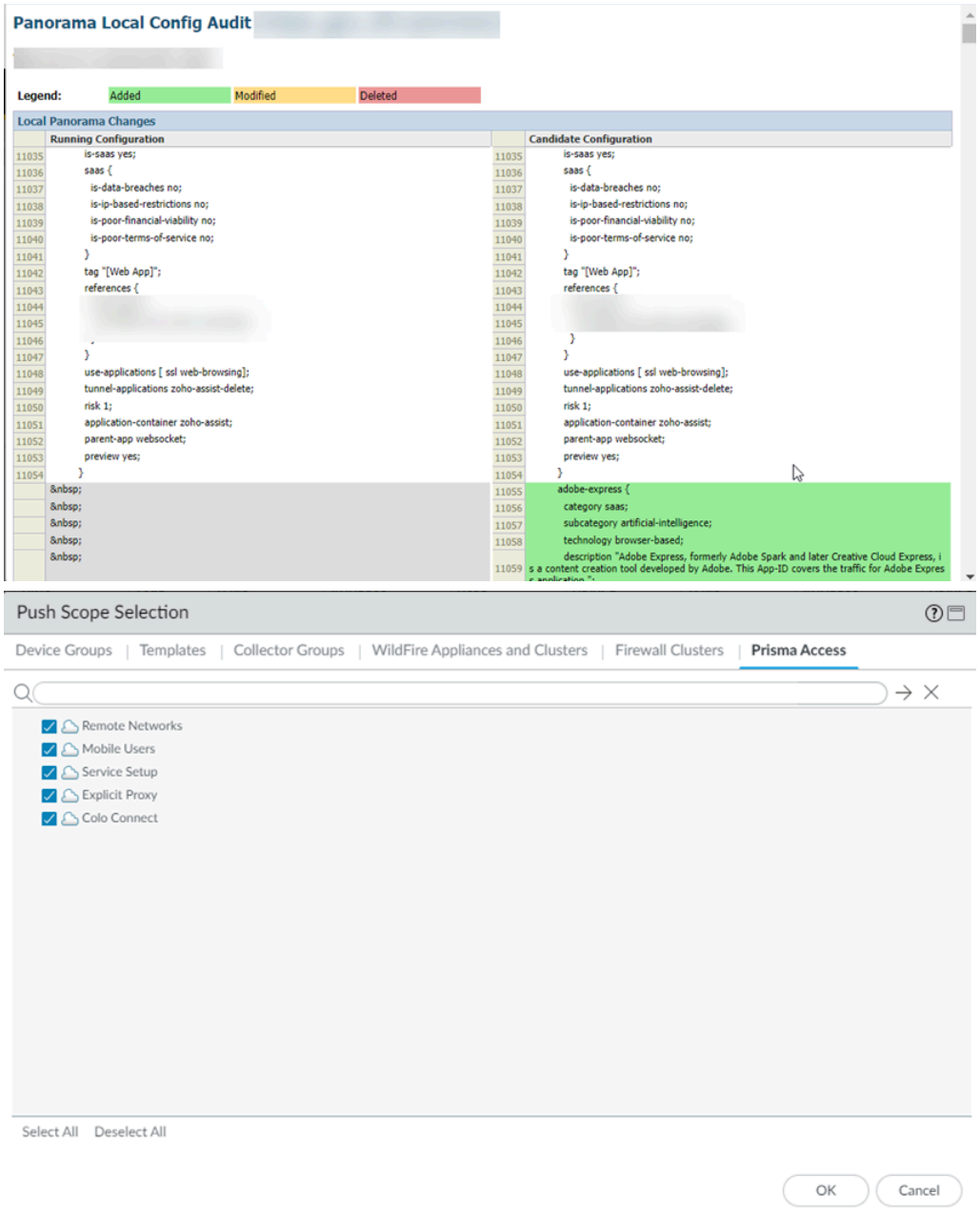
**STEP 1 |** Bereiten Sie Ihre Panorama-Instanz auf die Migration vor.

1. Melden Sie sich bei der Panorama-Instanz an, mit der Prisma Access über ein administratives Konto verwaltet wird, dem die Superuser-Rolle zugewiesen ist.
2. (Optional) Wenn Sie einen benutzerdefinierten Hauptschlüssel für Ihre Panorama-Instanz und für Prisma Access konfiguriert haben, notieren Sie sich diesen.

   Wenn Ihre Bereitstellung den Standard-Hauptschlüssel verwendet, ist dieser Schritt nicht erforderlich.
3. Stellen Sie sicher, dass Ihre aktuelle Panorama-Konfiguration auf dem neuesten Stand ist und Sie alle Ihre Änderungen festgeschrieben und an Panorama sowie an Prisma Access per Push übertragen haben, indem Sie **Commit** > **Commit und Push** sowie **Vorschau der Änderungen** aufrufen.
4. (Optional) Überprüfen Sie die Unterschiede zwischen der laufenden Konfiguration und der Kandidatenkonfiguration und geben Sie an, ob Sie diese Änderungen per Push übertragen möchten. Wenn Sie einen Commit für die Änderungen ausführen und diese

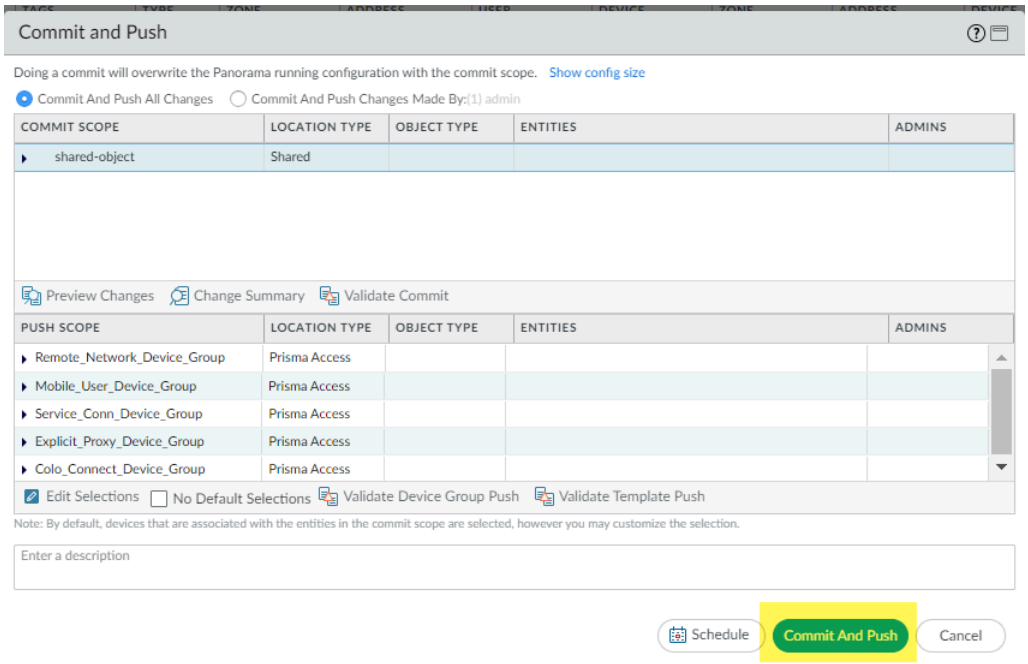
 ©2025 Palo Alto Networks, Inc.

per Push übertragen möchten, wählen Sie **Auswahl bearbeiten** und die Prisma Access-Komponenten aus, die per Push in den **Push-Bereich** übertragen werden sollen.




5. (Optional) Wählen Sie **Commit und Push** für Ihre Änderungen aus.

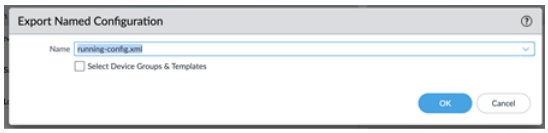
 ©2025 Palo Alto Networks, Inc.




6. Gehen Sie zu **Panorama** > **Einrichtung** > **Vorgänge** und zum **Panorama-Konfigurations-Snapshot mit dem Namen „Export“**.

   Diese XML-Datei muss während der Migration auf Strata Cloud Manager hochgeladen werden. **Laden Sie keine TechSupport-Datei oder eine andere Datei hoch, sondern nur eine XML-Konfigurationsdatei.**

7. Wählen Sie die Konfigurationsdatei **running-config.xml** und **OK** aus.

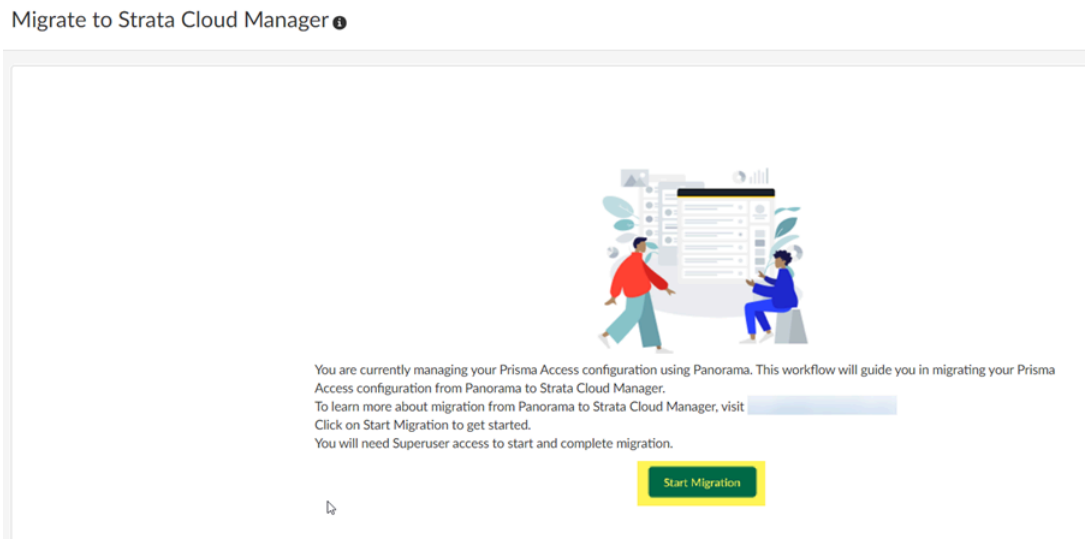



**STEP 2 |** Melden Sie sich als Administrator mit einer Superuser-Rolle bei Strata Cloud Manager an und gehen Sie zu **Verwalten** > **Konfiguration** > **NGFW und Prisma Access**.

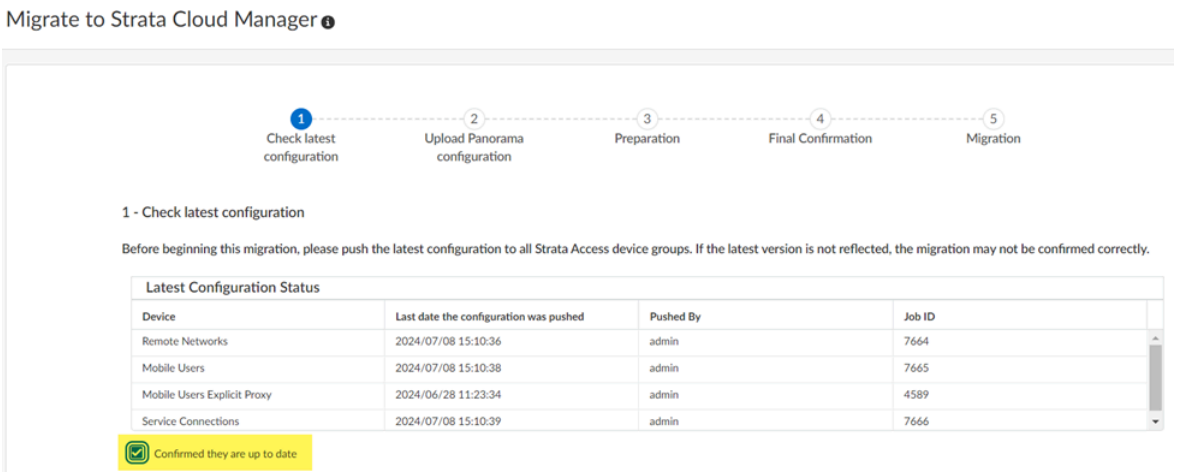
Das Migrationsprogramm erkennt, dass Sie über eine von Panorama verwaltete Bereitstellung verfügen.

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Wählen Sie **Migration starten** aus.



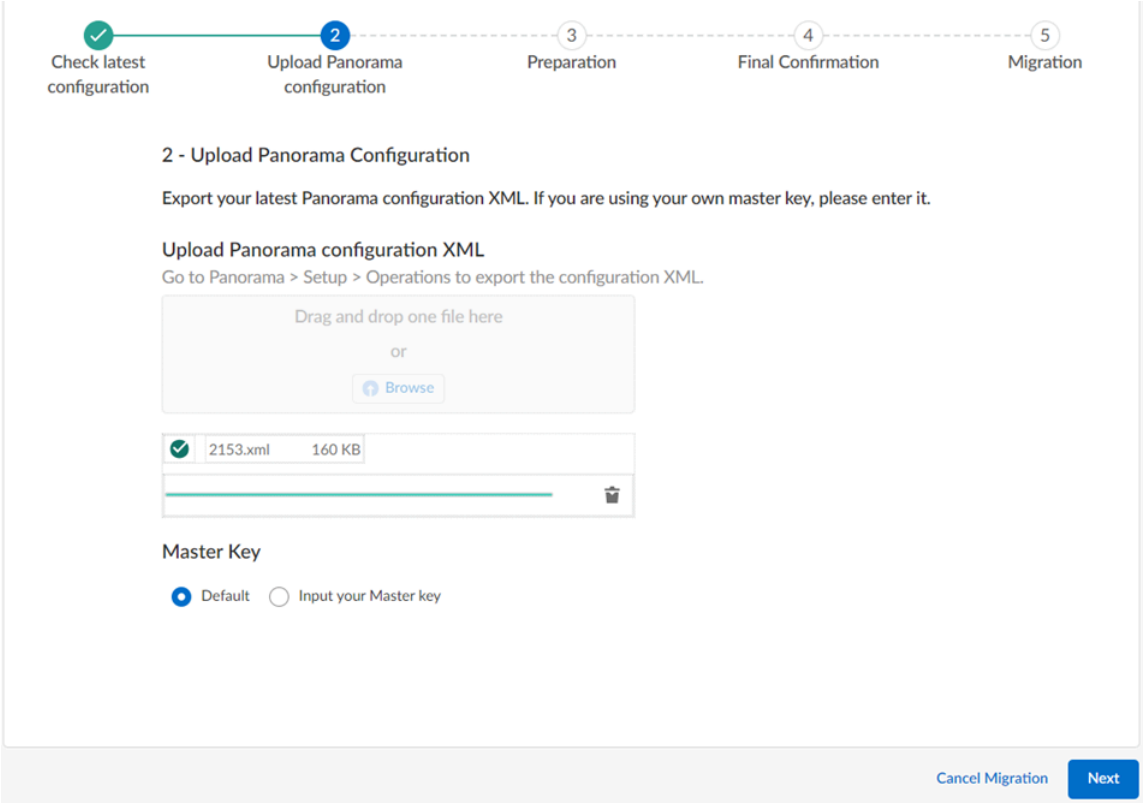

**STEP 4 |** Sie werden vom Migrationsprogramm aufgefordert, sicherzustellen, dass Ihre Konfiguration auf dem neuesten Stand ist. Es wird der Benutzer angezeigt, der die Konfiguration zuletzt aktualisiert hat. Nachdem Sie überprüft haben, dass diese Konfiguration die neuesten Änderungen umfasst, wählen Sie **Bestätigt, dass sie aktuell sind** aus und klicken Sie auf **Weiter**.



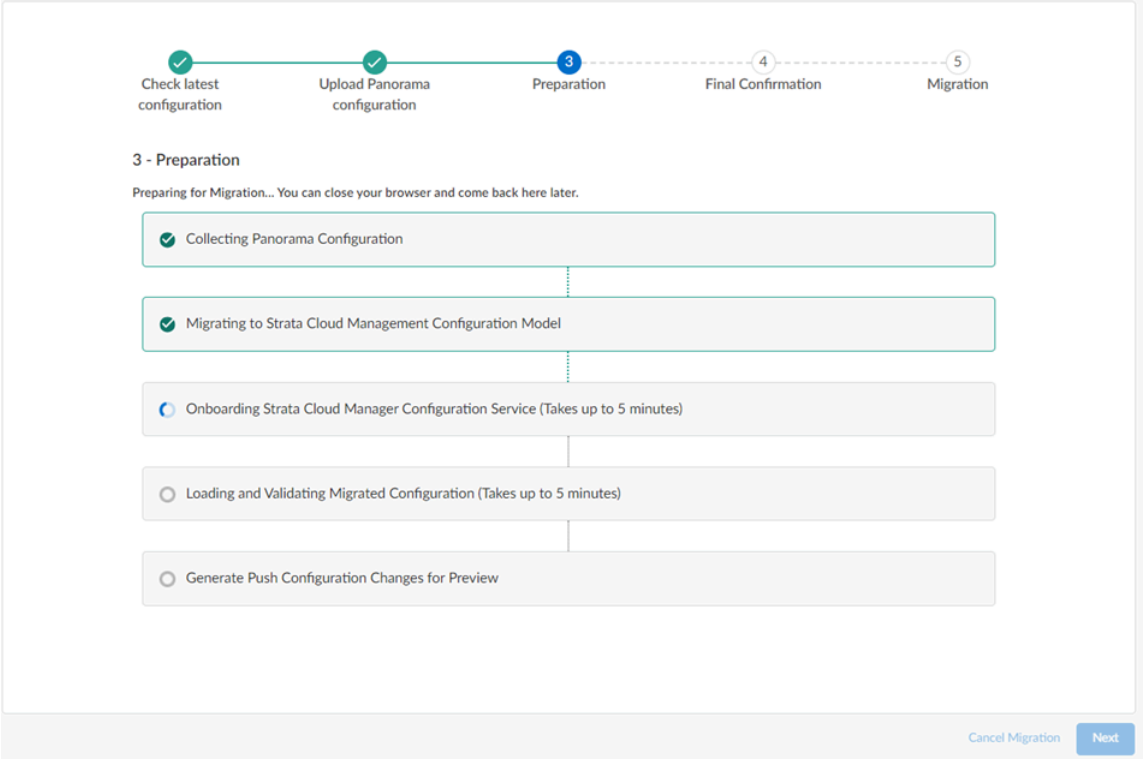

**STEP 5 |** Wählen Sie durch Ziehen und Ablegen oder durch Auswählen von **Datei auswählen** die XML-Datei mit der Panorama-Konfiguration aus, die Sie in einem früheren Schritt heruntergeladen haben.

 ©2025 Palo Alto Networks, Inc.

**STEP 6 |** Geben Sie Ihren **Hauptschlüssel** ein. Falls Sie keinen benutzerdefinierten Hauptschlüssel erstellt haben, bitten Sie Strata Cloud Manager, den **Standardschlüssel** zu verwenden, und klicken Sie auf **Weiter**.



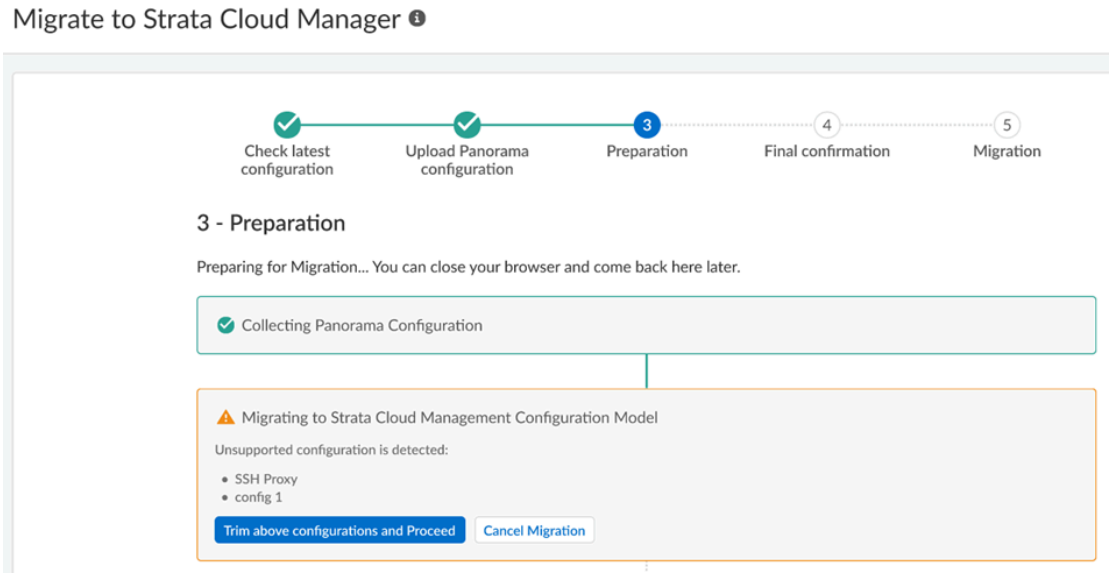

Das Migrationsprogramm beginnt.




 ©2025 Palo Alto Networks, Inc.

Warten Sie, bis alle Schritte abgeschlossen sind.

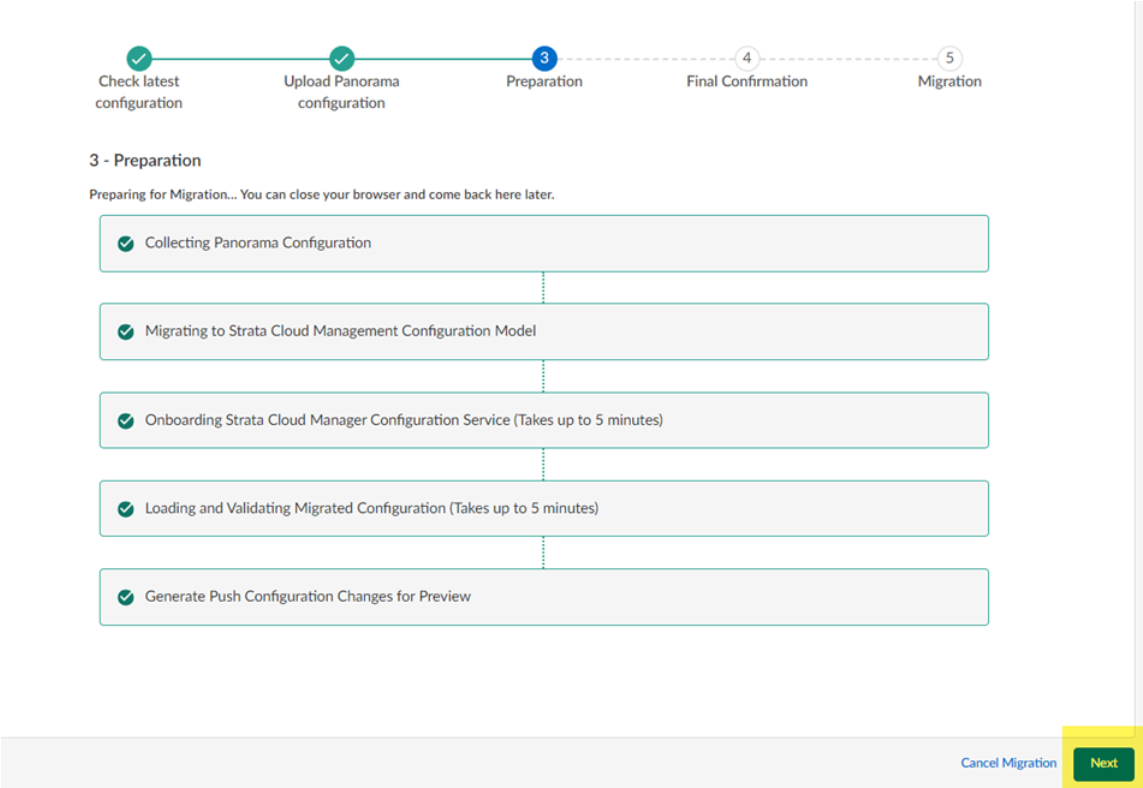
**STEP 7 |** Wenn das Programm während der Migration anzeigt, dass eine nicht unterstützte Konfiguration erkannt wurde, können Sie **Obige Konfigurationen trimmen und fortfahren** oder **Migration abbrechen** auswählen.




Durch einige nicht unterstützte Konfigurationen (z. B. eine Konfiguration mit mehreren Mandanten) wird die Migration abgebrochen, und das Migrationsprogramm kann das Problem nicht beheben. Wählen Sie in diesem Fall **Migration abbrechen** aus.

 ©2025 Palo Alto Networks, Inc.

**STEP 8 |** Klicken Sie nach Abschluss der Migration auf **Weiter**.




**STEP 9 |** Wenn das Migrationsprogramm Änderungen vorgenommen hat, überprüfen Sie diese im abschließenden Bestätigungsbildschirm.

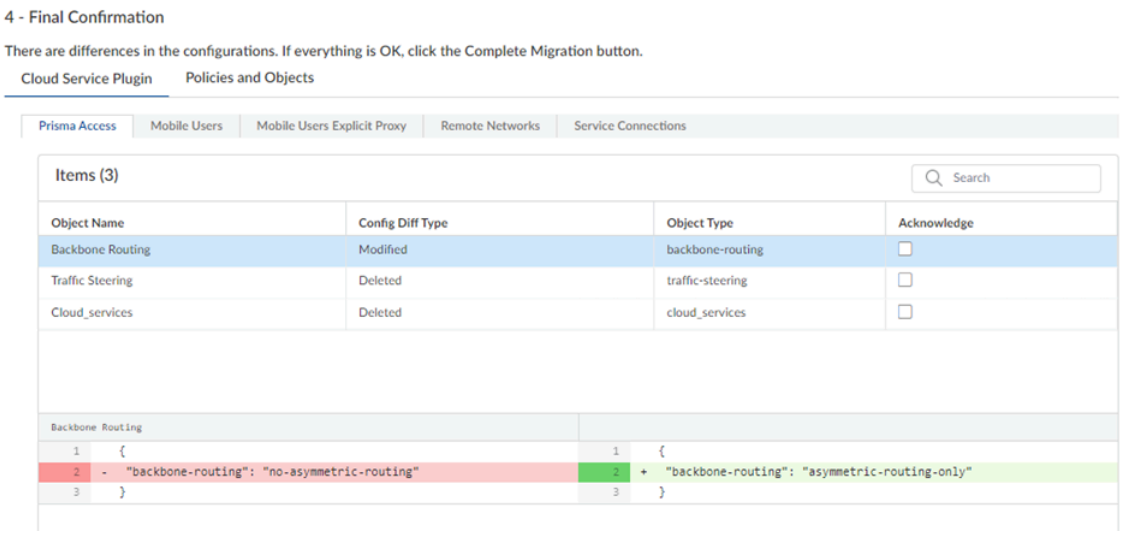
Das Migrationsprogramm kann Änderungen an Ihrer Konfiguration vornehmen, um Unterschiede zwischen der Panorama- und der Strata Cloud Manager-Konfiguration zu berücksichtigen oder um Lösungen für nicht unterstützte Funktionen zu finden. Sind

 ©2025 Palo Alto Networks, Inc.

Änderungen erforderlich, zeigt das Migrationsprogramm diese Änderungen in einer Vergleichsansicht mit den neuen Zeilen in Grün und den gelöschten Zeilen in Rot an.

*Ignorieren Sie alle Unterschiede, die für die folgenden Objektnamen angezeigt werden. Diese haben keinen Einfluss auf Ihre Konfiguration:*

- *Clientless-vpn crypto-settings*
- *Hip-profiles rename*
- *Mobile-user-redundancy*
- *Exclude-video-traffic*




**STEP 10 |** (Optional) Nehmen Sie Änderungen vor, um die Unterschiede zu beheben.

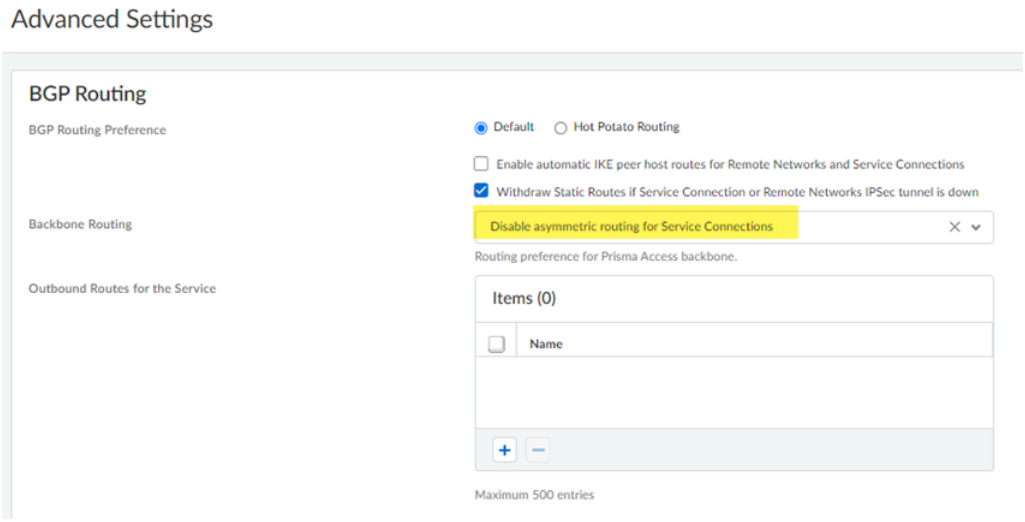
Alle Änderungen, die Sie vornehmen, werden erst dann in Ihrer Konfiguration festgeschrieben, wenn Sie die Migration abgeschlossen und Ihre Änderungen per Push an Strata Cloud Manager übertragen haben.

1. Navigieren Sie zu dem Bereich in der Prisma Access-Konfiguration, in dem Sie die Unterschiede gefunden haben, und nehmen Sie Änderungen an der Konfiguration vor.

   Für das Beispiel im vorherigen Schritt hat das Migrationsprogramm auf Backbone-Routing umgestellt (von **no-asymmetry-routing** zu **asymmetric-routing-only**). Um diese Einstellung auf die ursprüngliche Konfiguration zurückzusetzen, gehen Sie zu **Workflows** > **Einrichtung Prisma Access** > **Dienstverbindungen** > **Erweiterte Einstellungen** >

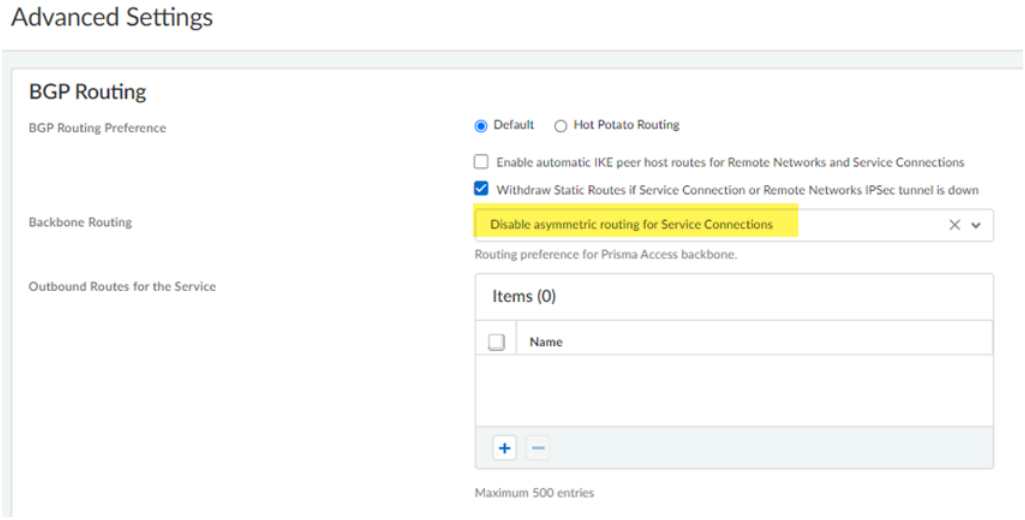
 ©2025 Palo Alto Networks, Inc.

und ändern Sie die Konfiguration **Backbone-Routing** in **Asymmetrisches Routing für Dienstverbindungen deaktivieren**.




2. (Optional) Um Ihre Änderungen nachzuverfolgen, wählen Sie abschließend **Anerkennen** aus.

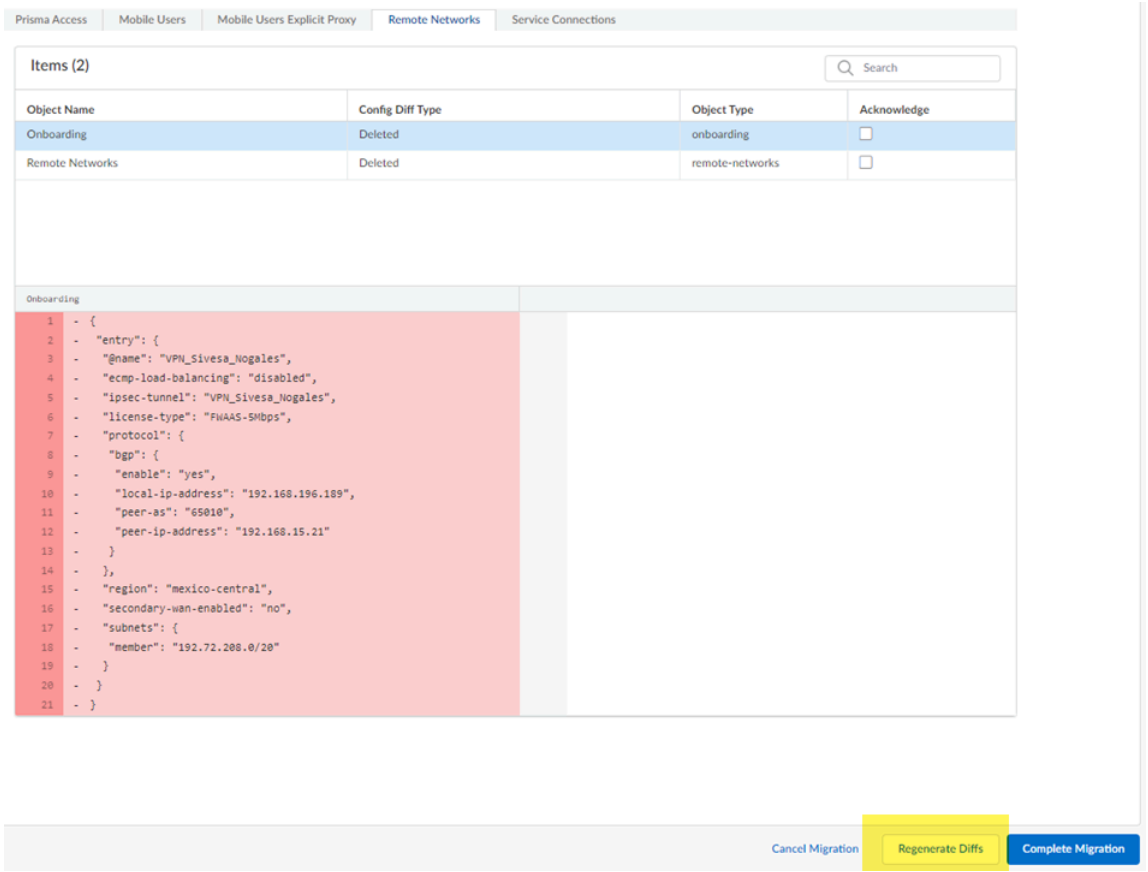
   Zwar ist dies nicht erforderlich, doch es kann nützlich sein, jede Änderung anzuerkennen, während Sie sie vornehmen, damit Sie die Änderungen nachverfolgen können.




3. Fahren Sie mit dem Überprüfen der Änderungen fort, nehmen Sie weiterhin Änderungen vor und erkennen Sie diese an.

 ©2025 Palo Alto Networks, Inc.

**STEP 11 |** (Optional) Wenn Sie Änderungen an der Konfiguration vorgenommen haben, wählen Sie **Unterschiede neu generieren** aus, um die aktualisierten Unterschiede anzuzeigen.

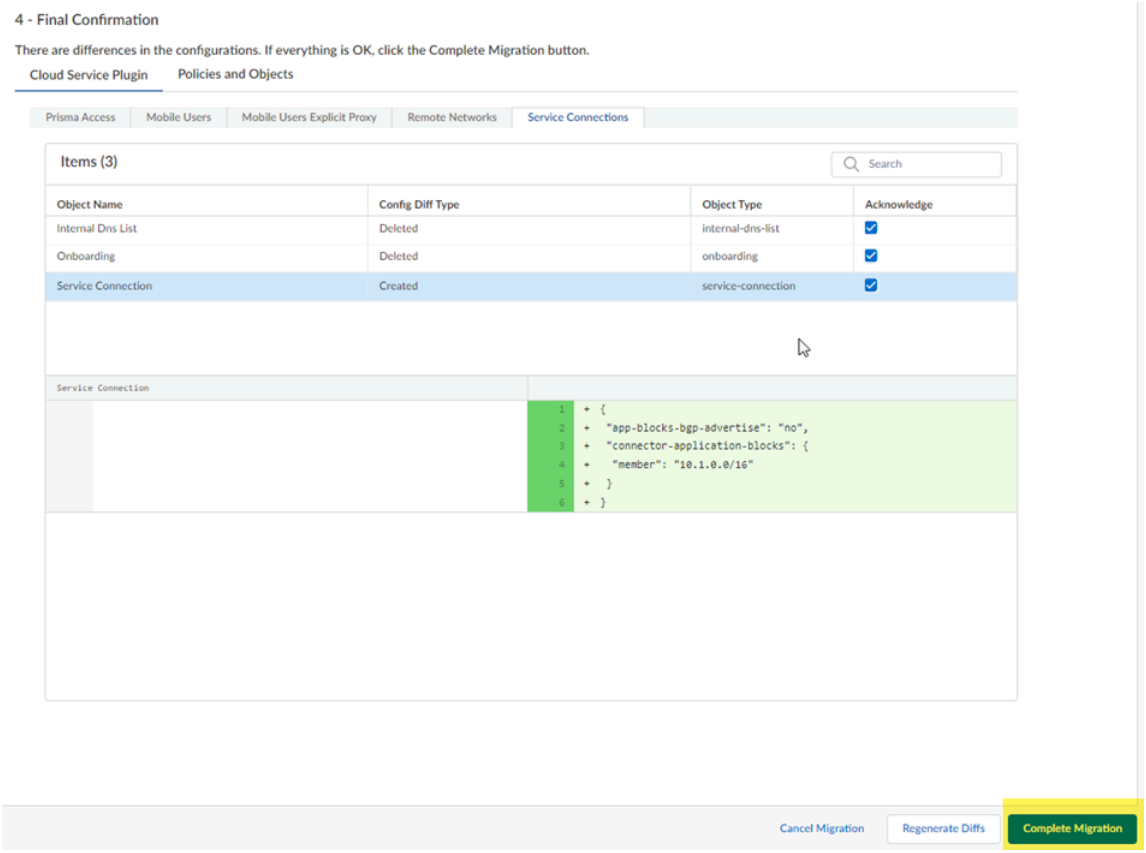



 ©2025 Palo Alto Networks, Inc.

**STEP 12 | Migration abschließen.**

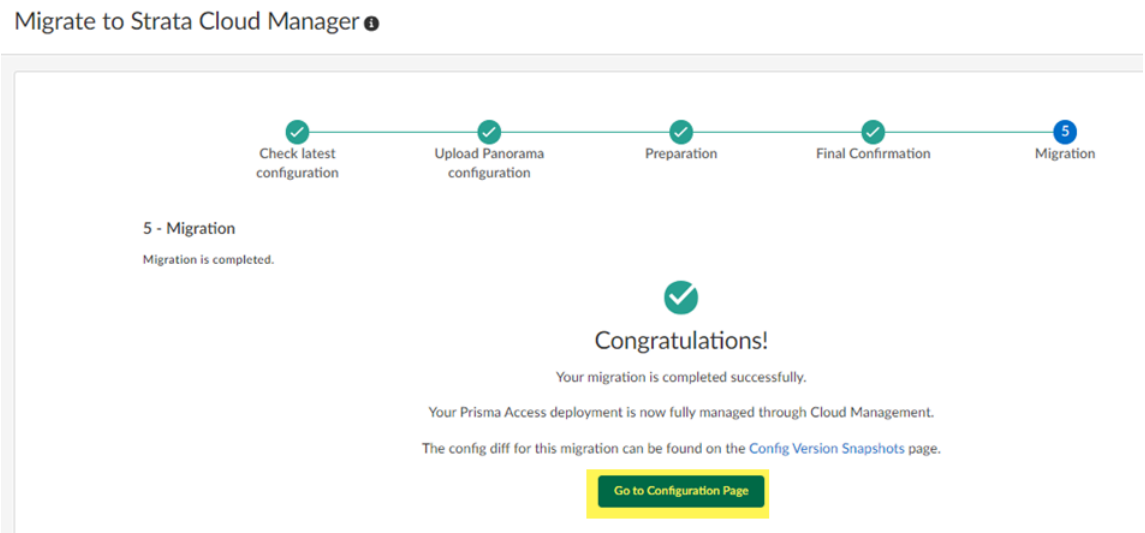
Zwar ist es nicht erforderlich, doch Sie können Ihre Änderungen auch bestätigen, indem Sie **Anerkennen** auswählen.

**Nachdem Sie Migration abschließen ausgewählt haben, können Sie nicht zu einer von Panorama verwalteten Bereitstellung zurückkehren und Ihre Bereitstellung verwendet dauerhaft Strata Cloud Manager für die Verwaltung.**

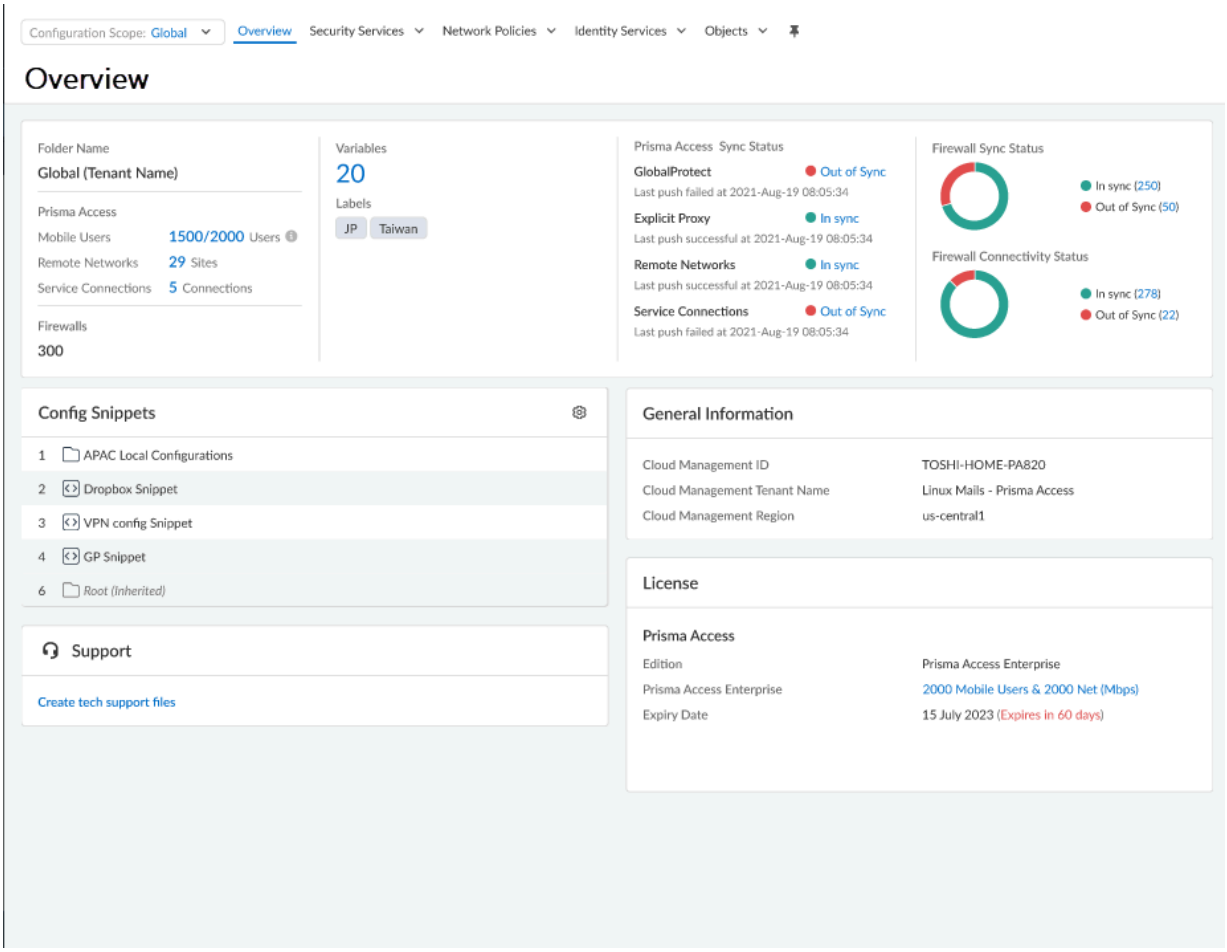



 ©2025 Palo Alto Networks, Inc.

**STEP 13 |** (Optional) Wählen Sie **Zur Konfigurationsseite gehen** aus, um Ihre migrierte Konfiguration anzuzeigen.




Die migrierte Bereitstellung wird angezeigt.




 ©2025 Palo Alto Networks, Inc.

**STEP 14 |** Wählen Sie **Konfiguration übertragen** > **Push** aus, um die Änderungen Ihrer migrierten Konfiguration anzuwenden.

Dieser Push-Vorgang stellt sicher, dass Ihre Migration erfolgreich abgeschlossen wurde und dass Prisma Access alle Änderungen auf Ihre migrierte Konfiguration angewendet hat.

**STEP 15 |** Notieren Sie sich alle Nachrichten, die während des Push-Vorgangs angezeigt werden, und nehmen Sie bei Problemen Änderungen an Ihrer Konfiguration vor.

 ©2025 Palo Alto Networks, Inc.

# Prisma Access – Versionen und Upgrades

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Durch Prisma Access-Versionen und -Updates bleiben Sie stets auf dem Laufenden und können Ihre Benutzer schützen. Einige der Updates werden von Palo Alto Networks verwaltet, wie z. B. Prisma Access-Infrastruktur-Updates, und Sie werden vorab darüber informiert, sodass Sie diese entsprechend planen können. Andere Updates liegen in Ihrer Verantwortung. Sie müssen die angegebene Version der Inhaltsaktualisierung, des Software-Updates und der Plug-in-Version (nach Bedarf) so schnell wie möglich planen.

*Sie können den Status aller Cloud Services, einschließlich Prisma Access und Strata Logging Service, sowie eine historische Aufzeichnung der Verfügbarkeit der einzelnen Dienste über die Website* https://sase.status.paloaltonetworks.com/ *abrufen. Sie können sich auch für E-Mail- oder SMS-Updates auf dieser Website anmelden, um im Voraus benachrichtigt zu werden, wenn Infrastruktur-Updates geplant sind, wenn Palo Alto Networks einen Vorfall erstellt, aktualisiert oder behebt und um Echtzeit-Benachrichtigungen zu Updates zu erhalten.*

# Prisma Access-Versionstypen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Prisma Access verfügt über Upgrades, einschließlich Hauptversionen und Infrastrukturwartung, die neue Funktionen und Optimierungen umfassen, um die bestmögliche Sicherheit für Ihre Remote-Netzwerke und mobilen Benutzer zu bieten.

Die folgende Liste definiert die Versionstypen, zusammen mit der Vorabbenachrichtigung, die wir Ihnen für jede Version zur Verfügung stellen. Zur Sicherstellung, dass Sie Benachrichtigungen für alle Versionen erhalten, registrieren Sie sich auf der Website https://sase.status.paloaltonetworks.com/ für E-Mail- oder Textbenachrichtigungen für Prisma Access und melden Sie sich für Benachrichtigungen in Strata Cloud Manager an.

- **Hauptversion** – Eine Hauptversion enthält in der Regel wichtige neue Funktionen und Optimierungen. Solche Aktualisierungen werden mit einem geplanten Wartungsfenster von Palo Alto Networks vorangetrieben. Palo Alto Networks informiert die Kunden über solche geplanten Wartungsarbeiten per E-Mail über sase.status.paloaltonetworks.com.

  **Benachrichtigung** – Palo Alto Networks stellt Ihnen folgende Benachrichtigungen für Hauptversionen zur Verfügung:

| Bereitstellungstyp | Mitteilungszeitraum |
|---|---|
| **Produktionsbereitstellungen** | Palo Alto Networks informiert Sie 21 Tage vor der Veröffentlichung einer Hauptversion. |
| **Lab-Bereitstellungen** | Palo Alto Networks informiert Sie 7 Tage vor der Veröffentlichung einer Hauptversion. |



*Zusätzlich zu dem geplanten Upgrade einer Hauptversion muss Palo Alto Networks möglicherweise dringend geplante Upgrades durchführen, die einem anderen Zeitplan folgen.*

Lab-Mandanten fallen nicht unter das Service Level Agreement (SLA) von Prisma Access. Kunden wird dringend empfohlen, die Mandanten nur für Test- und Qualifizierungszwecke vor der Produktion einzusetzen.


©2025 Palo Alto Networks, Inc.

- **Infrastrukturwartung** – Enthält inkrementelle Funktionen und Optimierungen. In einigen Fällen kann Palo Alto Networks einen Hotfix mit der Infrastrukturwartung kombinieren.

  **Benachrichtigung** – Palo Alto Networks stellt Ihnen folgende Benachrichtigungen zur Verfügung:

| Bereitstellungstyp | Mitteilungszeitraum |
|---|---|
| **Produktionsbereitstellungen** | Palo Alto Networks informiert Sie 10 Tage vor der Infrastrukturwartung. |
| **Lab-Bereitstellungen** | Palo Alto Networks informiert Sie 7 Tage vor der Infrastrukturwartung. |

  *Zusätzlich zu dem geplanten Upgrade einer Hauptversion muss Palo Alto Networks möglicherweise dringend geplante Upgrades durchführen, die einem anderen Zeitplan folgen.*

- **Release von Cloud Services-Plug-in (nur von Panorama verwaltete Bereitstellungen)** – Wenn Prisma Access ein neues Plug-in benötigt, wird es über das Customer Support Portal (CSP) von Palo Alto Networks und auf Panorama am Datum der allgemeinen Verfügbarkeit des Release zum Download bereitgestellt.

  Prisma Access kann alle Mandanten zwingen, ein Upgrade auf eine bestimmte Cloud Services-Plug-in-Version durchzuführen, um die Abwärtskompatibilität und unterstützte Softwareversionen aufrechtzuerhalten. Bei einer solchen Durchsetzungsmaßnahme wird eine **14-tägige Vorankündigung** (über die Seite sase.status.paloaltonetworks.com) bereitgestellt, um das Upgrade des Plug-ins zu planen. Der Dienst empfiehlt dringend, dass Sie ein Upgrade auf das neueste Plug-in durchführen, sobald es zum Download verfügbar ist.

## Dringend geplante Upgrades

Palo Alto Networks muss gelegentlich dringende Dataplane-Upgrades oder für die Infrastruktur durchführen, die Hotfixes oder dringende Fehlerkorrekturen beinhalten (z. B. Fehlerkorrekturen für Zero-Day-Bedrohungen oder Plug-in-Änderungen). Palo Alto Networks ist bemüht, Sie 48 Stunden vor einem dringenden geplanten Upgrade zu informieren. Gelegentlich wird ein dringendes geplantes Upgrade jedoch möglicherweise auch kurzfristiger angekündigt.

 ©2025 Palo Alto Networks, Inc.

# Prisma Access Upgrade-Arten

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Palo Alto Networks aktualisiert seine Cloud-basierte Infrastruktur, ohne dass Sie aktiv werden müssen. Bei einigen Upgrades werden Sie aufgefordert, bestimmte Aktionen wie beispielsweise die Installation eines neuen Plug-ins durchzuführen.

Die folgende Liste enthält die verschiedenen Arten von Prisma Access-Upgrades:

- **Upgrade der Infrastruktur**: Palo Alto Networks nimmt ein Upgrade der Prisma Access-Infrastruktur, auch bekannt als Prisma Access-*Steuerungsebene*, vor. Dieser Vorgang umfasst das zugrunde liegende Dienst-Back-End, die Orchestrierung und die Überwachungsinfrastruktur.

  Upgrades der Infrastruktur sind vier- bis sechsmal im Jahr zu erwarten.
- **Dataplane-Upgrade**: Palo Alto Networks nimmt ein Upgrade der Prisma Access Dataplane vor. Dies ermöglicht die Überprüfung des Datenverkehrs und die Durchsetzung von Sicherheitsrichtlinien für Ihr Netzwerk und den Benutzerdatenverkehr.

  Sie nutzen die App, um sich für E-Mail-Benachrichtigungen über Dataplane-Upgrades anzumelden und Ihre Präferenzen für Upgrades anzugeben.
- **Geplante Wartung von Prisma Access**: Prisma Access hält alle zwei Wochen ein Zeitfenster für Wartungsarbeiten im Zusammenhang mit Hotfixes und Notfall-Fehlerkorrekturen an der Infrastruktur frei.
- (Nur von Panorama verwaltete Bereitstellungen) **Upgrade des Cloud Services-Plug-ins**: Wenn eine neue Plug-in-Version verfügbar wird, muss Ihr Netzwerkadministrator das Plug-in „Cloud Services“ in der Panorama-Appliance aktualisieren, die Prisma Access verwaltet.
- (Nur von Panorama verwaltete Bereitstellungen) **Upgrade der Panorama-Softwareversion**: Unter Umständen ist ein Upgrade Ihrer Panorama-Software erforderlich, um die Kompatibilität mit Prisma Access sicherzustellen.

Aus der folgenden Tabelle geht hervor, was in jeder Version enthalten ist, einschließlich des von uns bereitgestellten Wartungsfensters und der Auswirkungen auf Ihren Prisma Access-Dienst.

| Art des Upgrades | Wartungsfenster | Auswirkung |
|---|---|---|
| Upgrade der Infrastruktur | 2–8 Stunden | Keine Auswirkungen auf den Netzwerkverkehr. Sie können jedoch während der Wartung keine Commits durchführen.<br>Palo Alto Networks plant die Upgrades zu einer Ortszeit, |

 ©2025 Palo Alto Networks, Inc.

| Art des Upgrades | Wartungsfenster | Auswirkung |
|---|---|---|
| | | zu der die Geschäftsabläufe nur minimal beeinträchtigt werden. |
| Dataplane-Upgrade | 72 Stunden | Palo Alto Networks verwendet dieses Fenster für alle Kunden zum Dataplane-Upgrade. Während dieser Zeit können Sie Konfigurationsänderungen und Commits vornehmen. Unser Ziel ist es, die Auswirkungen auf den Netzwerkverkehr so gering wie möglich zu halten. Nur in wenigen Fällen kann es zu einer kurzen Unterbrechung kommen. Weitere Informationen finden Sie unter Prisma Access Dataplane-Upgrades.<br><br>Sie nutzen die App, um sich für E-Mail-Benachrichtigungen über Dataplane-Upgrades anzumelden und Ihre Präferenzen für Upgrades einschließlich Ihres bevorzugten Zeitfensters für das Upgrade anzugeben. |
| Upgrade des Cloud Services-Plug-ins (nur von Panorama verwaltete Bereitstellungen) | Sie installieren das Plug-in, sobald es verfügbar ist. | Prisma Access kann Sie unter Umständen zwingen, ein Upgrade aller Mandanten auf eine bestimmte Plug-in-Version durchzuführen, um die Abwärtskompatibilität und unterstützte Softwareversionen aufrechtzuerhalten.<br><br>Während des Plug-in-Upgrades können Sie keine Konfigurationsänderungen und Commits in Panorama vornehmen. |


©2025 Palo Alto Networks, Inc.

| Art des Upgrades | Wartungsfenster | Auswirkung |
|---|---|---|
| Upgrade der Panorama-Softwareversion (nur von Panorama verwaltete Bereitstellungen) | Sie planen und führen das Upgrade der Panorama-Appliance durch, die Prisma Access verwaltet. | Wenn Prisma Access ein Upgrade seiner Infrastruktur und Dataplane nach einem Hauptrelease aktualisiert, sind die Upgrades möglicherweise inkompatibel mit früheren Panorama-Versionen. Aufgrund der schnell aufeinanderfolgenden Veröffentlichung von Prisma Access-Versionen und des Cloud Services-Plug-ins sind die Daten für die Softwarekompatibilität (End-of-Support) für Panorama kürzer als die End-of-Life-Daten für Panorama-Versionen und gelten nur für die Kompatibilität der Panorama-Version mit Prisma Access. Weitere Informationen, einschließlich der End-of-Support-Daten für Panorama bei Verwendung mit Prisma Access, finden Sie unter Kompatibilität der Prisma Access- und Panorama-Versionen in der Kompatibilitätsmatrix von Palo Alto Networks. |

 ©2025 Palo Alto Networks, Inc.

# Kadenz für Software- und Inhaltsaktualisierungen für Prisma Access

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

- Strata Cloud Manager
- Panorama

## Kadenz für Software- und Inhaltsaktualisierungen für Prisma Access (Managed by Strata Cloud Manager)

In der folgenden Tabelle wird beschrieben, wie Prisma Access seine Infrastrukturkomponenten einschließlich der Inhalts- und Softwareupdates aktualisiert. Diese Tabelle zeigt auch, ob die Software von Prisma Access automatisch aktualisiert wird. Wenn Updates nicht automatisch ausgeführt werden, erfahren Sie, wie Sie diese Infrastrukturupdates anwenden können.

*Sie können über den Hub auch den* Status aller Cloud-Dienste überprüfen.

| Komponente | Aktualisierungszeitplan | Bemerkungen |
|---|---|---|
| GlobalProtect-App | • **Hauptreleases für die GlobalProtect-App (z. B. *x*.0 oder 4.*x*) –** Prisma Access aktualisiert die App 7–10 Tage nach der allgemeinen Verfügbarkeit der Version *x*.0.1 mit dem neuesten Hauptrelease.<br>Bei dem App-Release 4.0 aktualisiert Prisma Access die App beispielsweise 7–10 Tage nach dem Release 4.0.1.<br>• **Unterreleases der GlobalProtect-App (z. B. 4.1.*x*) –** Prisma Access aktualisiert die App 7–10 Tage nach der allgemeinen Verfügbarkeit dieses Release mit dem neuesten Unterrelease. | Die Cloud steuert die Version der App, die zum Upgrade verfügbar ist. |
| PAN-OS-Software-Upgrades in der Prisma Access- | Palo Alto Networks® aktualisiert die PAN-OS-Infrastruktur, wenn eine neue Version von Prisma Access veröffentlicht wird. Palo Alto Networks® informiert Sie drei Wochen vor einem geplanten Upgrade. | Melden Sie sich an, um Infrastruktur-Upgrades per E-Mail- oder SMS-Benachrichtigung am Hub zu erhalten. |

 ©2025 Palo Alto Networks, Inc.

| Komponente | Aktualisierungszeitplan | Bemerkungen |
|---|---|---|
| Infrastruktur – geplant | | |
| Aktualisierungen zu Anwendungen und Bedrohungen | Täglich mit einem Schwellenwert von 24 Stunden.<br>Palo Alto Networks® veröffentlicht jeweils am dritten Dienstag im Monat neue App-IDs. Planen Sie, diese neuen App-IDs innerhalb des 24-Stunden-Schwellenwerts zu überprüfen und einzubinden. Verwenden Sie den Filter „Neue App-ID“, um die möglichen Auswirkungen auf den Datenverkehr zu minimieren.<br>Mit der Eigenschaft „Neue App-ID“ können Sie neue Anwendungen in Ihrem Netzwerk sehen und Details über neu kategorisierte Anwendungsaktivitäten anzeigen. Die so gewonnenen Informationen können Ihnen helfen, die richtigen Entscheidungen darüber zu treffen, wie Sie Ihre Sicherheitsrichtlinie aktualisieren sollten, um die zuletzt kategorisierten App-IDs durchzusetzen. | |
| Virenschutz | Jede Stunde, 10 Minuten nach der entsprechenden Stunde | Prisma Access ist immer auf dem neuesten Stand des aktuellsten Antivirus-Release. |
| WildFire | Echtzeit | Prisma Access ist immer auf dem neuesten Stand des aktuellsten WildFire-Release. |
| GlobalProtect-Datendatei | Jede Stunde | Prisma Access ist immer auf dem neuesten Stand des aktuellsten Release der GlobalProtect-Datendatei. |
| Clientloses VPN<br>Anwendungssignaturen | Jede Stunde | Prisma Access ist immer auf dem neuesten Stand des aktuellsten Release für die Anwendungssignatur des clientlosen VPN. |


©2025 Palo Alto Networks, Inc.

# Kadenz für Software- und Inhaltsaktualisierungen für Prisma Access (Managed by Panorama)

Die folgende Tabelle informiert Sie über die Software- und Inhaltsaktualisierungen, um die neuesten Anwendungen und Bedrohungssignaturen zu erhalten und die von Palo Alto Networks bereitgestellten Funktionen zur Abwehr von Bedrohungen (Threat-Prevention) zu nutzen. Wenn die Spalte **Cloud-gesteuert?** das Attribut **Nein** aufweist, führen Sie die erforderlichen Aktionen aus, um die Komponente zu aktualisieren.

| Komponente | Aktualisierungszeitplan | Cloud-gesteuert? (Ja/Nein) | Bemerkungen |
|---|---|---|---|
| Upgrades der Panorama-Software für Kompatibilität mit Prisma Access | Für Prisma Access-Hauptreleases müssen Sie Ihre Panorama-Version möglicherweise für die folgenden Anwendungsfälle aktualisieren:<br>• **Erforderliches Upgrade** – Gelegentlich müssen Sie die Softwareversion von Panorama aktualisieren, um die Kompatibilität mit Prisma Access sicherzustellen.<br>• **Wartungsfenster** – Ihre Organisation muss ein Wartungsfenster einplanen, um die Version der Panorama-Software zu aktualisieren.<br>• **Auswirkungen** – Sie können die neue Plug-in-Version erst verwenden, nachdem Sie Ihre Panorama-Version | Nein | Siehe End-of-Support (EoS)-Termine für die Kompatibilität der Panorama-Softwareversion mit Prisma Access, um zu erfahren, wann eine Panorama-Version mit Prisma Access inkompatibel wird. Siehe Prisma Access und die Kompatibilität der Version von Panorama für die derzeit unterstützten Panorama-Versionen, die mit Prisma Access verwendet werden können. Informationen zum Upgrade von Panorama auf eine neue Version finden Sie unter Installieren von Inhalts- und Softwareupdates für Panorama. |


©2025 Palo Alto Networks, Inc.

| Komponente | Aktualisierungszeitplan | Cloud-gesteuert? (Ja/ Nein) | Bemerkungen |
|---|---|---|---|
| | aktualisiert haben.<br>• **Benachrichtigung** – Palo Alto Networks wird Sie 100 Tage vor dem geplanten Upgrade der Hauptversion benachrichtigen.<br>• **Optionales Upgrade** – In anderen Fällen müssen Sie die Panorama-Softwareversion möglicherweise aktualisieren, um die neuen Funktionen zu nutzen, die Prisma Access im Hauptrelease unterstützt.<br>• **Wartungsfenster** – Ihre Organisation muss ein Wartungsfenster einplanen, um die Version der Panorama-Software zu aktualisieren.<br>• **Auswirkungen** – Sie können die neuen Funktionen, die Prisma Access unterstützt, erst nach dem Upgrade Ihrer Panorama-Software verwenden. | | |

 ©2025 Palo Alto Networks, Inc.

| Komponente | Aktualisierungszeitplan | Cloud-gesteuert? (Ja/ Nein) | Bemerkungen |
|---|---|---|---|
| | • **Benachrichtigung** – Palo Alto Networks informiert Sie 21 Tage vor einem geplanten Upgrade des Hauptrelease gemäß Prisma Access-Versionstypen über alle Panorama-Anforderungen. | | |
| Plug-in-Version für Cloud Services | Verfügbar nach der Veröffentlichung des Plug-in-Release. | Nein | Sie führen die Aufgaben aus, um das Plug-in zu aktualisieren. In Prisma Access-Versionstypen finden Sie Details darüber, wann Prisma Access seine Plug-in-Version aktualisiert. Siehe Upgrade des Cloud-Services-Plug-ins, um das Plug-in in den Panorama-Anwendungen zu aktualisieren. |
| GlobalProtect-App | • **Hauptreleases der GlobalProtect-App (z. B. *x*.0 oder 5.*x*) –** Prisma Access aktualisiert den Agenten im Portal 7–10 Tage nach der allgemeinen Verfügbarkeit der Version *x*.0.1 dieses Release | Ja | Die Cloud steuert die Versionen der App, die für ein Upgrade verfügbar sind. Sie können jedoch zwischen mehreren unterschiedlichen gehosteten Versionen der App wählen und steuern, wie und wann Updates der GlobalProtect-App |


©2025 Palo Alto Networks, Inc.

| Komponente | Aktualisierungszeitplan | Cloud-gesteuert? (Ja/Nein) | Bemerkungen |
|---|---|---|---|
| | mit dem neuesten Hauptrelease.<br><br>Beispielsweise aktualisiert Prisma Access beim Agentenrelease 5.1 den Agenten im Portal 7–10 Tage nach Freigabe von Version 5.1.1.<br>• **Unterreleases der GlobalProtect-App (z. B. 5.1.*x*)** – Prisma Access aktualisiert den Agenten im Portal 7–10 Tage nach der allgemeinen Verfügbarkeit dieses Release mit dem neuesten Infrastrukturwartungsrelease. | | für die Endbenutzer bereitgestellt werden sollen. Weitere Einzelheiten finden Sie unter GlobalProtect-App-Upgrades.<br><br>Wenn für Ihre Prisma Access-Bereitstellung ein Hotfix der GlobalProtect-App erforderlich ist, öffnen Sie einen Support-Fall beim technischen Support von Palo Alto Networks. |
| Aktualisierungen zu Anwendungen und Bedrohungen | Täglich mit einem Schwellenwert von 24 Stunden.<br><br>Palo Alto Networks veröffentlicht am dritten Dienstag im Monat neue App-IDs. Planen Sie, diese neuen App-IDs innerhalb des 24-Stunden-Schwellenwerts zu überprüfen und einzubinden.<br><br>Mit der Eigenschaft „Neue App-ID“ können Sie neue Anwendungen in Ihrem Netzwerk sehen und Details über neu | Ja | |


©2025 Palo Alto Networks, Inc.

| Komponente | Aktualisierungszeitplan | Cloud-gesteuert? (Ja/Nein) | Bemerkungen |
|---|---|---|---|
| | kategorisierte Anwendungsaktivitäten anzeigen. Die so gewonnenen Informationen können Ihnen helfen, die richtigen Entscheidungen darüber zu treffen, wie Sie Ihre Sicherheitsrichtlinie aktualisieren sollten, um die zuletzt kategorisierten App-IDs durchzusetzen. | | |
| Virenschutz | Jede Stunde, 10 Minuten nach der entsprechenden Stunde | Ja | Prisma Access ist immer auf dem neuesten Stand des aktuellsten Antivirus-Release. |
| WildFire | Echtzeit | Ja | Prisma Access ruft WildFire-Signaturen für neu erkannte Malware ab, sobald die WildFire-Public-Cloud diese generieren kann. |
| GlobalProtect-Datendatei | Jede Stunde | Ja | Prisma Access ist immer auf dem neuesten Stand des aktuellsten Release der GlobalProtect-Datendatei. |
| Anwendungssignaturen für Clientloses VPN | Jede Stunde | Ja | Prisma Access ist immer auf dem neuesten Stand des aktuellsten Release für die Anwendungssignatur des clientlosen VPN. |


©2025 Palo Alto Networks, Inc.

# Prisma Access Dataplane-Upgrades

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

*Prisma Access (Managed by Strata Cloud Manager) führt automatisch Dataplane-Upgrades durch, ohne dass Sie aktiv werden müssen.*

Prisma Access führt Dataplane-Upgrades durch, um neue Sicherheitsfunktionen und Leistungsmerkmale bereitzustellen, mit denen die Endbenutzer Ihres Unternehmens, Ihre Assets und der digitale Wandel geschützt werden. Wenn für eine neue Prisma Access-Version ein Dataplane-Upgrade erforderlich ist, müssen Sie verstehen, wie der Upgrade-Prozess funktioniert, und vor dem Upgrade die erforderlichen Voraussetzungen erfüllen.

Dataplane-Upgrades sind ein- bis zweimal im Jahr geplant. Einige Versionen bieten möglicherweise zusätzlich zu den erforderlichen Dataplane-Upgrades auch ein optionales Dataplane-Upgrade, um Prisma Access-Funktionen zu unterstützen, für die dies erforderlich ist.

- Übersicht über Dataplane-Upgrades
- Beispiel für ein Dataplane-Upgrade

### Übersicht über Dataplane-Upgrades

Prisma Access führt ein Dataplane-Upgrade an zwei Wochenendterminen in zwei Phasen durch und informiert Sie mittels Strata Cloud Manager über den aktuellen Status. Auf hoher Ebene werden während des Upgrades die nachfolgenden Schritte durchgeführt.

- 21 Tage vor dem geplanten Startdatum des Dataplane-Upgrades erhalten Sie eine E-Mail-Benachrichtigung von Strata Cloud Manager. Darin sind das Startdatum von Phase 1 des Upgrades sowie ein ausgewählter Standort angegeben.

  *Möglicherweise wird in Strata Cloud Manager ein Datum angezeigt, das vor dem Datum liegt, über das Sie 21 Tage vor dem geplanten Startdatum benachrichtigt wurden. Dieses Datum ist möglicherweise erst dann endgültig, wenn Sie Ihre Benachrichtigung 21 Tage vor dem geplanten Startdatum erhalten haben.*

- In der E-Mail werden Sie gebeten, über Strata Cloud Manager den Standort/die Standorte, an dem/denen das Upgrade zuerst durchgeführt werden soll, und das bevorzugte Zeitfenster für das Upgrade auszuwählen und zu übermitteln.

  Den Standort für den Start des Upgrades und das Zeitfenster können Sie für einen bestimmten Mandanten mehrmals ändern und bestätigen. Die letzte Übermittlung, die sieben Tage vor dem

 ©2025 Palo Alto Networks, Inc.

geplanten Startdatum erfolgt ist, wird vom Dienst für das Upgrade ausgewählt. Innerhalb von sieben Tagen nach dem Startdatum des Upgrades können Sie keine Änderungen vornehmen.

Sollten Sie Änderungen vornehmen, kann es bis zu 30 Minuten dauern, bis diese im Upgrade-Dashboard von Insights angezeigt werden. Sie werden per E-Mail benachrichtigt, wenn Prisma Access die Änderungen bearbeitet und abgeschlossen hat.

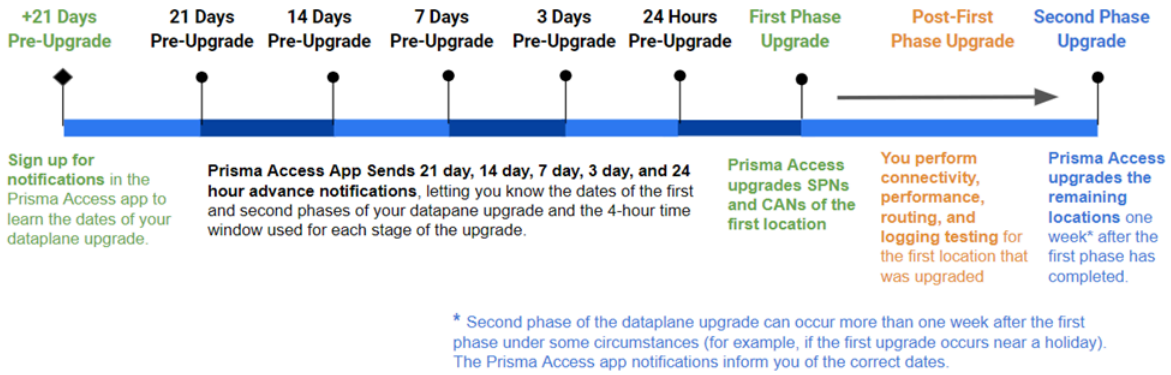
*Palo Alto Networks empfiehlt dringend, Standorte auszuwählen, die Ihrer gesamten Bereitstellung entsprechen. Wenn Sie beispielsweise über einen mobilen Benutzer, eine Dienstverbindung und eine Remote-Netzwerk-Bereitstellung verfügen, wählen Sie einen oder mehrere Standorte aus, die alle Bereitstellungsarten aufweisen.*

- Prisma Access führt die erste Phase des Upgrades an dem oder den ausgewählten Standorten innerhalb des für diese Standorte ausgewählten lokalen Zeitfensters durch.
- Wenn die ausgewählten Upgrade-Standorte eine beliebige Kombination aus mobilen Benutzern und GlobalProtect, mobilen Benutzern und explizitem Proxy, Dienstverbindungen oder Remote-Netzwerken aufweisen, wird ein Upgrade der Dataplane für jede Bereitstellung auf die erforderliche Dataplane-Version vorgenommen. Dies wird später in diesem Abschnitt beschrieben.
- Sobald das Upgrade am ersten Standort abgeschlossen ist, erhalten Sie über Strata Cloud Manager eine entsprechende E-Mail-Benachrichtigung. Palo Alto Networks empfiehlt Ihnen, den Dienst zu beobachten und zu prüfen, ob unmittelbar nach dem Dataplane-Upgrade neue Probleme auftreten.
- Für den unwahrscheinlichen Fall, dass tatsächlich ein neues Problem auftritt, melden Sie es bitte dem technischen Support von Palo Alto Networks.

  Das zuständige Team untersucht das Problem und ergreift Abhilfemaßnahmen, was auch das Zurücksetzen auf die vorherige Dataplane-Version bedeuten kann. Von der dort getroffenen Entscheidung werden Sie über den Fall des technischen Supports in Kenntnis gesetzt.
- Wenn keine neuen Probleme auftreten oder wenn ein neues Problem nicht mit dem Upgrade zusammenhängt, setzt Prisma Access das Dataplane-Upgrade am darauffolgenden Wochenende fort.
- Das Upgrade der verbleibenden Standorte erfolgt in dem Zeitfenster, das Sie für das erste Upgrade ausgewählt haben (Ortszeit).
- Nach Abschluss des Upgrades werden Sie per E-Mail benachrichtigt.
- Wenn nach dem Dataplane-Upgrade ein Plug-in-Upgrade erforderlich ist, empfiehlt Palo Alto Networks, das Plug-in nach Abschluss des Dataplane-Upgrades zu aktualisieren.

Die folgende Abbildung zeigt die für das Upgrade verwendete Zeitachse und enthält die Aufgaben, die Sie für das Dataplane-Upgrade ausführen müssen (in Grün), sowie die Schritte, die Prisma Access ausführt.

 ©2025 Palo Alto Networks, Inc.




Im folgenden Abschnitt finden Sie weitere Details zum Dataplane-Upgrade.

Nachdem Sie sich für Benachrichtigungen angemeldet haben, informiert Sie Prisma Access über die beiden für das Upgrade geplanten Wochenendtermine. Sie erhalten diese Benachrichtigungen 21 Tage, 14 Tage, 7 Tage, 3 Tage und 24 Stunden vor der ersten Upgrade-Phase. Das Upgrade verläuft in zwei Phasen:

- In Phase 1 wird das Upgrade der von Ihnen ausgewählten Standorte am ersten Wochenende innerhalb des von Ihnen angegebenen Zeitfensters aktualisiert. Sie werden per E-Mail benachrichtigt, sobald das Upgrade abgeschlossen ist. Wenn Sie keine Standorte für das Upgrade oder kein Zeitfenster ausgewählt haben, nimmt Prisma Access die Auswahl vor.

  *Palo Alto Networks versucht, das Upgrade der Standorte während des vierstündigen Zeitfensters durchzuführen, das Sie über Strata Cloud Manager auswählen. Doch auch wenn alles daran gesetzt wird, die Arbeiten in diesem Zeitfenster zu beenden, kann Palo Alto Networks nicht garantieren, dass das Upgrade des Standorts tatsächlich in dieser Zeit abgeschlossen wird. Sollte es während des Upgrades zu Problemen kommen, wird Palo Alto Networks versuchen, das Upgrade 24 Stunden nach dem ursprünglichen vierstündigen Fenster durchzuführen.*

  *Aus diesem Grund sollten Sie für jedes der beiden Wochenenden, an denen das Dataplane-Upgrade stattfindet, ein Zeitfenster von 72 Stunden für Änderungsanfragen einplanen, das am Freitag um 20:00 Uhr Ortszeit beginnt und am Montag um 20:00 Uhr Ortszeit endet. Nach Abschluss des Upgrades erhalten Sie eine entsprechende E-Mail.*

  Prisma Access nimmt während Phase 1 des Upgrades die folgenden Änderungen an Ihrer Bereitstellung vor.

| Bereitstellungstyp | Upgrade von |
|---|---|
| Mobile Benutzer – GlobalProtect | Prisma Access führt ein Upgrade für Folgendes durch:<br>• das GlobalProtect-Gateway, auch bekannt als *Mobile User Security Processing Node (MU-SPN)*, für den oder die von Ihnen angegebenen Standorte. |

 ©2025 Palo Alto Networks, Inc.

| Bereitstellungstyp | Upgrade von |
|---|---|
| | • das GlobalProtect-Portal, das dieser Region zugeordnet ist. |
| Mobile Benutzer – Expliziter Proxy | Prisma Access führt ein Upgrade der expliziten Proxy-Knoten für den oder die von Ihnen angegebenen expliziten Proxy-Standorte durch. |
| Remote-Netzwerk | Prisma Access führt ein Upgrade des Backup (HA)-Remote-Netzwerks, auch bekannt als *Remote Network Security Processing Node (RN-SPN)*, durch und macht das Backup-Remote-Netzwerk dann zum aktiven Knoten für den oder die von Ihnen angegebenen Standorte. Das Upgrade der Remote-Backup-Netzwerkverbindung erfolgt erst am zweiten Wochenende, wenn das Upgrade der aktiven und der Backup-Knoten für alle Standorte durchgeführt wird.<br><br>Wenn mehrere RN-SPNs am ausgewählten Standort vorhanden sind, erhalten alle Primärknoten ein Upgrade auf die neue Dataplane-Version. |
| Dienstverbindungen | Prisma Access führt ein Upgrade der Backup (HA)-Dienstverbindung, auch bekannt als Service Connection Corporate Access Node (SC-CAN), durch und macht die Backup-Dienstverbindung dann zum aktiven Knoten für den oder die von Ihnen angegebenen Standorte. Das Upgrade der Backup-Dienstverbindung erfolgt erst am zweiten Wochenende, wenn das Upgrade der aktiven und der Backup-Knoten für alle Standorte durchgeführt wird.<br><br>Wenn mehrere SC-CANs am ausgewählten Standort vorhanden sind, erhalten alle Backup-Knoten ein Upgrade auf die neue Dataplane-Version. |
| ZTNA-Connectors | ZTNA-Connectors erhalten kein Upgrade. Sie können jedoch bei Bedarf ein Upgrade der ZTNA-Connectors durchführen. |

Überwachen Sie zwischen dem ersten und dem zweiten Upgrade die ersten aktualisierten Standorte und führen Sie Konnektivitäts-, Leistungs-, Routing- und Protokollierungstests

 ©2025 Palo Alto Networks, Inc.

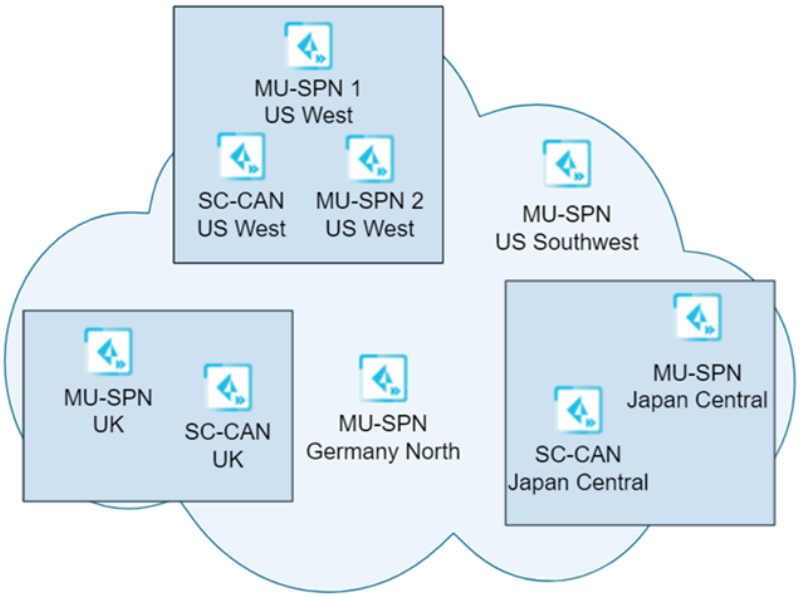
durch, um sicherzustellen, dass das Upgrade der Standorte erfolgreich war. Wenn nach dem Upgrade ein Service-Problem auftritt, öffnen Sie einen Supportfall mit dem technischen Support von Palo Alto Networks. Palo Alto Networks wird versuchen, das Problem zu beheben, indem es die Dataplane innerhalb von 24 Stunden auf eine frühere Version zurücksetzt.

- Sieben Tage nach dem Upgrade des ersten Standorts durch Prisma Access führt Prisma Access ein Upgrade Ihrer übrigen Standorte (Phase 2-Upgrade) in dem gleichen Zeitfenster durch, das Sie für die erste Phase ausgewählt haben. Auch hier erhalten Sie nach Abschluss des Upgrades eine Benachrichtigung per E-Mail.

*Das Upgrade-Zeitfenster kann länger sein. Fällt beispielsweise Phase 2 auf einen Nationalfeiertag in den USA, erfolgt sie 14 Tage nach Phase 1 (statt 7 Tage später). Die Benachrichtigungen, die Sie in Strata Cloud Manager erhalten, zeigen Ihnen die konkrete Zeitachse für das bevorstehende Dataplane-Upgrade.*

**Beispiel für ein Dataplane-Upgrade**

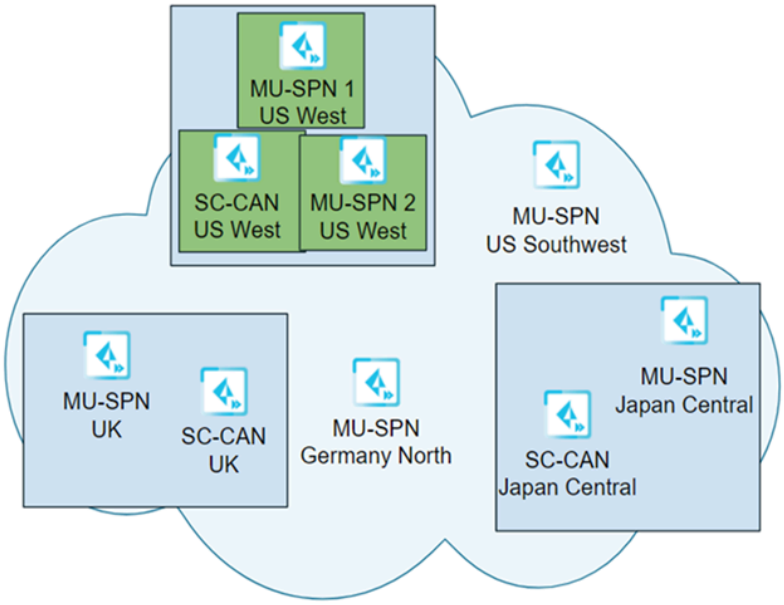
Das folgende Beispiel zeigt den Ablauf eines Dataplane-Upgrades für mobile Benutzer mit fünf Gateways (MU-SPNs) und drei SC-CANs. Der Standort im Westen der USA verfügt über zwei MU-SPNs als Ergebnis einer Autoskalierung (ein zusätzlicher MU-SPN wurde hinzugefügt, nachdem sich eine große Anzahl mobiler Benutzer an diesem Standort angemeldet hatte).




In diesem Beispiel haben Sie einen einzelnen Standort (Westen der USA) für das Upgrade ausgewählt und ein vierstündiges Upgrade-Zeitfenster von 8:00 Uhr bis 12:00 Uhr am Samstag für das Upgrade angefordert.

Am ersten Upgrade-Wochenende (Phase 1) findet das Upgrade für die SC-CANs und MU-SPNs am Standort im Westen der USA zwischen 8:00 Uhr und 12:00 Uhr Pacific Time am Samstag statt.

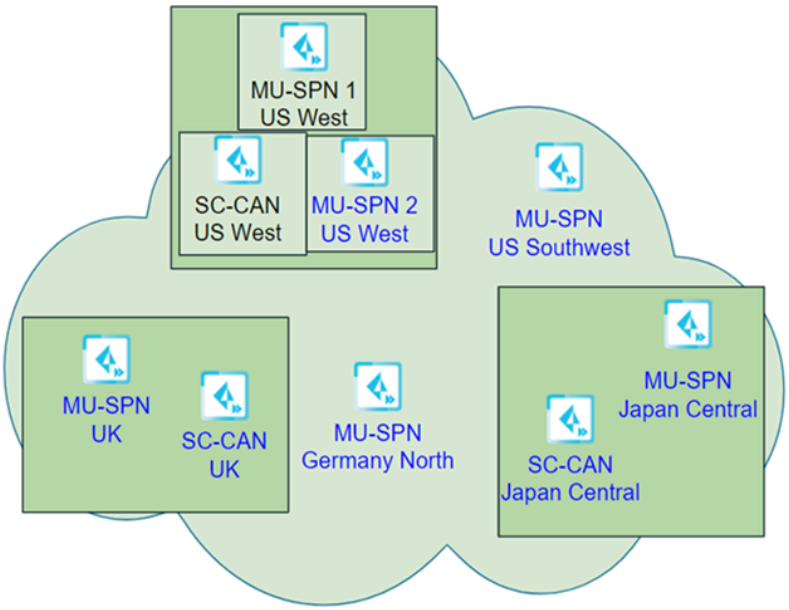
 ©2025 Palo Alto Networks, Inc.




Sieben Tage nach dem Upgrade des ersten Standorts nimmt Palo Alto Networks das Upgrade der restlichen Komponenten (Phase 2) vor und nutzt dafür dasselbe vierstündige Zeitfenster wie für die erste Phase des Upgrades (8:00 Uhr bis 12:00 Uhr am Samstag).

In diesem Beispiel verwendet Prisma Access beim Dataplane-Upgrade die folgenden Zeitzoneninformationen:

- Das Upgrade des MU-SPN und SC-CAN für Zentraljapan wird zur Ortszeit in Japan durchgeführt.
- Das Upgrade des MU-SPN und SC-CAN für das Vereinigte Königreich wird zur Ortszeit im Vereinigten Königreich durchgeführt.
- Das Upgrade des MU-SPN im Südwesten der USA wird zur Pacific Time durchgeführt.




 ©2025 Palo Alto Networks, Inc.

# Upgrade-Benachrichtigungen und Updates erhalten

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

Um über den Zeitplan für Ihr Dataplane-Upgrade auf dem Laufenden zu bleiben und Ihre Präferenzen für Upgrades auszuwählen, müssen Sie Strata Cloud Manager zum Abonnieren von Prisma Access-Benachrichtigungen verwenden. Strata Cloud Manager informiert Sie per E-Mail-Benachrichtigungen über die beiden Wochenenddaten, an denen Ihr Upgrade erfolgt. Sie wählen den Standort oder die Standorte, für die Sie zuerst ein Upgrade durchführen möchten, sowie das vierstündige Zeitfenster für das Upgrade aus.

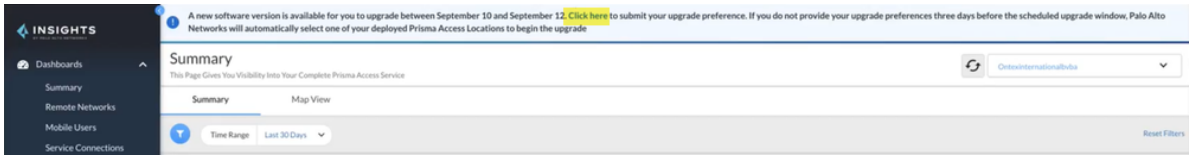
Nachdem das Upgrade gestartet wurde, können Sie seinen Status auch mit Strata Cloud Manager wie nachfolgend gezeigt überwachen.

**STEP 1 |** Anmelden für Benachrichtigungen in Strata Cloud Manager.

**STEP 2 |** Überprüfen Sie Ihre Benachrichtigungen, um über bevorstehende Dataplane-Upgrades informiert zu werden. Wählen Sie dann Ihre Präferenzen für Upgrades mit einer der folgenden Methoden aus.

- Wählen Sie **Workflows** > **Software-Upgrades** > **Prisma Access** > **Präferenzen für Upgrades**.

  Daraufhin wird das Upgrade-Dashboard angezeigt.




- Melden Sie sich bei Strata Cloud Manager an, zeigen Sie das Banner oben auf der Seite für Ihr geplantes Upgrade an und wählen Sie **Hier klicken** aus.
- Überprüfen Sie Ihre E-Mails auf Benachrichtigungen für Ihr geplantes Upgrade und klicken Sie auf den Hyperlink in der E-Mail.
- Wählen Sie **Workflows** > **Software-Upgrades** > **Prisma Access** > **Präferenzen für Upgrades**.

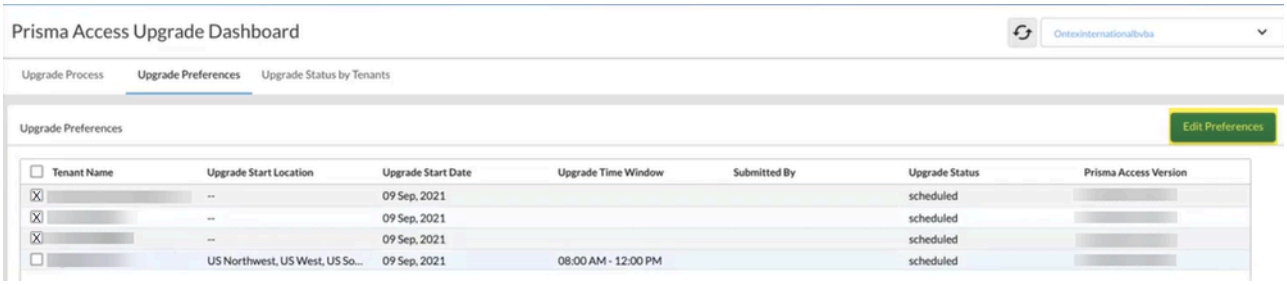
**STEP 3 |** (Optional) Lesen Sie die Informationen zum **Upgrade-Vorgang**, um mehr darüber zu erfahren.


©2025 Palo Alto Networks, Inc.

**STEP 4 |** Wählen Sie Ihre **Präferenzen für Upgrades** aus.

Wenn Sie eine Bereitstellung mit mehreren Mandanten haben, werden alle Mandanten in diesem Bereich angezeigt. Wenn Sie Ihre Präferenzen für Upgrades für Ihre Bereitstellung bereits ausgewählt haben, werden diese Auswahlen hier angezeigt.

1. Wählen Sie die Mandanten aus, für die Sie Präferenzen für Upgrades festlegen möchten, und wählen Sie dann die Option **Präferenzen bearbeiten** aus.




2. Wählen Sie unter **BevorzugtePrisma Access Standorte** die Standorte aus, an denen das Upgrade zuerst durchgeführt werden soll.

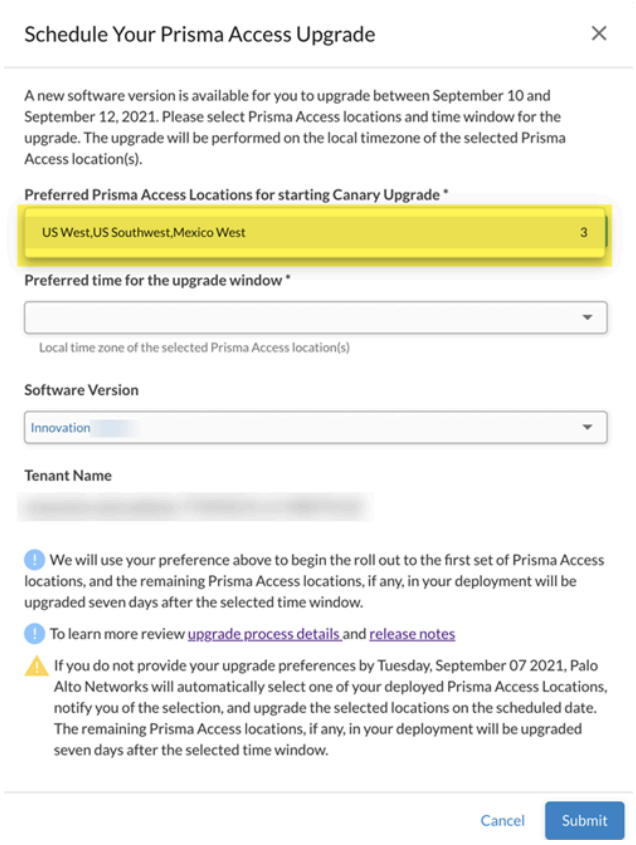
   *Palo Alto Networks empfiehlt dringend, Standorte auszuwählen, die Ihrer gesamten Bereitstellung entsprechen. Wenn Sie beispielsweise über einen mobilen Benutzer, eine Dienstverbindung und eine Remote-Netzwerk-Bereitstellung verfügen, wählen Sie einen oder mehrere Standorte aus, die alle Bereitstellungsarten aufweisen.*

   Wählen Sie aus den Optionen in der Dropdown-Liste aus.

   - Prisma Access zeigt nur die Speicherorte an, an denen Sie mobile Benutzer, Remote-Netzwerke, Dienstverbindungen oder eine beliebige Kombination davon bereitgestellt haben.
   - Die Gruppen in der Dropdown-Liste gehören zum selben Compute-Standort.

   Prisma Access benachrichtigt Sie per E-Mail, wenn das Upgrade an den Standorten durchgeführt wurde.

 ©2025 Palo Alto Networks, Inc.




Nach dem erfolgreichen Upgrade an den ersten Prisma Access-Standorten überwacht das Prisma Access-Team diese Standorte sieben Tage lang und führt anschließend das Upgrade an allen verbleibenden Prisma Access-Standorten durch. Wenn Sie einen einzelnen Standort oder nur sehr wenige Standorte auswählen, haben Sie die Möglichkeit, diese Standorte zu überwachen, bevor das Upgrade eine Woche später an den restlichen Standorten durchgeführt wird.

Wenn in der Dropdown-Liste keine Standorte angezeigt werden, haben Sie entweder mehrere Mandanten ausgewählt, für die keine gemeinsamen Standorte bereitgestellt


©2025 Palo Alto Networks, Inc.

wurden, oder Sie haben noch keine Standorte für die ausgewählten Mandanten integriert.

3. Wählen Sie aus der Liste der verfügbaren Optionen **Bevorzugtes Zeitfenster für das Upgrade** aus.

   Wählen Sie eine Option aus den folgenden Zeitfenstern für das Upgrade aus. Die Zeitfenster sind lokal auf den Standort oder die Standorte beschränkt, für den/die ein Upgrade durchgeführt wird, und umfassen jeweils vier Stunden:

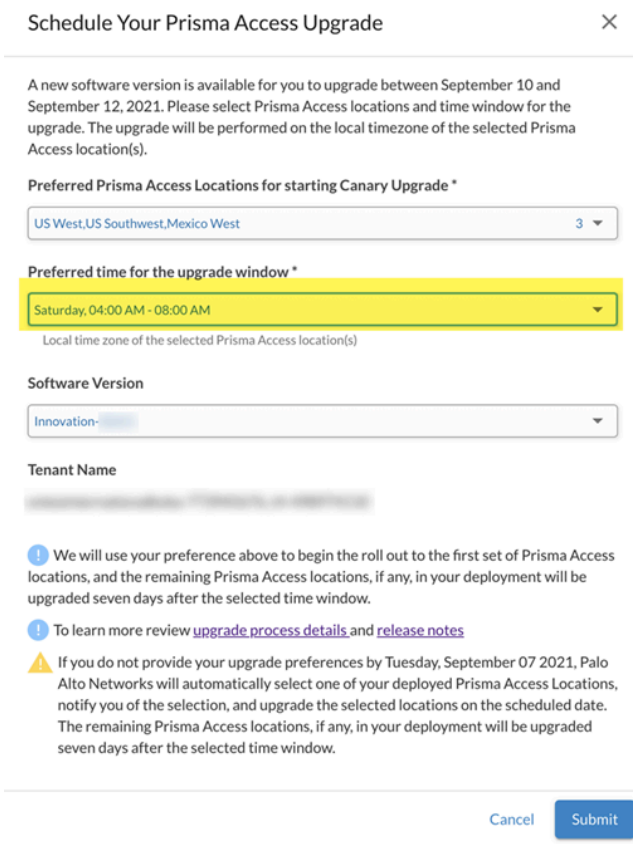
   - Freitag, 20:00 Uhr, bis Samstag, 00:00 Uhr
   - Samstag, 00:00 Uhr bis 4:00 Uhr
   - Samstag, 4:00 Uhr bis 8:00 Uhr
   - Samstag, 8:00 Uhr bis 12:00 Uhr
   - Samstag, 12:00 Uhr bis 16:00 Uhr
   - Samstag, 16:00 Uhr bis 20:00 Uhr

   Palo Alto Networks berücksichtigt Ihre Präferenz für das Rollout an den von Ihnen ausgewählten Prisma Access-Standorten. Die letzte Übermittlung, die sieben Tage vor dem geplanten Startdatum erfolgt ist, wird vom Dienst für das Upgrade ausgewählt. Sollten Sie Änderungen vornehmen, kann es bis zu 30 Minuten dauern, bis diese

 ©2025 Palo Alto Networks, Inc.

im Upgrade-Dashboard von Insights angezeigt werden. Sie werden per E-Mail benachrichtigt, wenn Prisma Access die Änderungen bearbeitet und abgeschlossen hat.

*Wenn Sie Ihre Präferenzen für Upgrades nicht sieben Tage vor dem geplanten Upgrade-Zeitfenster angeben, wählt Palo Alto Networks automatisch die erste Gruppe der Standorte in Ihrer Prisma Access-Bereitstellung aus, benachrichtigt Sie über diese Auswahl und führt das Upgrade an den ausgewählten Standorten zum geplanten Datum durch. Sieben Tage nach dem ausgewählten Zeitfenster wird das Upgrade an den restlichen Prisma Access-Standorten in Ihrer Bereitstellung, falls vorhanden, durchgeführt.*




4. Wenn mehrere Versionen verfügbar sind, wählen Sie die **Softwareversion** aus, auf die Sie ein Upgrade durchführen möchten.
5. Wählen Sie **Übermitteln** aus, um Ihre Änderungen zu senden.

 ©2025 Palo Alto Networks, Inc.

**STEP 5 |** Nachdem der Rollout begonnen hat, wählen Sie **Workflows** > **Software-Upgrades** > > **Prisma Access** > **Upgradestatus nach Mandanten** und sehen Sie sich den **Upgradestatus nach Standort** an.

Auf dieser Seite werden die folgenden Informationen für jeden Standort angezeigt, für den ein Upgrade durchgeführt wird:

- Name des Mandanten, für den ein Upgrade durchgeführt wird
- Start- und Enddatum des Upgrade-Vorgangs
- Dataplane-Version, auf die der Mandant aktualisiert wird
- Bevorzugtes Zeitfenster für das Upgrade
- Die ersten Standorte, für die ein Upgrade durchgeführt wird
- Datum, an dem das Upgrade für die verbleibenden Standorte durchgeführt wird

Darüber hinaus werden in einer Tabelle die Standorte, für die ein Upgrade durchgeführt wird, das Startdatum und Zeitfenster des Upgrades sowie die für das Upgrade verwendete Zeitzone angezeigt. Die Spalte **Upgradestatus** enthält folgende Informationen:

| Upgradestatus | Beschreibung |
|---|---|
| Geplant | Das Dataplane-Upgrade wurde geplant. |
| Gestartet | Das Upgrade wurde gestartet. |
| In Progress (In Bearbeitung) | Das Dataplane-Upgrade wird derzeit durchgeführt. |
| Erneuter Versuch | Das Dataplane-Upgrade wurde nicht erfolgreich abgeschlossen, aber Prisma Access ist weiterhin mit der älteren Dataplane-Version betriebsbereit. Prisma Access wird versuchen, das Upgrade zu wiederholen, bevor das Wartungsfenster für das Wochenende abläuft. |
| Erfolg | Das Upgrade wurde erfolgreich abgeschlossen. |

**STEP 6 |** Nachdem das Dataplane-Upgrade für die erste Gruppe von Standorten durchgeführt wurde, überwachen Sie diese Standorte und führen Sie Konnektivitäts-, Leistungs-, Routing- und Protokollierungstests durch, um sicherzustellen, dass das Upgrade erfolgreich abgeschlossen wurde.

**STEP 7 |** Wenn für die zweite Gruppe von Standorten ein Upgrade geplant ist, überwachen Sie diese Standorte und überprüfen Sie ihren Status, indem Sie **Workflows** > **Software-Upgrades** > **Prisma Access** > **Upgradestatus nach Mandanten**.

Prisma Access benachrichtigt Sie per E-Mail, nachdem das Dataplane-Upgrade abgeschlossen ist.

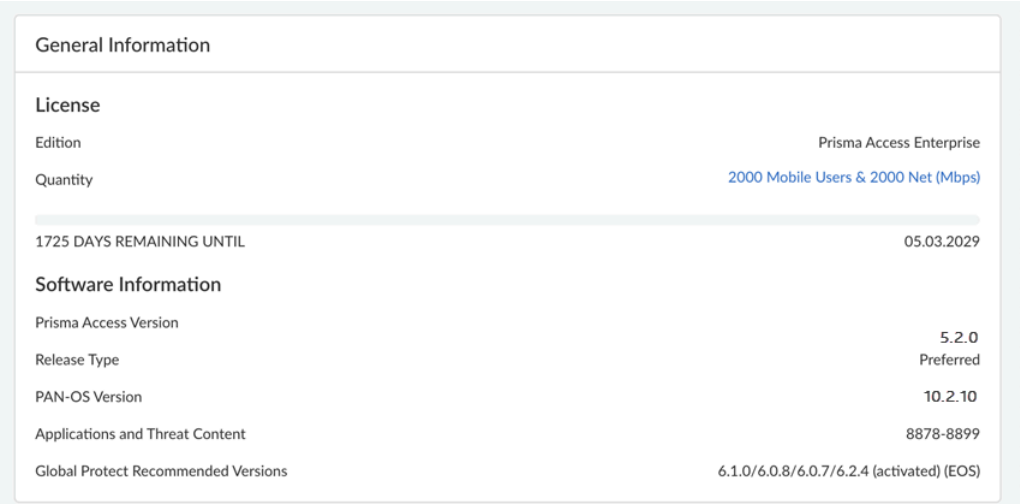
 ©2025 Palo Alto Networks, Inc.

# Anzeigen der Prisma Access-Softwareversionen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

## Prisma Access (Managed by Strata Cloud Manager)

Informationen zur Software- und Inhaltsversion finden Sie unter **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Übersicht** > **Allgemeine Informationen**. Wählen Sie den Konfigurationsumfang von **Prisma Access** aus.




Auf der Seite „Allgemeine Informationen“ finden Sie folgende Informationen:

| Bereich | Beschreibung |
|---|---|
| **Mandanten-ID** | Ermöglicht es Ihnen, Kontaktinformationen (Firmenname, Kontaktname, E-Mail-Adresse und Telefonnummer) zu teilen, damit Sie bezüglich Palo Alto Networks Service-Upgrades kontaktiert werden können.<br>Die ID des Mandanten. |
| **Mandantenname** | Der Name des Mandanten. |
| **Region** | Die Region des Mandanten. |
| **Prisma Access-Version** | Die aktuelle Version von Prisma Access. |


©2025 Palo Alto Networks, Inc.

| Bereich | Beschreibung |
|---|---|
| **PAN-OS-Version** | Die PAN-OS-Version, die auf Ihrer Datenebene ausgeführt wird. Die Datenebene ist die Komponente der Prisma Access-Infrastruktur, die die Überwachung des Datenverkehrs und die Durchsetzung von Richtlinien in Ihrem Netzwerk und im Datenverkehr der Benutzer ermöglicht. |
| **Veröffentlichungstyp** | Die Art des Release, das Sie ausführen (entweder Preferred oder Innovation).<br>Ein Innovation Release erfordert eine höhere PAN-OS-Datenebene als ein Preferred Release. |
| **Anwendungen und Bedrohungsinhalte** | Die von Ihnen ausgeführte Version von Anwendungen und Bedrohungsinhalten. |

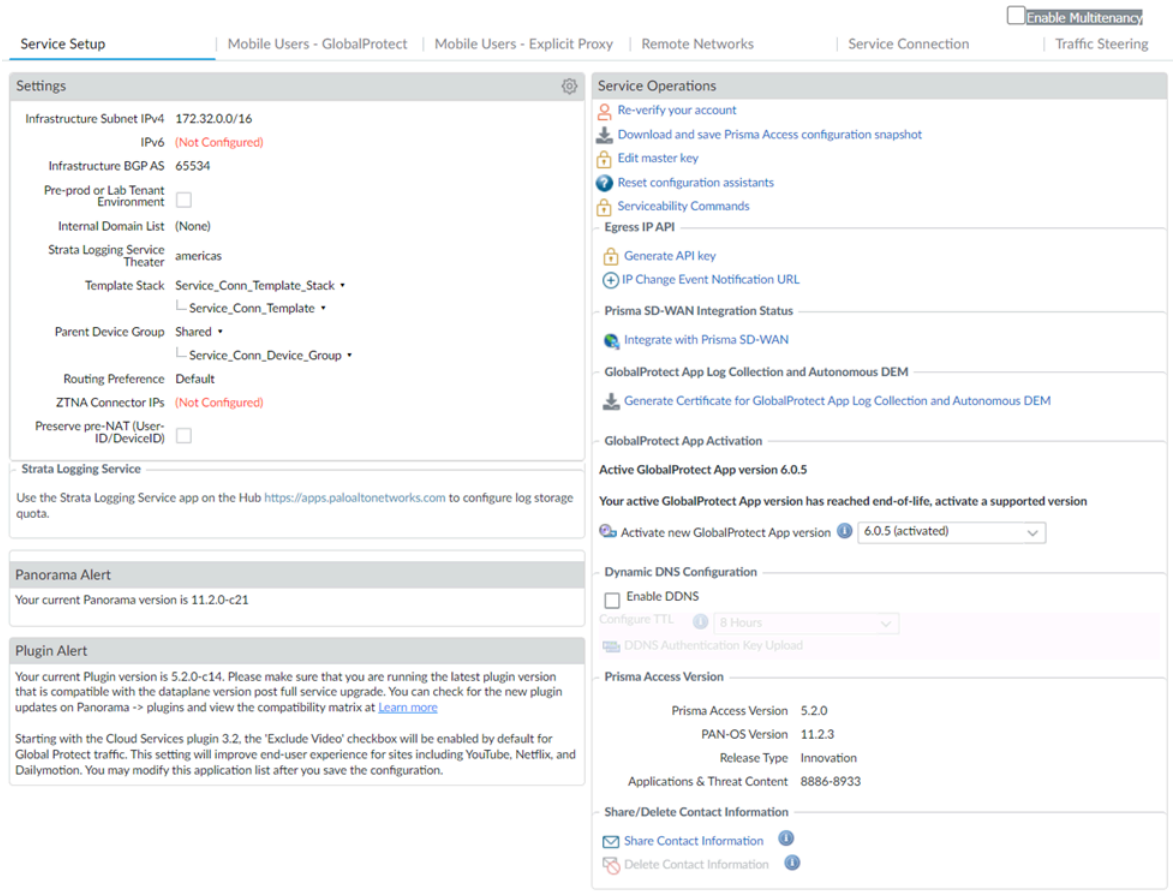
## Prisma Access (Managed by Panorama)

Prisma Access besteht aus von Ihnen verwalteten Komponenten wie Panorama und dem Cloud Services-Plug-in, aus von Prisma Access verwalteten Komponenten wie der Datenebenenversion und aus von Prisma Access verwalteten Komponenten, deren Version Sie jedoch steuern können (die auf dem Prisma Access-Portal gehostete GlobalProtect-Version). Auf der Seite „Diensteinrichtung“ (**Panorama** > **Cloud Services** > **Konfiguration** > **Diensteinrichtung**) wird der Status dieser Komponenten auf einer Seite angezeigt. Diese Seite enthält auch Benachrichtigungen, die Ihnen anzeigen, wann der Support für Ihre aktuelle Panorama-Version und die Plug-in-Versionen für die Verwendung mit Prisma Access eingestellt wird (End of Support, EoS). Palo Alto Networks informiert Sie vorab über EoS-Termine, um Ihrem Unternehmen ausreichend Zeit für die Planung des Upgrades zu geben.

*Alle Daten sind in koordinierter Weltzeit (UTC) angegeben.*

Auf der Seite „Diensteinrichtung“ finden Sie folgende Informationen:


©2025 Palo Alto Networks, Inc.




| Bereich | Beschreibung |
|---|---|
| **Benachrichtigung zu Panorama** | Zeigt die aktuelle Panorama-Version an, die Sie ausführen. Im Bereich **Upgrade-Anforderungen** finden Sie Informationen zu Panorama-Versionen, einschließlich der Daten, an denen die derzeit kompatiblen Panorama-Versionen das Ende des Supports (EoS) für die Verwaltung von Prisma Access erreichen. Planen Sie mithilfe dieser Informationen Ihr Panorama-Upgrade vor dem EoS-Datum. |
| **Plug-in-Benachrichtigung** | Zeigt das aktuelle Cloud Services-Plug-in an, das auf dem Panorama installiert ist, das Prisma Access verwaltet. Im Bereich **Upgrade-Anforderungen** finden Sie die Termine für die Veröffentlichung der nächsten Plug-in-Version, die Frist für das Upgrade auf das nächste Plug-in und das Datum, ab dem Sie mit der früheren Plug-in-Version keine Änderungen und Commits mehr vornehmen können. Planen Sie mithilfe dieser |

 ©2025 Palo Alto Networks, Inc.

| Bereich | Beschreibung |
| --- | --- |
| | Informationen das nächste Upgrade des Cloud Services-Plug-ins. |
| **Status Prisma SD-WAN-Integration** | Wählen Sie **In Prisma SD-WAN integrieren**, um den CloudBlade Thin Client zu aktivieren, der die Funktionalität zwischen Prisma SD-WAN und Prisma Access ermöglicht. |
| **GlobalProtect-App-Protokollerfassung und Autonomous DEM** | Wenn Sie die GlobalProtect-App-Protokollerfassung zur Fehlerbehebung aktiviert haben oder um Autonomous Digital Experience Management (ADEM) für Ihre mobilen Benutzer zu aktivieren, klicken Sie auf **Zertifikat für GlobalProtect-App-Protokollerfassung und Autonomous DEM generieren**, um ein Zertifikat zu erstellen. Mit diesem Zertifikat kann sich die GlobalProtect-App mit Strata Logging Service (zur Protokollerfassung) und mit Autonomous DEM authentifizieren. Wenn Sie das Zertifikat generieren, lädt Prisma Access das Zertifikat in Panorama (**Gerät** > **Zertifikatverwaltung** > **Zertifikate** > **Gerätezertifikate** unter der Vorlage **Mobile_User_Template** in **Freigegeben**) auch in die **Gerätezertifikate** herunter, die auf das mobile Gerät gepusht werden sollen. |
| **Aktivierung der GlobalProtect-App** | Zeigt die aktuell laufende (aktive) Version der GlobalProtect-App an, die mobile Benutzer über das Prisma Access-Portal herunterladen können, sowie die verfügbaren GlobalProtect-App-Versionen, auf die Sie upgraden können. |
| **Konfiguration für Dynamisches DNS** | Zeigt an, ob Sie Dynamisches DNS (DDNS) für die Fehlerbehebung von Remote-Netzwerken aktiviert haben. |
| **Prisma Access-Version** | Die aktuelle Version von Prisma Access. |
| **PAN-OS-Version** | Die PAN-OS-Version, die auf Ihrer Datenebene ausgeführt wird. Die Datenebene ist die Komponente der Prisma Access-Infrastruktur, die die Überwachung des Datenverkehrs und die Durchsetzung von Richtlinien in Ihrem Netzwerk und im Datenverkehr der Benutzer ermöglicht. |


©2025 Palo Alto Networks, Inc.

| Bereich | Beschreibung |
| --- | --- |
| **Veröffentlichungstyp** | Die Art des Release, das Sie ausführen (entweder Preferred oder Innovation).<br><br>Ein Innovation Release erfordert eine höhere PAN-OS-Datenebene als ein Preferred Release. |
| **Anwendungen und Bedrohungsinhalte** | Die von Ihnen ausgeführte Version von Anwendungen und Bedrohungsinhalten. |
| **Teilen/Löschen von Kontaktinformationen** | Ermöglicht Ihnen, Kontaktinformationen (Firmenname, Kontaktname, E-Mail-Adresse und Telefonnummer) zu teilen, damit Sie bezüglich Palo Alto Networks Service-Upgrades kontaktiert werden können.<br><br>Wenn Sie zuvor Kontaktinformationen eingegeben haben, können Sie die in diesem Bereich eingegebenen Informationen löschen.<br><br>Verwenden Sie im Kontaktinformationsbereich keine der folgenden Sonderzeichen:<br>• " (doppelte Anführungszeichen)<br>• ' (Apostroph)<br>• < (Kleiner-als-Zeichen)<br>• > (Größer-als-Zeichen)<br>• & (Et-Zeichen) |


©2025 Palo Alto Networks, Inc.

# Prisma Access-Einrichtung

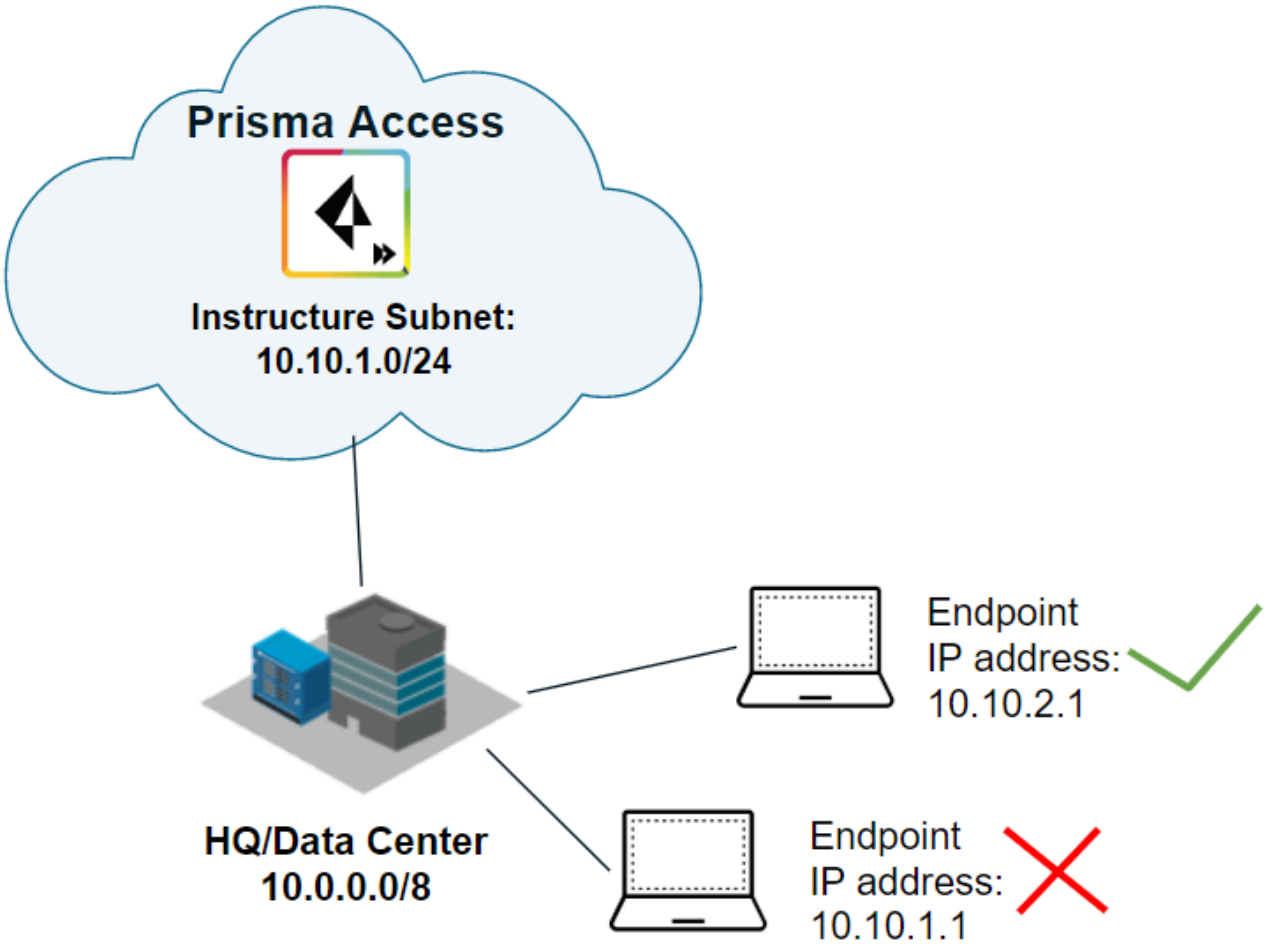
| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

Verwenden Sie folgende Empfehlungen und Anforderungen, wenn Sie ein Infrastruktursubnetz hinzufügen:

- Sie können Prisma Access ein Infrastruktursubnetz aus einem vorhandenen Supernetz im IP-Adresspool Ihres Unternehmens zuweisen, jedoch keine der IP-Adressen aus dem Infrastruktursubnetz für eine andere Verwendung in Ihrem bestehenden Netzwerk zuweisen.

  Das folgende Beispiel zeigt ein Prisma Access-Infrastruktursubnetz, 10.10.1.0/24, das Sie aus einem vorhandenen Supernetz, 10.0.0.0/8, zugewiesen haben. Nachdem Sie 10.10.1.0/24 als Infrastruktursubnetz zugewiesen haben, kann Ihr Unternehmen keine IP-Adressen aus diesem

Subnetz verwenden. Sie können z. B. einem Endpunkt 10.10.2.1 zuweisen, 10.10.1.1 ist jedoch nicht zulässig, da diese IP-Adresse Teil des Infrastruktursubnetzes ist.




- Wenn Sie ein neues Subnetz für das Infrastruktursubnetz erstellen, verwenden Sie ein Subnetz, das sich nicht mit anderen Ihrer intern verwendeten IP-Adressen überschneidet.
- (Empfohlen) Verwenden Sie ein RFC-1918-konformes Subnetz. Obwohl die Verwendung nicht RFC-1918-konformer (öffentlicher) IP-Adressen unterstützt wird, raten wir aufgrund möglicher Konflikte mit dem öffentlichen Internet-IP-Adressraum davon ab.
- Geben Sie keine Subnetze an, die sich mit den folgenden IP-Adressen und Subnetzen überschneiden, da Prisma Access diese IP-Adressen und Subnetze für den internen Gebrauch reserviert.
  - 169.254.0.0/16
  - 100.64.0.0/10
- Das Subnetz kann sich nicht mit den IP-Adresspools überschneiden, die Sie für die Adresspools verwenden möchten, die Sie für die Bereitstellung mobiler Benutzer zuweisen.
- Da die Dienstinfrastruktur sehr groß sein kann, müssen Sie mindestens ein /24-Subnetz festlegen.

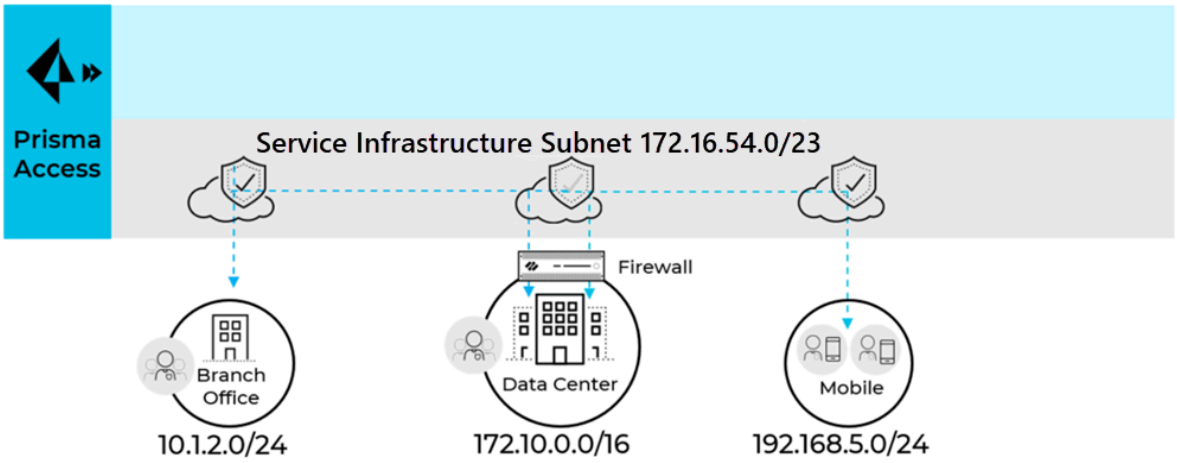
 ©2025 Palo Alto Networks, Inc.

# Prisma Access einrichten

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Bevor Sie Prisma Access zum Schutz Ihrer Remote-Netzwerke und mobilen Benutzer verwenden können, konfigurieren Sie ein Infrastruktursubnetz. Prisma Access verwendet IP-Adressen innerhalb dieses Subnetzes, um ein Netzwerk zwischen Ihren Remote-Netzwerkstandorten, mobilen Benutzern, der Zentrale und (falls zutreffend) Ihrem Rechenzentrum herzustellen. Prisma Access verwendet auch Dienstverbindungen, um von Ihrer Zentrale oder Ihrem Rechenzentrumsstandort aus auf interne Ressourcen zuzugreifen.

Dieses Subnetzwerk wird eine Erweiterung Ihres bestehenden Netzwerks sein. Daher sollte es sich nicht mit vorhandenen IP-Subnetzen in Ihrem Netzwerk überschneiden. Das folgende Beispiel zeigt ein 172.16.54.0/23-Subnetz, das für das Prisma Access-Infrastruktursubnetz verwendet wird.




Für kleine Netzwerke mit weniger als 50 Standorten und 2.500 mobilen Benutzern sollten Sie ein /24-Subnetz in Betracht ziehen. Bei mittelgroßen Netzwerken mit weniger als 100 Standorten und weniger als 5.000 mobilen Benutzern sollten Sie ein /23-Subnetz in Betracht ziehen. In den meisten Fällen ist ein /23-Subnetz ausreichend. Bei Netzwerken mit mehr als 100 Standorten oder 5.000 mobilen Benutzern oder wenn ein Wachstum des Netzwerks erwartet wird, kontaktieren Sie Palo Alto Networks, um zu bewerten, ob Sie ein größeres Subnetz benötigen.

Erfahren Sie, wie Sie Prisma Access einrichten.

- Strata Cloud Manager
- Panorama


©2025 Palo Alto Networks, Inc.

# Prisma Access (Strata Cloud Manager) einrichten

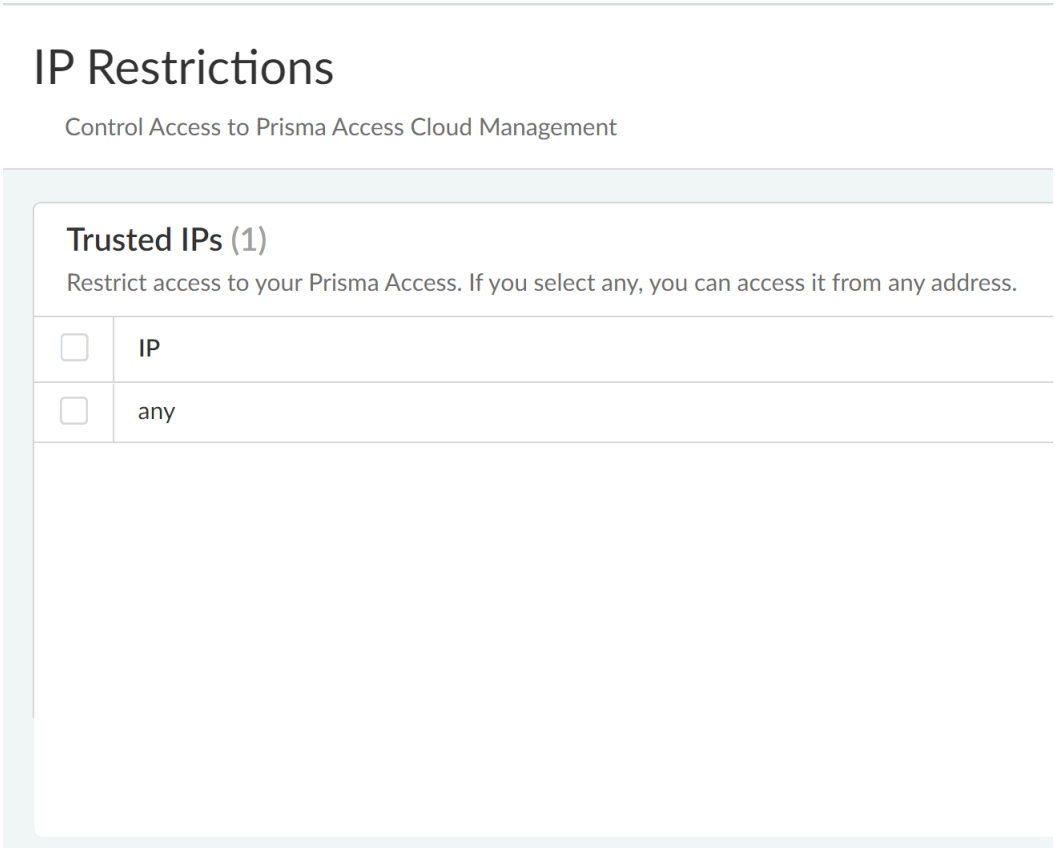
Der folgende Workflow bietet Ihnen eine Übersicht über die Schritte zur Installation und Konfiguration von Prisma Access.

**STEP 1 |** Starten Sie Strata Cloud Manager über den Hub.

1. Starten Sie einen Internet-Browser, um sich am Hub **anzumelden**.
2. Starten Sie Strata Cloud Manager.

**STEP 2 |** Geben Sie vertrauenswürdige IP-Adressen für Prisma Access (Managed by Strata Cloud Manager)-Administratoren an.

Nur Administratoren, die sich über diese Quell-IP-Adressen anmelden (und sich auch erfolgreich authentifizieren), können auf Prisma Access (Managed by Strata Cloud Manager) zugreifen. Die IP-Adressen müssen öffentliche Adressen sein. Standardmäßig werden keine vertrauenswürdigen Adressen erzwungen (die Liste ist auf „Beliebige“ festgelegt). Suchen Sie zu Beginn zunächst nach dem Menü **Einstellungen** im linken Navigationsbereich und klicken Sie auf **IP-Beschränkungen**.




**STEP 3 |** Ermitteln Sie Ihre Lizenzanforderungen. Anschließend können Sie die Prisma Access-Komponenten aktivieren und installieren.

**STEP 4 |** Aktivieren Sie die Dienstinfrastruktur und Dienstverbindungen, die die Kommunikation zwischen Prisma Access-Elementen ermöglichen.

 ©2025 Palo Alto Networks, Inc.

**STEP 5 |** Schützen Sie mobile Benutzer mit „GlobalProtect“ oder „Expliziter Proxy“, je nach Bedarf für Ihre Bereitstellung.

**STEP 6 |** Planen, erstellen und konfigurieren Sie Remote-Netzwerkverbindungen.

**STEP 7 |** (Optional) Ändern Sie die Authentifizierungsmethode von der lokalen Authentifizierung in die Authentifizierungsmethode Ihrer Organisation.

**STEP 8 |** (Optional) Sie müssen Protokolle weiterleiten (vom Strata Logging Service an einen externen Syslog-Empfänger).

**STEP 9 |** (Optional) Überprüfen Sie den Status von Prisma Access.

Sie können den Status aller Cloud-Dienste abrufen, einschließlich Prisma Access und Strata Logging Service, und einen historischen Datensatz zur Dienstverfügbarkeit abrufen, indem Sie über den Hub auf die App-Instanz zugreifen.

Sie können sich auch für E-Mail- oder Textbenachrichtigungen anmelden, damit Sie informiert werden, wann Infrastruktur-Updates geplant sind, wann Updates vorgenommen werden und wann Palo Alto Networks® einen Vorfall erstellt, aktualisiert oder behebt. Um sich für E-Mail-Updates anzumelden, wählen Sie im Abschnitt „Ressourcen“ auf der Startseite des Hubs die Option **Dienststatus** aus. Sie können dann bestimmte Updates und Vorfälle für Ihre Cloud-Dienste **abonnieren**.

## Prisma Access (Panorama) einrichten

Der folgende Workflow bietet Ihnen eine Übersicht über die Schritte zur Installation und Konfiguration von Prisma Access (Managed by Panorama) Access.

*Wenn Sie eine Bereitstellung einrichten, die mehrere Instanzen von Prisma Access auf einer einzigen Panorama-Instanz (Mehrmandantenfähigkeit) umfasst, lesen Sie den Abschnitt . Die meisten Organisationen müssen nicht mehrere Mandanten erstellen und verwalten.*

**STEP 1 |** Fügen Sie die folgenden URLs und Ports zu einer Zulassungsliste in allen Sicherheitsanwendungen hinzu, die Sie mit der Panorama-Appliance verwenden, von der Prisma Access verwaltet wird.

Wenn Ihre Panorama-Appliance außerdem einen verwendet (**Panorama** > **Einrichtung** > **Dienst** > **Proxy-Server**) oder wenn Sie SSL-Forward-Proxy mit Prisma Access verwenden, müssen

 ©2025 Palo Alto Networks, Inc.

Sie die folgenden URLs und Ports zu einer Zulassungsliste auf dem Proxy oder Proxyserver hinzufügen.

- api.gpcloudservice.com (für Prisma Access)
- api.paloaltonetworks.com (für Prisma Access)
- apitrusted.paloaltonetworks.com (für Prisma Access)
- Die für den Strata-Protokollierungsdienst erforderlichen FQDNs und Ports

> *Wenn sich zwischen der Panorama-Appliance und dem Internet eine Palo Alto Networks-Firewall der nächsten Generation befindet, müssen Sie der Firewall eine Sicherheitsrichtlinienregel hinzufügen, um den App-IDs **paloalto-logging-service** und **paloalto-shared-services** von der Panorama-Appliance aus den Zugriff auf das Internet zu ermöglichen. Diese Anwendungen ermöglichen SSL-gesicherte Kommunikation mit Prisma Access und mit dem Strata Logging Service, den die Panorama-Appliance zum Abfragen von Protokollen verwendet. Wenn sich die Panorama-Appliance hinter einer älteren Layer-4-Firewall befindet, lassen Sie den ausgehenden Datenverkehr der Ports 443 und 444 von der Panorama-Instanz zu, um diesen Datenverkehr von der Panorama-Instanz zu ermöglichen. Beachten Sie, dass das Öffnen von Layer-4-Ports anstelle der Verwendung von App-IDs von Palo Alto Networks weniger sicher ist und nicht empfohlen wird.*

**STEP 2 |** Fügen Sie die von Panorama verwendeten Ports den Zulassungslisten in Ihrem Netzwerk hinzu.

**STEP 3 |** Ermitteln Sie Ihre Lizenzanforderungen. Anschließend können Sie die Prisma Access-Komponenten aktivieren und installieren.

**STEP 4 |** Importieren Sie Ihre bestehende Panorama-Konfiguration in Prisma Access oder erstellen Sie neue Vorlagen und Gerätegruppen, um mit der Konfiguration von Prisma Access zu beginnen.

Um Ihre Konfigurationen – beispielsweise eine Sicherheitsrichtlinie, Authentifizierungsrichtlinie, Serverprofile, Sicherheitsprofile, Adressobjekte und Anwendungsgruppen – per Push an Prisma Access zu übertragen, müssen Sie entweder neue Vorlagen und Gerätegruppen mit den per Push an Prisma Access zu übertragenden Konfigurationseinstellungen erstellen oder Ihre vorhandenen Gerätegruppen und Vorlagen

 ©2025 Palo Alto Networks, Inc.

verwenden, indem Sie diese den Vorlagenstacks und Gerätegruppenhierarchien hinzufügen, die Prisma Access erstellt, wenn Sie den Dienst einbinden.

Prisma Access erstellt die folgenden Vorlagen und Gerätegruppen, abhängig davon, was Sie erworben haben (wenn Sie beispielsweise keine Lizenz für „Expliziter Proxy“ erwerben, werden Ihnen die Vorlagen und Gerätegruppen für „Expliziter Proxy“ nicht angezeigt):

- Vorlagen:
  - **Explicit_Proxy_Template**
  - **Explicit_Proxy_Template_Stack**
  - **Mobile_User_Template**
  - **Mobile_User_Template_Stack**
  - **Remote_Network_Template**
  - **Remote_Network_Template_Stack**
  - **Service_Conn_Template**
  - **Service_Conn_Template_Stack**
- Gerätegruppen:
  - **Explicit_Proxy_Device_Group**
  - **Mobile_User_Device_Group**
  - **Remote_Network_Device_Group**
  - **Service_Conn_Device_Group**

Die Konfiguration ist in Prisma Access vereinfacht, weil Sie keine Infrastruktureinstellungen wie Schnittstellen und Routing-Protokolle konfigurieren müssen. Diese Konfiguration ist automatisiert und wird von Panorama per Push in die Vorlagen und Gerätegruppen übertragen, die der Dienst automatisch erstellt. Sie können alle für den Dienst erforderlichen Infrastruktureinstellungen direkt vom Plug-in aus konfigurieren, z. B. die Einstellungen, die zum Erstellen von IPSec-VPN-Tunneln zu den IPSec-fähigen Geräten an Ihren Remote-Netzwerkstandorten erforderlich sind. Optional können Sie der Konfiguration Vorlagen und Gerätegruppenhierarchien hinzufügen, um die Einrichtung des Dienstes zu vereinfachen.

Zur Vereinfachung der Diensteinrichtung erstellen oder importieren Sie die erforderlichen Vorlagen und Gerätegruppen, bevor Sie mit der Einrichtung für die Verwendung von Prisma Access beginnen.

Beim Erstellen von Vorlagen und Gerätegruppen für Prisma Access, müssen Sie Prisma Access keine verwalteten Geräte zuweisen. Stattdessen fügen Sie diese den Vorlagenstacks und Gerätegruppenhierarchien hinzu, die von Prisma Access erstellt werden. Fügen Sie die von Prisma Access erstellten Vorlagen oder Gerätegruppen keinen anderen Vorlagenstapeln oder Gerätegruppen zu.

**STEP 5 |** Melden Sie sich für E-Mail-Benachrichtigungen mithilfe von Strata Cloud Manager an.

Prisma Access stellt Ihnen Benachrichtigungen zu diesem Dienst zur Verfügung, einschließlich aller Dataplane-Upgrades, und verwendet dazu Benachrichtigungen von dieser App.

 ©2025 Palo Alto Networks, Inc.

**STEP 6 |** Ändern Sie den Standard-Hauptschlüssel für Panorama und im Cloud Services-Plug-in.

Palo Alto Networks empfiehlt aus Sicherheitsgründen, den Hauptschlüssel in Panorama und im Cloud Services-Plug-in zu ändern – am besten monatlich.

Da die Panorama- und Prisma Access-Hauptschlüssel nicht synchronisiert werden, empfiehlt Palo Alto Networks, den Hauptschlüssel in Panorama nicht automatisch zu wechseln, ohne auch den Hauptschlüssel in Prisma Access zu synchronisieren. Sie können die Hauptschlüssel über die Panorama-Benutzeroberfläche oder mithilfe von API-Befehlen ändern.

*Merken Sie sich den von Ihnen verwendeten Hauptschlüssel gut, da Hauptschlüssel nicht wiederhergestellt werden können. Wenn ein Hauptschlüssel abläuft, müssen Sie den aktuellen Hauptschlüssel eingeben, um einen neuen Hauptschlüssel zu konfigurieren. Wenn Sie den aktuellen Hauptschlüssel nach Ablauf nicht bereitstellen können, müssen Sie Ihre Panorama-Appliance auf die Werkseinstellungen zurücksetzen.*

1. Ändern Sie den Hauptschlüssel in Panorama.
   1. Wählen Sie **Panorama** > **Hauptschlüssel und Diagnose** aus.

      Geben Sie keinen **aktuellen Hauptschlüssel** an.
   2. Konfigurieren Sie den **neuen Hauptschlüssel** und **bestätigen Sie den Hauptschlüssel**.

      Notieren Sie sich den von Ihnen konfigurierten Hauptschlüssel.
   3. Konfigurieren Sie die Lebensdauer des Hauptschlüssels und die Erinnerungszeit.
   4. Klicken Sie auf **OK**.
2. Ändern Sie den Hauptschlüssel für Prisma Access, indem Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Dienstvorgänge** > **Hauptschlüssel bearbeiten** auswählen und dann denselben Hauptschlüssel eingeben, den Sie für Panorama eingegeben haben.

Sie können den Hauptschlüssel auch mithilfe von API-Befehlen ändern. Hierzu sind zwei Schritte erforderlich: einer zum Ändern des Panorama-Hauptschlüssels und einer zum Ändern des Prisma Access-Hauptschlüssels. Verwenden Sie die folgenden API-Befehle, um den Hauptschlüssel zu ändern:

- Panorama: **XML-API** > **Betriebsbefehle** > **request** > **master-key**
- Prisma Access: **XML-API** > **Betriebsbefehle** > **request** > **plugins** > **cloud_services** > **prisma-access** > **sync**

**STEP 7 |** Aktivieren Sie die Dienstinfrastruktur und Dienstverbindungen, die die Kommunikation zwischen Prisma Access-Elementen ermöglichen.

1. Planen Sie die Aktivierung der Dienstinfrastruktur und Dienstverbindungen.
2. Aktivieren Sie die Dienstinfrastruktur.
3. Erstellen Sie eine Dienstverbindung, um den Zugriff auf Ihre Unternehmensressourcen zu ermöglichen.

   Wenn Sie keinen Zugriff auf Ihre Unternehmensressourcen benötigen, sollten Sie dennoch eine Dienstverbindung erstellen, um den Zugriff zwischen mobilen Benutzern und Remote-Netzwerken zu ermöglichen.

 ©2025 Palo Alto Networks, Inc.

**STEP 8 |** Prisma Access-Bereitstellungen für mobile Benutzer und sichere mobile Benutzer mit GlobalProtect oder Expliziter Proxy, je nach Bedarf für Ihre Bereitstellung.

So richten Sie GlobalProtect auf Prisma Access (Managed by Panorama) ein:

1. Konfigurieren Sie Zonen für mobile Benutzer, indem Sie in der Vorlage „Mobile_User_Template“ zwei Zonen erstellen (z. B. „Mobile-Benutzer“ und „Internet“) und die Zonen zuordnen. Sie sollten jede Zone, die nicht verbundenen Prisma Access-Benutzern oder der Zentrale bzw. den Zweigstellen entspricht, als „Nicht vertrauenswürdig“ festlegen.

   Legen Sie unter **Panorama** > **Cloud Services** > **Konfiguration** > **Mobile Benutzer** die Zone „Internet“ als „Nicht vertrauenswürdig“ und die Zone „Mobile-Users“ als „Vertrauenswürdig“ fest.
2. Konfigurieren Sie die Authentifizierung.

   Wir empfehlen die Verwendung der lokalen Authentifizierung als ersten Schritt, um zu überprüfen, ob der Dienst eingerichtet ist und Ihre Benutzer über Internetzugang verfügen. Später können Sie zur Verwendung Ihrer unternehmensspezifischen Authentifizierungsmethoden wechseln.
3. Konfigurieren Sie Sicherheitsrichtlinien für die Gerätegruppe.

   Zum Erstellen einer Sicherheitsrichtlinie, mit der der Datenverkehr zum Internet zugelassen werden kann, wählen Sie die Gerätegruppe „Mobile_User_Device_Group“ **Richtlinien** > **Sicherheit** > **Vor-Regeln** > **hinzuzufügen**. Beispiel: „Mobile-Users“ zu „Internet“.
4. Verwenden Sie „Commit und Push“, um Ihre Änderungen festzuschreiben und zu übertragen, damit die Nutzung des Dienstes gestartet werden kann.
5. Wählen Sie **Panorama** > **Cloud Services** > **Status** > **Überwachen** > **Mobile Benutzer** aus, um den **Status** anzuzeigen und zu überprüfen, ob Sie den FQDN des Portals mit einem Ping-Signal erreichen können.
6. Überprüfen Sie, ob Prisma Access den Internet-Verkehr für mobile Benutzer absichert, indem Sie die GlobalProtect-App herunterladen und installieren, sich mithilfe der App als mobiler Benutzer (lokaler Benutzer) mit dem Portal verbinden, einige Websites im Internet aufrufen und die Verkehrs-Protokolle auf Panorama überprüfen.

So sichern Sie mobile Benutzer mit einem expliziten Proxy:

1. Lesen Sie die Konfigurationsrichtlinien für den expliziten Proxy.
2. Konfigurieren Sie die SAML-Authentifizierung. Für „Expliziter Proxy“ ist eine SAML-Authentifizierung erforderlich.
3. Richten Sie die Gruppenzuordnung mithilfe der Cloud Identity Engine ein.
4. Schließen Sie die Konfiguration für den expliziten Proxy ab.
5. Führen Sie einen Commit aus und übertragen Sie die Änderung per Push.

 ©2025 Palo Alto Networks, Inc.

**STEP 9 |** Planen, erstellen und konfigurieren Sie Remote-Netzwerkverbindungen.

1. Fügen Sie Prisma Access ein oder mehrere Remote-Netzwerke hinzu.

   Sie können einen Standort einbinden und dann mithilfe der Massenimportfunktion weitere Standorte hinzufügen.
2. Erstellen Sie eine Sicherheitsrichtlinienregel, um beispielsweise den Datenverkehr von den Remote-Netzwerken zur Zentrale zuzulassen (z. B. „Vertrauenswürdig“ zu „Vertrauenswürdig“).
3. Überprüfen Sie die Konnektivität zwischen Dienstverbindung, Remote-Netzwerkverbindung und mobilen Benutzern.

**STEP 10 |** Führen Sie das API-Skript aus, das zum Abrufen von Prisma Access-IP-Adressen verwendet wird, und verwenden Sie das alte Skript zum Abrufen von IP-Adressen mobiler Benutzer.

Sie fügen diese Adressen einer Zulassungsliste im Netzwerk Ihrer Organisation hinzu, um den Inbound Access auf Ihr Unternehmensnetzwerk und Ihre Unternehmensanwendungen zu begrenzen.

**STEP 11 |** (Optional) Ändern Sie die Authentifizierungsmethode von der lokalen Authentifizierung in die Authentifizierungsmethode Ihrer Organisation.

1. Erstellen Sie ein Authentifizierungsprofil, das den Anforderungen Ihrer Organisation entspricht (SAML, LDAP, RADIUS usw.).
2. Wenn Ihre Organisation einen lokalen Authentifizierungsserver wie RADIUS oder Active Directory verwendet, fügen Sie die IP-Adressen, die Prisma Access als Quell-IP-Adresse für interne Anfragen (Abrufen der IP-Adressen für Prisma Access) verwendet, den Zulassungslisten in Ihrem Netzwerk hinzu, oder lassen Sie die IP-Adressen des gesamten Infrastruktursubnetzes zu (Prisma Access übernimmt die Loopback-IP-Adresse aus diesem Subnetz).
3. Aktualisieren Sie das Authentifizierungsprofil für das Prisma Access-Portal und -Gateway, um dieses neue Authentifizierungsprofil zu verwenden.

**STEP 12 |** (Optional) Sie müssen Protokolle weiterleiten (vom Strata Logging Service an einen externen Syslog-Empfänger).

 ©2025 Palo Alto Networks, Inc.

# Konfigurieren der Prisma Access-Serviceinfrastruktur

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz<br>❑ Erforderliche Mindestversion von Prisma Access für **Pre-Prod oder Lab-Mandant**: 3.0 Preferred |

Prisma Access verwendet dieses Subnetz, um den Netzwerk-Backbone für die Kommunikation zwischen Ihren Zweigstellennetzen, mobilen Benutzern und der Prisma Access-Sicherheitsinfrastruktur sowie für die Kommunikation mit den Netzwerken in Ihrer Zentrale und Ihrem Rechenzentrum zu erstellen, die Sie über Dienstverbindungen mit Prisma Access verbinden möchten.

Richten Sie das Subnetz der Dienstinfrastruktur ein, um die Kommunikation zwischen Ihren Remote-Netzwerkstandorten, mobilen Benutzern und der Zentrale oder den Rechenzentren zu ermöglichen, mit denen Sie eine Verbindung zu Prisma Access über Dienstverbindungen herstellen möchten. Prisma Access verwendet dieses Subnetz, um das Netzwerk-Backbone für die Kommunikation zwischen Ihren Zweigstellennetzwerken, mobilen Benutzern und der Prisma Access-Sicherheitsinfrastruktur sowie mit den Netzwerken Ihrer Zentrale und Ihres Rechenzentrums zu erstellen, mit denen Sie über Dienstverbindungen eine Verbindung zu Prisma Access herstellen möchten.

- Strata Cloud Manager
- Panorama

## Konfigurieren Sie die Prisma Access-Dienstinfrastruktur (Strata Cloud Manager)

Verwenden Sie folgende Empfehlungen und Anforderungen, wenn Sie ein Infrastruktursubnetz für Prisma Access hinzufügen:

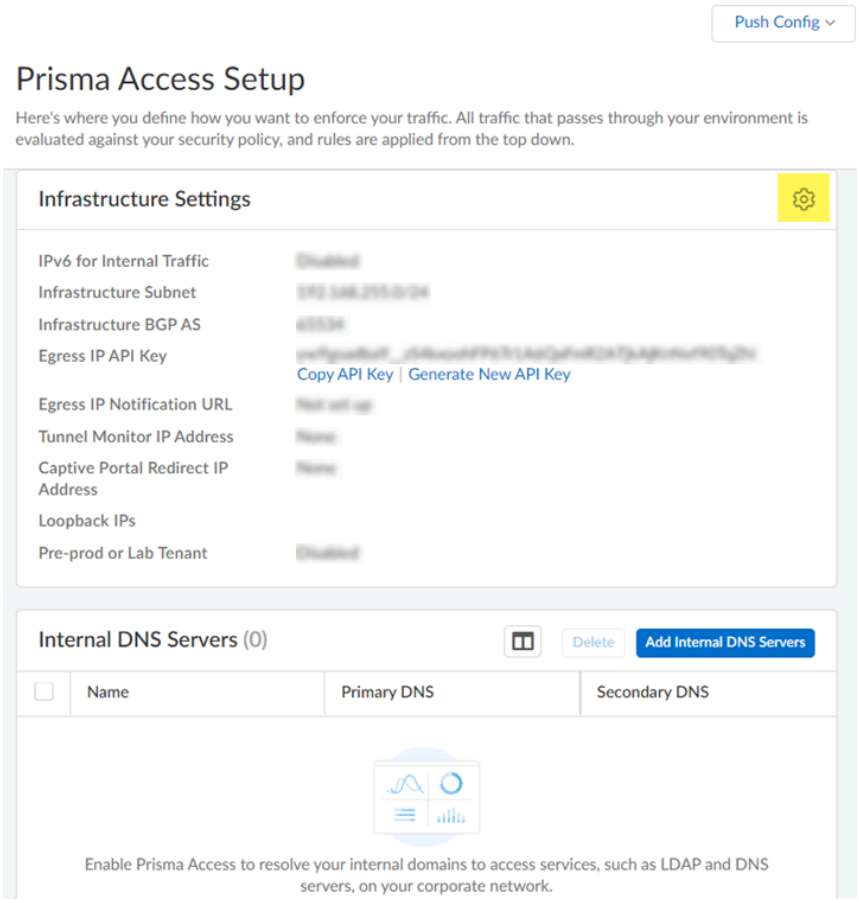
- ❑ Verwenden Sie ein RFC-1918-konformes Subnetz. Obwohl die Verwendung nicht RFC-1918-konformer (öffentlicher) IP-Adressen unterstützt wird, wird aufgrund möglicher Konflikte mit dem öffentlichen Internet-IP-Adressraum davon abgeraten.
- ❑ Geben Sie keine Subnetze an, die sich mit 169.254.0.0/16 und dem Subnetzbereich 100.64.0.0/10 überschneiden, da Prisma Access diese IP-Adressen und Subnetze für den internen Gebrauch reserviert.
- ❑ Dieses Subnetz ist eine Erweiterung Ihres bestehenden Netzwerks und darf sich daher nicht mit IP-Subnetzen überschneiden, die Sie innerhalb Ihres Unternehmensnetzwerks verwenden, oder mit den IP-Adresspools, die Sie Prisma Access für Benutzer oder Prisma Access für Netzwerke zuweisen.
- ❑ Da die Dienstinfrastruktur eine große Anzahl von IP-Adressen benötigt, müssen Sie ein /24-Subnetz zuweisen (z. B. 172.16.55.0/24).

 ©2025 Palo Alto Networks, Inc.

- ❑ Wenn Sie dynamisches Routing für Ihre Remote-Netzwerke oder Dienstverbindungen verwenden, müssen Sie auch eine RFC-6996-konforme private BGP-AS-Nummer konfigurieren.

**STEP 1 |** Starten Sie Prisma Access.

**STEP 2 |** Gehen Sie zu **Workflows** > **Einrichtung Prisma Access** > **Prisma Access** > **Infrastruktureinstellungen** und klicken Sie auf das Zahnrad, um die Einstellungen zu bearbeiten.




**STEP 3 |** Geben Sie ein **Infrastruktursubnetz** ein, mit dem Prisma Access die Kommunikation zwischen Remote-Netzwerkstandorten, mobilen Benutzern und dem Hauptsitz oder den Rechenzentren ermöglicht, die Sie über Dienstverbindungen mit Prisma Access verbinden möchten.

*Verwenden Sie ein RFC-1918-konformes Subnetz als Infrastruktursubnetz. Obwohl die Verwendung nicht RFC-1918-konformer (öffentlicher) IP-Adressen unterstützt wird, wird aufgrund möglicher Konflikte mit dem öffentlichen Internet-IP-Adressraum davon abgeraten.*

**STEP 4 |** (Optional) Wenn Sie IPv6 konfigurieren, wählen Sie **IPv6 für internen Datenverkehr** und anschließend ein IPv6-Subnetz aus.

 ©2025 Palo Alto Networks, Inc.

**STEP 5 |** Geben Sie die **Infrastruktur-BGP-AS** ein, den Sie innerhalb der Prisma Access-Infrastruktur verwenden möchten.

Wenn Sie dynamisches Routing aktivieren möchten, damit Prisma Access Routen zu Ressourcen in Ihren Remote-Netzwerken und an den Standorten Ihrer Zentrale oder Ihres Rechenzentrums dynamisch erkennen kann, müssen Sie das Border Gateway Protocol (BGP) verwenden. Die **Infrastruktur-BGP-AS** ist die Nummer des autonomen Systems (AS), die die Routen identifiziert, über die BGP Datenverkehr senden kann. Wenn Sie keine AS-Nummer angeben, verwendet Prisma Access die Standard-AS-Nummer (65534).

Wenn Sie Ihre eigene AS-Nummer angeben möchten, müssen Sie eine RFC-6996-konforme private AS-Nummer verwenden. Zulässige Formate sind die 4-Byte-Notation AS Plain [64512-65534], [4200000000-4294967294] oder AS Dot [0.64512-0.65534], [64086.59904-65535.65534].

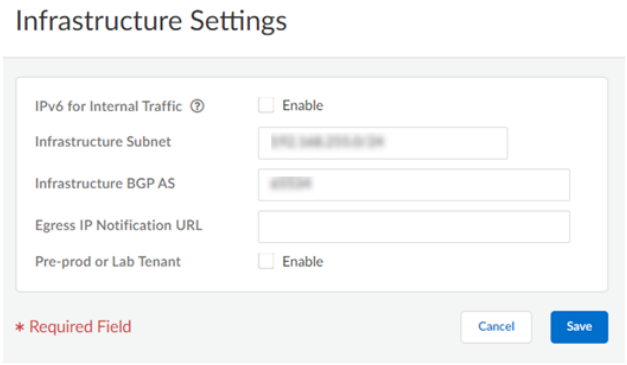
**STEP 6 |** Wenn Sie Ihren Benutzern den Zugriff auf Anwendungen basierend auf der Quell-IP-Adresse ermöglichen, müssen Sie die Liste der IP-Adressen abrufen, die vom Datenverkehr von Prisma Access als Quelladresse verwendet wird, damit Sie sie in Ihren Richtlinien für den Anwendungszugriff zulassen können.

**Kopieren Sie** den **API-Schlüssel für die Ausgangs-IP**, um die Verwendung der API der Ausgangs-IP-Adresse von Prisma Access zu aktivieren. Da sich die von Prisma Access verwendeten IP-Adressen regelmäßig ändern – zum Beispiel, wenn Sie einen neuen Standort hinzufügen, wenn Prisma Access Ressourcen an einem vorhandenen Standort skalieren muss oder wenn es ein Infrastruktur-Upgrade gibt –, müssen Sie wissen, wann sich die IP-Adressen ändern, damit Sie Ihre Richtlinienregeln aktualisieren oder diese Aktualisierungen automatisieren können, indem Sie eine **Benachrichtigungs-URL für die Ausgangs-IP** definieren. Weitere Informationen finden Sie unter IP-Adressen für Prisma Access abrufen.

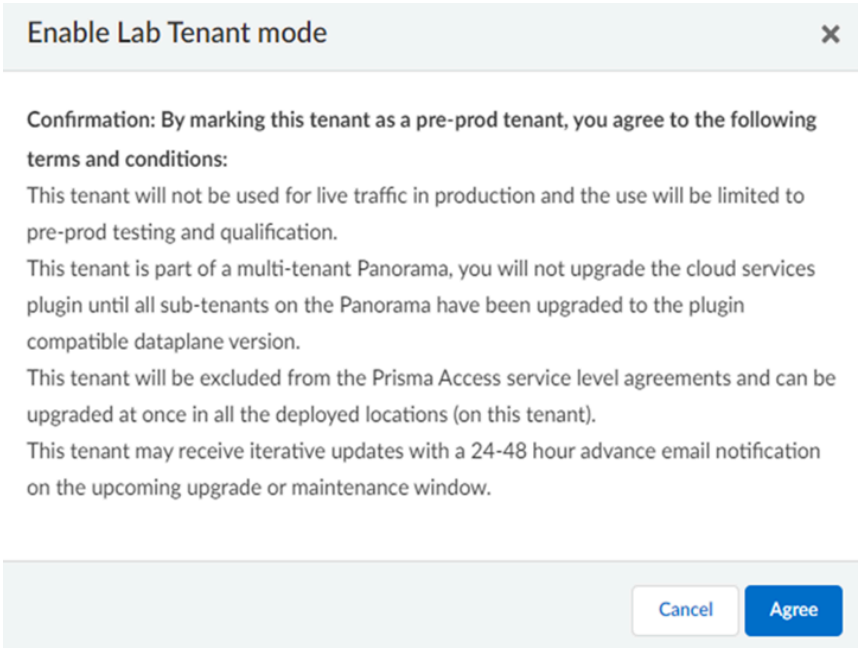
 ©2025 Palo Alto Networks, Inc.

**STEP 7 |** (Optional) Aktivieren Sie den Mandanten als Pre-Prod- oder Lab-Mandanten.

1. **Aktivieren Sie** den Mandanten als **Pre-Prod- oder Lab-Mandanten**.




2. **Stimmen Sie zu**, um den Vorgang zu bestätigen.




   Wenn Sie einen Mandanten als Pre-Prod- oder Lab-Mandanten aktivieren, können Sie Upgrades nur für diesen Mandanten planen, bevor Sie ein Upgrade für andere Produktionsmandanten durchführen. Der Mandant erhält 24 bis 48 Stunden vor einem bevorstehenden Upgrade entsprechende Benachrichtigungen. Wenn Sie den Mandanten als Pre-Prod- oder Lab-Mandanten deaktivieren, gilt er als Produktionsmandant.

3. **Save (Speichern)** Sie Ihre Änderungen.

**STEP 8 |** Wenn Sie Prisma Access zum Auflösen Ihrer internen Domänen aktivieren möchten, **fügen Sie interne DNS-Server hinzu**.

Wenn Sie Dienstverbindungen konfigurieren möchten, um den Zugriff auf Ressourcen in Ihrem Unternehmensnetzwerk zu ermöglichen und Prisma Access Ihre internen Domänen auflösen muss, müssen Sie die Liste der internen Domänen definieren. DNS-Abfragen für Domänen in der Liste mit internen Domänen werden an Ihre lokalen DNS-Server gesendet,

 ©2025 Palo Alto Networks, Inc.

um sicherzustellen, dass Ressourcen für Remote-Netzwerkbenutzer und mobile Benutzer von Prisma Access verfügbar sind.

1. Geben Sie den **primären DNS-Server** und den **sekundären DNS-Server** ein, die Prisma Access zur Auflösung der internen Domainnamen verwenden soll.
2. Sie sollten die internen **Domänennamen hinzufügen**, die Prisma Access auflösen soll.

   Sie können einen Platzhalter (*) vor den Domänen in der Domänenliste verwenden, z. B. *.acme.local oder *.acme.com.

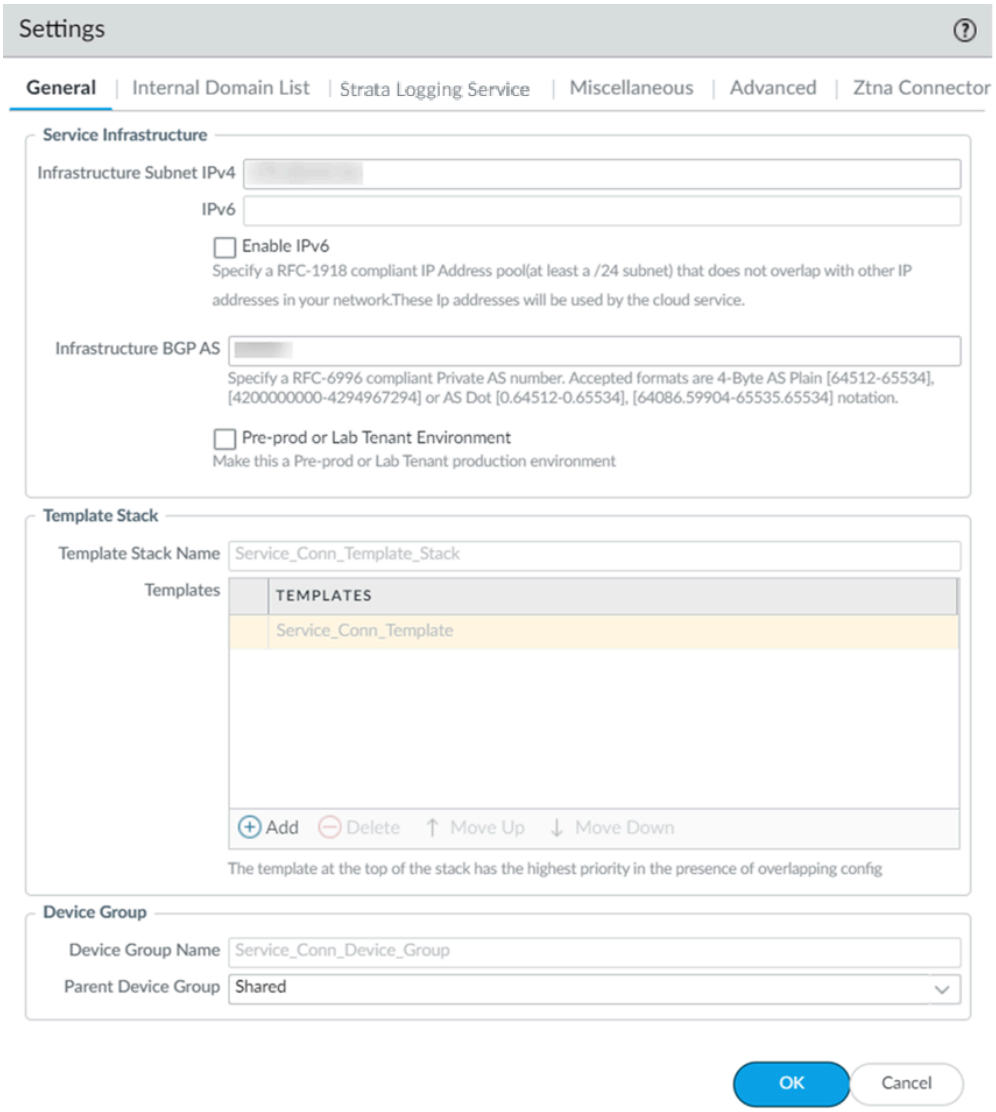
**STEP 9 |** Drücken Sie **Konfiguration übertragen**, um die Einstellungen Ihrer Dienstinfrastruktur in Prisma Access zu speichern.

## Konfigurieren Sie die Prisma Access-Dienstinfrastruktur (Panorama)

Bevor Sie mit der Einrichtung von Prisma Access zum Schutz Ihrer Remote-Netzwerke und/oder mobilen Benutzer beginnen können, müssen Sie ein Infrastruktursubnetz konfigurieren, mit dem Prisma Access das Netzwerk-Backbone für die Kommunikation zwischen Ihren Dienstverbindungen, Remote-Netzwerken und mobilen Benutzern sowie mit den Unternehmensnetzwerken erstellt, die Sie über Dienstverbindungen mit Prisma Access verbinden möchten. Da für die Einrichtung der Infrastruktur eine große Anzahl von IP-Adressen erforderlich ist, müssen Sie mindestens ein /24-Subnetz (z. B. 172.16.55.0/24) verwenden. Achten Sie darauf, alle Richtlinien und Anforderungen zu befolgen.

 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Diensteinrichtung** aus und klicken Sie auf das Zahnradsymbol, um die Einstellungen zu bearbeiten.




**STEP 2 |** Geben Sie auf der Registerkarte **Allgemein** ein **Infrastruktursubnetz** an, das die Anforderungen erfüllt, z. B. 172.16.55.0/24.

**STEP 3 |** (Optional) Wenn Sie IPv6 konfigurieren, wählen Sie **IPv6 für internen Datenverkehr** und anschließend ein IPv6-Subnetz aus.

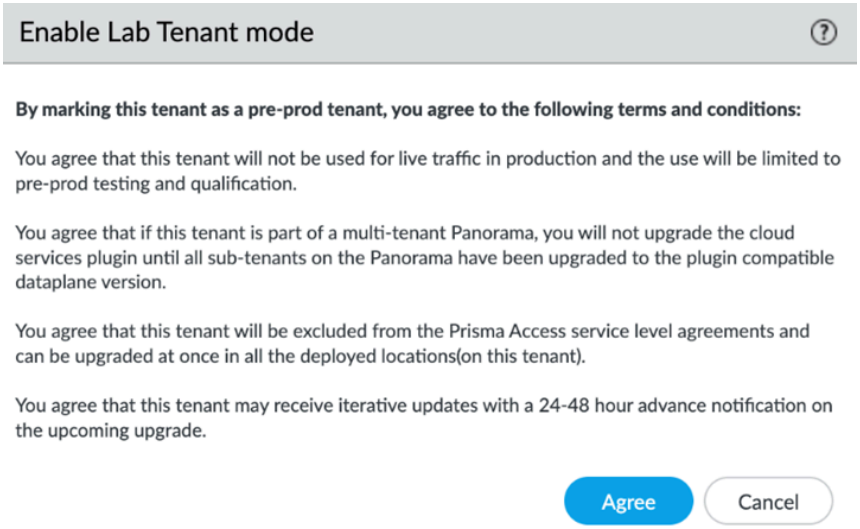
**STEP 4 |** (Optional) Wenn Sie Prisma Access die Verwendung von BGP zur dynamischen Erkennung von Routen zu Ressourcen in Ihren Remote-Netzwerken und Standorten in der Zentrale/im Rechenzentrum ermöglichen möchten, geben Sie in der Prisma Access-Infrastruktur die gewünschte **Infrastruktur-BGP-AS** ein.

Wenn Sie keine AS-Nummer angeben, wird die Standard-AS-Nummer 65534 verwendet.


©2025 Palo Alto Networks, Inc.

**STEP 5 |** (Optional) Aktivieren Sie einen Mandanten als **Pre-Prod- oder Lab-Mandanten**.

Wenn Sie einen Mandanten als Pre-Prod- oder Lab-Mandanten aktivieren, können Sie Upgrades nur für diesen Mandanten planen, bevor Sie ein Upgrade für andere Produktionsmandanten durchführen. Der Mandant erhält 24 bis 48 Stunden vor einem bevorstehenden Upgrade entsprechende Benachrichtigungen.




Wenn Sie den Mandanten als Pre-Prod- oder Lab-Mandanten deaktivieren, gilt er als Produktionsmandant.

*Prisma Access for Clean Pipe unterstützt diese Funktionalität nicht.*

**STEP 6 |** (Optional) Aktivieren Sie Prisma Access, um Ihre internen Domänen mithilfe Ihrer Unternehmens-DNS-Server aufzulösen.

Verwenden Sie diesen Schritt, wenn Prisma Access in der Lage sein soll, Ihre internen Domänen aufzulösen, um in Ihrem Unternehmensnetzwerk über Dienstverbindungen auf Dienste wie LDAP-Server zuzugreifen. Wenn Sie beispielsweise möchten, dass ein DNS-Lookup für Ihre Unternehmensdomäne ausschließlich an den Unternehmens-DNS-Server geht, geben Sie hier die Unternehmensdomäne und die Unternehmens-DNS-Server an.

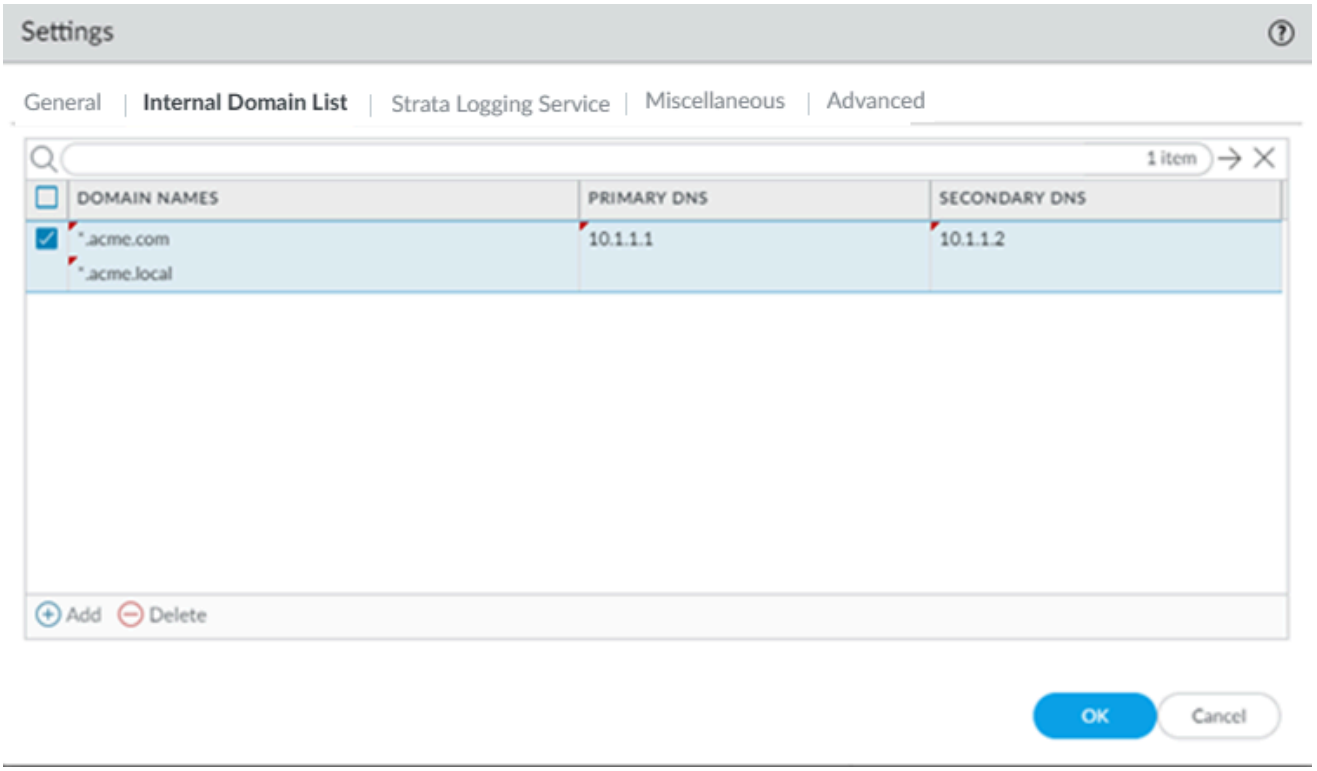
1. Wählen Sie die Registerkarte **Liste interner Domänen** aus.

 ©2025 Palo Alto Networks, Inc.

2. **Fügen Sie** die **Domänennamen**, die **primären DNS**- und **sekundären DNS**-Server hinzu, die Prisma Access zur Auflösung Ihrer internen Domänennamen verwenden soll.

   Sie können einen Platzhalter (*) vor den Domänen in der Domänenliste verwenden, z. B. *.acme.local oder *.acme.com.

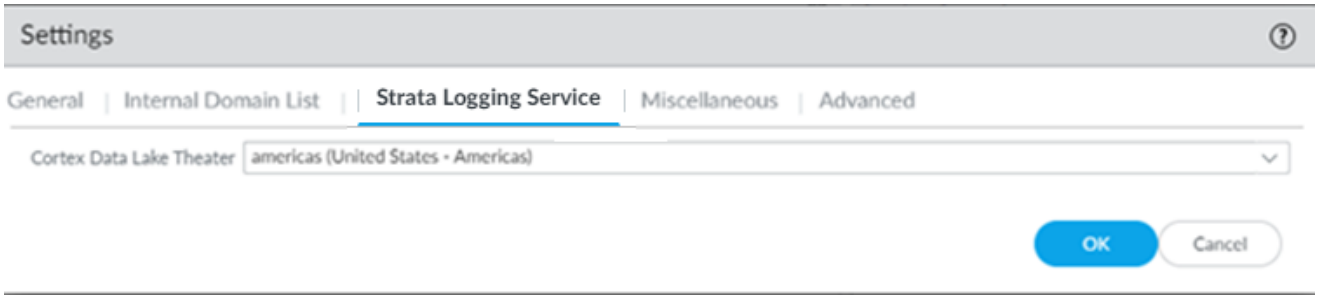
   *Geben Sie keine 127.0.0.1-Adresse ein, da dies zu internen Routingproblemen mit Prisma Access führen kann.*




 ©2025 Palo Alto Networks, Inc.

**STEP 7 |** Aktivieren Sie Strata Logging Service.

1. Wählen Sie die Registerkarte **Strata-Protokollierungsdienst** aus.
2. Wählen Sie einen **Schauplatz für den Strata-Protokollierungsdienst** aus und klicken Sie auf **OK**.




3. Konfigurieren Sie die Gerätegruppen, mit denen Sie Einstellungen per Push an Prisma Access mit einem Protokollweiterleitungsprofil übertragen, das die gewünschten Protokolltypen an den **Panorama/Strata-Protokollierungsdienst** weiterleitet.

   Das Cloud Services-Plug-in fügt nach einer Neuinstallation oder beim Entfernen von Prisma Access-Nichtvorlagen aus einem Prisma Access-Vorlagenstapel automatisch folgende Protokolleinstellungen (**Gerät** > **Protokolleinstellungen**) hinzu:

   - Protokolleinstellungen für Systemprotokolle (**system-gpcs-default**), Benutzer-ID-Protokolle (**userid-gpcs-default**), HIP-Übereinstimmungsprotokolle (**hipmatch-gpcs-default**) und GlobalProtect-Protokolle (**gp-prismaaccess-default**) werden der Mobile_User_Template hinzugefügt.
   - Protokolleinstellungen für Systemprotokolle (**system-gpcs-default**), Benutzer-ID-Protokolle (**userid-gpcs-default**) und GlobalProtect-Protokolle (**gp-prismaaccess-default**) werden der Remote_Network_Template hinzugefügt.
   - Protokolleinstellungen für Systemprotokolle (**system-gpcs-default**) und GlobalProtect-Protokolle (**gp-prismaaccess-default**) werden der Service_Conn_Template hinzugefügt.

   Diese Protokolleinstellungskonfigurationen leiten automatisch System-, Benutzer-ID-, HIP-Übereinstimmungs- und GlobalProtect-Protokolle an Strata Logging Service weiter.

   Führen Sie folgende Schritte aus, um Änderungen an den Protokolleinstellungen anzuwenden. Führen Sie anschließend einen Commit für die Änderungen aus und übertragen Sie diese per Push:

   - Wenn Sie die Protokolleinstellung auf die Vorlage für mobile Benutzer anwenden möchten, wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Mobile Benutzer** aus und klicken Sie auf das Zahnradsymbol, um die Einstellungen zu bearbeiten. Klicken Sie anschließend auf „OK“.
   - Wenn Sie die Protokolleinstellung auf die Vorlage für Remote-Netzwerke anwenden möchten, wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Remote-Netzwerke** aus und klicken Sie auf das Zahnradsymbol, um die Einstellungen zu bearbeiten. Klicken Sie anschließend auf „OK“.
   - Wenn Sie die Protokolleinstellung auf die Vorlage für Dienstverbindungen anwenden möchten, wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** >

 ©2025 Palo Alto Networks, Inc.

**Diensteinrichtung** aus und klicken Sie auf das Zahnradsymbol, um die Einstellungen zu bearbeiten. Klicken Sie anschließend auf „OK“.

Wie Sie die Protokollweiterleitung für andere Protokolltypen aktivieren, hängt vom Typ ab. Verwenden Sie für Protokolle, die basierend auf einer Richtlinienübereinstimmung generiert werden, ein Protokollweiterleitungsprofil. Weitere Informationen finden Sie im Handbuch Erste Schritte mit dem Strata-Protokollierungsdienst.

**STEP 8 |** (Optional) Konfigurieren Sie unter **Verschiedenes** weitere Einstellungen.

1. (Optional) Fügen Sie das Ending-Token für URLs in externen dynamischen Listen (EDLs) oder benutzerdefinierten URL-Kategorien hinzu, indem Sie **Ending-Token an die URLs in der URL-Filterkonfiguration anhängen** auswählen.

   Wenn Sie URLs in EDLs oder benutzerdefinierten URL-Kategorien verwenden und keinen Schrägstrich (**/**) an die URL anhängen, ist es möglich, mehr URLs zuzulassen, als Sie beabsichtigt haben. Wenn Sie beispielsweise **`example.com`** als übereinstimmende URL anstelle von **`example.com/`** eingeben, würde dies auch example.com.website.info oder example.com.br entsprechen.

   Durch die Auswahl von **Ending-Token an die URLs in der URL-Filterkonfiguration anhängen** legt Prisma Access ein Ending-Token für URLs in EDLs oder benutzerdefinierten URL-Kategorien fest, sodass Prisma Access bei der Eingabe von **`example.com`** diese URL wie example.com/ behandelt und nur mit dieser URL übereinstimmt.
2. (Optional) **Deaktivieren Sie die Datenverkehrsprotokollierung bei Dienstverbindungen**, um die Protokollierung in den Dienstverbindungen für Ihre Prisma Access-Bereitstellung zu deaktivieren.

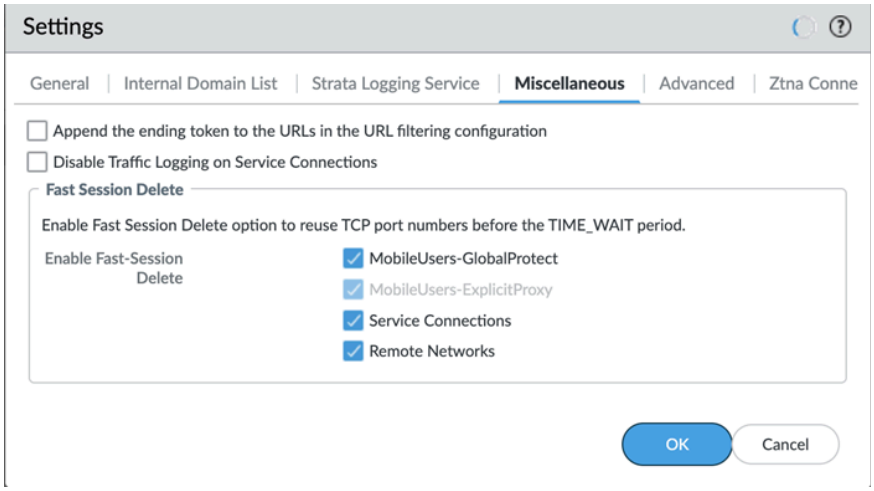
   Wenn die Mehrzahl der von den Dienstverbindungen protokollierten Datenverkehrsflüsse asymmetrisch ist, ist möglicherweise die Deaktivierung der Dienstverbindungsprotokollierung erforderlich, um den Verbrauch von Strata Logging Service-Protokollspeicher zu reduzieren. Wenn Ihre Bereitstellung keine asymmetrischen Flüsse über die Dienstverbindungen aufweist, müssen Sie die Protokollierung nicht deaktivieren.
3. (Optional) Aktivieren Sie die Kontrollkästchen für **Mobile Benutzer – GlobalProtect**, **Dienstverbindungen** oder **Remote-Netzwerke**, um die schnelle Sitzungslöschung für die

 ©2025 Palo Alto Networks, Inc.

Bereitstellungen „Remote-Netzwerke“, „Dienstverbindungen“ oder „Mobile Benutzer – GlobalProtect“ zu aktivieren.

Die schnelle Sitzungslöschung ermöglicht Prisma Access die Wiederverwendung von TCP-Portnummern vor Ablauf des TCP TIME_WAIT-Zeitraums und kann für SSL-entschlüsselte Sitzungen nützlich sein, die möglicherweise kurzlebig sind.

Für Bereitstellungen des Typs „Mobile Benutzer – Expliziter Proxy“ ist die schnelle Sitzungslöschung ein wichtiger Teil der Funktionalität und kann nicht deaktiviert werden.




**STEP 9 |** (Optional) Konfigurieren Sie **erweiterte** Einstellungen (Routingeinstellungen, Optionen für einen symmetrischen Netzwerkpfad für Dienstverbindungen und HIP-Umverteilung).

1. Geben Sie die **Routingpräferenz** für Dienstverbindungen an.

   Sie können Netzwerkeinstellungen festlegen, um den Dienstverbindungsverkehr entweder über das Netzwerk Ihres Unternehmens oder über das Prisma Access-Netzwerk zu verarbeiten.

   - **Standard** – Prisma Access verwendet Standard-Routing im internen Netzwerk.
   - **Hot-Potato-Routing** – Prisma Access leitet Dienstverbindungsverkehr so schnell wie möglich an das WAN Ihres Unternehmens weiter.

   *Die Änderung der Routingmethode für die Prisma Access-Dienstverbindung erfordert ein gründliches Verständnis der Topologie und der Routinggeräte Ihres Unternehmens sowie ein Verständnis der Funktionsweise des Prisma Access-Routings. Wir empfehlen Ihnen, Routing für Dienstverbindungsverkehr sorgfältig zu lesen, bevor Sie die Routingmethode standardmäßig ändern.*

2. Konfigurieren Sie das **Backbone-Routing** für die Dienstverbindungen.

   Standardmäßig erfordert das Prisma Access-Backbone, dass Sie einen symmetrischen Netzwerkpfad für den Datenverkehr haben, der über eine Dienstverbindung vom Standort des Rechenzentrums oder der Zentrale zurückkehrt. Wenn Sie ECMP oder einen anderen Lastausgleichsmechanismus für Dienstverbindungen von Ihrem CPE

 ©2025 Palo Alto Networks, Inc.

verwenden möchten, können Sie asymmetrische Flüsse über das Prisma Access-Backbone aktivieren.

- Wählen Sie **no-asymmetry-routing** aus, um symmetrische Flüsse über das Backbone von Dienstverbindungen anzufordern.
- Wählen Sie **asymmetric-routing-only** aus, damit Prisma Access asymmetrische Flüsse über das Backbone der Dienstverbindung verwenden kann.
- Wenn Sie mehrere Dienstverbindungen zu einem Standort haben, können Sie den Lastausgleich in Ihrer Prisma Access-Bereitstellung nutzen, indem Sie **asymmetric-routing-with-load-share** (Standardeinstellung) auswählen. Der Lastausgleich erfolgt jedoch auf Best-Effort-Basis und schlägt fehl, wenn eine der Dienstverbindungen ausfällt.

3. HIP-Informationen mit Prisma Access weitergeben zur Weitergabe von HIP-Informationen von mobilen Benutzern und Benutzern in Remote-Netzwerken.
4. Kompromittierte Geräte in einer GlobalProtect-Bereitstellung von Prisma Access identifizieren und unter Quarantäne stellen, damit Prisma Access kompromittierte Geräte identifiziert und unter Quarantäne stellt, die mit der GlobalProtect-App verbunden sind.
5. **Statische Routen zurückziehen, wenn der IPSec-Tunnel für Dienstverbindungen oder Remote-Netzwerke ausgefallen ist**, wenn Prisma Access statische Routen entfernen soll, wenn ein Tunnel ohne Backup-Tunnel ausgefallen ist.

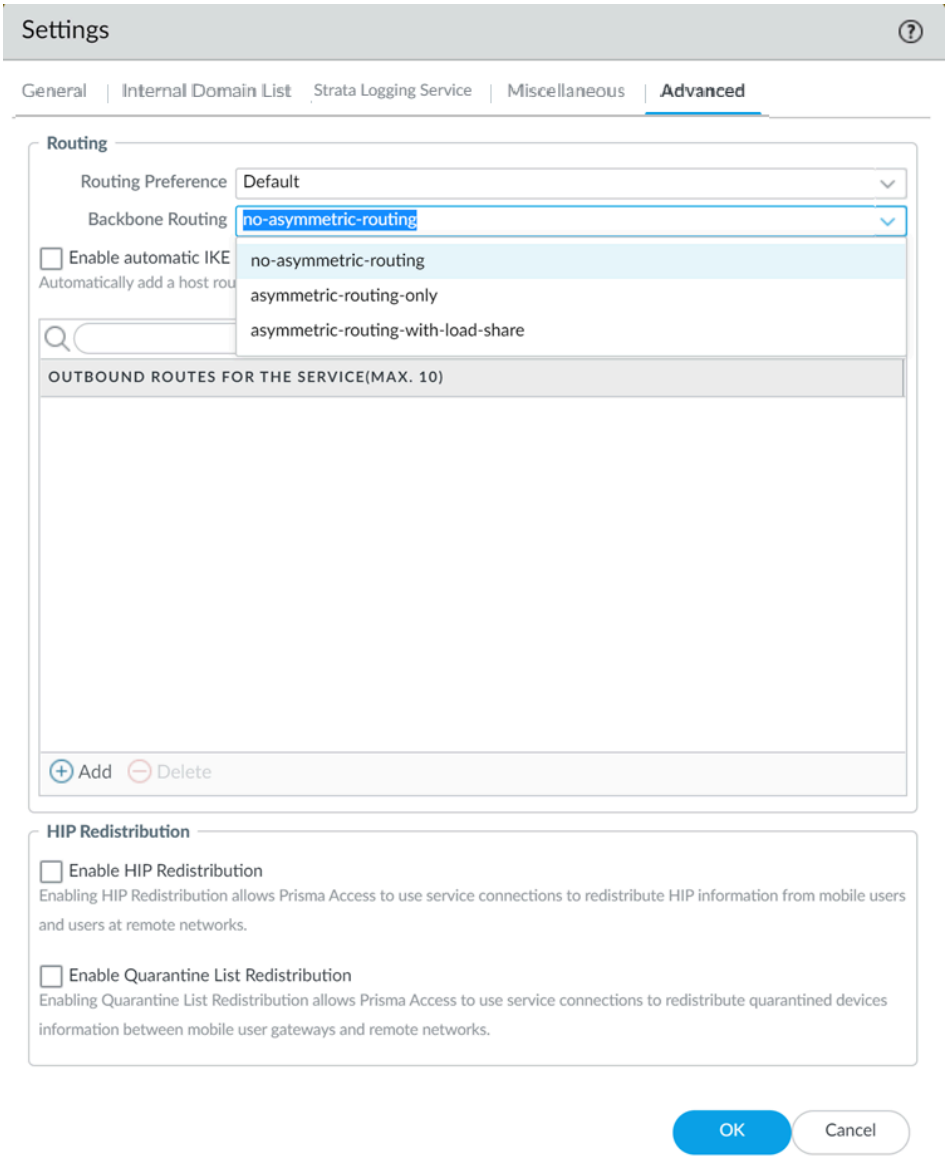
   Prisma Access entfernt die Route in folgenden Situationen:

   - Der primäre Tunnel fällt aus und es gibt keinen sekundären Tunnel.
   - Wenn ein primärer und ein sekundärer Tunnel konfiguriert ist, aber beide ausfallen.

   Sie können diese Änderung nicht anwenden, wenn die Tunnelüberwachung nicht aktiviert ist.
6. (Optional) Wenn Sie IPSec-Tunnelpakete für Remote-Netzwerke und Dienstverbindungen über das Internet an die statischen IKE-Gateways weiterleiten möchten, **aktivieren Sie automatische IKE-Peer-Hostrouten für Remote-Netzwerke und Dienstverbindungen**.
7. (Optional) **Geben Sie Outboundrouten für den Dienst (Max 10) an**, indem Sie bis zu 10 Präfixe hinzufügen, für die Prisma Access statische Routen für alle

 ©2025 Palo Alto Networks, Inc.

Dienstverbindungen und Remote-Netzwerkverbindungen hinzufügt. Prisma Access leitet den Datenverkehr dann über das Internet zu diesen Präfixen weiter.



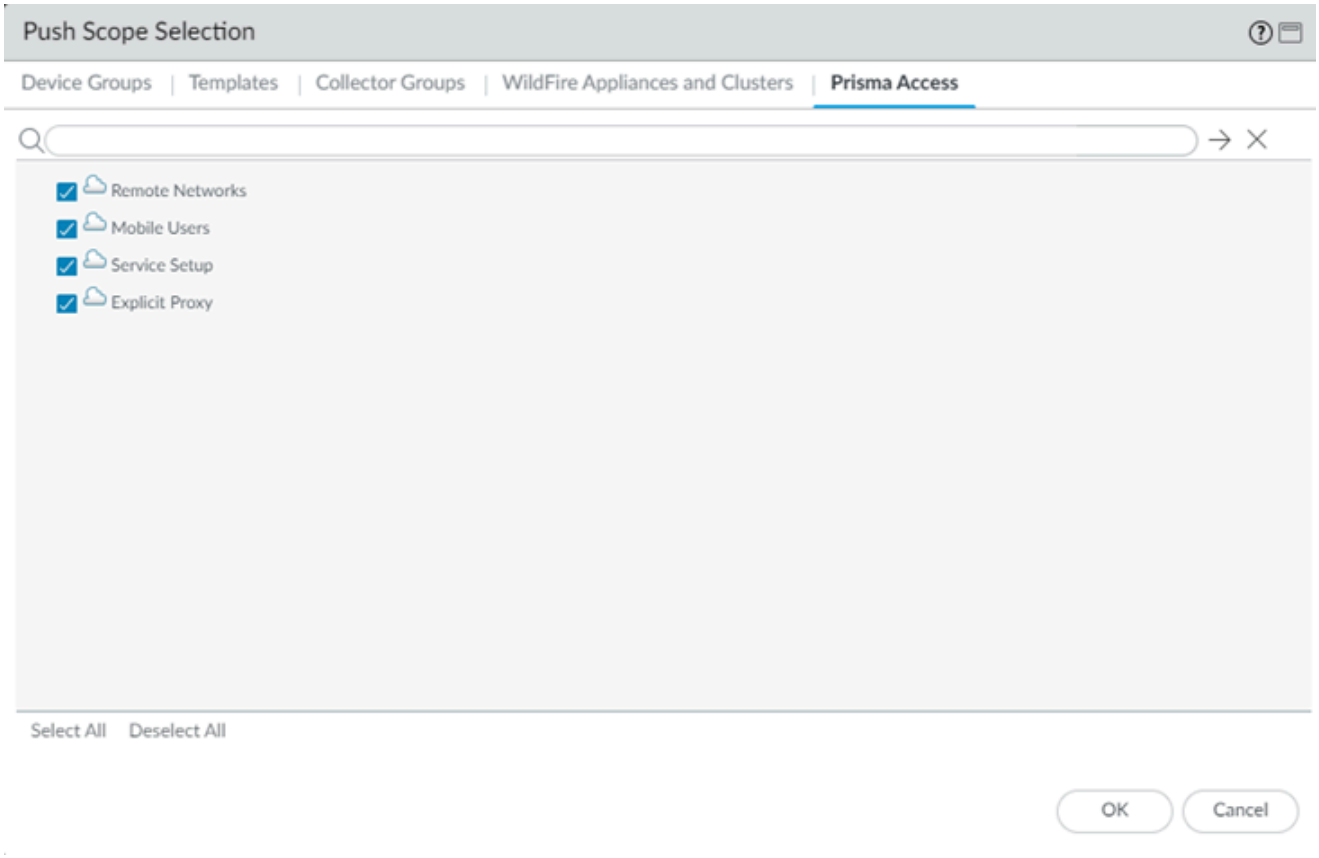

**STEP 10 |** Klicken Sie auf **OK**, um die Einstellungen für die Diensteinrichtung zu speichern.


©2025 Palo Alto Networks, Inc.

**STEP 11 |** Übertragen Sie alle Änderungen an Panorama und übertragen sie die Konfigurationsänderungen per Push an Prisma Access.

1. Klicken Sie auf **Commit** > **Commit in Panorama**.
2. Klicken Sie auf **Commit** > **Per Push auf Geräte übertragen** und klicken Sie auf **Auswahl bearbeiten**.
3. Stellen Sie auf der Registerkarte **Prisma Access** sicher, dass **Diensteinrichtung** ausgewählt ist, und klicken Sie dann auf **OK**.

   Prisma Access sollte automatisch die Komponenten auswählen, für die ein Commit ausgeführt werden soll.

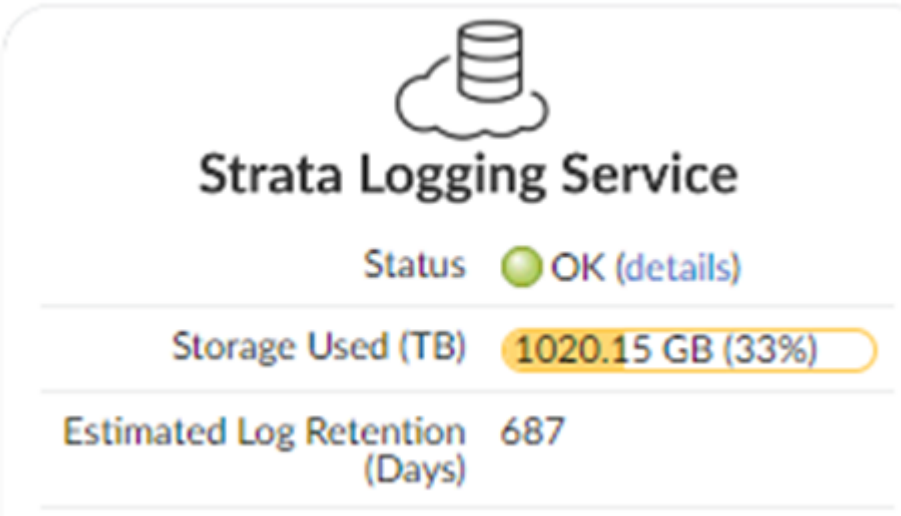



4. Klicken Sie auf **Push**.

 ©2025 Palo Alto Networks, Inc.

**STEP 12 |** Stellen Sie sicher, dass Prisma Access erfolgreich mit Strata Logging Service verbunden wurde.

1. Wählen Sie **Panorama** > **Cloud Services** > **Status** > **Status** > **Strata-Protokollierungsdienst** aus und stellen Sie sicher, dass der Status **OK** lautet.




   Wenn der Status **Fehler** lautet, klicken Sie auf den Detail-Link, um Fehler anzuzeigen.

**STEP 13 |** Richten Sie Prisma Access weiter ein:

- Erstellen Sie eine Dienstverbindung, um Zugriff auf private Apps zu ermöglichen
- Konfigurieren Sie Prisma Access für Netzwerke
- Konfigurieren Sie Prisma Access für Benutzer

 ©2025 Palo Alto Networks, Inc.

# Mobile Benutzer: IP-Adresszuweisung

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Nachdem Sie Ihre Prisma Access-Bereitstellung eingerichtet haben, ist es nützlich zu wissen, wann sich IP-Adressen ändern, damit Sie Ihre Infrastruktur proaktiv planen, die IP-Adressen abrufen und die erforderlichen IP-Adressen hinzufügen können, um Listen entsprechend zuzulassen. Die IP-Adressänderungen können das Ergebnis von Änderungen sein, die Sie vorgenommen haben (z. B. wenn ein anderer Standort für mobile Benutzer hinzugefügt wurde), oder von Änderungen, die Prisma Access automatisch vornimmt (z. B. wenn eine große Anzahl mobiler Benutzer auf ein einzelnes Prisma Access-Gateway zugreift).

Nachdem Sie Prisma Access zum ersten Mal für Benutzer bereitgestellt haben, weist Prisma Access jedem Portal und Gateway zwei *öffentliche und ggf. ausgehende IP-Adressen* zu. Diese IP-Adressen sind eindeutig, werden nicht gemeinsam verwendet, sind eigens für Ihre Prisma Access-Bereitstellung bestimmt und bleiben Ihrem Mandanten zugewiesen, bis das Prisma Access-Abonnement abläuft und die Karenzzeit abgelaufen ist.

Wenn Sie mit einer Einrichtung mit mehreren Mandanten arbeiten, fügt Prisma Access für jeden Mandanten dedizierte IP-Adressen hinzu.

Da es sich bei der öffentlichen IP-Adresse um die Quell-IP-Adresse handelt, die von Prisma Access für Anfragen an ein internetbasiertes Ziel verwendet wird, müssen Sie möglicherweise wissen, wie die öffentliche IP-Adresse lautet, und diese einer Zulassungsliste in Ihrem Netzwerk hinzufügen, um Ihren Benutzern Zugriff auf Ressourcen wie SaaS-Anwendungen oder öffentlich zugängliche Partneranwendungen zu ermöglichen.

Neue öffentliche IP-Adressen können dem Mandanten hinzugefügt werden, wenn folgende Ereignisse auftreten:

- Wenn eine große Anzahl mobiler Benutzer auf einen Standort am selben Ort zugreift.

  Um dem Kapazitätsbedarf für die Bedienung einer großen Anzahl von Benutzern gerecht zu werden, kann Prisma Access ein oder mehrere Gateways hinzufügen. Prisma Access fügt dabei ein oder mehrere Gateways hinzu, um die erhöhte Anzahl von Benutzern aufzunehmen, weist dem neuen Gateway eine oder mehrere der vorhandenen öffentlichen IP-Adressen zu und fügt den Standorten mobiler Benutzer einen neuen Satz von IP-Adressen hinzu, um die verwendeten Adressen zu ersetzen.
- Sie fügen Ihrer Bereitstellung mindestens einen Standort hinzu.

  Wenn Sie weitere Standorte hinzufügen, fügt Prisma Access für jeden neu hinzugefügten Standort ein weiteres Gateway und einen neuen Satz von IP-Adressen hinzu.

Da Prisma Access nach einem Skalierungsereignis und nach dem Hinzufügen eines Standorts mehr öffentliche IP-Adressen aktiviert, sollten Sie eine IP-Ereignisbenachrichtigungs-URL hinzufügen oder die API zum Abrufen mobiler Benutzeradressen verwenden, um über IP-Adressänderungen

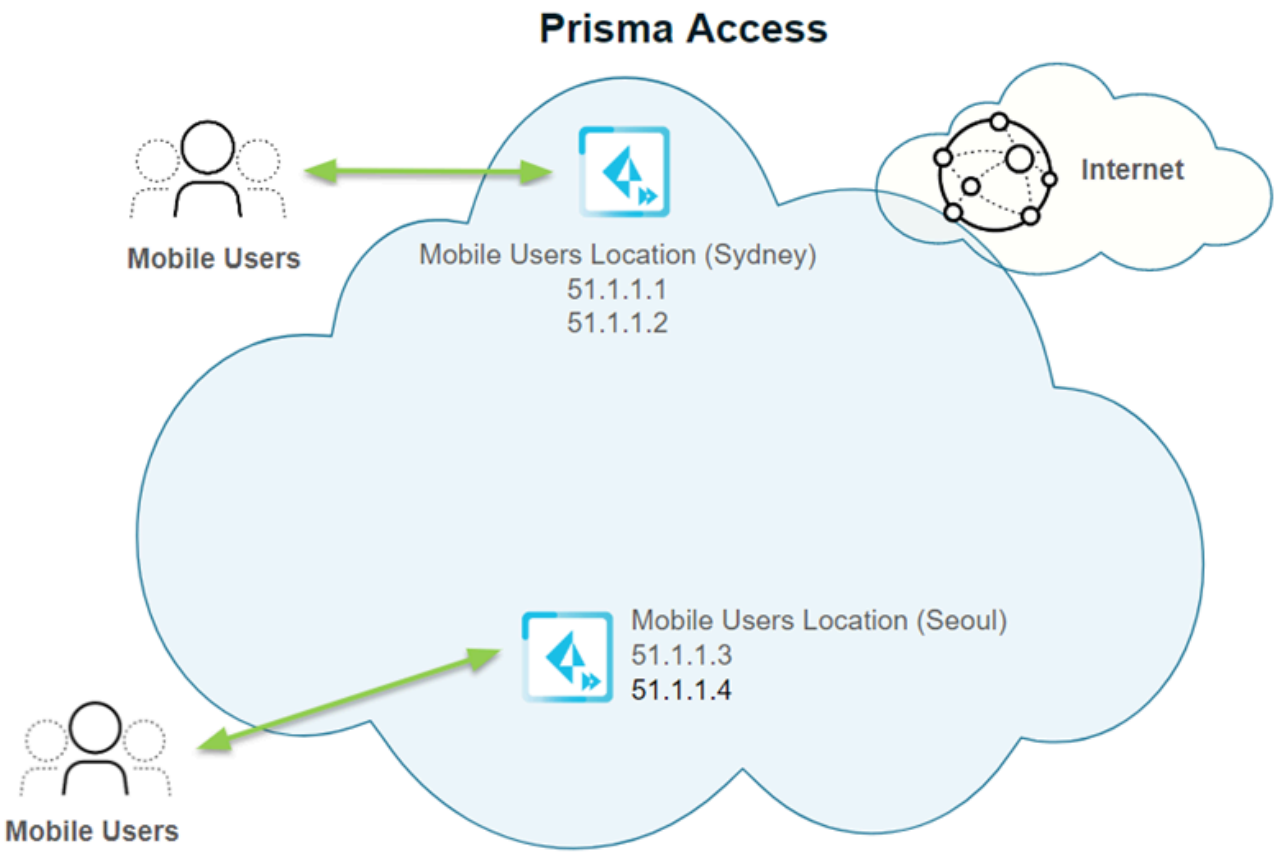
 ©2025 Palo Alto Networks, Inc.

in Ihrer Prisma Access-Infrastruktur benachrichtigt zu werden. Sie können dann alle hinzugefügten oder geänderten Adressen zu einer Zulassungsliste hinzufügen.

## Beispiel: Beispiele für die Skalierung öffentlicher IP-Adressen (Mobile Benutzer)

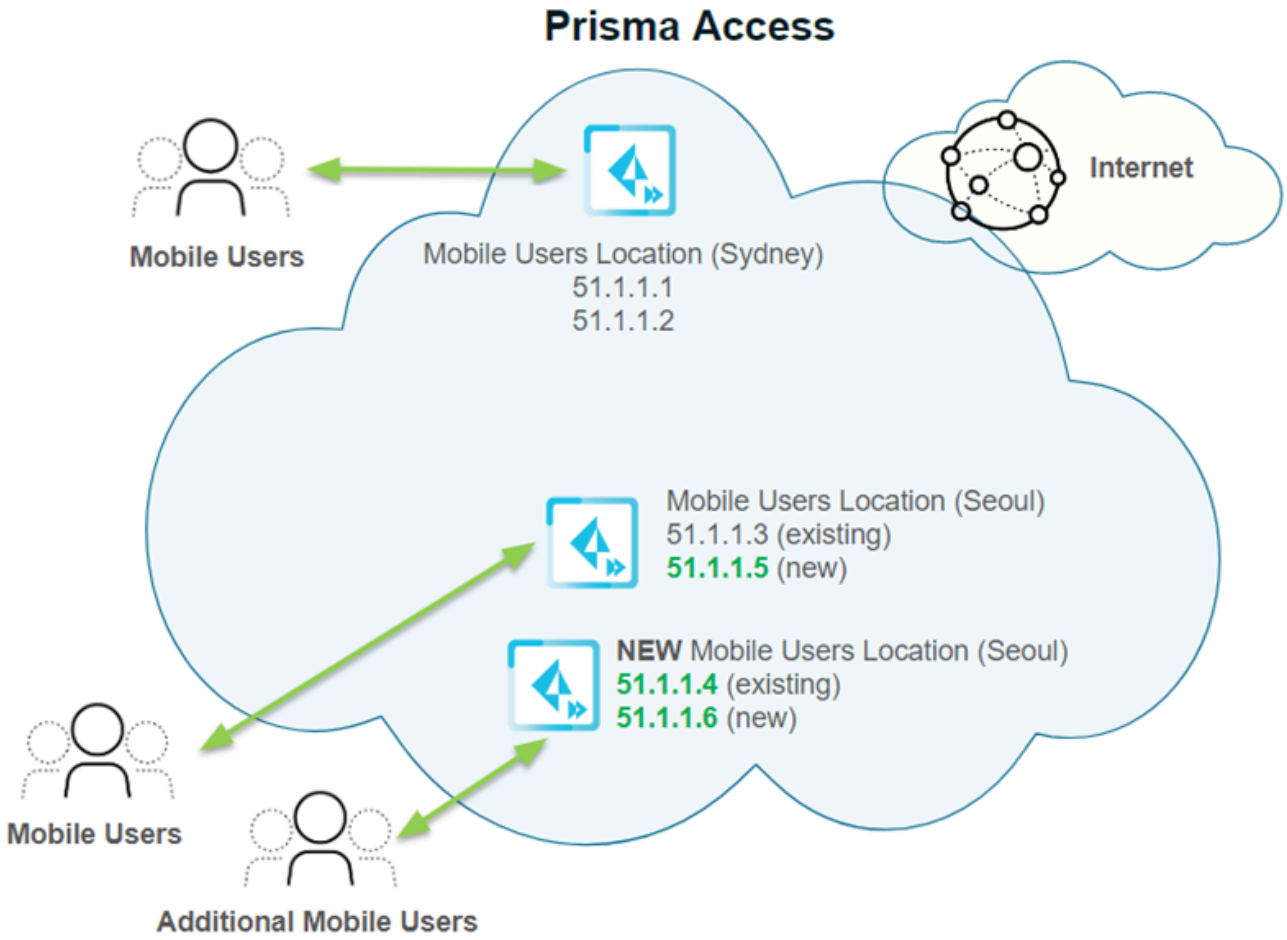
Die folgenden Beispiele veranschaulichen die Zuweisung öffentlicher IP-Adressen für mobile Benutzer, die Prisma Access während eines Skalierungsereignisses oder beim Hinzufügen eines neuen Standorts durchführt.

Im folgenden Beispiel haben Sie zwei Standorte in der Region Asien/Pazifik für eine neue Bereitstellung für mobile Benutzer angegeben: Sydney und Seoul. Jeder Standort erhält zwei Gateway-IP-Adressen.



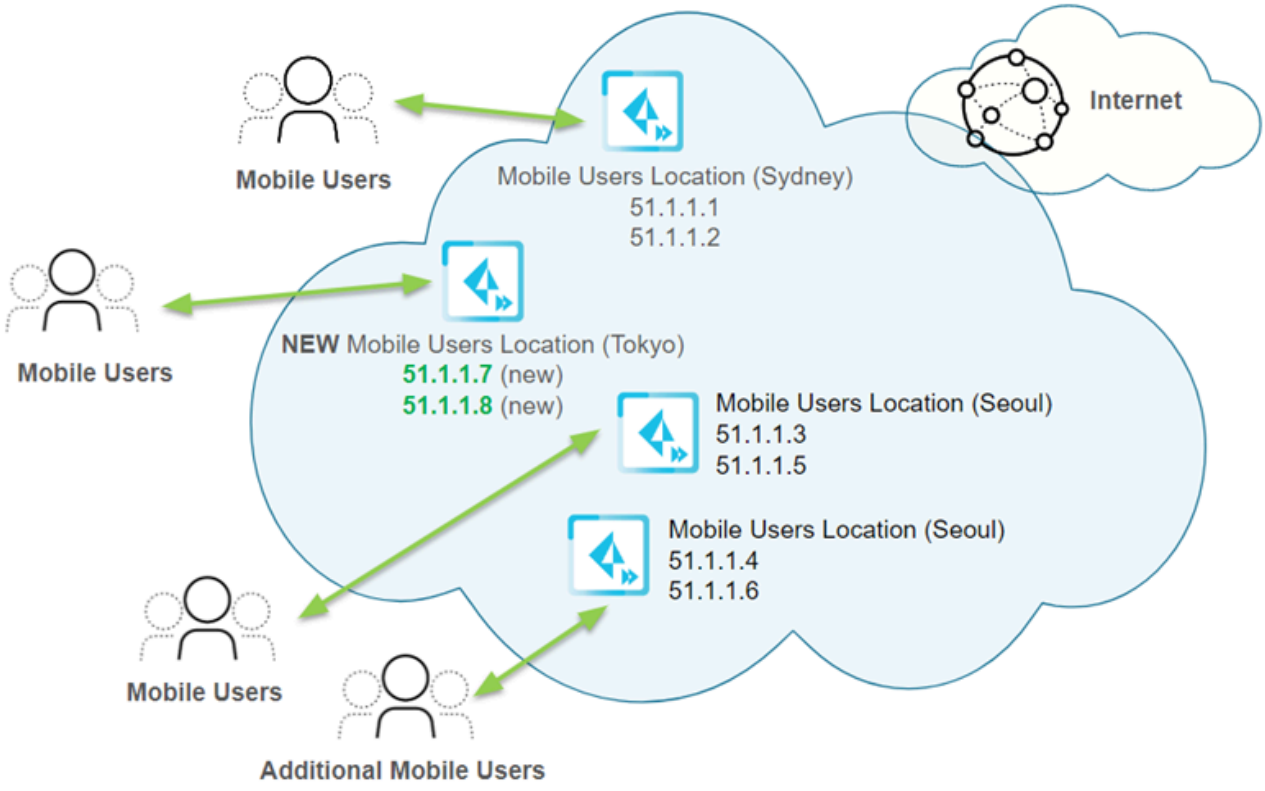

Dann melden sich viele Nutzer am Standort Seoul an. Um diesen zusätzlichen Nutzern gerecht zu werden, fügt Prisma Access ein zweites Gateway für den Standort Seoul hinzu, nimmt eine der Gateway-Adressen vom ersten Seoul-Gateway (51.1.1.4) und weist sie dem zweiten Seoul-Gateway zu. Es fügt dann zwei zusätzliche IP-Adressen (51.1.1.5 und 51.1.1.6 in diesem Beispiel) den beiden Seoul-Gateways hinzu.

 ©2025 Palo Alto Networks, Inc.




Dann folgt ein weiterer Standort, Tokio, in der Region Asien/Pazifik: Prisma Access erstellt zwei neue IP-Adressen für das neue Gateway (51.1.1.7 und 51.1.1.8).

 ©2025 Palo Alto Networks, Inc.




Jedes Mal, wenn Sie einen Standort hinzufügen oder ein Skalierungsereignis auftritt, sollten Sie die neuen IP-Adressen für Ausgang und Gateway abrufen, die Prisma Access zugewiesen hat, und zu einer Liste mit zulässigen IP-Adressen in Ihrem Netzwerk hinzufügen. Prisma Access behält jederzeit zwei Sätze von IP-Adressen für alle aktiven Gateways an jedem Standort bei.

## Loopback-IP-Adresszuweisung (Mobile Benutzer)

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

Loopback-Adressen sind IP-Adressen, die von Prisma Access für Anfragen an eine interne Quelle verwendet und aus dem Infrastruktursubnetz zugewiesen werden. Loopback-IP-Adressen können sich für mobile Benutzer während eines Infrastruktur- oder Dataplane-Upgrades ändern.

*Loopback-IP-Adressen ändern sich für Dienstverbindungen oder Remote-Netzwerkverbindungen während eines Infrastruktur- oder Dataplane-Upgrades nicht. Nur Loopback-IP-Adressen mobiler Benutzer können sich ändern.*

Prisma Access weist die Loopback-IP-Adressen aus dem Infrastruktursubnetz zu, die Sie beim Aktivieren der Prisma Access-Infrastruktur angeben. Sie können das gesamte Infrastruktursubnetz

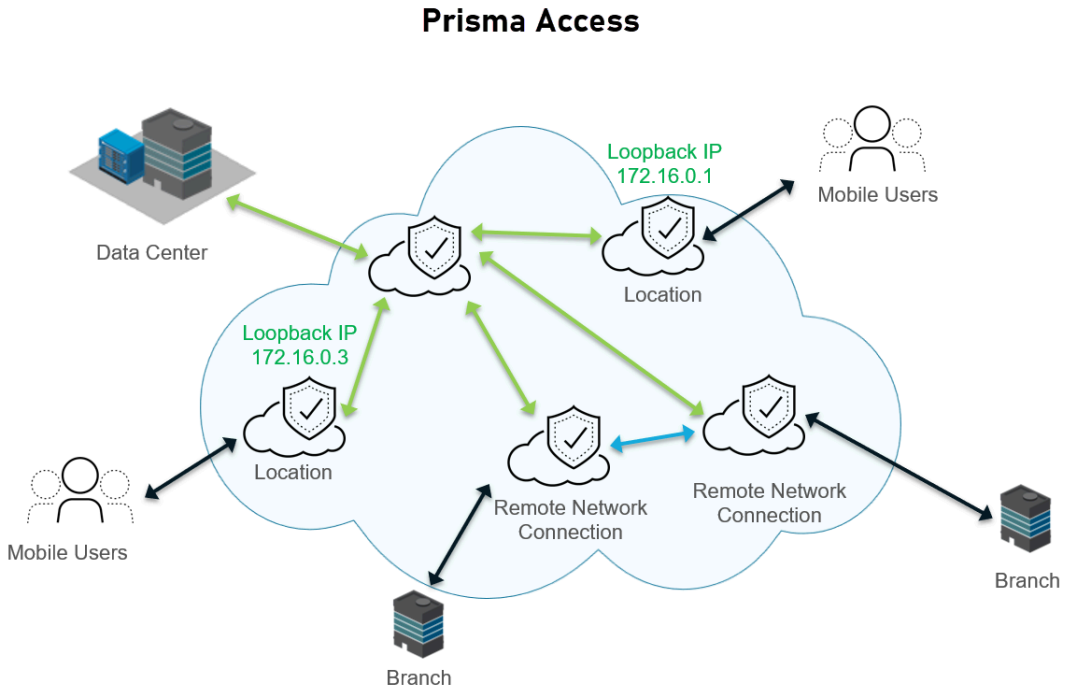
 ©2025 Palo Alto Networks, Inc.

zu einer Genehmigungsliste hinzufügen, damit während eines Infrastruktur- oder Dataplane-Upgrades keine Loopback-IP-Änderungen für mobile Benutzer geplant werden müssen. Um das Infrastruktursubnetz zu finden, wählen Sie Folgendes aus:

- Prisma Access (Managed by Strata Cloud Manager): **Workflows** > **Einrichten Prisma Access** > **Prisma Access** > **Infrastruktureinstellungen**. Zeigen Sie das **Infrastruktursubnetz**
- Prisma Access (Managed by Panorama): **Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Dienstinfrastruktur** und zeigen Sie das **Infrastruktursubnetz**

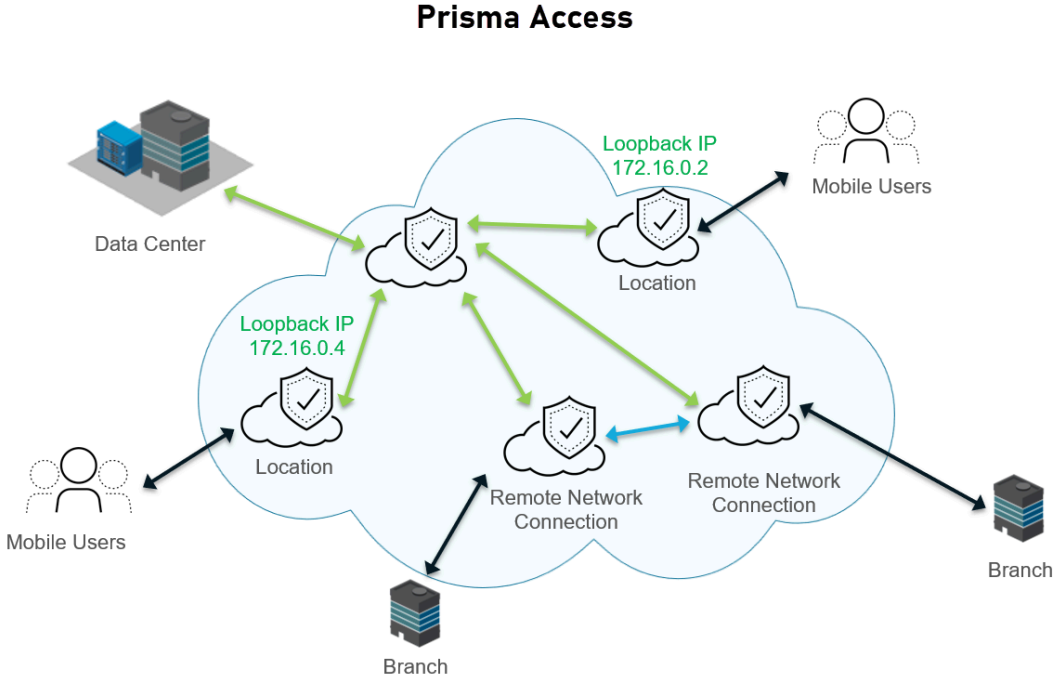
Rufen Sie diese Adressen mithilfe der API ab, die zum Abrufen von öffentlichen IP- und Loopback-IP-Adressen verwendet wird.

Im folgenden Beispiel ist eine Prisma Access-Bereitstellung mit dem Infrastruktursubnetz 172.16.0.0/16 dargestellt. Prisma Access hat die Loopback-IP-Adressen 172.16.0.1 und 172.16.0.3 für mobile Benutzer aus dem Infrastruktursubnetz zugewiesen.




Nach einem Infrastruktur- oder Dataplane-Upgrade (z. B. zur Vorbereitung auf ein neues Release des Cloud Services-Plug-ins) weist Prisma Access zwei verschiedene IP-Adressen für mobile Benutzer aus dem Infrastruktursubnetz zu (172.16.0.1 wird in 172.16.0.2 und 172.16.0.3 in 172.16.0.4 geändert).

 ©2025 Palo Alto Networks, Inc.

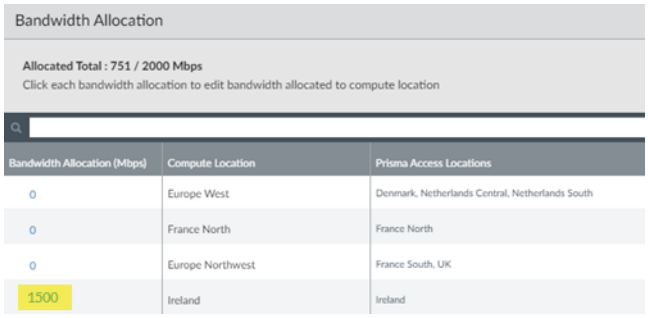



 ©2025 Palo Alto Networks, Inc.

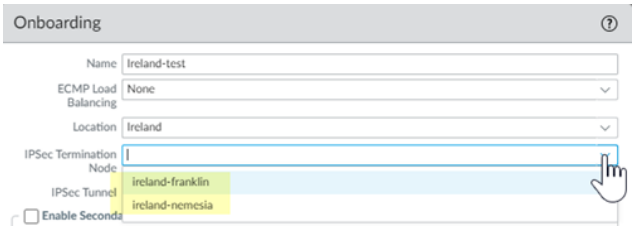
# Remote-Netzwerke: IPSec-Terminierungsknoten und Dienst-IP-Adressen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

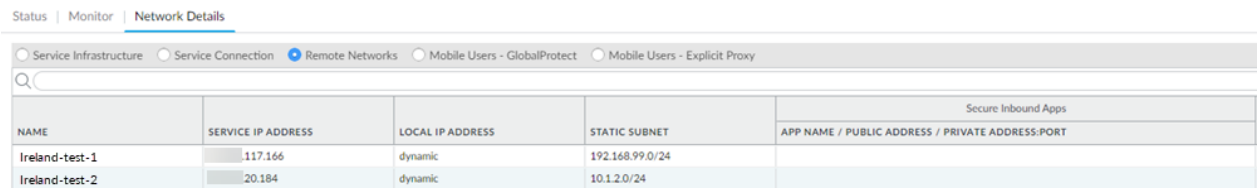
Wenn Sie das Onboarding für ein Remote-Netzwerk durchführen, ordnen Sie es einem *IPSec-Terminierungsknoten* zu. Jedem IPSec-Terminierungsknoten ist eine **Dienst-IP-Adresse** zugeordnet. Sie verwenden diese Adresse als Peer-IP-Adresse für Ihr CPE, wenn Sie den IPSec-Tunnel für die Remote-Netzwerkverbindung einrichten. Jeder Terminierungsknoten kann Ihnen eine Bandbreite von bis zu 1.000 Mbit/s zur Verfügung stellen. Wenn Sie einem Compute-Standort eine Bandbreite von mehr als 1.000 Mbit/s zuweisen, erhalten Sie mehrere **Dienst-IP-Adressen**.




Wenn Sie das Onboarding für ein Remote-Netzwerk an einem Compute-Standort in Irland durchführen, haben Sie die Wahl zwischen zwei IPSec-Terminierungsknoten, da die Gesamtbandbreite mehr als 1.000 Mbit/s beträgt.




Jeder IPSec-Terminierungsknoten hat seine eigene **Dienst-IP-Adresse**, wie unter **Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Remote-Netzwerke** zu sehen ist.




 ©2025 Palo Alto Networks, Inc.

# Remote-Netzwerke: Änderungen der IP-Adresse im Zusammenhang mit der Bandbreitenzuweisung

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

Dieser Abschnitt findet Anwendung, wenn Sie über eine veraltete Prisma Access-Bereitstellung verfügen, bei der Bandbreite nach Standort zugewiesen wird. Bei allen neuen Bereitstellungen wird Bandbreite nach Compute-Standort zugewiesen. Weitere Informationen darüber, wie Prisma Access diese IP-Adressen zuweist, finden Sie unter Remote-Netzwerke: IPSec-Terminierungsknoten und Dienst-IP-Adressen.

IP-Adressen für Remote-Netzwerkverbindungen sind eindeutig, werden nicht gemeinsam verwendet und sind für Ihre Prisma Access-Bereitstellung bestimmt. Diese IP-Adressen ändern sich nicht, nachdem sie von Prisma Access im Rahmen des Onboardings von Remote-Netzwerken erstellt wurden. Sie bleiben auch nach einem Upgrade erhalten. Seien Sie jedoch vorsichtig, wenn Sie die Bandbreite einer vorhandenen Verbindung erhöhen, da sich die IP-Adresse eines Remote-Netzwerks ändern kann, wenn durch diese Erhöhung die Bandbreite an einem Standort 500 Mbit/s überschreitet.

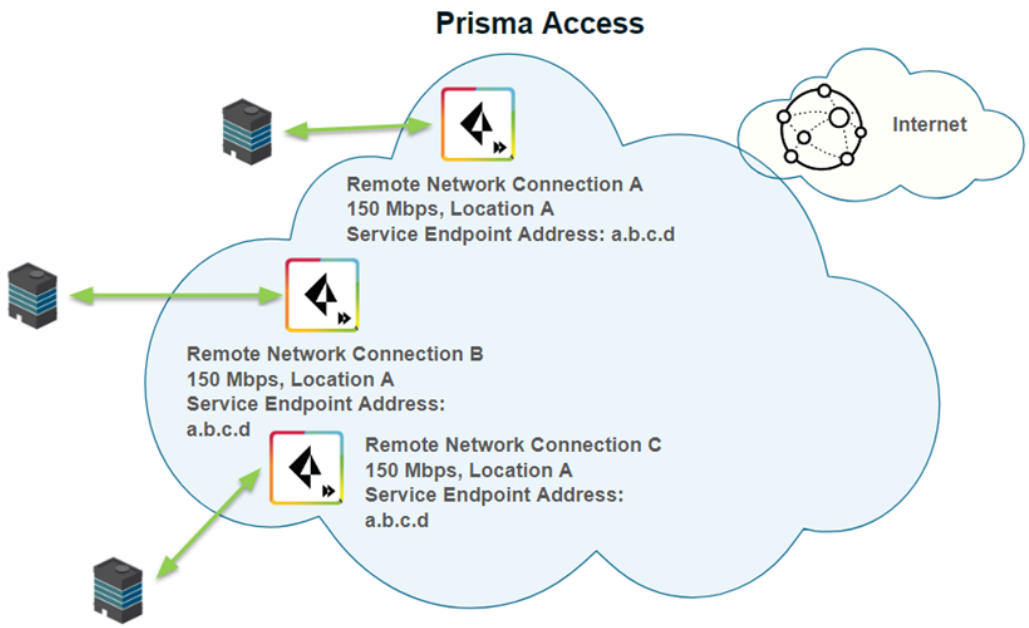
*Darüber hinaus können sich Ausgangs-IP-Adressen ändern, wenn Prisma Access einen neuen Prisma Access-Compute-Standort erstellt und Sie entscheiden, diesen neuen Compute-Standort zusammen mit Standorten zu verwenden, die Sie bereits integriert haben.*

Diese Bandbreitenrichtlinien gelten nur, wenn Sie eine vorhandene Verbindung aktualisieren. Eine einzelne Remote-Netzwerkverbindung, selbst eine Verbindung mit einer Bandbreite von 1.000 Mbit/s (Vorschau), erhält immer eine einzelne **Dienst-IP-Adresse**, unabhängig von der Größe.

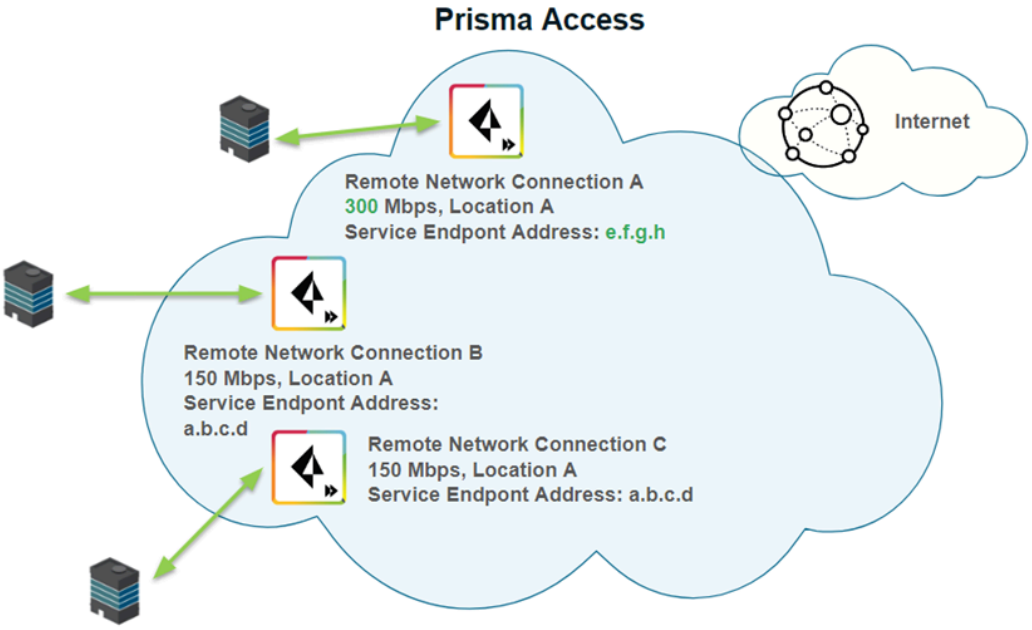
*Die Bandbreitenoption von 1.000 Mbit/s befindet sich im Vorschaumodus. Der Durchsatz während der Vorschau wird nach bestem Wissen und Gewissen bereitgestellt. Die tatsächliche Leistung variiert je nach Datenverkehrsmix.*

Das folgende Beispiel zeigt drei Remote-Netzwerkverbindungen an demselben Standort mit einer Bandbreite von jeweils 150 MBit/s. Da die Gesamtbandbreite 500 Mbit/s beträgt, weist Prisma Access allen Verbindungen am Standort eine einzige IP-Adresse zu.

 ©2025 Palo Alto Networks, Inc.




Das folgende Beispiel zeigt, wie die Bandbreite der Remote-Netzwerkverbindung A von 150 Mbit/s auf 300 Mbit/s erhöht wird. Da die Gesamtbandbreite aller Verbindungen nun mehr als 500 Mbit/s beträgt, weist Prisma Access der Verbindung mit der zusätzlichen Bandbreite eine neue Dienst-IP-Adresse zu. Die anderen Dienst-IP-Adressen bleiben unverändert.




Umgekehrt wird bei vier Remote-Netzwerken mit einer Bandbreite von 100 Mbit/s die **Dienst-IP-Adresse** eines Remote-Netzwerks nicht geändert, wenn Sie die Bandbreite bei einem der Remote-Netzwerke auf 100 Mbit/s erhöhen, da die Gesamtbandbreite jetzt 500 Mbit/s beträgt.

 ©2025 Palo Alto Networks, Inc.

*Wenn Sie die Bandbreite einer Remote-Netzwerkverbindung reduzieren, ändert sich die **Dienst-IP-Adresse** nicht.*

Wenn Sie die Dienst-IP-Adressen in Panorama finden möchten, wählen Sie **Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** aus und klicken Sie auf das Optionsfeld **Remote-Netzwerke**, um die **Dienst-IP-Adresse** für die Remote-Netzwerke anzuzeigen. Alternativ können Sie das API-Skript verwenden.

 ©2025 Palo Alto Networks, Inc.

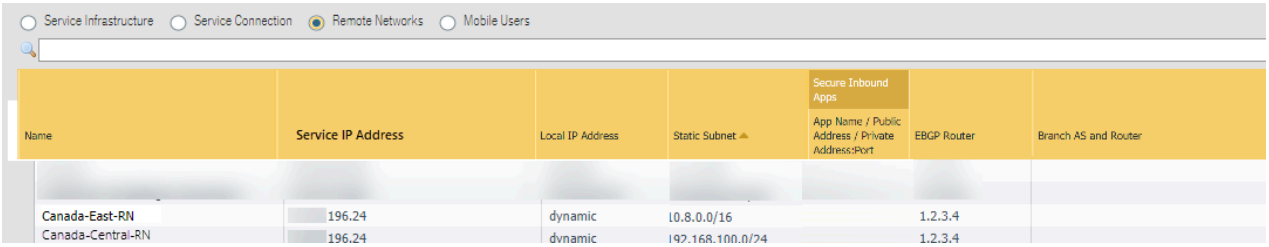
# Remote-Netzwerke: Zuweisung von Dienst-IP-Adressen und Ausgangs-IP-Adressen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

Prisma Access verfügt über mehr als 100 Standorte, um weltweite Bereitstellungen zu ermöglichen und eine lokalisierte Erfahrung zu bieten. Zwei Standorte können demselben Standort zugeordnet werden, den Sie beim Einrichten des IPSec-Tunnels für die Remote-Netzwerkverbindung als Peer-IP-Adresse verwenden. Die Standorte können jedoch unterschiedliche Ausgangs-IP-Adressen verwenden. So wird sichergestellt, dass der Benutzer die richtige Standardsprache für die Region erhält.

Dienstverbindungen *unterstützen die Sprachlokalisierung nicht, da der Ausgang in das Internet über Dienstverbindungen nicht unterstützt wird. Prisma Access weist nur eine Dienst-IP-Adresse pro Dienstverbindung zu. Diese IP-Adresse ist geografisch bei dem* Compute-Standort *registriert, der dem Standort entspricht, den Sie während des Onboardings angegeben haben.*

Das folgende Beispiel zeigt eine Kundenbereitstellung mit zwei Remote-Netzwerkstandorten, die in Kanada bereitgestellt werden: Zentral- und Ostkanada. Prisma Access hat beiden Standorten die gleiche **Dienst-IP-Adresse** zugewiesen. Wenn Sie den Remote-Netzwerktunnel konfigurieren, verwenden Sie bei der Erstellung des IPSec-Tunnels für die Remote-Netzwerkverbindung diese IP-Adresse als Peer-IP-Adresse.




In Ostkanada wird jedoch eine andere Standardsprache (Französisch) verwendet als in Zentralkanada (Englisch). Daher weist Prisma Access ihnen unterschiedliche Ausgangs-IP-Adressen zu. Wenn Sie das API-Skript für Ausgangs-IP-Adressen ausführen, erhalten Sie zwei verschiedene IP-Adressen für diese beiden Standorte.

 ©2025 Palo Alto Networks, Inc.

# Abrufen der IP-Adressen für Prisma Access

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Wenn Sie IP-Adressen Ihrer Prisma Access-Infrastruktur manuell zu einer Zulassungsliste in Ihrem Netzwerk hinzufügen oder wenn Sie ein Automatisierungsskript verwenden, um IP-basierte Beschränkungen durchzusetzen, um den eingehenden Zugriff auf Unternehmensanwendungen zu begrenzen, sollten Sie verstehen, was diese Adressen bewirken und warum Sie sie zulassen müssen. Zudem sollten Sie wissen, welche Aufgaben Sie ausführen müssen, um diese abzurufen.

Prisma Access stellt diese IP-Adressen erst nach Abschluss Ihrer Prisma Access-Konfiguration zur Verfügung. Nach Abschluss der Bereitstellung rufen Sie diese IP-Adressen über ein API-Skript ab. Das API-Skript verwendet einen API-Schlüssel, den Sie von der Prisma Access-Benutzeroberfläche erhalten, und eine von Ihnen erstellte Textdatei (.txt), die die Adressen enthält, die Sie abrufen möchten.

Während Sie diese Aufgaben erst nach Abschluss der Prisma Access-Konfiguration ausführen, ist es nützlich, diese Konzepte im Voraus zu verstehen, damit Sie wissen, was nach Abschluss der Bereitstellung zu tun ist.

- Strata Cloud Manager
- Panorama

## Abrufen der IP-Adressen für Prisma Access (Strata Cloud Manager)

### IP-Adressen der Prisma Access-Infrastruktur

In der folgenden Tabelle finden Sie eine Liste der IP-Adressen, die Prisma Access für die einzelnen Bereitstellungstypen verwendet, zusammen mit dem Schlüsselwort, das Sie verwenden, wenn Sie das API-Skript zum Abrufen der IP-Adressen ausführen, und der Angabe, ob Sie sie einer Liste mit zulässigen Adressen hinzufügen müssen oder nicht.

| Bereitstellungstyp | IP-Adresstyp | Beschreibung |
|---|---|---|
| **Mobiler Benutzer** | Prisma Access-Gateway (**gp_gateway**) | Ruft die Gateway-IP-Adressen ab. Fügen Sie Gateway- und Portal-IP-Adressen zu Zulassungslisten für Ihre Bereitstellungen für mobile Benutzer hinzu.<br><br>Mobile Benutzer verbinden sich mit einem Prisma Access-Gateway, um auf interne oder Internetressourcen wie SaaS oder |

 ©2025 Palo Alto Networks, Inc.

| Bereitstellungstyp | IP-Adresstyp | Beschreibung |
|---|---|---|
| | | öffentliche Anwendungen zuzugreifen, für die Sie Zugriff gewährt haben. |
| | Prisma Access-Portal (**gp_portal**) | Ruft die Portal-IP-Adressen ab. Fügen Sie Gateway- und Portal-IP-Adressen zu Zulassungslisten für Ihre Bereitstellungen für mobile Benutzer hinzu.<br><br>Mobile Benutzer melden sich im Prisma Access-Portal an, um ihre Erstkonfiguration und ihren Gateway-Standort zu erhalten. |
| | Loopback-IP-Adressen | Bei dieser Adresse handelt es sich um die Quell-IP-Adresse, die von Prisma Access für Anfragen an eine interne Quelle verwendet und von der Infrastruktur zugewiesen wird. Fügen Sie die Loopback-IP-Adresse zu einer Zulassungsliste in Ihrem Netzwerk hinzu, damit Prisma Access auf interne Ressourcen wie RADIUS- oder Active Directory-Authentifizierungsserver zugreifen kann.<br><br>Da sich Loopback-Adressen für mobile Benutzer ändern können, empfiehlt Palo Alto Networks, alle IP-Adressen des gesamten Infrastruktursubnetzes in Ihrem Netzwerk zuzulassen. |
| **Mobile Benutzer – Expliziter Proxy** | Authentifizierungs-Cache-Dienst (Authentication Cache Service, ACS) | Die Adresse für den Prisma Access-Dienst, der den Authentifizierungsstatus der Benutzer von explizitem Proxy speichert.<br><br>Diese Adresse wird nur für Bereitstellungen für mobile Benutzer (mit explizitem Proxy) verwendet. |
| | Load-Balancer des Netzwerks | Die Adresse, die Prisma Access für den Load-Balancer des Netzwerks für explizite Proxys verwendet.<br><br>Diese Adresse wird nur für Bereitstellungen für mobile Benutzer (mit explizitem Proxy) verwendet. |
| **Remote-Netzwerk** | IP-Adressen des Remote-Netzwerks (**remote_network**) | Enthält **Dienst-IP-Adressen**, die Prisma Access für die Prisma Access-Remote-Netzwerkverbindung zuweist, und |

 ©2025 Palo Alto Networks, Inc.

| Bereitstellungstyp | IP-Adresstyp | Beschreibung |
|---|---|---|
| | | Ausgangs-IP-Adressen, die Prisma Access verwendet, um sicherzustellen, dass Remote-Netzwerkbenutzer die richtige Standardsprache für ihre Region erhalten. Fügen Sie diese Adressen zu Zulassungslisten in Ihrem Netzwerk hinzu, um Prisma Access zu Internetressourcen zuzuordnen. |
| | Loopback-IP-Adressen | Dies ist die Quell-IP-Adresse, die Prisma Access für Anfragen an eine interne Quelle verwendet und vom Infrastruktursubnetz zugewiesen wird. Fügen Sie die Loopback-IP-Adresse zu einer Zulassungsliste hinzu, damit Prisma Access auf interne Ressourcen wie RADIUS- oder Active Directory-Authentifizierungsserver zugreifen kann. |

## Ausführen des API-Skripts zum Abrufen von IP-Adressen

Führen Sie die folgenden Schritte aus, um die IP-Adressen abzurufen, die Prisma Access in seiner Infrastruktur verwendet.

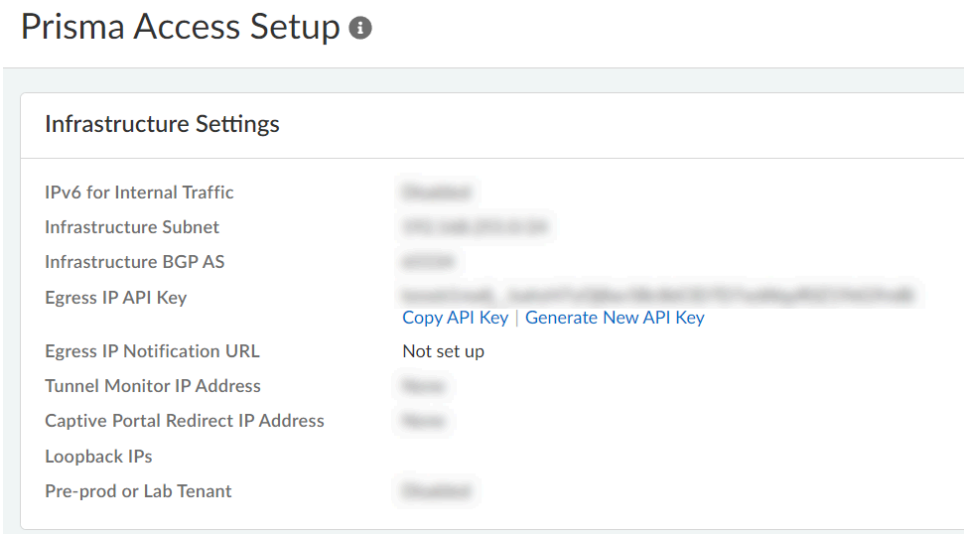
*Mit diesem Befehl werden keine Loopback-Adressen abgerufen. Zum Abrufen von Loopback-IP-Adressen* verwenden Sie den Legacy-API-Befehl.

 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** Rufen Sie den API-Schlüssel ab.

Sie benötigen diesen Schlüssel, um sich bei Prisma Access zu authentifizieren und die Liste der IP-Adressen mit dem API-Befehl abzurufen.

1. Gehen Sie zu Prisma Access (Managed by Strata Cloud Manager) und wählen Sie **Workflows** > **Prisma Access-Einrichtung** > **Prisma Access** > **Infrastruktureinstellungen** aus.
2. Wählen Sie **Neuen API-Schlüssel generieren** aus.




Wenn Sie bereits einen API-Schlüssel generiert haben, wird der aktuelle Schlüssel angezeigt. Wenn Sie noch keinen Schlüssel generiert haben oder den vorhandenen Schlüssel ersetzen möchten, um die Überprüfung der Audit- oder Compliance-Prüfung für die Schlüsselrotation zu erfüllen, klicken Sie für den Erhalt eines neuen Schlüssels auf **Neuen API-Schlüssel generieren**.

**STEP 2 |** Erstellen Sie eine Textdatei (.txt) und legen Sie die API-Befehlsoptionen in die Datei.

Die Verwendung des API-Befehls ist ein zweistufiger Prozess. Zuerst erstellen Sie eine Textdatei (.txt), in der die Parameter für die abzurufenden IP-Adressen angegeben sind, und speichern die Datei in einem Ordner, der von dem Ort aus erreichbar ist, an dem Sie den Befehl ausführen. Anschließend führen Sie die API aus und geben den Namen und Speicherort der Textdatei (.txt) an, die Sie im Befehl erstellt haben.

Geben Sie folgende Schlüsselwörter und Argumente in der Textdatei (.txt) an. Bei den Beispielen in diesem Abschnitt wird der Dateiname **options.txt** verwendet. Solange Sie im Befehl darauf verweisen, können Sie aber einen beliebigen Dateinamen angeben.

| Argument | Mögliche Auswahl (Schlüsselwörter) | Bemerkungen |
|---|---|---|
| **serviceType** | **all**<br>**remote_network**<br>**gp_gateway**<br>**gp_portal** | **all** – Ruft IP-Adressen ab, die Sie zu einer Zulassungsliste für alle Diensttypen hinzufügen müssen (Remote-Netzwerke, mobile Benutzer – sowohl Gateways als auch |

 ©2025 Palo Alto Networks, Inc.

| Argument | Mögliche Auswahl (Schlüsselwörter) | Bemerkungen |
|---|---|---|
| | **swg_proxy**<br>**rbi** | Portale – und Clean Pipe, abhängig von Ihrer Bereitstellung).<br>**remote_network** – Ruft IP-Adressen ab, die Sie zu einer Zulassungsliste für Remote-Netzwerkbereitstellungen hinzufügen müssen.<br>**gp_gateway** – Ruft die Gateway-IP-Adressen ab, die Sie zu einer Zulassungsliste für Bereitstellungen für mobile Benutzer hinzufügen müssen.<br>**gp_portal** – Ruft die Portal-IP-Adressen ab, die Sie zu einer Zulassungsliste für Bereitstellungen für mobile Benutzer hinzufügen müssen.<br>**swg_proxy** – Ruft die Ausgangs-IP-Adressen für die einzelnen bereitgestellten Standorte mit explizitem Proxy, den ACS (Authentication Cache Service) und die Load-Balancer des Netzwerks ab.<br>**rbi** – Ruft die Ausgangs-IP-Adressen ab, die Sie zu einer Zulassungsliste für RBI-Bereitstellungen (Remote-Browser-Isolation) hinzufügen müssen, um eine Verbindung zu SaaS-Anwendungen herzustellen. |
| **addrType** | **all**<br>**aktiv**<br>**service_ip**<br>**auth_cache_service**<br>**network_load_balancer** | **all** oder **active** – Ruft alle IP-Adressen ab, die Sie zu einer Zulassungsliste hinzufügen müssen.<br>Diese API ruft keine Loopback-IP-Adressen ab. Verwenden Sie den Legacy-API-Befehl, um Loopback-IP-Adressen abzurufen.<br>**service_ip** – Ruft die **Dienst-IP-Adresse** ab, die Sie als Peer-IP-Adresse verwenden, wenn Sie den IPSec-Tunnel für die Remote-Netzwerkverbindung einrichten.<br>**auth_cache_service** – Ruft die IP-Adresse für den ACS des expliziten Proxy ab (gilt nur für Bereitstellungen mit explizitem Proxy für mobile Benutzer).<br>**network_load_balancer** – Ruft die IP-Adresse für den Load-Balancer des Netzwerks für explizite Proxys ab (gilt nur |


©2025 Palo Alto Networks, Inc.

| Argument | Mögliche Auswahl (Schlüsselwörter) | Bemerkungen |
|---|---|---|
| | | für Bereitstellungen mit explizitem Proxy für mobile Benutzer). |
| **actionType** | **pre_allocate** | Nur Bereitstellungen für mobile Benutzer – Ein **actionType** von **pre_allocate** ermöglicht Ihnen das Abrufen von IP-Adressen oder Subnetzen für Prisma Access-Gateways und -Portale für Bereitstellungen für mobile Benutzer. Verwenden Sie diesen mit einem **serviceType** von **gp_gateway**, um vorab zugewiesene Gateway-IP-Adressen abzurufen, und einem **serviceType** von **gp_portal**, um vorab zugewiesene Portal-IP-Adressen abzurufen.<br><br>Durch das Abrufen der vorab zugewiesenen IP-Adressen können Sie die Gateway- und Portal-IP-Adressen zu den Zulassungslisten Ihrer Organisation hinzufügen, bevor Sie Standorte mobiler Benutzer einbinden. Dadurch wiederum wird mobilen Benutzern unmittelbar nach dem Einbinden der Standorte Zugriff auf externe SaaS-Apps gewährt. |
| **location** | **all**<br><br>**deployed** | **all** – Ruft die IP-Adressen von allen Standorten ab. Bei Bereitstellungen für mobile Benutzer ruft dieses Schlüsselwort die IP-Adressen sowohl für Standorte ab, die Sie während des Onboardings hinzugefügt haben, als auch für Standorte, die Sie nicht hinzugefügt haben.<br><br>**deployed** – Ruft IP-Adressen an allen Standorten ab, die Sie beim Onboarding mobiler Benutzer hinzugefügt haben.<br><br>Dieses Schlüsselwort gilt nur für Bereitstellungen für mobile Benutzer. Prisma Access weist während der Bereitstellung jedem Standort mobiler Benutzer IP-Adressen zu, auch wenn Sie diesen Standort beim Onboarding mobiler Benutzer nicht ausgewählt haben. Wenn Sie **all** angeben, ruft der API-Befehl die IP-Adressen für alle Standorte mobiler Benutzer ab, einschließlich derjenigen, die Sie nicht für die Bereitstellung ausgewählt haben. Wenn Sie **deployed** angeben, werden mit dem API-Befehl nur die |

 ©2025 Palo Alto Networks, Inc.

| Argument | Mögliche Auswahl (Schlüsselwörter) | Bemerkungen |
|---|---|---|
| | | IP-Adressen für die Standorte abgerufen, die Sie beim Onboarding ausgewählt haben. |

Geben Sie die Optionen in der Textdatei (.txt) im folgenden Format an:

```
 { "serviceType": "service-type", "addrType": "address-type",
"location": "location" }
```

**STEP 3 |** Geben Sie folgenden Befehl ein, um die IP-Adressen abzurufen:

- Geben Sie folgenden Befehl ein, um die neuere API zu verwenden, die in Prisma Access 2.1 eingeführt wurde:

```
  curl -X POST --data @option.txt -H header-api-key:Current-
API-Key "https://api.prod.datapath.prismaaccess.com/
getPrismaAccessIP/v2"
```

  *Ab Mai 2023 verwenden einige von der Cloud verwaltete Bereitstellungen https://api.prod6.datapath.prismaaccess.com/getPrismaAccessIP/v2 (beachten Sie das `prod6` in der URL anstelle von `prod`).*

- Geben Sie folgenden Befehl ein, um die Legacy-API zu verwenden. Dieser Befehl verwendet einen älteren API-Endpunkt, der seit Mai 2022 nicht mehr unterstützt wird:

```
  curl -X POST --data @option.txt -k -H header-api-key:Current-
API-Key "https://api.gpcloudservice.com/getPrismaAccessIP/v2"
```

Dabei ist *option.txt* die Textdatei (.txt), die Sie in einem vorherigen Schritt erstellt haben, und *Current-API-Key* der Prisma Access-API-Schlüssel.

Beispiel: Wenn der Name der Textdatei **option.txt** und der API-Schlüssel **12345abcde** lautet, verwenden Sie den folgenden API-Befehl, um die öffentliche IP-Adresse für alle Standorte abzurufen:

```
 curl -X POST --data @option.txt -H header-api-key:12345abcde
"https://api.prod.datapath.prismaaccess.com/getPrismaAccessIP/v2"
```

*Der API-Befehl kann eine große Menge an Informationen zurückgeben. Wenn Sie Python installiert haben, können Sie am Ende des cURL-Befehls `| python -m json.tool` hinzufügen, um die Ausgabe besser lesbar zu machen.*

Der API-Befehl gibt die Adressen im folgenden Format zurück:

```
{"result": [ { "address_details": [ { "address": "1.2.3.4"
"allow_listed": false "addressType": "address-type" "serviceType":
```

 ©2025 Palo Alto Networks, Inc.

```
 "service-type" } ], "addresses": [ "1.2.3.4" ] "zone": "zone-
name", "zone_subnet": [zone-subnet ] }, "status": "erfolg"
```

Dabei gilt:

- **address_details** zeigt die Details der Adresse für jeden Standort an.
  - **serviceType** zeigt die Art der IP-Adresse an (entweder Remote-Netzwerk (**remote_network**), Prisma Access-Gateway (**gp_gateway**), Prisma Access-Portal (**gp_portal**), Clean Pipe (**clean_pipe**) oder Remote-Browser-Isolation (**rbi**).
  - **addressType** gibt den Typ der Adresse an, die mit dem Schlüsselwort `addrType` angegeben wurde (entweder **aktiv** oder **vorab zugewiesen**, wenn Sie IP-Adressen für Standorte mobiler Benutzer vorab zuweisen).
  - **address** zeigt die IP-Adresse an, die Sie zu Ihren Zulassungslisten hinzufügen müssen.

    Wenn die API mehrere IP-Adressen zurückgibt, fasst Prisma Access die IP-Adressen im Feld **addresses** zusammen.
- **addresses** listet alle IP-Adressen für den Standort auf, die Sie zu Ihren Zulassungslisten hinzufügen müssen.
- **zone** ist der den IP-Adressen zugeordnete Prisma Access-Standort.
- **zone_subnet** ist das Subnetz für Gateways und Portale für mobile Benutzer. Prisma Access stellt dieses Subnetz auch zur Verfügung, wenn Sie vorab IP-Adressen für Standorte mobiler Benutzer zuweisen.

Wenn Probleme mit den Optionen in der Textdatei (.txt) auftreten, gibt die API einen Fehler ähnlich dem folgenden zurück:

```
 {"status": "error","result": "Ungültiges JSON-Format in der
Anfrage. trace_id: xxxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx "}
```

**STEP 4 |** Aktualisieren Sie die Zulassungslisten auf Ihren lokalen Servern oder in den Richtlinienregeln für Ihre SaaS-Anwendung und fügen Sie die von Ihnen abgerufenen IP-Adressen hinzu.

## Beispiele für API-Befehle

Verwenden Sie die folgenden Beispiele, wenn Sie Schlüsselwörter und Argumente in der Textdatei (.txt) für den API-Befehl eingeben. Ändern Sie die Optionen in der Textdatei (.txt), um die Ausgabe des Befehls zu ändern. Der Befehl selbst ändert sich hierbei nicht.

| Diese IP-Adressen abrufen | Geben Sie diese Parameter in der Textdatei (.txt) an | Bemerkungen |
|---|---|---|
| **IP-Adressen für mobile Benutzer** | | |
| Alle IP-Adressen mobiler Benutzer | `{"serviceType": "gp_gateway", "addrType": "all", "location": "all"}` | Wird für *addrType* die Einstellung *all* angegeben, bedeutet dies, dass Prisma Access alle Gateway-IP-Adressen mobiler Benutzer abruft. |

 ©2025 Palo Alto Networks, Inc.

| Diese IP-Adressen abrufen | Geben Sie diese Parameter in der Textdatei (.txt) an | Bemerkungen |
|---|---|---|
| | | Wird für *location* die Einstellung *all* angegeben, dann ruft Prisma Access IP-Adressen für alle verfügbaren Standorte ab. Dies gilt auch für Standorte, die Sie nicht eingebunden haben. Prisma Access reserviert IP-Adressen für nicht eingebundene Standorte, damit Sie diese IP-Adressen zu Ihren Zulassungslisten hinzufügen können, bevor Sie sie einbinden. |
| IP-Adressen für eingebundene Standorte mobiler Benutzer | `{"serviceType": "gp_gateway", "addrType": "all", "location": "deployed"}` | Wird als Typ für *location* die Einstellung *deployed* angegeben, ruft Prisma Access ausschließlich die IP-Adressen für die Standorte ab, die Sie beim Onboarding mobiler Benutzer ausgewählt haben. |
| Alle aktiven IP-Adressen für eingebundene Standorte mobiler Benutzer | `{"serviceType": "gp_gateway", "addrType": "active", "location": "deployed"}` | Wird für *addrType* die Einstellung *active* angegeben, ruft Prisma Access ausschließlich die IP-Adressen für Standorte ab, die Sie eingebunden haben. |
| **IP-Adressen des Remote-Netzwerks** | | |
| Abrufen aller Remote-Netzwerk-IP-Adressen | `{"serviceType": "remote_network", "addrType": "all", "location": "all"}` | Mit diesem Befehl können die öffentlichen und die Ausgangs-IP-Adressen von Remote-Netzwerken abgerufen werden, die Sie eingebunden haben. Verwenden Sie für *location* nicht die Einstellung *deployed*. Sie können für *addrType* die Einstellung *active* verwenden, mit der jedoch dieselben Adressen abgerufen werden, die auch abgerufen werden, wenn Sie für *addrType* die Einstellung *all* benutzen. |
| **IP-Adressen des expliziten Proxy** | | |


©2025 Palo Alto Networks, Inc.

| Diese IP-Adressen abrufen | Geben Sie diese Parameter in der Textdatei (.txt) an | Bemerkungen |
|---|---|---|
| Abrufen der ACS-IP-Adressen für bereitgestellte Standorte | `{ "serviceType": "swg_proxy", "location": "deployed", "addrType": "auth_cache_service" }` | Mit diesem Befehl wird die ACS-IP-Adresse für Ihre Bereitstellung mit explizitem Proxy abgerufen. Durch die Eingabe von *addrType* mit der Einstellung *all* werden alle Adresstypen abgerufen (die IP-Adressen des ACS und Load-Balancers des Netzwerks). |
| **IP-Adressen für Remote-Browser-Isolation** | | |
| Abrufen der IP-Adressen für Remote-Browser-Isolation (RBI) für bereitgestellte Standorte | `{"serviceType": "rbi", "location": "all", "addrType": "all"}` | Mit diesem Befehl können die Ausgangs-IP-Adressen für jeden bereitgestellten RBI-Standort abgerufen werden. Sie können diese IP-Adressen zu einer Zulassungsliste hinzufügen, um eine Verbindung zu SaaS-Anwendungen herzustellen. |

## Legacy-Skripte zum Abrufen von IP- und Loopback-Adressen

Die folgende Tabelle zeigt die Schlüsselwörter und Parameter, die in den veralteten API-Skripten in Prisma Access verfügbar sind. Sie enthält außerdem Informationen und Empfehlungen dazu, welche API für die Art Ihrer Bereitstellung verwendet werden soll.

Mit diesen Legacy-Befehlen werden zwei Arten von IP-Adressen abgerufen: *öffentliche IP-Adressen* und *Ausgangs-IP-Adressen*. Wir stellen Ihnen zwei verschiedene Legacy-API-Befehle zur Verfügung, damit Sie alle IP-Adressen abrufen können, die Sie zu einer Zulassungsliste hinzufügen müssen.

- Eine *öffentliche IP-Adresse* ist die Quell-IP-Adresse, die Prisma Access für Anfragen an eine internetbasierte Quelle verwendet. Fügen Sie die öffentliche IP-Adresse zu einer Zulassungsliste in Ihrem Netzwerk hinzu, um Prisma Access Zugriff auf Internetressourcen wie SaaS-Anwendungen oder öffentlich zugängliche Partneranwendungen zu erteilen.

  Bereitstellungen für mobile Benutzer, Remote-Netzwerke und Clean Pipe verwenden öffentliche IP-Adressen.
- Eine *Ausgangs-IP-Adresse* ist eine IP-Adresse, die Prisma Access für den ausgehenden Datenverkehr zum Internet verwendet. Damit auch Prisma Access auf die Internetressourcen zugreifen kann, müssen Sie diese Adressen zu einer Zulassungsliste hinzufügen.

  Prisma Access verwendet Ausgangs-IP-Adressen unter anderem, damit Benutzer Webseiten an einem Prisma Access-Standort in der entsprechend erwarteten Sprache erhalten. Alle

 ©2025 Palo Alto Networks, Inc.

Standorte haben zwar öffentliche IP-Adressen, aber nicht alle verwenden auch Ausgangs-IP-Adressen. Folgende Standorte verwenden keine Ausgangs-IP-Adressen:

- Bahrain
- Belgien
- Frankreich (Nord)
- Frankreich (Süd)
- Hongkong
- Irland
- Südkorea
- Taiwan
- Vereinigtes Königreich

Bereitstellungen für mobile Benutzer, Remote-Netzwerke und Clean Pipe verwenden Ausgangs-IP-Adressen.

| In Bereitstellungen für mobile Benutzer verwendete Befehle | |
|---|---|
| **Befehlsname** | **Bemerkungen** |
| Befehl **get_egress_ip_all=yes**<br>`curl -k -H header-api-key:`*Current-API-Key*`"https://api.gpcloudservice.com/getAddrList/latest?get_egress_ip_all=yes` | Mit diesem Befehl werden alle IP-Adressen abgerufen, die Sie einer Zulassungsliste hinzufügen, um Prisma Access Zugang zu Internetressourcen wie SaaS-Anwendungen oder öffentlich zugänglichen Partneranwendungen zu gewähren. Für diesen Befehl gelten folgende Einschränkungen:<br>• Dieser Befehl kann eine große Anzahl von Adressen (mehr als 200) abrufen. Wenn Ihr Unternehmen diese Anzahl von IP-Adressen nicht zu einer Zulassungsliste hinzufügen kann, können Sie mit den Schlüsselwörtern *gpcs_gp_gw* und *gpcs_gp_portal* nur die IP-Adressen abrufen, die Sie derzeit verwenden. Sie müssen diese Befehle jedoch jedes Mal wiederholen, wenn Sie einen Standort hinzufügen. Im Falle eines Skalierungsereignisses müssen Sie die neuen IP-Adressen außerdem in eine Zulassungsliste eingeben.<br>• Prisma Access listet nicht die Standorte auf, die mit diesen IP-Adressen verknüpft sind. Daher empfehlen wir Ihnen, alle IP-Adressen, die mit diesem Befehl zurückgegeben werden, zu einer Zulassungsliste hinzuzufügen.<br>• Dieser Befehl liefert Ihnen keine Loopback-Adressen. |
| Schlüsselwörter **gpcs_gp_gw** und **gpcs_gp_portal**<br>`curl -k -H header-api-key:`*Current-* | Verwenden Sie diesen Befehl, wenn Ihre Bereitstellung die Anzahl der IP-Adressen begrenzt, die Sie einer Zulassungsliste hinzufügen können. Fügen Sie alle IP-Adressen, die mit diesem Befehl zurückgegeben werden, zu |

 ©2025 Palo Alto Networks, Inc.

| In Bereitstellungen für mobile Benutzer verwendete Befehle | |
|---|---|
| **Befehlsname** | **Bemerkungen** |
| *API-Key*"https://api.gpcloudservice.com/getAddrList/latest?fwType=gpcs_gp_gw \| gpcs_gp_portal&addrType=public_ip \| egress_ip_list \| loopback_ip" | einer Zulassungsliste in Ihrem Netzwerk hinzu. Mit diesem Befehl können Sie auch die Loopback-IP-Adressen abrufen. |

| In Remote-Netzwerkbereitstellungen verwendete Befehle | |
|---|---|
| **Befehlsname** | **Bemerkungen** |
| Schlüsselwort **gpcs_remote_network**<br>curl -k -H header-api-key:*Current-API-Key*"https://api.gpcloudservice.com/getAddrList/latest?fwType=gpcs_remote_network&addrType=public_ip \| egress_ip_list \| loopback_ip" | Suchen Sie mit diesem Befehl nach den IP-Adressen, die Sie einer Zulassungsliste für Remote-Netzwerkbereitstellungen hinzufügen müssen.<br>Sie können diesen Befehl auch verwenden, um die Ausgangs-IP-Adressen für Remote-Netzwerkbereitstellungen zu finden. Die Ausgangs- und IP-Adressen können in einigen Fällen unterschiedlich sein. |

| Befehle, die in Clean Pipe-Bereitstellungen verwendet werden | |
|---|---|
| **Befehlsname** | **Bemerkungen** |
| Schlüsselwort **gpcs_clean_pipe**<br>curl -k -H header-api-key:*Current-API-Key*"https://api.gpcloudservice.com/getAddrList/latest?fwType=gpcs_clean_pipe&addrType=public_ip \| egress_ip_list \| loopback_ip" | Verwenden Sie diesen Befehl, um die IP-Adressen zu finden, die Sie einer Zulassungsliste für Clean Pipe-Bereitstellungen hinzufügen müssen. |

### Abrufen von öffentlichen und Ausgangs-IP-Adressen für Bereitstellungen für mobile Benutzer

Dieses Legacy-Skript wurde durch ein neueres API-Skript ersetzt. Palo Alto Networks empfiehlt, für das Abrufen sämtlicher IP-Adressen mit Ausnahme von Loopback-Adressen das neuere Skript zu verwenden.

Wenn Sie öffentliche IP-Adressen zu Zulassungslisten hinzufügen, um mobilen Benutzern Zugriff auf SaaS oder öffentliche Anwendungen zu gewähren, stellt Prisma Access zwei IP-Adressen für jedes Gateway und jede Portal-IP-Adresse bereit, sodass eine IP-Adresse während einer

 ©2025 Palo Alto Networks, Inc.

Skalierung oder eines anderen Ereignisses verwendet werden kann. Sie können diesen Satz von IP-Adressen vor der Verwendung zu einer Zulassungsliste hinzufügen, um Probleme zu vermeiden, wenn mobile Benutzer während eines Skalierungsereignisses auf SaaS oder öffentliche Anwendungen zugreifen können.

Führen Sie die folgenden Schritte aus, um diese neuen Adressen abzurufen:

**STEP 1 |** Rufen Sie den API-Schlüssel ab, indem Sie **Workflows** > **Prisma Access-Einrichtung** > **Prisma Access** > **Infrastruktureinstellungen** > **Neuen API-Schlüssel generieren**auswählen.

Sie benötigen diesen Schlüssel, um sich bei Prisma Access zu authentifizieren und die Liste der IP-Adressen mit dem unten aufgeführten cURL-Befehl abzurufen. Nur ein Panorama-Administrator oder Superuser kann diesen API-Schlüssel generieren oder darauf zugreifen.

**STEP 2 |** Geben Sie folgenden Befehl ein, um die öffentlichen IP-Adressen des mobilen Benutzers abzurufen:

```
  curl -k -H header-api-key:Current-API-Key "https://
api.gpcloudservice.com/getAddrList/latest?get_egress_ip_all=yes"
```

Dabei ist *Current-API-Key* der Prisma Access-API-Schlüssel.

Beispiel: Verwenden Sie bei dem API-Schlüssel **12345abcde** folgenden API-Befehl, um die öffentliche IP-Adresse für alle Standorte abzurufen:

```
  curl -k -H header-api-key:12345abcde "https://
api.gpcloudservice.com/getAddrList/latest?get_egress_ip_all=yes"
```

### Abrufen von öffentlichen IP-Adressen sowie Loopback- und Ausgangs-IP-Adressen

Führen Sie die folgenden Schritte aus, um öffentliche IP-Adressen sowie Loopback- und Ausgangs-IP-Adressen abzurufen.

**STEP 1 |** Rufen Sie die öffentlichen IP-Adressen, Loopback-IP-Adressen oder beide für Prisma Access ab.

Verwenden Sie den API-Schlüssel und die API-Endpunkt-URL manuell oder in einem Automatisierungsskript:

```
 header-api-key:Current API Key "https://api.gpcloudservice.com/
getAddrList/latest?fwType=$fwType&addrType=$addrType"
```

Dabei müssen Sie „Current API Key“ durch Ihren API-Schlüssel ersetzen und eines oder beide der folgenden Schlüsselwörter und Argumente verwenden:

| Schlüsselwort | Beschreibung |
|---|---|
| Schlüsselwort **fwType** | |
| **gpcs_gp_gw** | Ruft Prisma Access-Gateway-IP-Adressen ab (für Bereitstellungen für mobile Benutzer). |

 ©2025 Palo Alto Networks, Inc.

| Schlüsselwort | Beschreibung |
|---|---|
| **gpcs_gp_portal** | Ruft Prisma Access-Portal-IP-Adressen ab (für Bereitstellungen für mobile Benutzer). |
| **gpcs_remote_network** | Ruft Prisma Access-Remote-Netzwerk-IP-Adressen ab (für Remote-Netzwerkbereitstellungen). |
| **gpcs_clean_pipe** | Ruft Prisma Access-Clean-Pipe-IP-Adressen ab. |
| Schlüsselwort **addrType** | |
| **public_ip** | Ruft die Quell-IP-Adressen ab, die Prisma Access für Anfragen an eine internetbasierte Quelle verwendet.<br>Bei Standorten mobiler Benutzer listet Prisma Access die IP-Adressen nach Standort auf. Bei Remote-Netzwerken listet Prisma Access die IP-Adressen nach Namen der Remote-Netzwerke auf. |
| **egress_ip_list** | Ruft die IP-Adressen ab, die Prisma Access mit öffentlichen IP-Adressen für zusätzlichen ausgehenden Datenverkehr zum Internet verwendet.<br>Bei Standorten mobiler Benutzer listet Prisma Access die IP-Adressen nach Standort auf. Bei Remote-Netzwerken listet Prisma Access die IP-Adressen nach Namen der Remote-Netzwerke auf. |
| **loopback_ip** | Ruft die Quell-IP-Adressen ab, die von Prisma Access für Anfragen an eine interne Quelle verwendet werden (z. B. einen RADIUS- oder Active Directory-Server) und wird über das Infrastruktursubnetz zugewiesen. |

Wenn Sie kein Schlüsselwort angeben, ruft Prisma Access alle IP-Adressen ab.

Sie können beispielsweise versuchen, folgenden cURL-Befehl auszuführen, um die Liste der öffentlichen IP-Adressen für sämtliche Remote-Netzwerke manuell abzurufen:

```
curl -k -H header-api-
key:1234y9ydxb__0UmxetVTbC8XTyFMaoT4RBZBKBjfX419YVufeFG7
 "https://api.gpcloudservice.com/getAddrList/latest?
fwType=gpcs_remote_network&addrType=public_ip"
```

Alternativ können Sie ein einfaches Python-Skript verwenden, um die Liste aller IP-Adressen abzurufen. Beispiel:

```
  #!/usr/bin/python import subprocess import json api_key
 = '1234y9ydxb__0UmxetVTbC8XTyFMaoT4RBZBKBjfX419YVufeFG7'
 # Durch Ihren Schlüssel ersetzen api_end_point = 'https://
api.gpcloudservice.com/getAddrList/latest' # Bei diesem Aufruf
 werden IP-Adressen für alle Ihre Prisma Access-Firewalls
 abgerufen args = ['curl', '-k', '-H', 'header-api-key:' + api_key,
```

 ©2025 Palo Alto Networks, Inc.

```
api_end_point] p = subprocess.Popen(args, stdout=subprocess.PIPE)
output = p.communicate() dout = json.loads(output[0]) addrStrList
= dout['result']['addrList'] addrList = [] for addr_str
in addrStrList: addrList.append(addr_str.split(":")[1])
print(addrList)
```

**STEP 2 |** Aktualisieren Sie die Zulassungslisten auf Ihren lokalen Servern oder in den Richtlinienregeln für Ihre SaaS-Anwendung und fügen Sie die von Ihnen abgerufenen IP-Adressen hinzu.

## Vorabzuweisung von IP-Adressen für Standorte mobiler Benutzer

Prisma Access verwendet für GlobalProtect-Bereitstellungen für mobile Benutzer Gateway- und Portal-IP-Adressen und für Bereitstellungen mit explizitem Proxy für mobile Benutzer IP-Adressen des Authentication Cache Service (ACS) und des Load-Balancers des Netzwerks. GlobalProtect-IP-Adressen für mobile Benutzer werden als *Ausgangs-IP-Adressen* bezeichnet. Wenn Sie die IP-Adressen mobiler Benutzer vor dem Onboarding des Standorts vorab zuweisen müssen (z. B. wenn Ihre Organisation die IP-Adressen für GlobalProtect-Bereitstellungen für mobile Benutzer zu Zulassungslisten hinzufügen muss, damit mobile Benutzer Zugriff auf externe SaaS-Anwendungen haben), können Sie ein API-Skript ausführen, damit Prisma Access diese IP-Adressen für einen Standort vor dem Onboarding vorab zuweist. Sie können dann die Ausgangs-IP-Adressen des Standorts zu den Zulassungslisten Ihrer Organisation hinzufügen, bevor Sie den Standort einbinden.

Die API-Antwort umfasst auch die öffentlichen IP-Pool-Subnetze für die Ausgangs-IP-Adressen des angefragten Standorts. Die Ausgangs-IP-Adressen aller Standorte, die Sie hinzufügen, sind Teil dieses Subnetzes. Das Hinzufügen der Subnetze zu Ihren Zulassungslisten ermöglicht zukünftige Standortzusätze, ohne dass weitere Änderungen an der Zulassungsliste vorgenommen werden müssen.

Prisma Access weist Ihre IP-Adressen und Subnetze nur dann vorab zu, wenn Sie sie über das API-Skript anfordern. Nachdem Sie das Skript für die Vorabzuweisung ausgeführt haben, sind diese 90 Tage gültig. Diese IP-Adressen und Subnetze sind eindeutig, werden nicht geteilt und sind während der Gültigkeitsdauer für Ihre Prisma Access-Bereitstellung bestimmt. Sie müssen Ihre Standorte einbinden, bevor der Gültigkeitszeitraum endet. Andernfalls verlieren Sie die Adressen. Führen Sie das API-Skript aus, um jederzeit nach dem Gültigkeitszeitraum zu suchen.

*Palo Alto Networks empfiehlt, IP-Adressen nur für Standorte vorab zuzuweisen, die Sie später einbinden möchten.*

Führen Sie die folgenden Schritte aus, um IP-Adressen vorab zuzuweisen.

**STEP 1 |** Rufen Sie den Prisma Access-API-Schlüssel ab.

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Weisen Sie die Ausgangs-IP-Adressen mobiler Benutzer vorab zu, indem Sie eine Textdatei (.txt) erstellen und folgende Optionen in der von Ihnen erstellten Textdatei (.txt) angeben.

Geben Sie folgenden Text in die Textdatei (.txt) ein:

- **GlobalProtect-Bereitstellungen für mobile Benutzer:**

```
 { "actionType": "pre_allocate", "serviceType": "gp_gateway",
"location": ["location"] }
```

- **Bereitstellungen mit explizitem Proxy für mobile Benutzer:**

```
{ "actionType": "pre_allocate", "serviceType": "swg_proxy",
 "location": ["location"]}
```

Dabei steht *location* für den Standort von Prisma Access, an dem Sie die IP-Adressen vorab zuweisen möchten.

Geben Sie maximal 12 Standorte ein. Die Eingabe von mehr als 12 Standorten kann zu Timeoutfehlern führen, wenn Prisma Access die vorab zugewiesenen IP-Adressen abruft.

**STEP 3 |** Geben Sie diesen cURL-Befehl ein.

**STEP 4 |** Rufen Sie die von Ihnen angeforderten IP-Adressen und Subnetze einschließlich ihrer Gültigkeitsdauer ab, indem Sie die Textdatei (.txt) erneut öffnen, die vorhandenen Informationen entfernen und sie bearbeiten.

- **GlobalProtect-Bereitstellungen für mobile Benutzer:**
  - Geben Sie folgenden Text in die Textdatei (.txt) ein, wenn Sie Prisma Access dazu auffordern möchten, alle vorab zugewiesenen IP-Adressen abzurufen.

```
 {"serviceType": "all", "addrType": "pre_allocated",
"location": "all"}
```

  - Wenn Sie Prisma Access dazu auffordern möchten, alle vorab zugewiesenen IP-Adressen für Prisma Access-Gateways für einen bestimmten Standort abzurufen, geben Sie die gleichen Informationen in die Textdatei (.txt) ein, ersetzen Sie darin jedoch `all` durch `gp_gateway`.
  - Wenn Sie Prisma Access dazu auffordern möchten, alle vorab zugewiesenen IP-Adressen für Prisma Access-Portale für einen bestimmten Standort abzurufen, geben Sie die

 ©2025 Palo Alto Networks, Inc.

gleichen Informationen in die Textdatei (.txt) ein, ersetzen Sie darin jedoch `all` durch `gp_portal`.

- **Bereitstellungen mit explizitem Proxy für mobile Benutzer:**

  Geben Sie folgenden Text in die Textdatei (.txt) ein, wenn Sie Prisma Access dazu auffordern möchten, alle IP-Adressen vorab zuzuweisen, die Sie zu Zulassungslisten für eine Bereitstellung mit explizitem Proxy hinzufügen müssen.

```
{"actionType": "pre_allocate", "serviceType": "swg_proxy",
 "location": ["all"]}
```

Palo Alto Networks empfiehlt Ihnen, `all` einzugeben, damit Sie alle erforderlichen vorab zugewiesenen Ausgangs-IP-Adressen abrufen können, die Ihren Zulassungslisten hinzugefügt werden sollen.

*Bei GlobalProtect-Bereitstellungen für mobile Benutzer kann der API-Befehl eine große Menge an Informationen zurückgeben. Wenn Sie Python installiert haben, können Sie am Ende des cURL-Befehls | `python -m json.tool` hinzufügen, um die Ausgabe besser lesbar zu machen.*

**STEP 5 |** Geben Sie diesen cURL-Befehl erneut ein, um die vorab zugewiesenen Adressen abzurufen.

Prisma Access gibt die Informationen im folgenden Format zurück:

```
    "result": [ { "zone": "prisma-access-zone1", "addresses":
 [["ip-address1","ip-address2"] "zone_subnet" : [subnet-and-
mask1","subnet-and-mask2"] "address_details":[ "address":"ip-
address1", "service_type":"service-type", "addressType":"pre-
allocated", "expiring_in" : "validity-period" }, {"address":"ip-
address2", "service_type":"gp_gateway", "addressType":"pre-
allocation", "validity_period_remaining" : "90 days" } , },
```

Dabei stehen die Variablen für folgende API-Befehlsausgabe:

| Variable | Erklärung |
|---|---|
| *prisma-access-zone1* | Der Prisma Access-Standort, für den vorab zugewiesene IP-Adressen abgerufen wurden. |
| *ip-address1* und *ip-address2* | Die Ausgangs-IP-Adressen, die Prisma Access für den angegebenen Standort vorab zugewiesen hat.<br>Prisma Access ruft für jeden Standort zwei IP-Adressen ab. Sie müssen beide IP-Adressen zu Ihren Zulassungslisten hinzufügen. |
| *subnet-and-mask1* und *subnet-and-mask2* | Die Subnetze, die Prisma Access für die Ausgangs-IP-Adressen in Ihrer Bereitstellung vorab zugewiesen und reserviert hat. |

 ©2025 Palo Alto Networks, Inc.

| Variable | Erklärung |
|---|---|
| *service-type* | Der Typ der vorab zugewiesenen Ausgangs-IP-Adresse (`gp_portal` bei einem Prisma Access-Portal oder `gp_gateway` bei einem Prisma Access-Gateway). |
| *validity-period* | Die verbleibende Zeit in Tagen, die die vorab zugewiesene IP-Adresse gültig ist.<br>Binden Sie den Standort Ihrer mobilen Benutzer ein, bevor der Gültigkeitszeitraum der IP-Adressen endet. Wenn die vorab zugewiesenen IP-Adressen ablaufen, können Sie das API-Skript erneut ausführen, um einen anderen Satz vorab zugewiesener IP-Adressen abzurufen. |

Wenn Sie versuchen, IP-Adressen für Standorte vorab zuzuweisen, die eines der folgenden Kriterien erfüllen, erhalten Sie möglicherweise eine Fehlermeldung:

- Sie haben das Onboarding des Standorts bereits durchgeführt.
- Sie haben das Onboarding abgeschlossen und den Standort anschließend gelöscht.

  Geben Sie in diesem Fall folgenden Text in die Textdatei (.txt) ein, um die GlobalProtect-IP-Adressen für mobile Benutzer für den Standort abzurufen:

```
 {"serviceType": "gp_gateway", "addrType": "all", "location":
"all"}
```

- Sie haben die maximale Anzahl an Standorten mobiler Benutzer erreicht, die durch Ihre Lizenz zulässig sind. Sie können keine weiteren Standorte hinzufügen.
- Sie haben den Standortnamen falsch eingegeben.
- Sie haben einen anderen **serviceType** als **gp_gateway** eingegeben.
- Sie haben einen anderen **actionType** als **pre_allocate** eingegeben.

## Einrichten von Benachrichtigungen zur Änderung von Prisma Access-IP-Adressen

Wenn Sie über Änderungen der öffentlichen IP-Adresse für Remote-Netzwerke und der Loopback-IP-Adresse für Dienstverbindungen, Remote-Netzwerkverbindungen und mobile Benutzer benachrichtigt werden möchten, können Sie eine URL angeben, über die Sie über eine Änderung benachrichtigt werden können. Prisma Access verwendet eine HTTP-POST-Anfrage zum Senden der Benachrichtigung. Diese POST-Anfrage enthält die folgenden Benachrichtigungsdaten im JSON-Format:

```
 {"addrType": "public_ip", "addrChangeType": "add", "utc_timestamp":
"2019-01-31 23:08:19.383894", "text": "Address List Change
Notification"}
```

 ©2025 Palo Alto Networks, Inc.

```
 {"addrType": "public_ip", "addrChangeType": "delete",
"utc_timestamp": "2019-01-31 23:13:35.882151", "text": "Address List
Change Notification"}
```

```
 {"addrType": "loopback_ip", "addrChangeType": "update",
"utc_timestamp": "2019-01-31 23:29:27.100329", "text": "2018-05-11
23:29:27.100329"}
```

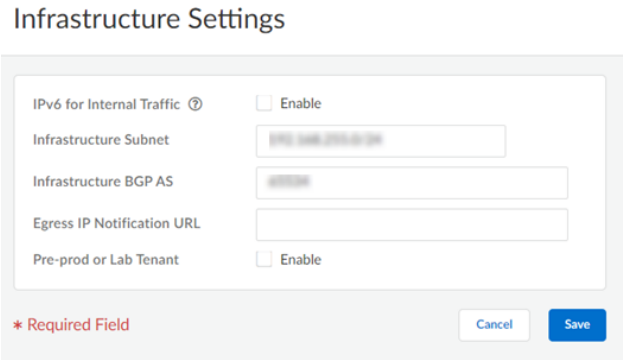
Wenn Sie eine Benachrichtigung erhalten, müssen Sie einen zweistufigen Prozess befolgen. Zunächst müssen Sie die IP- oder Loopback-Adressen manuell oder programmgesteuert abrufen. Anschließend müssen Sie die IP-Adressen in der entsprechenden Zulassungsliste Ihrer Organisation aktualisieren, um sicherzustellen, dass es für die Benutzer zu keiner Dienstunterbrechung kommt.

*Prisma Access sendet diese Benachrichtigung einige Sekunden, bevor die neue IP-Adresse aktiv wird. Wir empfehlen, dass Sie Automatisierungsskripte verwenden, um die neuen IP-Adressen abzurufen und zu einer Zulassungsliste in Ihrem Netzwerk hinzuzufügen.*

Führen Sie die folgenden Schritte aus, um eine Benachrichtigungs-URL für eine Ausgangs-IP hinzuzufügen.

**STEP 1 |** Gehen Sie zu **Workflows** > **Prisma Access-Einrichtung** > **Prisma Access** > **Infrastruktureinstellungen**.

**STEP 2 |** Fügen Sie eine **Benachrichtigungs-URL für Ausgangs-IP** hinzu, über die Sie über Änderungen der IP-Adresse in Ihrer Prisma Access-Infrastruktur benachrichtigt werden können.




Sie können eine IP-Adresse oder einen FQDN für einen HTTP- oder HTTPS-Webdienst angeben, der auf Änderungsbenachrichtigungen wartet. Prisma Access sendet diese Benachrichtigungen aus dem Internet über eine öffentliche IP-Adresse.

Sie müssen Ihre Konfiguration nicht per Push übertragen, damit die Benachrichtigungs-URL wirksam wird.

## Abrufen der IP-Adressen für Prisma Access (Panorama)

Wenn Sie IP-Adressen Ihrer Prisma Access-Infrastruktur manuell zu einer Zulassungsliste in Ihrem Netzwerk hinzufügen oder wenn Sie ein Automatisierungsskript verwenden, um IP-basierte Beschränkungen durchzusetzen, um den eingehenden Zugriff auf Unternehmensanwendungen

 ©2025 Palo Alto Networks, Inc.

zu begrenzen, sollten Sie verstehen, was diese Adressen bewirken und warum Sie sie zulassen müssen. Zudem sollten Sie wissen, welche Aufgaben Sie ausführen müssen, um diese abzurufen.

Prisma Access stellt diese IP-Adressen erst nach Abschluss Ihrer Prisma Access-Konfiguration bereit. Nach Abschluss der Bereitstellung rufen Sie diese IP-Adressen über ein API-Skript ab. Das API-Skript verwendet einen API-Schlüssel, den Sie von der Prisma Access-Benutzeroberfläche erhalten, und eine von Ihnen erstellte Textdatei (.txt), die die Adressen enthält, die Sie abrufen möchten.

*Wenn Sie über eine GlobalProtect-Bereitstellung für mobile Benutzer verfügen, können Sie die Prisma Access-Benutzeroberfläche anstelle dieser API verwenden, um die Zuweisung öffentlicher IP-Adressen zu verwalten und zu bestätigen, dass die IP-Adressen zu Ihren Zulassungslisten hinzugefügt wurden, bevor Prisma Access die IP-Adressen freigibt. Auf diese Weise stellt Prisma Access nur die von Ihnen zugelassenen IP-Adressen zur Verfügung.*

In der folgenden Tabelle finden Sie eine Liste der IP-Adressen, die Prisma Access für jeden Bereitstellungstyp verwendet, zusammen mit dem Schlüsselwort, das Sie beim Ausführen des API-Skripts zum Abrufen der IP-Adressen verwenden. Darüber hinaus wird angegeben, ob Sie diese zu den Zulassungslisten Ihrer Organisation hinzufügen sollten oder nicht.

| Bereitstellungstyp | IP-Adresstyp | Beschreibung |
|---|---|---|
| **Mobile Benutzer – GlobalProtect** | Prisma Access-Gateway (**gp_gateway**) | Gateway-IP-Adressen. Sie müssen Gateway- und Portal-IP-Adressen zu Zulassungslisten für Ihre Bereitstellungen für mobile Benutzer hinzufügen.<br><br>Mobile Benutzer verbinden sich mit einem Prisma Access-Gateway, um auf interne oder Internetressourcen wie SaaS oder öffentliche Anwendungen zuzugreifen, für die Sie Zugriff gewährt haben.<br><br>Für mobile Benutzer weist Prisma Access während der ersten Bereitstellung jedem der von Ihnen bereitgestellten Standorte zwei IP-Adressen zu. |
| | Prisma Access-Portal (**gp_portal**) | Portal-IP-Adressen. Sie müssen Gateway- und Portal-IP-Adressen zu Zulassungslisten für Ihre |

 ©2025 Palo Alto Networks, Inc.

| Bereitstellungstyp | IP-Adresstyp | Beschreibung |
|---|---|---|
| | | Bereitstellungen für mobile Benutzer hinzufügen.<br><br>Mobile Benutzer melden sich im Prisma Access-Portal an, um ihre Erstkonfiguration und ihren Gateway-Standort zu erhalten. |
| | Loopback-IP-Adressen | Die Quell-IP-Adresse, die von Prisma Access für Anfragen an eine interne Quelle verwendet und von der Konfigurieren Sie die Prisma Access-Dienstinfrastruktur (Panorama) zugewiesen wird. Fügen Sie die Loopback-IP-Adresse zu einer Zulassungsliste in Ihrem Netzwerk hinzu, damit Prisma Access auf interne Ressourcen wie RADIUS- oder Active Directory-Authentifizierungsserver zugreifen kann.<br><br>Da sich Loopback-IP-Adressen ändern können, empfiehlt Palo Alto Networks, alle IP-Adressen des gesamten Infrastruktursubnetzes in Ihrem Netzwerk zuzulassen. Wählen Sie **Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Dienstinfrastruktur** aus, um nach dem Infrastrukursubnetz zu suchen. Das Subnetz wird im Bereich **Infrastruktursubnetz** angezeigt.<br><br>Verwenden Sie das Legacy-API-Skript, um Loopback-IP-Adressen abzurufen. |
| **Mobile Benutzer – Expliziter Proxy** | Authentication Cache Service (ACS) | Die Adresse für den Prisma Access-Dienst, der den Authentifizierungsstatus der |

 ©2025 Palo Alto Networks, Inc.

| Bereitstellungstyp | IP-Adresstyp | Beschreibung |
|---|---|---|
| | | Benutzer von explizitem Proxy speichert.<br><br>Diese Adresse wird nur für explizite Proxys für mobile Benutzer verwendet. |
| | Load-Balancer des Netzwerks | Die Adresse, die Prisma Access für den Load-Balancer des Netzwerks für explizite Proxys verwendet.<br><br>Diese Adresse wird nur für explizite Proxys für mobile Benutzer verwendet. |
| **Remote-Netzwerk** | IP-Adressen des Remote-Netzwerks (**remote_network**) | Die **Dienst-IP-Adressen**, die Prisma Access für die Prisma Access-Remote-Netzwerkverbindung zuweist, und Remote-Netzwerke: Zuweisung von Dienst-IP-Adressen und Ausgangs-IP-Adressen, die Prisma Access verwendet, um sicherzustellen, dass Remote-Netzwerkbenutzer die richtige Standardsprache für ihre Region erhalten. Fügen Sie diese Adressen zu Zulassungslisten in Ihrem Netzwerk hinzu, um Prisma Access zu Internetressourcen zuzuordnen. |
| | Loopback-IP-Adressen | Die Quell-IP-Adresse, die von Prisma Access für Anfragen an eine interne Quelle verwendet und von der Konfigurieren Sie die Prisma Access-Dienstinfrastruktur (Panorama) zugewiesen wird. Fügen Sie die Loopback-IP-Adresse zu einer Zulassungsliste hinzu, damit Prisma Access auf interne Ressourcen wie RADIUS- oder Active Directory-Authentifizierungsserver |

 ©2025 Palo Alto Networks, Inc.

| Bereitstellungstyp | IP-Adresstyp | Beschreibung |
|---|---|---|
| | | zugreifen kann. Verwenden Sie das Legacy-API-Skript, um Loopback-IP-Adressen abzurufen. |
| **Clean Pipe** | Clean Pipe-IP-Adressen (**clean_pipe**) | Fügen Sie diese IP-Adressen zu einer Zulassungsliste hinzu, um dem Clean Pipe-Dienst Zugriff auf Internetressourcen zu gewähren. |
| | Loopback-IP-Adressen | Die Quell-IP-Adresse, die von Prisma Access für Anfragen an eine interne Quelle verwendet und von der Konfigurieren Sie die Prisma Access-Dienstinfrastruktur (Panorama) zugewiesen wird. Fügen Sie die Loopback-IP-Adresse zu einer Zulassungsliste hinzu, damit Prisma Access auf interne Ressourcen wie RADIUS- oder Active Directory-Authentifizierungsserver zugreifen kann. Verwenden Sie das Legacy-API-Skript, um Loopback-IP-Adressen abzurufen. |

## Ausführen des API-Skripts zum Abrufen von Prisma Access-IP-Adressen

Prisma Access stellt ein API-Skript bereit, mit dem Sie die öffentlichen und privaten IP-Adressen abrufen können, die es in seiner Infrastruktur verwendet. Wenn Sie öffentliche IP-Adressen zu Zulassungslisten im Netzwerk Ihrer Organisation hinzufügen müssen, führen Sie die folgenden Schritte aus, um diese IP-Adressen mit dem API-Skript abzurufen.

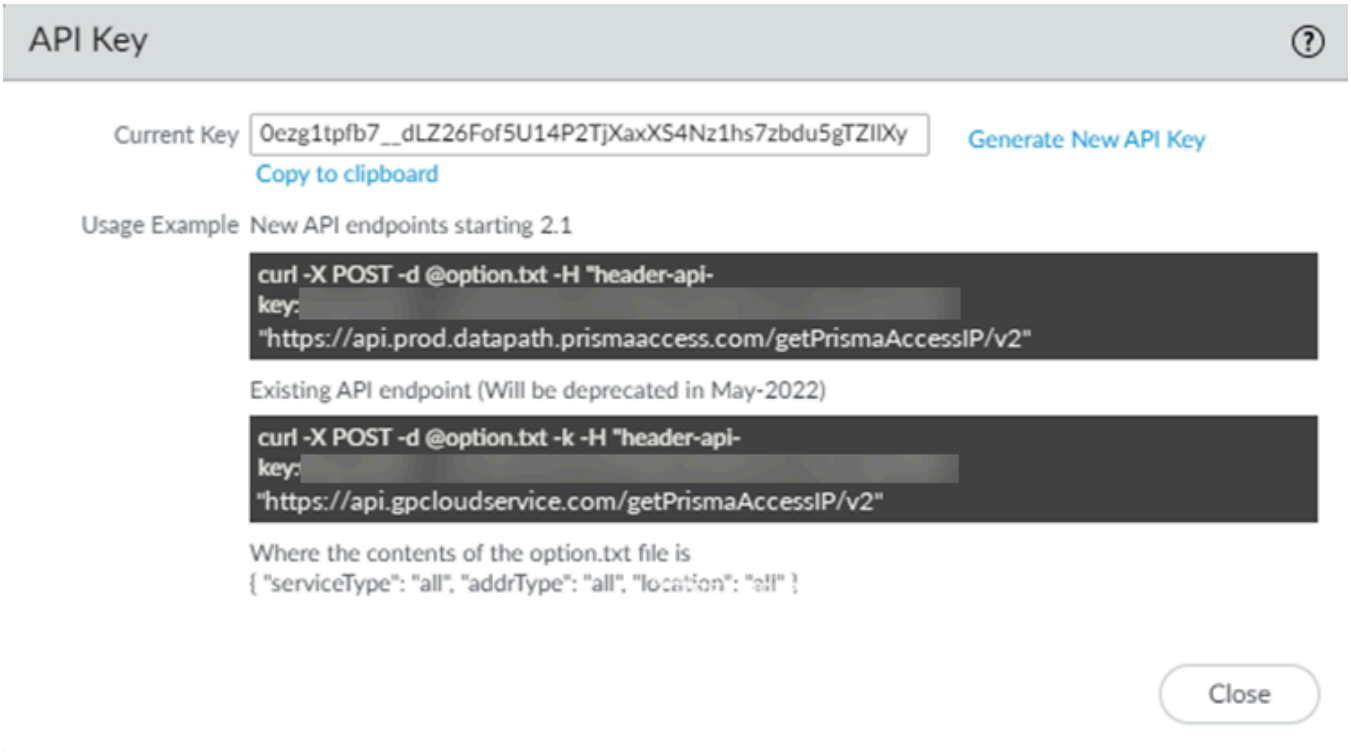
*Mit diesem Befehl werden keine Loopback-Adressen abgerufen. Verwenden Sie zum Abrufen von Loopback-IP-Adressen die* Legacy-API.


©2025 Palo Alto Networks, Inc.

**STEP 1 |** Rufen Sie den API-Schlüssel ab.

Sie benötigen diesen Schlüssel, um sich bei Prisma Access zu authentifizieren und die Liste der IP-Adressen mit dem API-Befehl abzurufen. Nur ein Panorama-Administrator oder Superuser kann diesen API-Schlüssel generieren oder darauf zugreifen.

1. Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Diensteinrichtung** aus.
2. Wählen Sie **API-Schlüssel generieren** aus.




Wenn Sie bereits einen API-Schlüssel generiert haben, wird der **Aktuelle Schlüssel** angezeigt. Wenn Sie noch keinen Schlüssel generiert haben oder den vorhandenen Schlüssel ersetzen möchten, um die Überprüfung der Audit- oder Compliance-Prüfung für die Schlüsselrotation zu erfüllen, klicken Sie für den Erhalt eines neuen Schlüssels auf **Neuen API-Schlüssel generieren**.

**STEP 2 |** Erstellen Sie eine Textdatei (.txt) und legen Sie die API-Befehlsoptionen in die Datei.

Die Verwendung des API-Befehls ist ein zweistufiger Prozess. Zuerst erstellen Sie eine Textdatei (.txt), in der die Parameter für die abzurufenden IP-Adressen angegeben sind, und speichern die Datei in einem Ordner, der von dem Ort aus erreichbar ist, an dem Sie den Befehl ausführen. Anschließend führen Sie die API aus und geben den Namen und Speicherort der Textdatei (.txt) an, die Sie im Befehl erstellt haben.

Geben Sie folgende Schlüsselwörter und Argumente in der Textdatei (.txt) an. Siehe API-Beispiele zum Abrufen von Prisma Access-IP-Adressen für Beispiele. Bei den Beispielen in

 ©2025 Palo Alto Networks, Inc.

diesem Dokument wird der Dateiname **options.txt** verwendet. Solange Sie im Befehl darauf verweisen, können Sie aber einen beliebigen Dateinamen angeben.

| Argument | Mögliche Auswahl (Schlüsselwörter) | Bemerkungen |
|---|---|---|
| **serviceType** | **all**<br>**remote_network**<br>**gp_gateway**<br>**gp_portal**<br>**clean_pipe**<br>**swg_proxy**<br>**rbi** | **all** – Ruft IP-Adressen ab, die Sie zu einer Zulassungsliste für alle Diensttypen hinzufügen müssen (Remote-Netzwerke, mobile Benutzer – sowohl Gateways als auch Portale – und Clean Pipe, abhängig von Ihrer Bereitstellung).<br>**remote_network** – Ruft IP-Adressen ab, die Sie zu einer Zulassungsliste für Remote-Netzwerkbereitstellungen hinzufügen müssen.<br>**gp_gateway** – Ruft die GlobalProtect-Gateway-IP-Adressen für mobile Benutzer ab, die Sie zu einer Zulassungsliste für Bereitstellungen für mobile Benutzer hinzufügen müssen.<br>**gp_portal** – Ruft die IP-Adressen des GlobalProtect-Portals für mobile Benutzer ab, die Sie zu einer Zulassungsliste für Bereitstellungen für mobile Benutzer hinzufügen müssen.<br>**clean_pipe** – Ruft die IP-Adressen ab, die Sie zu einer Zulassungsliste für Clean Pipe-Bereitstellungen hinzufügen müssen.<br>**swg_proxy** – Ruft die Ausgangs-IP-Adressen für die einzelnen bereitgestellten Standorte mit explizitem Proxy, den Authentication Cache Service (ACS) und die Load-Balancer des Netzwerks ab. |

 ©2025 Palo Alto Networks, Inc.

| Argument | Mögliche Auswahl (Schlüsselwörter) | Bemerkungen |
|---|---|---|
| | | **rbi** – Ruft die Ausgangs-IP-Adressen ab, die Sie zu einer Zulassungsliste für RBI-Bereitstellungen (Remote-Browser-Isolation) hinzufügen müssen, um eine Verbindung zu SaaS-Anwendungen herzustellen. |
| **addrType** | **all**<br>**aktiv**<br>**service_ip**<br>**auth_cache_service**<br>**network_load_balancer** | **all** oder **active** – Ruft alle IP-Adressen ab, die Sie zu einer Zulassungsliste hinzufügen müssen.<br>Diese API ruft keine Loopback-IP-Adressen ab. Verwenden Sie die Legacy-API, um Loopback-IP-Adressen abzurufen.<br>**service_ip** – Ruft die **Dienst-IP-Adresse** ab, die Sie als Peer-IP-Adresse verwenden, wenn Sie den IPSec-Tunnel für die Remote-Netzwerkverbindung einrichten.<br>**auth_cache_service** – Ruft die IP-Adresse für den ACS des expliziten Proxy ab (gilt nur für Bereitstellungen mit explizitem Proxy).<br>**network_load_balancer** – Ruft die IP-Adresse für den Load-Balancer des Netzwerks für explizite Proxys ab (gilt nur für Bereitstellungen mit explizitem Proxy). |
| **actionType** | **pre_allocate** | Nur Bereitstellungen für mobile Benutzer – Ein **actionType** von **pre_allocate** ermöglicht Ihnen das Abrufen von IP-Adressen oder Subnetzen für Prisma Access-Gateways und -Portale für Bereitstellungen für mobile |

 ©2025 Palo Alto Networks, Inc.

| Argument | Mögliche Auswahl (Schlüsselwörter) | Bemerkungen |
|---|---|---|
| | | Benutzer. Verwenden Sie diesen mit einem **serviceType** von **gp_gateway,** um vorab zugewiesene Gateway-IP-Adressen abzurufen, und einem **serviceType** von **gp_portal,** um vorab zugewiesene Portal-IP-Adressen abzurufen.<br><br>Durch das Abrufen der vorab zugewiesenen IP-Adressen können Sie die Gateway- und Portal-IP-Adressen zu den Zulassungslisten Ihrer Organisation hinzufügen, bevor Sie Standorte mobiler Benutzer einbinden. Dadurch wiederum wird mobilen Benutzern unmittelbar nach dem Einbinden der Standorte Zugriff auf externe SaaS-Apps gewährt. |
| **location** | **all**<br><br>**deployed** | **all** – Ruft die IP-Adressen von allen Standorten ab. Bei Bereitstellungen für mobile Benutzer ruft dieses Schlüsselwort die IP-Adressen sowohl für Standorte ab, die Sie während des Onboardings hinzugefügt haben, als auch für Standorte, die Sie nicht hinzugefügt haben.<br><br>**deployed** – Ruft IP-Adressen an allen Standorten ab, die Sie beim Onboarding mobiler Benutzer hinzugefügt haben.<br><br>Dieses Schlüsselwort gilt nur für Bereitstellungen für mobile Benutzer. Prisma Access weist während der Bereitstellung jedem Standort mobiler Benutzer IP-Adressen zu, auch wenn Sie diesen Standort beim Onboarding mobiler Benutzer nicht |

 ©2025 Palo Alto Networks, Inc.

| Argument | Mögliche Auswahl (Schlüsselwörter) | Bemerkungen |
|---|---|---|
| | | ausgewählt haben. Wenn Sie **all** angeben, ruft der API-Befehl die IP-Adressen für alle Standorte mobiler Benutzer ab, einschließlich derjenigen, die Sie nicht für die Bereitstellung ausgewählt haben. Wenn Sie **deployed** angeben, werden mit dem API-Befehl nur die IP-Adressen für die Standorte abgerufen, die Sie beim Onboarding ausgewählt haben. |

Geben Sie die Optionen in der Textdatei (.txt) im folgenden Format an:

```
 { "serviceType": "service-type", "addrType": "address-type",
"location": "location" }
```

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Geben Sie folgenden Befehl ein, um die IP-Adressen abzurufen:

- Geben Sie folgenden Befehl ein, um die neuere API zu verwenden, die in Prisma Access 2.1 eingeführt wurde:

```
curl -X POST --data @option.txt -H header-api-key:Current-API-Key "https://api.prod.datapath.prismaaccess.com/getPrismaAccessIP/v2"
```



*Ab Mai 2023 verwenden einige von Panorama verwaltete Bereitstellungen https://api.prod6.datapath.prismaaccess.com/getPrismaAccessIP/v2 (beachten Sie das `prod6` in der URL anstelle von `prod`).*

- Geben Sie folgenden Befehl ein, um die Legacy-API zu verwenden. Dieser Befehl verwendet einen älteren API-Endpunkt, der seit Mai 2022 nicht mehr unterstützt wird:

```
curl -X POST --data @option.txt -k -H header-api-key:Current-API-Key "https://api.gpcloudservice.com/getPrismaAccessIP/v2"
```

Dabei ist *option.txt* die Textdatei (.txt), die Sie in einem vorherigen Schritt erstellt haben, und *Current-API-Key* der Prisma Access-API-Schlüssel.

Beispiel: Wenn der Name der Textdatei **option.txt** und der API-Schlüssel **12345abcde** lautet, verwenden Sie den folgenden API-Befehl, um die öffentliche IP-Adresse für alle Standorte abzurufen:

```
curl -X POST --data @option.txt -H header-api-key:12345abcde "https://api.prod.datapath.prismaaccess.com/getPrismaAccessIP/v2"
```



*Der API-Befehl kann eine große Menge an Informationen zurückgeben. Wenn Sie Python installiert haben, können Sie am Ende des cURL-Befehls `| python -m json.tool` hinzufügen, um die Ausgabe besser lesbar zu machen.*

Der API-Befehl gibt die Adressen im folgenden Format zurück:

```
{"result": [ { "address_details": [ { "address": "1.2.3.4" "allow_listed": false "addressType": "address-type" "serviceType":
```

 ©2025 Palo Alto Networks, Inc.

```
 "service-type" } ], "addresses": [ "1.2.3.4" ] "zone": "zone-
name", "zone_subnet": [zone-subnet ] }, "status": "erfolg"
```

Dabei gilt:

- **address_details** zeigt die Details der Adresse für jeden Standort an.
  - **serviceType** zeigt die Art der IP-Adresse an (entweder Remote-Netzwerk (**remote_network**), Prisma Access-Gateway (**gp_gateway**), Prisma Access-Portal (**gp_portal**), Clean Pipe (**clean_pipe**) oder Remote-Browser-Isolation (**rbi**).
  - **addressType** gibt den Typ der Adresse an, die mit dem Schlüsselwort `addrType` angegeben wurde (entweder **aktiv** oder **vorab zugewiesen**, wenn Sie IP-Adressen für Standorte mobiler Benutzer vorab zuweisen).
  - **address** zeigt die IP-Adresse an, die Sie zu Ihren Zulassungslisten hinzufügen müssen.

    Wenn die API mehrere IP-Adressen zurückgibt, fasst Prisma Access die IP-Adressen im Feld **addresses** zusammen.
- **addresses** listet alle IP-Adressen für den Standort auf, die Sie zu Ihren Zulassungslisten hinzufügen müssen.
- **zone** ist der den IP-Adressen zugeordnete Prisma Access-Standort.
- **zone_subnet** ist das Subnetz für Gateways und Portale für mobile Benutzer. Prisma Access stellt dieses Subnetz auch zur Verfügung, wenn Sie vorab IP-Adressen für Standorte mobiler Benutzer zuweisen.

Wenn Probleme mit den Optionen in der Textdatei (.txt) auftreten, gibt die API einen Fehler ähnlich dem folgenden zurück:

```
 {"status": "error","result": "Ungültiges JSON-Format in der
Anfrage. trace_id: xxxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx "}
```

**STEP 4 |** Aktualisieren Sie die Zulassungslisten auf Ihren lokalen Servern oder in den Richtlinienregeln für Ihre SaaS-Anwendung und fügen Sie die von Ihnen abgerufenen IP-Adressen hinzu.

## IP-Optimierung für Bereitstellungen des Typs „Mobile Benutzer – GlobalProtect“ und

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama)<br>• Prisma Access (Managed by Strata Cloud Manager) | • Prisma Access-Lizenz<br>• Prisma Access Version 5.0 oder höher |

Bei der IP-Optimierung handelt es sich um einen Satz von Architekturverbesserungen, die die Gesamtzahl der IP-Adressen in Ihrer Bereitstellung reduzieren, Ihre Workflows für Zulassungslisten vereinfachen und gleichzeitig die Ausfallsicherheit verbessern und ein schnelleres Onboarding von Prisma Access-Mandanten ermöglichen.

 ©2025 Palo Alto Networks, Inc.

- **Einfacheres Erstellen von Zulassungslisten öffentlicher IP-Adressen für Bereitstellungen des Typs „Mobile Benutzer – GlobalProtect“**: Das Hinzufügen eines Prisma Access-Standorts oder das Auftreten eines Skalierungsereignisses an einem vorhandenen Prisma Access-Standort kann dazu führen, dass dem Sicherheitsverarbeitungsknoten für mobile Benutzer (Mobile User Security Processing Node, MU-SPN) neue IP-Adressen zugewiesen werden. Es hat sich bewährt, die neuen Ausgangs- und Gateway-IP-Adressen, die Prisma Access zuweist, abzurufen und sie einer Zulassungsliste in Ihrem Netzwerk hinzuzufügen, um Störungen der SaaS-Anwendung oder der Unternehmens-Firewall zu vermeiden. Dies kann zu einer Situation führen, in der Sie eine große Anzahl von IP-Adressen verwalten müssen. Durch die IP-Optimierung wird die Anzahl der IP-Adressen reduziert, die Sie verwalten müssen.
- **Schnelleres Onboarding von Prisma Access-Mandanten**: Ohne IP-Optimierung müssten Sie jedem Gerät in Prisma Access und in Ihren privaten Netzwerken eindeutige private IP-Adressen zuweisen und daher große IP-Blöcke aus Ihrem begrenzten, routingfähigen IP-Adressraum Ihres Unternehmens zuweisen. Mit der IP-Optimierung kann Prisma Access standardmäßig Adressen aus einem gemeinsam genutzten Adressraum und NAT-Datenverkehr für private Anwendungen zuweisen.

*IP-Optimierung ist nur für neue GlobalProtect-Bereitstellungen von Prisma Access vorgesehen. Bestehende GlobalProtect-Bereitstellungen sind nicht berechtigt, einschließlich neuer Mandanten, die Sie aus einer vorhandenen Bereitstellung mit mehreren Mandanten erstellen. Wenn Sie Ihre GlobalProtect-Bereitstellung von lokalen Gateways und Portalen nach Prisma Access migrieren, stellen Sie außerdem sicher, dass alle Benutzer eine GlobalProtect-App-Version von 6.1.4 und höher, 6.2.3 und höher oder 6.3.0 und höher ausführen, bevor Sie diese Funktion aktivieren.*

*Beachten Sie die folgenden zusätzlichen Anforderungen für die IP-Optimierung:*

- *IP-Optimierung erfordert Prisma Access 5.0 oder höher für die Optimierung von „Mobile Benutzer“ und kann aktiviert werden, wenn Sie GlobalProtect zum ersten Mal einrichten.*
- *Wenn Sie GlobalProtect zum ersten Mal einrichten, werden Sie gefragt, ob Sie die Prisma Access-IP-Optimierung aktivieren möchten.*
- *Bereitstellungen mit IP-Optimierung unterstützen IPv6 nicht für den Zugriff auf öffentliche (externe) Apps. Der Zugriff auf private Apps wird unterstützt. Um IPv6 für Ihre neue Prisma Access-Bereitstellung zu aktivieren, wenden Sie sich an Ihr Palo Alto Networks Account-Team, das einen TAC-Fall zur Bearbeitung Ihrer Anfrage eröffnen wird.*
- *Die API zum Abrufen von Prisma Access-IP-Adressen funktioniert weiterhin wie gewohnt, auch wenn die IP-Optimierung aktiviert ist.*

 ©2025 Palo Alto Networks, Inc.

# API-Beispiele zum Abrufen von Prisma Access-IP-Adressen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

Verwenden Sie die folgenden Beispiele zur Eingabe von Schlüsselwörtern und Argumenten in die Textdatei (.txt), damit der API-Befehl Infrastruktur-IP-Adressen abrufen kann. Um die Ausgabe des Befehls zu ändern, müssen Sie die Optionen in der Textdatei (.txt) ändern; der Befehl selbst ändert sich hierbei nicht.

| Diese IP-Adressen abrufen | Geben Sie diese Parameter in der Textdatei (.txt) an | Bemerkungen |
|---|---|---|
| **IP-Adressen für mobile Benutzer** | | |
| Alle IP-Adressen mobiler Benutzer | `{"serviceType": "gp_gateway", "addrType": "all", "location": "all"}` | Wird für *addrType* die Einstellung *all* angegeben, dann werden von Prisma Access alle IP-Adressen für die Standorte abgerufen, die von Ihnen ausgewählt wurden GlobalProtect für mobile Benutzer einrichten (Panorama).<br>Wird für *location* die Einstellung *all* verwendet, dann ruft Prisma Access IP-Adressen für alle verfügbaren Standorte ab. Dies gilt auch für Standorte, die Sie nicht eingebunden haben. Prisma Access reserviert IP-Adressen für nicht eingebundene Standorte, damit Sie diese IP-Adressen zu Ihren Zulassungslisten hinzufügen können, bevor Sie sie einbinden. |
| IP-Adressen für eingebundene Standorte mobiler Benutzer | `{"serviceType": "gp_gateway", "addrType": "all", "location": "deployed"}` | Wird als Typ für *location* die Einstellung *deployed* angegeben, werden von Prisma Access ausschließlich die IP-Adressen für die |

 ©2025 Palo Alto Networks, Inc.

| Diese IP-Adressen abrufen | Geben Sie diese Parameter in der Textdatei (.txt) an | Bemerkungen |
|---|---|---|
| | Oder<br><br>`{"serviceType": "gp_gateway", "addrType": "active", "location": "deployed"}` | Standorte abgerufen, die Sie eingebunden haben.<br><br>Verwenden Sie entweder für *addrType* die Einstellung *all* oder *active*, um diese Gateway-IP-Adressen abzurufen. |
| **IP-Adressen des Remote-Netzwerks** | | |
| Abrufen aller Remote-Netzwerk-IP-Adressen | `{"serviceType": "remote_network", "addrType": "all", "location": "all"}` | Mit diesem Befehl können die öffentlichen und die Ausgangs-IP-Adressen von Remote-Netzwerken abgerufen werden, die Sie eingebunden haben. Verwenden Sie für *location* nicht die Einstellung *deployed*. Sie können für *addrType* die Einstellung *active* verwenden, mit der jedoch dieselben Adressen abgerufen werden, die auch abgerufen werden, wenn Sie für *addrType* die Einstellung *all* benutzen. |
| **Clean Pipe-IP-Adressen** | | |
| Abrufen aller Clean Pipe-IP-Adressen | `{"serviceType": "clean_pipe", "addrType": "all", "location": "all"}` | Mit diesem Befehl können die öffentlichen und die Ausgangs-IP-Adressen von Clean Pipes abgerufen werden, die Sie eingebunden haben. Verwenden Sie für *location* nicht die Einstellung *deployed*. Sie können für *addrType* die Einstellung *active* verwenden, mit der jedoch dieselben Adressen abgerufen werden, die auch abgerufen werden, wenn Sie für *addrType* die Einstellung *all* benutzen. |
| **IP-Adressen des expliziten Proxy** | | |

 ©2025 Palo Alto Networks, Inc.

| Diese IP-Adressen abrufen | Geben Sie diese Parameter in der Textdatei (.txt) an | Bemerkungen |
|---|---|---|
| Abrufen der ACS-IP-Adressen für bereitgestellte Standorte | `{"serviceType": "swg_proxy", "location": "all", "addrType": "all"}` | Dieser Befehl ruft die Ausgangs-IP-Adressen für jeden bereitgestellten Standort mit explizitem Proxy, den ACS (Authentication Cache Service) und die Netzwerklastausgleichssysteme (nur relevant für Bereitstellungen mit explizitem Proxy) ab. |
| **IP-Adressen für Remote-Browser-Isolation** | | |
| Abrufen der IP-Adressen für Remote-Browser-Isolation (RBI) für bereitgestellte Standorte | `{"serviceType": "rbi", "location": "all", "addrType": "all"}` | Mit diesem Befehl können die Ausgangs-IP-Adressen für jeden bereitgestellten RBI-Standort abgerufen werden. Sie können diese IP-Adressen einer Zulassungsliste hinzufügen, um eine Verbindung zu SaaS-Anwendungen herzustellen. |

 ©2025 Palo Alto Networks, Inc.

# Benachrichtigungen erhalten, wenn IP-Adressen von Prisma Access sich ändern

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Um über Änderungen der öffentlichen IP-Adresse für Remote-Netzwerke und der Loopback-IP-Adresse für Dienstverbindungen, Remote-Netzwerkverbindungen und mobile Benutzer benachrichtigt zu werden, können Sie eine URL angeben, über die Sie über eine Änderung benachrichtigt werden können. Prisma Access verwendet eine HTTP-POST-Anfrage, um die Benachrichtigung zu senden. Diese POST-Anfrage enthält die folgenden Benachrichtigungsdaten im JSON-Format:

```
 {"addrType": "public_ip", "addrChangeType": "add", "utc_timestamp":
"2019-01-31 23:08:19.383894", "text": "Address List Change
Notification"}
```

```
 {"addrType": "public_ip", "addrChangeType": "delete",
"utc_timestamp": "2019-01-31 23:13:35.882151", "text": "Address List
Change Notification"}
```

```
 {"addrType": "loopback_ip", "addrChangeType": "update",
"utc_timestamp": "2019-01-31 23:29:27.100329", "text": "2018-05-11
23:29:27.100329"}
```

Wenn Sie eine Benachrichtigung erhalten, müssen Sie einen zweistufigen Prozess befolgen. Zunächst müssen Sie die IP- oder Loopback-Adressen manuell oder programmgesteuert abrufen. Anschließend müssen Sie die IP-Adressen in der entsprechenden Zulassungsliste Ihrer Organisation aktualisieren, um sicherzustellen, dass es für die Benutzer zu keiner Dienstunterbrechung kommt.

*Prisma Access sendet diese Benachrichtigung einige Sekunden, bevor die neue IP-Adresse aktiv wird. Wir empfehlen, dass Sie Automatisierungsskripte verwenden, um die neuen IP-Adressen abzurufen und zu einer Zulassungsliste in Ihrem Netzwerk hinzuzufügen.*

Führen Sie die folgende Aufgabe aus, um eine Benachrichtigungs-URL für eine IP-Adresse hinzuzufügen.

- Für Prisma Access (Managed by Strata Cloud Manager)-Bereitstellungen gehen Sie zu **Workflows** > **Einrichtung Prisma Access** > **Prisma Access** > **Infrastruktureinstellungen**, klicken Sie auf das Zahnrad, um die Einstellungen zu bearbeiten, fügen Sie eine **Benachrichtigungs-**

 ©2025 Palo Alto Networks, Inc.

**URL für Ausgangs-IP** hinzu, über die Sie über IP-Adressänderungen in Ihrer Prisma Access-Infrastruktur benachrichtigt werden, und **speichern** Sie Ihre Änderungen.

- Für Prisma Access (Managed by Panorama)-Bereitstellungen gehen Sie zu **Panorama** > **Cloud Services** > **Konfiguration** > **Diensteinrichtung** und fügen Sie eine **Benachrichtigungs-URL für IP-Änderungsereignis** hinzu, über die Sie über IP-Adressänderungen in Ihrer Prisma Access-Infrastruktur benachrichtigt werden, und klicken Sie auf **OK**.




Sie können eine IP-Adresse oder einen FQDN für einen HTTP- oder HTTPS-Webdienst angeben, der auf Änderungsbenachrichtigungen wartet. Prisma Access sendet diese Benachrichtigungen aus dem Internet über eine öffentliche IP-Adresse.

Sie müssen Ihre Änderungen nicht bestätigen, damit die Benachrichtigungs-URL wirksam wird.

 ©2025 Palo Alto Networks, Inc.

# Verwenden von Legacy-Skripten zum Abrufen von IP-Adressen

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

*Ab Prisma Access Version 1.5 ersetzt ein neueres API-Skript die in diesem Abschnitt beschriebenen Befehle. Diese werden jedoch weiterhin unterstützt, wenn Sie die Loopback-Adresse abrufen müssen oder für Bereitstellungen, die die Befehle in Skripten oder anderen automatisierten Tools verwenden.*

Die folgende Tabelle zeigt die Schlüsselwörter und Parameter, die in den veralteten API-Skripten in Prisma Access verfügbar sind. Sie enthält außerdem Informationen und Empfehlungen dazu, welche API für die Art der Bereitstellung verwendet werden soll.

Diese Legacy-Befehle rufen auch *öffentliche IP-* und *Ausgangs-IP-*Adressen ab. Palo Alto Networks empfiehlt jedoch, diese Befehle mit dem neueren API-Skript abzurufen und die Legacy-API nur zum Abrufen der Loopback-IP-Adressen zu verwenden.

- Eine *öffentliche IP-Adresse* ist die Quell-IP-Adresse, die Prisma Access für Anfragen an eine internetbasierte Quelle verwendet. Fügen Sie die öffentliche IP-Adresse zu einer Zulassungsliste in Ihrem Netzwerk hinzu, um Prisma Access Zugriff auf Internetressourcen wie SaaS-Anwendungen oder öffentlich zugängliche Partneranwendungen zu erteilen.

  Mobile Benutzer, Remote-Netzwerke und Clean-Pipe-Bereitstellungen verwenden öffentliche IP-Adressen.
- Eine *Ausgangs-IP-Adresse* ist eine IP-Adresse, die Prisma Access für den ausgehenden Datenverkehr zum Internet verwendet. Damit auch Prisma Access auf die Internetressourcen zugreifen kann, müssen Sie diese Adressen zu einer Zulassungsliste hinzufügen.

  Prisma Access verwendet Ausgangs-IP-Adressen unter anderem, damit Benutzer Webseiten an einem Prisma Access-Standort in der entsprechend erwarteten Sprache erhalten. Alle

 ©2025 Palo Alto Networks, Inc.

Standorte haben zwar öffentliche IP-Adressen, aber nicht alle verwenden auch Ausgangs-IP-Adressen. Folgende Standorte verwenden keine Ausgangs-IP-Adressen:

- Standorte, die Sie vor der Veröffentlichung von Prisma Access Version 1.4 hinzugefügt haben
- Bahrain
- Belgien
- Nordfrankreich
- Südfrankreich
- Hongkong
- Irland
- Südkorea
- Taiwan
- Vereinigtes Königreich

Mobile Benutzer, Remote-Netzwerke und Clean-Pipe-Bereitstellungen verwenden Ausgangs-IP-Adressen.

| In mobilen Benutzerbereitstellungen verwendete Befehle | |
|---|---|
| **Befehlsname** | **Bemerkungen** |
| Befehl **get_egress_ip_all=yes**<br>`curl -H header-api-key:`*Current-API-Key*`"https://api.prod.datapath.prismaaccess.com/getAddrList/latest?get_egress_ip_all=yes` | Mit diesem Befehl werden alle IP-Adressen abgerufen, die Sie einer Zulassungsliste hinzufügen, um Prisma Access Zugang zu Internetressourcen wie SaaS-Anwendungen oder öffentlich zugänglichen Partneranwendungen zu gewähren. Für diesen Befehl gelten folgende Einschränkungen:<br>• Dieser Befehl kann eine große Anzahl von Adressen (mehr als 200) abrufen. Wenn Ihr Unternehmen diese Anzahl von IP-Adressen nicht zu einer Zulassungsliste hinzufügen kann, können Sie mit den Schlüsselwörtern *gpcs_gp_gw* und *gpcs_gp_portal* nur die IP-Adressen abrufen, die Sie derzeit verwenden. Sie müssen diese Befehle jedoch jedes Mal wiederholen, wenn Sie einen Standort hinzufügen. Im Falle eines Skalierungsereignisses müssen Sie die neuen IP-Adressen außerdem in eine Zulassungsliste eingeben.<br>• Prisma Access listet nicht die Standorte auf, die mit diesen IP-Adressen verknüpft sind. Daher empfehlen wir Ihnen, alle IP-Adressen, die mit diesem Befehl |

 ©2025 Palo Alto Networks, Inc.

| In mobilen Benutzerbereitstellungen verwendete Befehle | |
|---|---|
| **Befehlsname** | **Bemerkungen** |
| | zurückgegeben werden, zu einer Zulassungsliste hinzuzufügen.<br>• Dieser Befehl liefert Ihnen keine Loopback-Adressen. |
| Schlüsselwörter **gpcs_gp_gw** und **gpcs_gp_portal**<br>`curl -H header-api-key:`*Current-API-Key*`"https://api.prod.datapath.prismaaccess.com/getAddrList/latest?fwType=gpcs_gp_gw \| gpcs_gp_portal&addrType=public_ip \| egress_ip_list \| loopback_ip"` | Verwenden Sie diesen Befehl, wenn Ihre Bereitstellung die Anzahl der IP-Adressen begrenzt, die Sie einer Zulassungsliste hinzufügen können. Sie müssen alle IP-Adressen, die mit diesem Befehl zurückgegeben werden, einer Zulassungsliste in Ihrem Netzwerk hinzufügen. Mit diesem Befehl können Sie auch die Loopback-IP-Adressen abrufen. |

| In Remote-Netzwerkbereitstellungen verwendete Befehle | |
|---|---|
| **Befehlsname** | **Bemerkungen** |
| Schlüsselwort **gpcs_remote_network**<br>`curl -H header-api-key:`*Current-API-Key*`"https://api.prod.datapath.prismaaccess.com/getAddrList/latest?fwType=gpcs_remote_network &addrType=public_ip \| egress_ip_list \| loopback_ip"` | Suchen Sie mit diesem Befehl nach den IP-Adressen, die Sie einer Zulassungsliste für Remote-Netzwerkbereitstellungen hinzufügen müssen.<br>Sie können diesen Befehl auch verwenden, um die Ausgangs-IP-Adressen für Remote-Netzwerkbereitstellungen zu finden. Die Ausgangs- und IP-Adressen können in einigen Fällen unterschiedlich sein. |

| In Clean-Pipe-Bereitstellungen verwendete Befehle | |
|---|---|
| **Befehlsname** | **Bemerkungen** |
| Schlüsselwort **gpcs_clean_pipe**<br>`curl -H header-api-key:`*Current-API-Key*`"https://api.prod.datapath.prismaaccess.com/getAddrList/latest?fwType=gpcs_clean_pipe&addrType=public_ip \| egress_ip_list \| loopback_ip"` | Verwenden Sie diesen Befehl, um die IP-Adressen zu finden, die Sie einer Zulassungsliste für Clean-Pipe-Bereitstellungen hinzufügen müssen. |


©2025 Palo Alto Networks, Inc.

# Abrufen von IP-Adressen mobiler Benutzer

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

*Dieses Legacy-Skript wurde ab Prisma Access 1.5 durch ein neues API-Skript ersetzt. Palo Alto Networks empfiehlt, das neuere Skript zu verwenden, um alle IP-Adressen mit Ausnahme von Loopback-Adressen abzurufen.*

Wenn Sie öffentliche IP-Adressen zu Zulassungslisten hinzufügen, um mobilen Benutzern Zugriff auf SaaS oder öffentliche Anwendungen zu gewähren, stellt Prisma Access zwei IP-Adressen für jedes Gateway und jede Portal-IP-Adresse bereit, sodass eine IP-Adresse während einer Skalierung oder eines anderen Ereignisses verwendet werden kann. Sie können diesen Satz von IP-Adressen vor der Verwendung zu einer Zulassungsliste hinzufügen, um Probleme zu vermeiden, wenn mobile Benutzer während eines Skalierungsereignisses auf SaaS oder öffentliche Anwendungen zugreifen können.

Führen Sie die folgenden Schritte aus, um diese neuen Adressen abzurufen:

**STEP 1 |** Rufen Sie den API-Schlüssel ab, indem Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Diensteinrichtung** und anschließend **API-Schlüssel generieren** auswählen.

Sie benötigen diesen Schlüssel, um sich bei Prisma Access zu authentifizieren und die Liste der IP-Adressen mit dem unten aufgeführten cURL-Befehl abzurufen. Nur ein Panorama-Administrator oder Superuser kann diesen API-Schlüssel generieren oder darauf zugreifen.

**STEP 2 |** Geben Sie folgenden Befehl ein, um die öffentlichen IP-Adressen des mobilen Benutzers abzurufen:

```
  curl -H header-api-key:Current-API-Key "https://
api.prod.datapath.prismaaccess.com/getAddrList/latest?
get_egress_ip_all=yes"
```

Dabei ist *Current-API-Key* der Prisma Access-API-Schlüssel.

Beispiel: Verwenden Sie bei dem API-Schlüssel **12345abcde** folgenden API-Befehl, um die öffentliche IP-Adresse für alle Standorte abzurufen:

```
  curl -H header-api-key:12345abcde "https://
api.prod.datapath.prismaaccess.com/getAddrList/latest?
get_egress_ip_all=yes"
```

Jedes Mal, wenn Prisma Access den einen Satz öffentlicher IP-Adressen verwendet, weist es einen anderen Satz IP-Adressen zu. Wenn Sie glauben, dass Prisma Access den hinzugefügten Satz öffentlicher IP-Adressen verwendet hat (z. B. wenn eine große Anzahl mobiler Benutzer auf einen einzelnen Standort zugegriffen hat), können Sie diesen API-Befehl erneut ausführen, um den neuen Satz öffentlicher IP-Adressen zu ermitteln. Alle IP-Adressen bleiben nach einem Upgrade bestehen.

 ©2025 Palo Alto Networks, Inc.

# Abrufen von öffentlichen IP-Adressen sowie Loopback- und Ausgangs-IP-Adressen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

*Dieses Legacy-Skript wurde ab Prisma Access 1.5 durch ein neueres Skript ersetzt. Palo Alto Networks empfiehlt, das neuere Skript zu verwenden, um alle IP-Adressen mit Ausnahme von Loopback-Adressen abzurufen.*

Führen Sie die folgenden Schritte aus, um öffentliche IP-Adressen sowie Loopback- und Ausgangs-IP-Adressen abzurufen.

**STEP 1 |** Rufen Sie den API-Schlüssel ab und fügen Sie eine **Benachrichtigungs-URL für IP-Änderungsereignis** hinzu, über die Sie über Änderungen der IP-Adresse in Ihrer Prisma Access-Infrastruktur benachrichtigt werden können.

Weitere Einzelheiten finden Sie unter Benachrichtigungen erhalten, wenn IP-Adressen von Prisma Access sich ändern.

**STEP 2 |** Rufen Sie die öffentlichen IP-Adressen, Loopback-IP-Adressen oder beide für Prisma Access ab.

Verwenden Sie den API-Schlüssel und die API-Endpunkt-URL manuell oder in einem Automatisierungsskript:

```
 header-api-key:Current API Key "https://
api.prod.datapath.prismaaccess.com/getAddrList/latest?
fwType=$fwType&addrType=$addrType"
```

Dabei müssen Sie „Current API Key“ durch Ihren API-Schlüssel ersetzen und eines oder beide der folgenden Schlüsselwörter und Argumente verwenden:

| Schlüsselwort | Beschreibung |
|---|---|
| Schlüsselwort **fwType** | |
| **gpcs_gp_gw** | Ruft Prisma Access-Gateway-IP-Adressen ab (für Bereitstellungen für mobile Benutzer). |
| **gpcs_gp_portal** | Ruft Prisma Access-Portal-IP-Adressen ab (für Bereitstellungen für mobile Benutzer). |
| **gpcs_remote_network** | Ruft Prisma Access-Remote-Netzwerk-IP-Adressen ab (für Remote-Netzwerkbereitstellungen). |
| **gpcs_clean_pipe** | Ruft Prisma Access-Clean-Pipe-IP-Adressen ab. |

 ©2025 Palo Alto Networks, Inc.

| Schlüsselwort | Beschreibung |
|---|---|
| Schlüsselwort **addrType** | |
| **public_ip** | Ruft die Quell-IP-Adressen ab, die Prisma Access für Anfragen an eine internetbasierte Quelle verwendet.<br><br>Bei Standorten mobiler Benutzer listet Prisma Access die IP-Adressen nach Standort auf. Bei Remote-Netzwerken listet Prisma Access die IP-Adressen nach Namen der Remote-Netzwerke auf. |
| **egress_ip_list** | Ruft die IP-Adressen ab, die Prisma Access mit öffentlichen IP-Adressen für zusätzlichen ausgehenden Datenverkehr zum Internet verwendet.<br><br>Für Standorte mobiler Benutzer listet Prisma Access die IP-Adressen nach Standort auf. Bei Remote-Netzwerken listet Prisma Access die IP-Adressen nach Namen der Remote-Netzwerke auf. |
| **loopback_ip** | Ruft die Quell-IP-Adressen ab, die von Prisma Access für Anfragen an eine interne Quelle verwendet werden (z. B. einen RADIUS- oder Active Directory-Server) und wird über das Infrastruktursubnetz zugewiesen. |

Wenn Sie kein Schlüsselwort angeben, ruft Prisma Access alle IP-Adressen ab.

Sie können beispielsweise versuchen, folgenden cURL-Befehl auszuführen, um die Liste der öffentlichen IP-Adressen für sämtliche Remote-Netzwerke manuell abzurufen:

```
curl -H header-api-
key:1234y9ydxb__0UmxetVTbC8XTyFMaoT4RBZBKBjfX419YVufeFG7
 "https://api.prod.datapath.prismaaccess.com/getAddrList/latest?
fwType=gpcs_remote_network&addrType=public_ip"
```

Alternativ können Sie ein einfaches Python-Skript verwenden, um die Liste aller IP-Adressen abzurufen. Beispiel:

```
  #!/usr/bin/python import subprocess import json api_key
 = '1234y9ydxb__0UmxetVTbC8XTyFMaoT4RBZBKBjfX419YVufeFG7'
 # Durch Ihren Schlüssel ersetzen api_end_point = 'https://
api.prod.datapath.prismaaccess.com/getAddrList/latest' # Bei diesem
 Aufruf werden IP-Adressen für alle Ihre Prisma Access-Firewalls
 abgerufen args = ['curl', '-k', '-H', 'header-api-key:' + api_key,
 api_end_point] p = subprocess.Popen(args, stdout=subprocess.PIPE)
```

 ©2025 Palo Alto Networks, Inc.

```
output = p.communicate() dout = json.loads(output[0]) addrStrList
= dout['result']['addrList'] addrList = [] for addr_str
in addrStrList: addrList.append(addr_str.split(":")[1])
print(addrList)
```

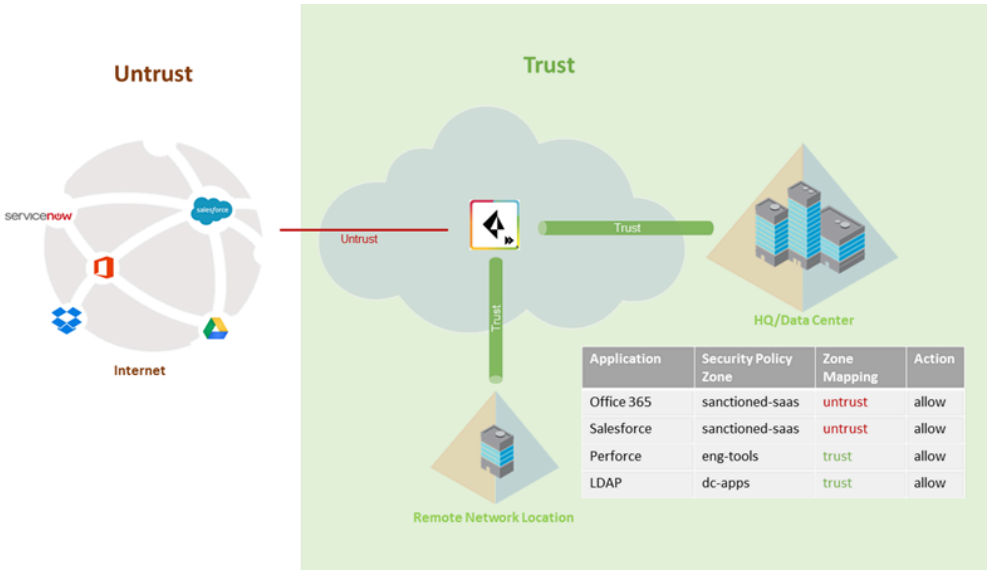
**STEP 3 |** Aktualisieren Sie die Zulassungslisten auf Ihren lokalen Servern oder in den Richtlinienregeln für Ihre SaaS-Anwendung und fügen Sie die von Ihnen abgerufenen IP-Adressen hinzu.

 ©2025 Palo Alto Networks, Inc.

# Prisma Access-Zonen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Auf einer Firewall werden Zonen Schnittstellen zugeordnet. Doch innerhalb von Prisma Access wird die Netzwerkinfrastruktur automatisch für Sie eingerichtet. Das bedeutet, dass Sie sich nicht mehr um die Konfiguration von Schnittstellen und deren Zuordnung zu den von Ihnen erstellten Zonen kümmern müssen. Für eine konsistente Durchsetzung von Sicherheitsrichtlinien müssen Sie jedoch Zonenzuordnungen erstellen, damit Prisma Access weiß, ob eine Zone einer internen (Vertrauens-)Schnittstelle oder einer externen (Nichtvertrauens-)Schnittstelle zugeordnet werden soll. So stellen Sie sicher, dass Ihre Sicherheitsrichtlinienregeln ordnungsgemäß durchgesetzt werden. Standardmäßig sind alle Zonen, die Sie in Prisma Access per Push übertragen, auf „Nicht vertrauenswürdig“ eingestellt. Sie sollten alle Zonen, die mit internetfähigem Datenverkehr verbunden sind, einschließlich Ihrer sanktionierten SaaS-Anwendungen, auf „Nicht vertrauenswürdig“ setzen. Für alle Zonen, die den Zugriff auf Anwendungen in Ihrem internen Netzwerk oder in Ihrem Rechenzentrum ermöglichen, müssen Sie diese jedoch als „Vertrauenswürdig“ zuordnen. Beachten Sie im folgenden Beispiel, dass alle sanktionierten SaaS-Anwendungen – in diesem Fall Office 365 und Salesforce – in die Zone der sanktionierten SaaS-Anwendungen segmentiert sind, um Transparenz und Richtliniendurchsetzung bei der Verwendung dieser Anwendungen zu ermöglichen. Damit Prisma Access die sanktionierte SaaS-Zone mit einer nach außen gerichteten Schnittstelle verknüpfen kann, müssen Sie diese Zone als „Nicht vertrauenswürdig“ zuordnen. Ebenso bieten die Zonen „eng-tools“ und „dc-apps“ Zugriff auf Anwendungen in der Firmenzentrale. Daher müssen Sie diese als vertrauenswürdige Zonen ausweisen.




Prisma Access unterstützt drei Zonen („Vertrauenswürdig“, „Nicht vertrauenswürdig“ und „Clientloses VPN“) und vereinfacht die Richtlinienerstellung, indem es sie für Sie einrichtet.

 ©2025 Palo Alto Networks, Inc.

| Zone | Beschreibung |
|---|---|
| Vertrauenswürdig | Zone mit allen vertrauenswürdigen und integrierten IP-Adressen, Dienstverbindungen oder mobilen Benutzern innerhalb des Unternehmensnetzwerks. |
| Nicht vertrauenswürdig | Alle nicht vertrauenswürdigen IP-Adressen, Dienstverbindungen oder mobilen Benutzer außerhalb des Unternehmensnetzwerks. Standardmäßig ist jede IP-Adresse oder jeder mobile Benutzer, dem nicht vertraut wird, nicht vertrauenswürdig. |
| Clientloses VPN | Sicherer Remote-Zugriff auf gängige Unternehmens-Webanwendungen, die HTML-, HTML5- und Javascript-Technologien verwenden. Benutzer haben den Vorteil, dass sie sicheren Zugriff über SSL-fähige Webbrowser haben, ohne dass sie Clientsoftware installieren müssen. Dies ist nützlich, wenn Sie Partnern oder Auftragnehmern den Zugriff auf Anwendungen ermöglichen und nicht verwaltete Assets, einschließlich persönlicher Geräte, sicher aktivieren müssen.<br><br>*Die Zone für clientloses VPN ist standardmäßig der vertrauenswürdigen Zone zugeordnet. Diese Einstellung kann nicht geändert werden.* |

Prisma Access-Protokolle, die eine Zone von **inter-fw** anzeigen, sind Protokolle, die zur Kommunikation innerhalb der Prisma Access-Infrastruktur verwendet werden.

Verwenden Sie beim Erstellen von Zonen keinen der folgenden Namen für die Zonen, da dies Namen für interne Zonen sind:

- vertrauenswürdig
- nicht vertrauenswürdig
- inter-fw
- Jeder Name, den Sie für die Remote-Netzwerke verwenden (Remote-Netzwerknamen werden als Quellzone in Strata Logging Service-Protokollen verwendet)

*Prisma Access-Protokolle, die eine Zone von „inter-fw“ anzeigen, sind Protokolle, die zur Kommunikation innerhalb der Prisma Access-Infrastruktur verwendet werden.*


©2025 Palo Alto Networks, Inc.

# DNS für Prisma Access

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Mit Prisma Access können Sie DNS-Server angeben, um sowohl unternehmensinterne als auch externe Domänen aufzulösen. Dadurch wird der Zugriff auf Dienste in Ihrem Unternehmensnetzwerk wie LDAP- und DNS-Server ermöglicht, insbesondere wenn Sie Dienstverbindungen einrichten möchten, um am Hauptsitz oder in Rechenzentren Zugriff auf diese Art von Ressourcen bereitzustellen.Prisma Access unterstützt die DNS-Auflösung für die Bereitstellungen für mobile Benutzer – Global Protect und Remote-Netzwerke. DNS-Abfragen für Domänen in der Liste mit internen Domänen werden an Ihre lokalen DNS-Server gesendet, um sicherzustellen, dass Ressourcen für Remote-Netzwerkbenutzer und mobile Benutzer von Prisma Access verfügbar sind.

Wenn Sie beispielsweise möchten, dass ein DNS-Lookup für Ihre Unternehmensdomäne ausschließlich an den Unternehmens-DNS-Server geht, geben Sie hier die Unternehmensdomäne und die Unternehmens-DNS-Server an. Um sicherzustellen, dass Endpunkte die **DNS-Proxy-IP-Adresse** verwenden, müssen sie so konfiguriert sein, dass sie DNS über die IP-Adresse auflösen, die unter **Workflow** > **Einrichtung Prisma Access** > **Prisma Access** > **Prisma Access-DNS-Proxy-IP-Adresse** angezeigt wird.

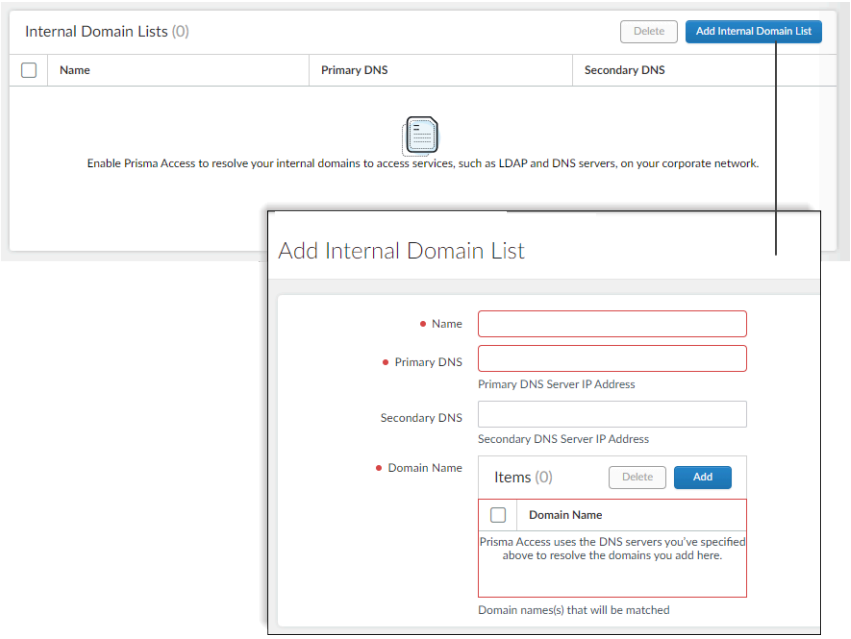
- Strata Cloud Manager
- Panorama

## DNS für Prisma Access (Strata Cloud Manager)

Hier erfahren Sie, wie Sie Prisma Access zur Auflösung interner Domänen einrichten und DNS-Einstellungen (zur Auflösung interner und öffentlicher Domänen) für Bereitstellungen mobiler Benutzer und Remote-Netzwerkstandorte anpassen.

 ©2025 Palo Alto Networks, Inc.

- Richten Sie Listen mit internen Domänen ein, die für den gesamten Datenverkehr gelten.
  1. Wählen Sie **Workflows** > **Einrichtung Prisma Access** > **Prisma Access** und **Interne DNS-Server hinzufügen** aus.




  2. Geben Sie den primären und den sekundären DNS-Server ein, die Prisma Access zur Auflösung der internen Domänennamen verwenden soll.
  3. Fügen Sie die internen Domänennamen hinzu, die zur Auflösung an diese DNS-Server gesendet werden sollen.

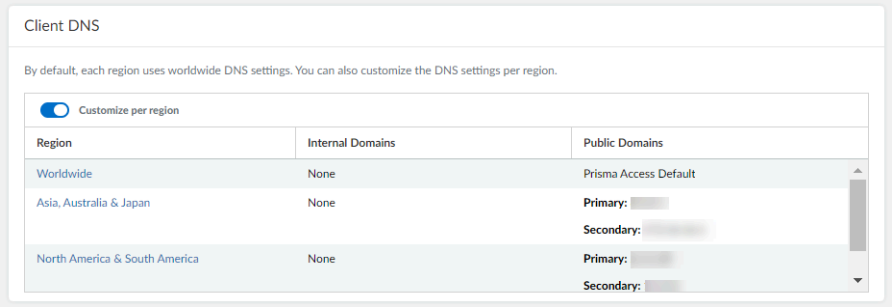
     Sie können einen Platzhalter (*) vor den Domänen in der Domänenliste verwenden, z. B. *.acme.local oder *.acme.com.

 ©2025 Palo Alto Networks, Inc.

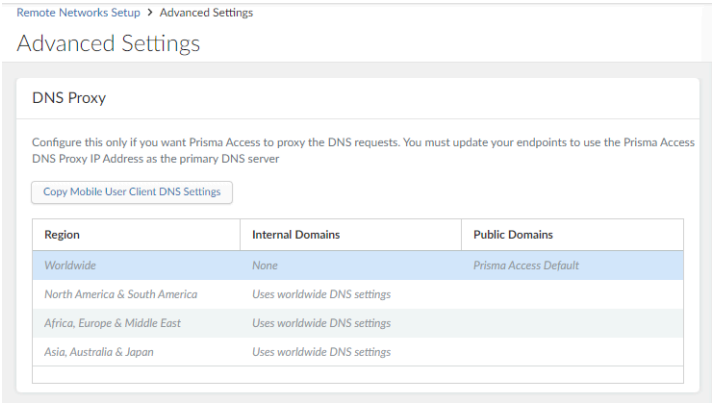
- Fügen Sie Listen mit internen Domänen hinzu, die nur für bestimmte Bereitstellungen mobiler Benutzer oder Remote-Netzwerkstandorte gelten.

  1. Konfigurieren Sie DNS-Einstellungen:

     - **Mobile Benutzer** – Gehen Sie zu **Workflows** > **Einrichtung Prisma Access** > **GlobalProtect** > **Infrastruktureinstellungen** und finden Sie **Client-DNS**.




     - **Remote-Netzwerke** – Gehen Sie zu **Workflows** > **Einrichtung Prisma Access** > **Remote-Netzwerke** > **Erweiterte Einstellungen** und finden Sie **DNS-Proxy**.




  2. Verwenden Sie die Standardeinstellung „Weltweit“ (Standard-DNS-Server von Prisma Access) oder passen Sie die Einstellungen je nach Region an. Wählen Sie in beiden Fällen die Region aus, um die DNS-Einstellungen für diese Region anzupassen.
  3. Aktivieren Sie die Option **Diese DNS-Einstellungen für die Auflösung interner Domänen verwenden** und optional auch die Option**Internen DNS-Server auch für die Auflösung von öffentlichen Domänen verwenden**. Wenn Sie diese Option nicht auswählen, verwendet Prisma Access seinen Cloud-Standard-DNS-Server zur Auflösung von Anfragen für öffentliche Domänen.
  4. Erlauben Sie Datenverkehr von allen Adressen in Ihrem IP-Adresspool für mobile Benutzer zu Ihren DNS-Servern.

     Der DNS-Proxy in Prisma Access sendet die Anfragen an die von Ihnen angegebenen DNS-Server. Die Quelladresse in der DNS-Anfrage ist die erste IP-Adresse in dem IP-Pool, den Sie der Region zuweisen. Um zu gewährleisten, dass Ihre DNS-Anfragen die Server erreichen können, müssen Sie sicherstellen, dass Sie den Datenverkehr von allen Adressen in Ihrem IP-Adresspool für mobile Benutzer zu Ihren DNS-Servern zulassen.

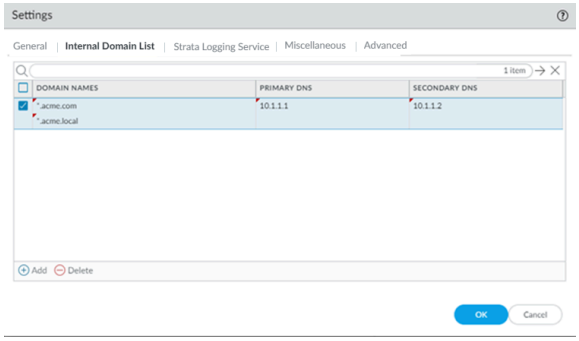
 ©2025 Palo Alto Networks, Inc.

# DNS für Prisma Access (Panorama)

Richten Sie Prisma Access ein, um interne Domänen aufzulösen.

- Richten Sie Listen mit internen Domänen ein, die für den gesamten Datenverkehr gelten.
  1. Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Diensteinrichtung** aus und klicken Sie auf das Zahnradsymbol, um die Einstellungen zu bearbeiten.
  2. Wählen Sie die Registerkarte **Liste interner Domänen** aus.
  3. Fügen Sie die Domänennamen sowie die primären und sekundären DNS-Server hinzu, die Prisma Access zur Auflösung Ihrer internen Domänennamen verwenden soll.

     Sie können einen Platzhalter (*) vor den Domänen in der Domänenliste verwenden, z. B. *.acme.local oder *.acme.com.

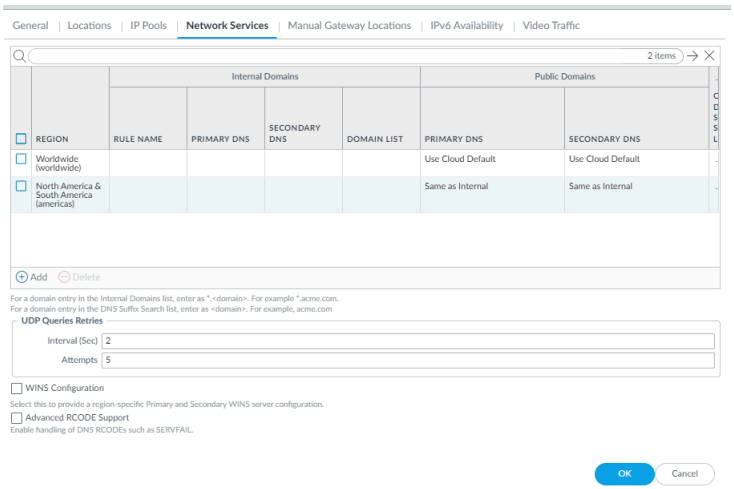



 ©2025 Palo Alto Networks, Inc.

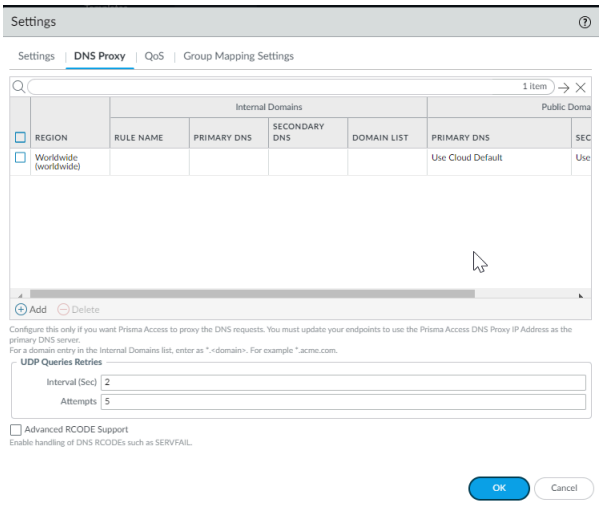
- Fügen Sie Listen mit internen Domänen hinzu, die nur für bestimmte Bereitstellungen mobiler Benutzer oder Remote-Netzwerkstandorte gelten.

  1. Konfigurieren Sie DNS-Einstellungen:

     - **Mobile Benutzer** – Gehen Sie zu **Panorama** > **Cloud Services** > **Konfiguration** > **Mobile Benutzer – GlobalProtect**, wählen Sie das externe Gateway aus und klicken Sie auf **Netzwerkdienste**.




     - **Remote-Netzwerke** – Gehen Sie zu **Panorama** > **Cloud Services** > **Konfiguration** > **Remote-Netzwerke** > **Einstellungen** > **DNS-Proxy**.




  2. Verwenden Sie die Standardeinstellung „Weltweit“ (Standard-DNS-Server von Prisma Access) oder passen Sie die Einstellungen je nach Region an. Wählen Sie in beiden Fällen die Region aus, um die DNS-Einstellungen für diese Region anzupassen.
  3. Fügen Sie eine oder mehrere Regeln hinzu, um die DNS-Einstellungen für **Interne Domäne** zu konfigurieren.

     - Geben Sie einen eindeutigen Regelnamen für die Regel ein.
     - Wenn Ihr interner DNS-Server nur die von Ihnen angegebenen Domänen auflösen soll, geben Sie die aufzulösenden Domänen in die Domänenliste ein. Geben

 ©2025 Palo Alto Networks, Inc.

Sie vor der Domäne ein Sternchen an, z. B. *.acme.com. Sie können maximal 1.024 Domäneneinträge angeben.

Prisma Access hat eine vordefinierte Regel, um *.amazonaws.com-Domänen über den Cloud-Standardserver aufzulösen. Wenn Sie möchten, dass Ihre internen DNS-Server eine spezifischere *.amazonaws.com-Domäne auflösen (z. B. *.s3.amazonaws.com), geben Sie die URL in die Domänenliste ein. Prisma Access wertet die Domänennamen vom längsten bis zum kürzesten Namen aus, dann von oben bis nach unten in der Liste.

- Wenn Sie über einen benutzerdefinierten DNS-Server verfügen, der auf Ihre internen Domänen zugreifen kann, geben Sie die IP-Adressen des primären und des sekundären DNS-Servers an oder wählen Sie „Cloud-Standard verwenden“ aus, um den Standard-DNS-Server von Prisma Accesszu verwenden.

4. Geben Sie die DNS-Einstellungen für **Öffentliche Domänen** an.
   - **Cloud-Standard verwenden** – Verwenden Sie den Standard-DNS-Server von Prisma Access.
   - **Wie internes DNS** – Verwenden Sie denselben Server, den Sie zum Auflösen interner Domänen verwenden. Wenn Sie diese Option aktivieren, entspricht der DNS-Server, der zur Auflösung öffentlicher Domänen verwendet wird, dem Server, der für die erste Regel im Abschnitt **Interne Domänen** konfiguriert ist.
   - **Benutzerdefinierter DNS-Server** – Wenn Sie über einen DNS-Server verfügen, der auf Ihre öffentlichen (externen) Domänen zugreifen kann, geben Sie in dieses Feld die primäre DNS-Serveradresse ein.
5. (Optional) Sie können ein DNS-Suffix hinzufügen, um das Suffix anzugeben, das der Client lokal verwenden soll, wenn ein nicht qualifizierter Hostname eingegeben wird, den er nicht auflösen kann, z. B. acme.local. Geben Sie kein Platzhalterzeichen (*) vor dem Domänensuffix ein (z. B. acme.com). Sie können mehrere Suffixe hinzufügen.
6. Erlauben Sie Datenverkehr von allen Adressen in Ihrem IP-Adresspool für mobile Benutzer zu Ihren DNS-Servern.

   Der DNS-Proxy in Prisma Access sendet die Anfragen an die von Ihnen angegebenen DNS-Server. Die Quelladresse in der DNS-Anfrage ist die erste IP-Adresse in dem IP-Pool, den Sie der Region zuweisen. Um zu gewährleisten, dass Ihre DNS-Anfragen die Server erreichen können, müssen Sie sicherstellen, dass Sie den Datenverkehr von allen Adressen in Ihrem IP-Adresspool für mobile Benutzer zu Ihren DNS-Servern zulassen.

 ©2025 Palo Alto Networks, Inc.

# Hochverfügbarkeit für Prisma Access

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

Die Bereitstellung von Panorama-Appliances in einer Hochverfügbarkeitskonfiguration (High Availability, HA) bietet Redundanz im Falle eines System- oder Netzwerkausfalls und gewährleistet die kontinuierliche Konnektivität mit Prisma Access. In einer HA-Konfiguration ist einer der Panorama-Appliance-Peers der aktiv-primäre Peer und der andere ist der passiv-sekundäre Peer. Bei einem Failover wird der sekundäre Peer aktiv und übernimmt die Rolle zur Verwaltung von Prisma Access.

Zur Vereinfachung der HA-Einrichtung konfigurieren Sie die Panorama-Appliances in HA, nachdem Sie Prisma Access- und Strata Logging Service-Authentifizierungscodes sowie entsprechende Komponenten erworben haben, und verknüpfen Sie die Seriennummer der primären Panorama-Appliance, auf der Sie das Cloud Services-Plug-in installieren möchten, mit den Authentifizierungscodes – allerdings bevor Sie von Panorama verwaltetes Prisma Access aktivieren und installieren. Sie können diesen Prozess jedoch auch verwenden, um bestehende Panorama-Appliances zu konfigurieren, auf denen das Plug-in bereits installiert ist.

Unabhängig davon, ob Sie gerade mit einem neuen Paar Panorama-Appliances beginnen oder ob Sie Ihre eigenständige Panorama-Appliance bereits eingerichtet und die Lizenzierungs- und Installationsverfahren abgeschlossen haben, überprüfen Sie die Voraussetzungen, bevor Sie HA aktivieren:

- Sie müssen die HA-Peers der Panorama-Appliance im Kunden-Support-Portal (Customer Support Portal, CSP) beim selben Kundenkonto registrieren.
- Die Peers der Panorama-Appliance müssen den gleichen Formfaktor (Hardware-Appliances desselben Modells oder identische virtuelle Appliances) und die gleiche Betriebssystemversion aufweisen und über den gleichen Satz von Lizenzen verfügen. Die Premium-Support-Lizenz ist für Prisma Access und Strata Logging Service erforderlich.
- Die Seriennummer der primären Panorama-Appliance ist an Ihre Authentifizierungscodes für Prisma Access und Strata Logging Service gebunden. Wenn Sie das Plug-in auf einer eigenständigen Panorama-Appliance installiert und eingerichtet haben, stellen Sie sicher, dass Sie diese Panorama-Appliance als primären Peer verwenden. Wenn Sie diesen eigenständigen Peer als sekundäre Panorama-Appliance zuweisen müssen, wenden Sie sich an den Palo Alto Networks Support, um Unterstützung bei der Übertragung der Lizenz auf den primären Panorama-Appliance-Peer zu erhalten, bevor Sie fortfahren.

*Wenn Sie HA für ein Panorama-Paar deaktivieren und zu einer Konfiguration zurückkehren, in der Prisma Access von einer einzelnen Panorama-Instanz verwaltet wird, müssen Sie Ihr Konto erneut verifizieren, um Fehler beim Abrufen des Status von Prisma Access-Komponenten zu vermeiden.*

Gehen Sie wie folgt vor, um Ihre Panorama-Appliances in einer HA-Konfiguration einzurichten.

 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** HA auf Panorama einrichten.

Legen Sie die primäre Panorama-Appliance als **primär** und die sekundäre Panorama-Appliance als **sekundär** fest und stellen Sie sicher, dass die Seriennummer Ihrer primären Panorama-Appliance mit Ihren Authentifizierungscodes von Prisma Access und Strata Logging Service verknüpft ist.

**STEP 2 |** Stellen Sie sicher, dass die primären (aktiven) und sekundären (passiven) Panorama-Appliances synchronisiert sind und der HA-Link-Status zwischen ihnen aktiviert ist.

1. Greifen Sie auf das **Dashboard** der primären Panorama-Appliance zu und wählen Sie **Widgets** > **System** > **Hochverfügbarkeit** aus, um das HA-Widget anzuzeigen.
2. **Mit Peer synchronisieren**: Klicken Sie auf **Ja** und warten Sie, bis für **Aktive Konfiguration** der Wert **Synchronisiert** anzeigt wird.
3. Stellen Sie sicher, dass der **lokale** Peer **aktiv** ist.
4. Greifen Sie auf das **Dashboard** in der passiven Panorama-Appliance zu und wählen Sie **Widgets** > **System** > **Hochverfügbarkeit** aus, um das HA-Widget anzuzeigen.
5. Stellen Sie sicher, dass für **Aktive Konfiguration** der Wert **Synchronisiert** angezeigt wird.
6. Vergewissern Sie sich, dass der **lokale** Peer **passiv** ist.

**STEP 3 |** Installieren Sie die Prisma Access-Komponenten auf der primären Panorama-Appliance.

1. Melden Sie sich bei der primären Panorama-Appliance an und wählen Sie **Panorama** > **Lizenzen** aus.
2. Klicken Sie auf **Lizenzschlüssel vom Lizenzserver abrufen**.
3. Aktivieren und installieren Sie von Panorama verwaltetes Prisma Access, einschließlich der Generierung eines Einmalpassworts (One-Time Password, OTP) und der Überprüfung Ihres Kontos.

**STEP 4 |** Überprüfen Sie, ob HA aktiviert ist.

1. Sie müssen auf der primären Panorama-Appliance auf die CLI zugreifen und den folgenden Befehl eingeben:

   **`tail follow yes mp-log plugin_cloud_services.log`**

2. In der Protokollausgabe finden Sie den folgenden Text, wobei *X* die Seriennummer der primären Panorama-Appliance und *Y* die Seriennummer der sekundären Panorama-Appliance ist:

```
2017-11-06 15:14:07.790 -0800 INFO: [hainfo] Sending
 update to CSP for HA peer serial information to https://
updates.paloaltonetworks.com/licensesvc/licenseservice.asmx/
PanoramaHAInfo (https://updates.paloaltonetworks.com/
licensesvc/licenseservice.asmx/PanoramaHAInfo)
 2017-11-06 15:14:07.791 -0800 INFO: [hainfo] Data
 string is primarypanoramasn=<varname>X</varname>
 &secondarypanoramasn=<varname>Y</varname> 2017-11-06
 15:14:17.595 -0800 INFO: [hainfo] HTTP_CODE 200, RESPONSE:
 <?xml version="1.0" encoding="utf-8"?> <PanoramaHA
 xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance (http://
www.w3.org/2001/XMLSchema-instance)" xmlns:xsd="http://
www.w3.org/2001/XMLSchema (http://www.w3.org/2001/
```

 ©2025 Palo Alto Networks, Inc.

```
XMLSchema)" xmlns="http://www.paloaltonetworks.com/ (http://
www.paloaltonetworks.com/)"> <success>true</success> </
PanoramaHA> 2017-11-06 15:14:17.596 -0800 INFO: [hainfo]
 Cached HA Peer's serial number <varname>Y</varname>
```

3. Melden Sie sich im Kunden-Support-Portal (CSP) an und wählen Sie **Assets** > **Cloud Services** aus, um zu überprüfen, ob beide Panorama-Peers mit Ihren Prisma Access- und Strata Logging Service-Lizenzen verbunden sind.
4. Überprüfen Sie die Felder für die primäre und sekundäre Panorama-Appliance.

   Die Felder „Authentifizierungscode“, „Modellname“, „Lizenzbeschreibung“ und „Ablaufdatum“ sollten für die primäre und sekundäre Panorama-Appliance identisch sein, da Palo Alto Networks die Prisma Access-Lizenz automatisch mit der sekundären Panorama-Appliance verknüpft hat.

**STEP 5 |** Melden Sie sich bei der sekundären Panorama-Appliance an, um von Panorama verwaltetes Prisma Access zu aktivieren und zu installieren.

Wenn Sie sich beim Kunden-Support-Portal (CSP) anmelden, um das OTP zu generieren, stellen Sie sicher, dass Sie die Seriennummer für die sekundäre Panorama-Appliance angeben.

**STEP 6 |** Führen Sie einen Commit für Ihre Änderungen auf der primären und der sekundären Panorama-Appliance aus.

1. Wählen Sie **Commit** > **Commit und Push** aus, um die Änderung per Push zu übertragen.
2. Klicken Sie auf **OK** und **Push**.

**STEP 7 |** Überprüfen Sie, ob sich die primären und sekundären Panorama-Appliances noch in einem synchronisierten Zustand befinden.

 ©2025 Palo Alto Networks, Inc.

# Vordefinierte Vorlagen: Dienstverbindung oder Remote-Netzwerk einbinden

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

Prisma Access enthält vordefinierte IPSec-Vorlagen für gängige IPSec- und SD-WAN-Geräte von Drittanbietern. Diese Profile beschleunigen und vereinfachen das Onboarding von Dienstverbindungen und Remote-Netzwerkverbindungen, die eines dieser Geräte zum Terminieren der Verbindung verwenden.

Die Freigabe einer gemeinsamen Vorlage ermöglicht es Ihnen auch, mehrere Remote-Verbindungen des Typs „sane“ mit häufig freigegebenen Verschlüsselungen, vorinstallierten Schlüsseln und Peer-IDs einzubinden.

- Vordefinierte Vorlagen: Dienstverbindung oder Remote-Netzwerk einbinden
- Unterstützte IKE- und IPSec-Verschlüsselungsprofile für gängige SD-WAN-Geräte

Prisma Access stellt Ihnen die folgenden vordefinierten Vorlagen zur Verfügung, mit denen Sie IPSec-Tunnel zwischen Ihrem lokalen Gerät und Prisma Access einrichten können:

- IPSec-Tunnel (**Netzwerk** > **IPSec-Tunnel**) unter „Remote_Network_Template“ und „Service_Conn_Template“.
- IKE-Gateways (**Netzwerk** > **Netzwerkprofile** > **IKE-Gateways**) unter „Remote_Network_Template“ und „Service_Conn_Template“.
- IPSec-Verschlüsselungsprofile (**Netzwerk** > **Netzwerkprofile** > **IPSec-Verschlüsselung**) unter „Remote_Network_Template“ und „Service_Conn_Template“.
- IKE-Verschlüsselungsprofile (**Netzwerk** > **Netzwerkprofile** > **IKE-Verschlüsselung**) unter „Remote_Network_Template“ und „Service_Conn_Template“.

Derzeit sind Vorlagen für die folgenden Anbieter verfügbar:

*Zusätzlich zu den folgenden Vorlagen stellen wir eine generische Vorlage bereit, die Sie mit jedem lokalen Gerät verwenden können, das hier nicht aufgeführt ist.*

- Cisco-Appliances:
  - Cisco Integrated Services Router (ISRs)
  - Cisco Adaptive Security Appliances (ASAs)
- Citrix
- Prisma SD-WAN (ehemals CloudGenix)
- Riverbed
- Silver Peak

Gehen Sie wie folgt vor, um eine Dienstverbindung oder eine Remote-Netzwerkverbindung mithilfe der Vorlagen, die von Prisma Access bereitgestellt werden, einzubinden.

 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** Führen Sie in Panorama die Konfiguration so durch, dass die Vorlagen in Panorama angezeigt werden.

Wenn Sie das Cloud Services-Plug-in aktualisieren, werden die neuen Vorlagen nicht automatisch angezeigt. Führen Sie diesen Schritt nach dem Upgrade einmal aus, damit die Vorlagen dauerhaft angezeigt werden. Bei neuen Installationen wird diese Erstkonfiguration als Teil der Ersteinrichtung durchgeführt, und dieser zusätzliche Schritt ist nicht erforderlich.



*Sie können diesen Schritt auch ausführen, wenn Sie diese Vorlagen löschen und sie abrufen müssen.*

- Wählen Sie für Dienstverbindungen **Panorama** > **Cloud Services** > **Konfiguration** > **Diensteinrichtung** aus, klicken Sie auf das Zahnradsymbol im Bereich **Einstellungen**, um die **Einstellungen** zu öffnen, und klicken Sie dann auf **OK**.
- Wählen Sie für Remote-Netzwerkverbindungen die Optionen **Panorama** > **Cloud Services** > **Konfiguration** > **Remote-Netzwerke** aus, klicken Sie auf das Zahnradsymbol im Bereich **Einstellungen**, um die **Einstellungen** zu öffnen, und klicken Sie dann auf **OK**.

**STEP 2 |** Wählen Sie **Netzwerk** und anschließend die richtige **Vorlage** aus (entweder **Remote_Network_Template**, wenn Sie eine Remote-Netzwerkverbindung erstellen, oder **Service_Conn_Template**, wenn Sie eine Dienstverbindung erstellen).

**STEP 3 |** Bestimmen Sie den Gerätetyp, der zum Beenden der Dienstverbindung oder der Remote-Netzwerkverbindung verwendet wird, und suchen Sie eine Vorlage, die mit diesem Gerät verwendet werden soll.



*Wenn Ihr SD-WAN- oder IPSec-Gerät nicht in der Liste aufgeführt ist, verwenden Sie die generischen Profile.*

**STEP 4 |** Wählen Sie **Netzwerk** > **Netzwerkprofile** > **IKE-Gateways** aus und nehmen Sie die folgenden Änderungen am IKE-Gateway-Profil für Ihr Gerät vor:

Sie können die IPSec-Verschlüsselung und IKE-Verschlüsselungsprofile ohne Änderungen verwenden. Sie müssen jedoch bestimmte Änderungen am IKE-Gateway-Profil vornehmen, um es auf die Netzwerkeinstellungen abzustimmen.

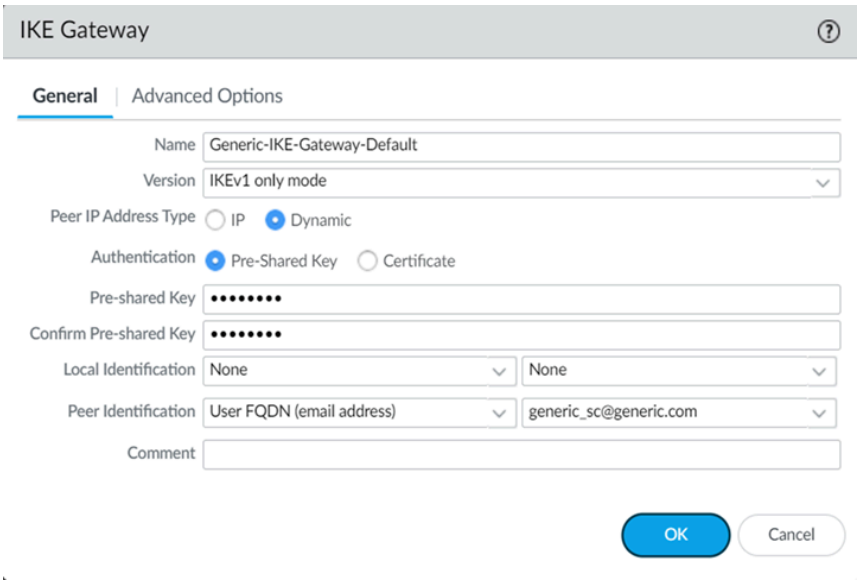
- (Optional) Wenn Sie die öffentliche IP-Adresse des lokalen Geräts kennen, das zum Einrichten des IPSec-Tunnels mit Prisma Access verwendet wird, legen Sie eine statische IP-

 ©2025 Palo Alto Networks, Inc.

Adresse fest, indem Sie den **Peer-IP-Adresstyp IP** angeben und die **Peer-Adresse** für den IPSec-Tunnel eingeben.

- Wenn Sie einen vorab freigegebenen Schlüssel für den IPSec-Tunnel verwenden, geben Sie einen **PSK (Pre-Shared Key)** an.
- Geben Sie als **Peer-Identifizierung** entweder **IP-Adresse** oder **Benutzer-FQDN** an.

  Stellen Sie sicher, dass eine Übereinstimmung mit den hier angegebenen Einstellungen vorliegt, wenn Sie das Gerät konfigurieren, das zum Terminieren der anderen Seite des IPSec-Tunnels verwendet wird.




**STEP 5 |** Binden Sie die Dienstverbindung oder die Remote-Netzwerkverbindung ein, indem Sie die **IPSec-Tunnel**-Konfiguration angeben, die mit dem Gerät auf der anderen Seite des IPSec-Tunnels übereinstimmt.

 ©2025 Palo Alto Networks, Inc.

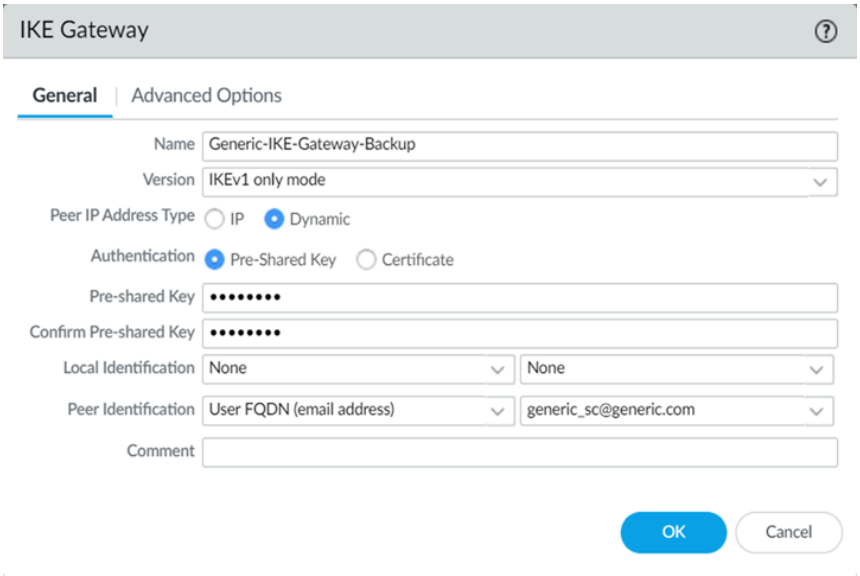
**STEP 6 |** (Optional) Wenn Sie einen Backup-Tunnel (sekundäres WAN) für eine Dienstverbindung oder eine Remoteverbindung hinzufügen müssen, führen Sie die folgenden zusätzlichen Konfigurationsschritte aus.

Die Konfiguration eines sekundären WAN wird in den folgenden Bereitstellungen nicht unterstützt:

- Wenn Ihr sekundäres WAN im Aktiv-Aktiv-Modus mit dem primären IPSec-Tunnel eingerichtet ist.
- Wenn Ihre Kundenendgeräte (Customer Premises Equipment, CPE) in einer Equal Cost Multipath(ECMP)-Konfiguration mit dem primären und sekundären IPSec-Tunnel eingerichtet sind.

1. Erstellen Sie einen neuen IKE-Gateway für den Backup-Tunnel, kopieren Sie die Einstellungen aus der vordefinierten Vorlage, die Sie duplizieren möchten.

   Im folgenden Beispiel wird eine Backup-Tunnel-Konfiguration für generische Netzwerkgeräte erstellt.

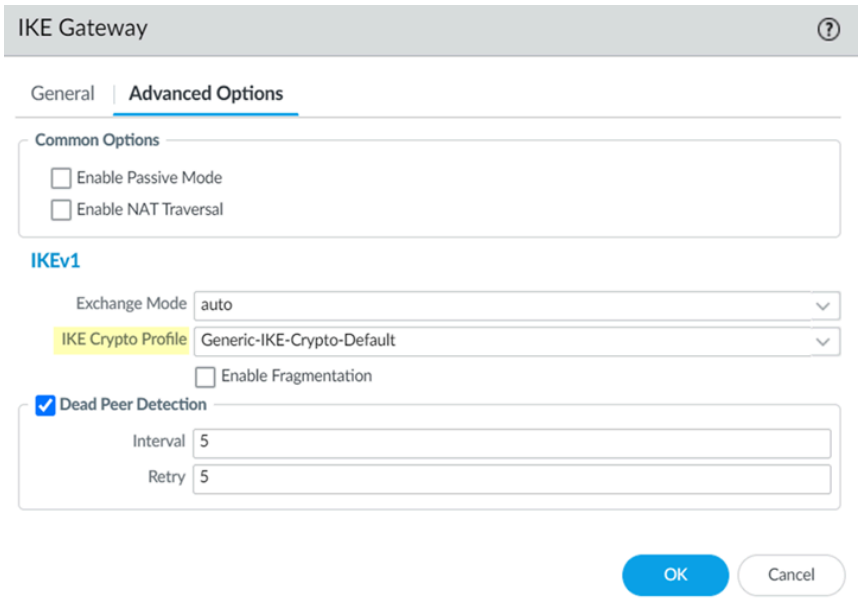



2. Geben Sie unter **Erweiterte Optionen** die Option **IKE-Verschlüsselungsprofil** für die vordefinierte Vorlage an, die Sie verwenden möchten.

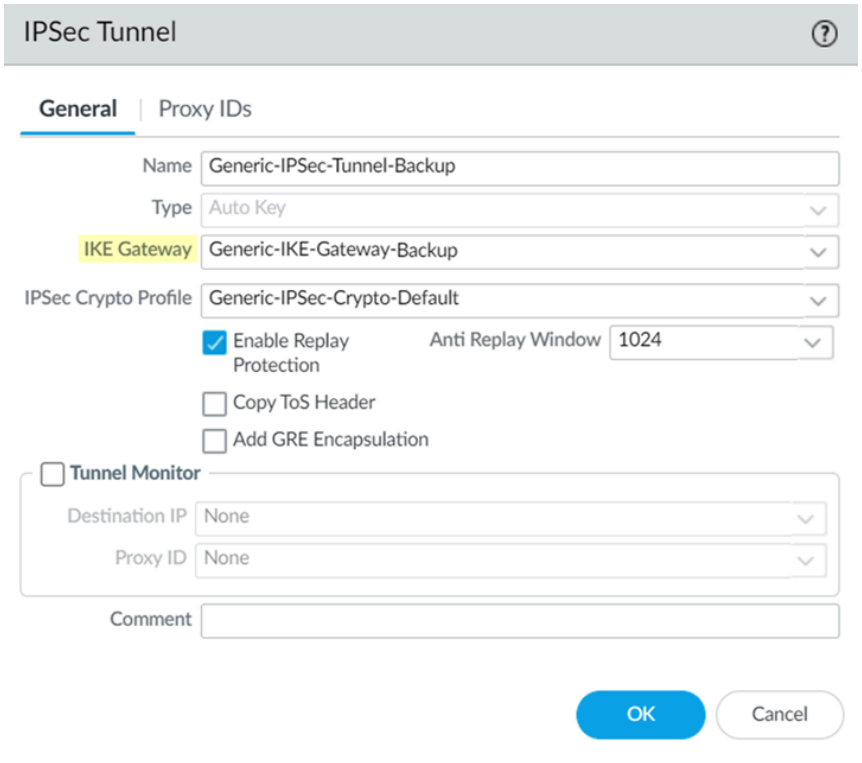
   Palo Alto Networks empfiehlt, für IPSec-Tunnel GCM-Verschlüsselungen anstelle von CBC-Verschlüsselungen zu verwenden.

   Wenn Sie ein Prisma SD-WAN einbinden, wählen Sie **Passiven Modus aktivieren** aus.

 ©2025 Palo Alto Networks, Inc.

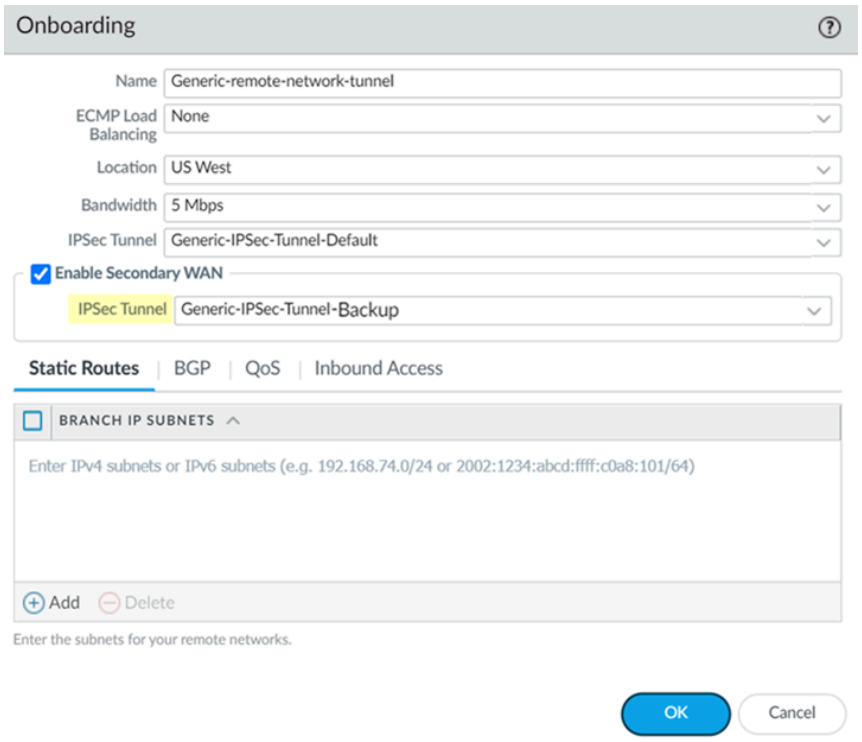



3. Erstellen Sie einen neuen IPSec-Tunnel, indem Sie das neue IKE-Gateway angeben, das Sie erstellt haben, aber alle anderen Einstellungen aus der Standardvorlage kopieren.




4. Wenn Sie die Dienstverbindung oder die Remote-Netzwerkverbindung einbinden, **aktivieren Sie das sekundäre WAN** und geben Sie den Tunnel an, den Sie für das Backup-WAN erstellt haben.

 ©2025 Palo Alto Networks, Inc.




**STEP 7 |** Schließen Sie die Konfiguration der Dienstverbindung oder der Remote-Netzwerkverbindung ab, indem Sie die Verschlüsselungen, den vorab freigegebenen Schlüssel (PSK) und die Peer-IDs auf dem Gerät abgleichen, das zum Beenden der anderen Seite des IPSec-Tunnels verwendet wird.

**STEP 8 |** (Optional) Wenn Sie mehrere Remote-Netzwerkverbindungen einbinden müssen, die dieselben Netzwerkgerätetypen verwenden, **exportieren** Sie die Konfiguration des Remote-Netzwerks, bearbeiten Sie die Einstellungen und **importieren** Sie anschließend diese Konfiguration.

# Unterstützte IKE- und IPSec-Verschlüsselungsprofile für gängige SD-WAN-Geräte

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

In diesem Abschnitt erhalten Sie eine Übersicht über die unterstützten Verschlüsselungsprofile für viele gängige SD-WAN-Geräte. Wenn Sie ein SD-WAN-Gerät konfigurieren, verwenden Sie diese Profile als Richtlinie dafür, was Sie für das Remote-Netzwerk in Prisma Access konfigurieren können.

- Von Aruba SD-WAN unterstützte IKE- und IPSec-Verschlüsselungsprofile

 ©2025 Palo Alto Networks, Inc.

- Von Aryaka SD-WAN unterstützte IKE- und IPSec-Verschlüsselungsprofile
- Von Citrix SD-WAN unterstützte IKE- und IPSec-Verschlüsselungsprofile
- Von Prisma SD-WAN-Geräten unterstützt IKE- und IPSec-Verschlüsselungsprofile
- Von Nuage Networks SD-WAN unterstützte IKE- und IPSec-Verschlüsselungsprofile
- Von Riverbed SteelConnect SD-WAN unterstützte IKE- und IPSec-Verschlüsselungsprofile
- Von Silver Peak SD-WAN unterstützte IKE- und IPSec-Verschlüsselungsprofile
- Von Viptela SD-WAN unterstützte IKE- und IPSec-Verschlüsselungsprofile

 ©2025 Palo Alto Networks, Inc.

 ©2025 Palo Alto Networks, Inc.

# Prisma Access-Dienstverbindungen

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Eine Dienstverbindung, auch als Corporate Access Node (CAN) bezeichnet, ermöglicht mobilen Benutzern und Benutzern in Remote-Netzwerken den Zugriff auf private Apps und Ressourcen sowie die Kommunikation zwischen mobilen Benutzern und Remote-Netzwerken.

Neben Dienstverbindungen bietet Ihnen Palo Alto Networks weitere Dienste, mit denen Sie auf private Apps zugreifen können:

- ZTNA-Connector – Mit dem ZTNA-Connector (Zero Trust Network Access) können Sie Prisma Access einfach und sicher mit privaten Apps Ihres Unternehmens verbinden. Der ZTNA-Connector bietet mobilen Benutzern und Benutzern an Zweigstellen über einen automatisierten sicheren Tunnel Zugriff auf Ihre privaten Apps. Sie können auch private Apps automatisch erkennen für ZTNA, um die Verwendung der Cloud Identity Engine zu schützen.
- Prisma Access Colo-Connect – Colo-Connect ermöglicht Ihnen die Verwendung von Prisma Access, um private Apps mithilfe einer Cloud-Verbindung zu sichern, die Dienstverbindungen mit hoher Bandbreite bereitstellen kann.

Palo Alto Networks empfiehlt, immer eine Dienstverbindung in Ihrer Prisma Access-Bereitstellung zu erstellen. Alle Dienstverbindungen weisen folgende Merkmale auf:

- Eine Dienstverbindung ermöglicht den Zugriff auf die Ressourcen in Ihrer Zentrale oder Ihrem Rechenzentrum.

  Wenn Ihre Sicherheitsrichtlinie beispielsweise die Benutzerauthentifizierung mit einem lokalen Authentifizierungsdienst wie Active Directory erfordert, müssen Sie Prisma Access aktivieren, um auf den Unternehmensstandort zugreifen zu können, an dem sich der Dienst befindet (und ein Dienstkonto einrichten, über das der Dienst darauf zugreifen kann). Wenn Sie über Unternehmensressourcen verfügen, auf die Ihre Remote-Netzwerke und mobilen Benutzer zugreifen müssen, müssen Sie analog dazu Prisma Access aktivieren, um auf das entsprechende Unternehmensnetzwerk zuzugreifen.

  Wenn Sie aus diesem Grund Dienstverbindungen erstellen, sollten Sie die Dienstverbindungen planen, bevor Sie diese implementieren.
- Über eine Dienstverbindung können Remote-Netzwerke und mobile Benutzer miteinander kommunizieren.

  Auch wenn Sie keinen Zugriff auf Ihre Zentrale oder Ihr Rechenzentrum benötigen, müssen Sie Ihren mobilen Benutzern möglicherweise den Zugriff auf Ihre Remote-Netzwerkstandorte ermöglichen. In diesem Fall können Sie eine Dienstverbindung mit Platzhalterwerten

erstellen. Dies ist erforderlich, da zwar alle Remote-Netzwerkverbindungen vollständig vermascht sind, mobile Benutzer jedoch über die Dienstverbindung in einem Hub-and-Spoke-Netzwerk eine Verbindung mit Remote-Netzwerken herstellen. Aus diesem Grund können Sie auch eine Dienstverbindung mit Platzhalterwerten erstellen, wenn sich Ihre vorhandene Dienstverbindung nicht an einem idealen geografischen Standort befindet.

- Dienstverbindungen unterstützen die Sprachlokalisierung nicht, da der Ausgang in das Internet über Dienstverbindungen nicht unterstützt wird. Prisma Access weist nur eine Dienst-IP-Adresse pro Dienstverbindung zu. Diese IP-Adresse ist geografisch bei dem Compute-Standort registriert, der dem Standort entspricht, den Sie während des Onboardings angegeben haben.

Wie viele Dienstverbindungen Sie erhalten, hängt von Ihrer Prisma Access-Lizenz ab.

- Wenn Sie eine ZTNA- oder Enterprise-Lizenz haben, hängt die Anzahl der Dienstverbindungen von Ihrer Lizenzedition ab. Wenn Sie über eine lokale Edition verfügen, können Sie maximal zwei Dienstverbindungen konfigurieren. Wenn Sie über eine weltweite Edition verfügen, können Sie maximal fünf Dienstverbindungen konfigurieren.
  - Mit dem ZTNA Connector können Sie Prisma Access mit den privaten Apps Ihres Unternehmens verbinden. Der ZTNA-Connector bietet mobilen Benutzern und Benutzern an Zweigstellen über einen automatisierten sicheren Tunnel Zugriff auf Ihre privaten Apps. Weitere Informationen finden Sie unter Prisma Access ZTNA-Connector.
- Wenn Sie mehrere Mandanten verwalten und über eine ZTNA- oder Enterprise-Lizenz verfügen, hängt die Anzahl der Dienstverbindungen pro Mandant von der Anzahl der Einheiten ab, die Sie pro Mandant zuweisen, und von der Art der Lizenz, die Sie besitzen.
  - Wenn Sie über eine globale Lizenz verfügen und einem Mandanten mindestens 1.000 Einheiten zuweisen, können Sie diesem Mandanten maximal fünf Dienstverbindungen zuweisen.
  - Wenn Sie über eine globale Lizenz verfügen und einem Mandanten zwischen 200 und 999 Einheiten zuweisen, können Sie diesem Mandanten maximal zwei Dienstverbindungen zuweisen (entsprechend der Anzahl der Verbindungen für eine lokale Bereitstellung).
  - Wenn Sie über eine lokale Lizenz verfügen, können Sie maximal zwei Dienstverbindungen pro Mandant zuweisen, unabhängig von der Anzahl der Einheiten, die Sie über das Minimum von 200 hinaus zuweisen.

  Sie können sowohl für globale als auch für lokale Lizenzen zusätzliche Lizenzen für Dienstverbindungen erwerben, sollten mehr erforderlich sein. Informationen zu Dienstverbindungen in erweiterten Bereitstellungen finden Sie unter Prisma Access-Dienstverbindungen – Erweiterte Bereitstellungen.

Bevor Sie mit der Konfiguration Ihrer Dienstverbindungen beginnen können, überprüfen Sie, welche Informationen Sie zunächst sammeln müssen.

 ©2025 Palo Alto Networks, Inc.

# Dienstverbindung planen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Erstellen Sie Dienstverbindungen, damit Prisma Access die folgenden Aufgaben ausführen kann:

- **Zulassen des Zugriffs auf die Ressourcen in Ihrer Zentrale oder Ihrem Rechenzentrum.**

  Wenn Sie über Unternehmensressourcen verfügen, auf die Ihre Remote-Netzwerke und mobilen Benutzer Zugriff benötigen, dann müssen Sie für Prisma Access den Zugriff auf das entsprechende Unternehmensnetzwerk aktivieren.
- **Erlauben Sie Remote-Netzwerken und mobilen Benutzern, miteinander zu kommunizieren.**

  Auch wenn Ihre Prisma Access-Benutzer keine Verbindung zu Ihrer Zentrale oder Ihrem Rechenzentrum benötigen, sollten Sie Ihren mobilen Benutzern möglicherweise den Zugriff auf Ihre Remote-Netzwerkstandorte erlauben. Für diesen Anwendungsfall sind Dienstverbindungen erforderlich, da zwar alle Remote-Netzwerkstandorte vollständig vermascht sind, die Infrastruktur der mobilen Benutzer jedoch nicht. Die Einrichtung einer Minimalkonfiguration für eine Dienstverbindung ermöglicht die Erstellung eines Hub-and-Spoke-Netzwerks, das mobile Benutzer für den Zugriff auf ein Zweignetzwerk benötigen.

  Um die Netzwerkeffizienz zu verbessern, platzieren Sie Dienstverbindungen in der Nähe des Remote-Netzwerks oder der Netzwerke, auf die mobile Benutzer am häufigsten zugreifen.

## Sammeln dieser Informationen zu Ihren Zentralen oder Rechenzentren

**Konfigurieren Sie vor Beginn** eine Dienstverbindung, sammeln Sie die folgenden Informationen für jede Ihrer Zentralen oder Rechenzentren, mit denen Prisma Access eine Verbindung herstellen können soll.

*Sie müssen diese Informationen nicht sammeln, wenn Sie eine Dienstverbindung nur erstellen, um mobilen Benutzern den Zugriff auf Remote-Netzwerkstandorte zu ermöglichen.*

Für **Prisma Access (Managed by Strata Cloud Manager)**- und **Prisma Access (Managed by Panorama)**-Dienstverbindungen:

- ❑ IPSec-fähige Firewall-, Router- oder SD-WAN-Geräteverbindung an Ihrem Unternehmensstandort.
- ❑ IPSec-Einstellungen zum Abschluss des primären VPN-Tunnels von Prisma Access zum IPSec-fähigen Gerät in Ihrem Unternehmensnetzwerk.

 ©2025 Palo Alto Networks, Inc.

- IPSec-Einstellungen zum Abschluss des sekundären VPN-Tunnels von Prisma Access zum IPSec-fähigen Gerät in Ihrem Unternehmensnetzwerk.

  Wenn Ihre vorhandene Vorlage Konfigurationen für IPSec-Tunnel, Tunnelüberwachung und IPSec-Verschlüsselungsprofile umfasst, können Sie diese Vorlage zum Vorlagenstack hinzufügen, um den Prozess der Erstellung von IPSec-Tunneln zu vereinfachen. Alternativ hierzu können Sie auch die Vorlage Service_Conn_Template bearbeiten, die automatisch erstellt wird, und die IPSec-Konfigurationen erstellen, die für die Erstellung des IPSec-Tunnels zum Unternehmensstandort erforderlich sind. Prisma Access stellt Ihnen außerdem einen Satz vordefinierter IPSec-Vorlagen für einige häufig verwendete Netzwerkgeräte und eine generische Vorlage für jedes Gerät zur Verfügung, das nicht in den vordefinierten Vorlagen enthalten ist.
- Liste der IP-Subnetze am Standort.
- Liste der internen Domänen, die Prisma Access auflösen können muss.
- IP-Adresse eines Unternehmenszugriffsknotens am Standort Ihres Netzwerks, an dem Prisma Access ICMP-Ping-Anfragen für die IPSec-Tunnelüberwachung senden können muss.

  Stellen Sie sicher, dass diese Adresse für ICMP aus dem gesamten Prisma Access-Infrastruktursubnetz erreichbar ist.
- Einstellungen für die Netzwerkerreichbarkeit des Subnetzes für die Dienstinfrastruktur.

  Definieren Sie das gesamte Subnetz für die Dienstinfrastruktur so, dass es von der Zentrale oder dem Rechenzentrum aus erreichbar ist. Prisma Access verwendet IP-Adressen für den gesamten Datenverkehr der Kontrollebene, der aus diesem Subnetz stammt.

Nur für **Prisma Access Panorama**-Dienstverbindungen:

*Diese Informationen werden nur bei der Planung von Dienstverbindungen in **Prisma Access (Managed by Panorama)** benötigt.*

- Das Dienstkonto für Ihre Authentifizierung, falls für den Zugriff erforderlich.
- Der Routingtyp (statisch oder dynamisch (BGP)), der für Dienstverbindungen verwendet werden soll.

  Damit Benutzer von Prisma Access (Managed by Panorama) an die erforderlichen Ressourcen weitergeleitet werden können, müssen Sie die Routen den Ressourcen bereitstellen. Sie können dazu eine oder mehrere der folgenden Vorgehensweisen nutzen:

  - Definieren Sie eine statische Route zu jedem Subnetz oder zu jeder einzelnen Ressource, auf die Ihre Benutzer zugreifen können sollen.
  - Konfigurieren Sie BGP zwischen Ihren Dienstverbindungsstandorten und Prisma Access.
  - Verwenden Sie eine Kombination aus beiden Methoden

 ©2025 Palo Alto Networks, Inc.

# Konfigurieren einer Dienstverbindung in Prisma Access

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Erstellen Sie Dienstverbindungen, damit Prisma Access die folgenden Aufgaben ausführen kann:

- **Zulassen des Zugriffs auf die Ressourcen in Ihrer Zentrale oder Ihrem Rechenzentrum.**

  Wenn Sie über Unternehmensressourcen verfügen, auf die Ihre Remote-Netzwerke und mobilen Benutzer Zugriff benötigen, dann müssen Sie für Prisma Access den Zugriff auf das entsprechende Unternehmensnetzwerk aktivieren. Bevor Sie mit der Konfiguration einer Dienstverbindung beginnen, erfassen Sie die folgenden Informationen für alle Ihre Zentralen oder Rechenzentren, zu denen Prisma Access eine Verbindung herstellen können soll.

  - IPSec-fähige Firewall-, Router- oder SD-WAN-Geräteverbindung an Ihrem Unternehmensstandort.
  - IPSec-Einstellungen zum Abschluss des primären VPN-Tunnels von Prisma Access zum IPSec-fähigen Gerät in Ihrem Unternehmensnetzwerk.
  - IPSec-Einstellungen zum Abschluss des sekundären VPN-Tunnels von Prisma Access zum IPSec-fähigen Gerät in Ihrem Unternehmensnetzwerk.

    Wenn Sie über eine vorhandene Vorlage verfügen, die Konfigurationen für IPSec-Tunnel, die Tunnelüberwachung und IPSec-Verschlüsselungsprofile enthält, können Sie diese Vorlage zum Vorlagenstack hinzufügen, um den Prozess der Erstellung von IPSec-Tunneln zu vereinfachen. Alternativ hierzu können Sie auch die Vorlage Service_Conn_Template bearbeiten, die automatisch erstellt wird, und die IPSec-Konfigurationen erstellen, die für die Erstellung des IPSec-Tunnels zum Unternehmensstandort erforderlich sind. Prisma Access stellt Ihnen außerdem einen Satz vordefinierter IPSec-Vorlagen für einige häufig verwendete Netzwerkgeräte und eine generische Vorlage für jedes Gerät zur Verfügung, das nicht in den vordefinierten Vorlagen enthalten ist.
  - Liste der IP-Subnetzwerke am Standort.
  - Liste der internen Domänen, die Prisma Access auflösen können muss.
  - IP-Adresse eines Unternehmenszugriffsknotens am Standort Ihres Netzwerks, an die Prisma Access ICMP-Ping-Anfragen für die IPSec-Tunnelüberwachung senden können muss.

    Stellen Sie sicher, dass diese Adresse für ICMP aus dem gesamten Prisma Access-Infrastruktursubnetz erreichbar ist.
  - Einstellungen für die Netzwerkerreichbarkeit des Subnetzes für die Dienstinfrastruktur.

    Definieren Sie das gesamte Subnetz für die Dienstinfrastruktur so, dass es von der Zentrale oder dem Rechenzentrum aus erreichbar ist. Prisma Access verwendet IP-Adressen für den gesamten Datenverkehr der Kontrollebene, der aus diesem Subnetz stammt.

 ©2025 Palo Alto Networks, Inc.

- (Nur für Prisma Access (Managed by Panorama)) Das Dienstkonto für Ihre Authentifizierung, falls für den Zugriff erforderlich.
- (Nur für Prisma Access (Managed by Panorama)) Der Routingtyp (statisch oder dynamisch (BGP)), der für Dienstverbindungen verwendet werden soll.
- (Nur für Prisma Access (Managed by Panorama)) Um Benutzer zu den von ihnen benötigten Ressourcen weiterzuleiten, müssen Sie die Routen zu den Ressourcen bereitstellen. Sie können dazu eine oder mehrere der folgenden Vorgehensweisen nutzen:
  - Definieren Sie eine statische Route zu jedem Subnetzwerk oder zu jeder einzelnen Ressource, auf die Ihre Benutzer zugreifen können sollen.
  - Konfigurieren Sie BGP zwischen Ihren Dienstverbindungsstandorten und Prisma Access .
  - Verwenden Sie eine Kombination beider Methoden

- **Erlauben Sie Remote-Netzwerken und mobilen Benutzern, miteinander zu kommunizieren.**

  Auch wenn Ihre Prisma Access-Benutzer keine Verbindung zu Ihrer Zentrale oder Ihrem Rechenzentrum benötigen, sollten Sie Ihren mobilen Benutzern möglicherweise den Zugriff auf Ihre Remote-Netzwerkstandorte erlauben. Für diesen Anwendungsfall sind Dienstverbindungen erforderlich, da zwar alle Remote-Netzwerkstandorte vollständig vernetzt sind, die Infrastruktur der mobilen Benutzer jedoch nicht. Die Einrichtung einer Minimalkonfiguration für eine Dienstverbindung ermöglicht die Erstellung eines Hub-and-Spoke-Netzwerks, das mobile Benutzer für den Zugriff auf ein Zweignetzwerk benötigen.

  Um die Netzwerkeffizienz zu verbessern, platzieren Sie Dienstverbindungen in der Nähe des Remote-Netzwerks oder der Netzwerke, auf die mobile Benutzer am häufigsten zugreifen.

- Strata Cloud Manager
- Panorama

## Konfigurieren einer Dienstverbindung in Prisma Access (Strata Cloud Manager)

Führen Sie die folgenden Schritte aus, um eine Dienstverbindung für Prisma Access (Managed by Strata Cloud Manager) zu konfigurieren, mit der Sie Zugriff auf private Apps oder interne Unternehmensressourcen erhalten.

**STEP 1 |** Wählen Sie **Workflows** > **Prisma Access-Einrichtung** > **Dienstverbindungen** und **Dienstverbindung hinzufügen** aus.

**STEP 2 |** Ordnen Sie der Dienstverbindung im Feld **Name** einen aussagekräftigen Namen zu.

**STEP 3 |** Wählen Sie den **Prisma Access-Standort** Ihrer Zentrale oder Ihres Rechenzentrums aus.

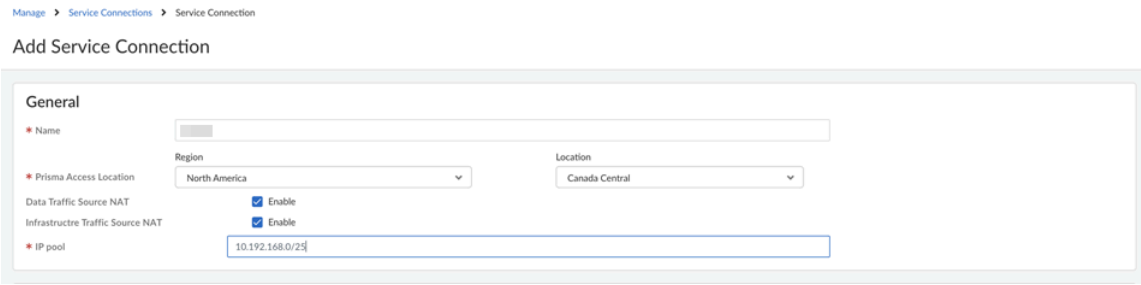
 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** (Optional) Aktivieren Sie die Quell-NAT für mobile Benutzer – GlobalProtect-IP-Pooladressen, IP-Adressen im Infrastruktursubnetz oder beides.

Sie können ein Subnetz an einer oder mehreren Dienstverbindungen angeben, die für den NAT-Datenverkehr zwischen mobilen Prisma Access-GlobalProtect-Benutzern und privaten Anwendungen und Ressourcen in einem Rechenzentrum verwendet werden.

- **Quell-NAT des Datenverkehrs** – Führt die NAT für Adressen des IP-Adresspools mobiler Benutzer aus, sodass diese nicht ans Rechenzentrum mitgeteilt werden und nur die von Ihnen bei den Dienstverbindungen angegebenen Subnetze ans Rechenzentrum mitgeteilt und geroutet werden.
- **Quell-NAT des Infrastrukturdatenverkehrs** – Führt die NAT für Adressen aus dem Infrastruktursubnetz aus, sodass diese nicht ans Rechenzentrum mitgeteilt werden und nur die von Ihnen bei den Dienstverbindungen angegebenen Subnetze im Rechenzentrum mitgeteilt und geroutet werden.
- **Benutzer-ID** – Wird diese Option ausgewählt, verwendet Prisma Access diese Dienstverbindung zur Identitätsweitergabe.

  ***Verwaltung der Umverteilung von Benutzer-IDs*** *– In bestimmten Fällen sind bei der Umverteilung von Benutzer-IDs in besonders umfangreichen Prisma Access-Bereitstellungen detaillierte Kontrollen erforderlich. Mithilfe der Umverteilungsverwaltung für Benutzer-IDs können Sie das standardmäßige Identitätsumverteilungsverhalten für bestimmte Dienstverbindungen manuell deaktivieren, indem Sie das Häkchen in der Spalte* ***Benutzer-ID*** *entfernen und dann bestimmte Dienstverbindungen auswählen, die für die Identitätsweitergabe verwendet werden sollen. Für die meisten Konfigurationen ist dieser Arbeitsschritt nicht erforderlich. Wenden Sie sich an den Support von Palo Alto Networks, um diese Funktionalität zu aktivieren.*
- **Quell-NAT-Pool** – Geben Sie den IP-Adresspool an, der zum Ausführen von NAT im IP-Adresspool für mobile Benutzer und/oder im Infrastruktursubnetz verwendet wird.
  - Verwenden Sie ein privates IP-Subnetz (RFC 1918) oder ein geeignetes Subnetz, das in Ihrer Routingdomäne weitergeleitet werden kann.
  - Stellen Sie sicher, dass sich das Subnetz nicht mit dem GlobalProtect-IP-Adresspool für mobile Benutzer, dem Infrastruktursubnetz oder anderen für diesen Mandanten verwendeten Quell-NAT-Adressen überschneidet.
  - Geben Sie ein Subnetz zwischen /25 und /32 ein.




 ©2025 Palo Alto Networks, Inc.

**STEP 5 |** Wählen Sie einen **IPSec-Tunnel**aus. Wenn Sie noch keinen primären oder sekundären IPSec-Tunnel eingerichtet haben, wählen Sie **Einrichtung** aus und führen Sie dann die folgenden Schritte aus.

1. Geben Sie im Feld **Name** einen aussagekräftigen Namen für den Tunnel ein.
2. Wählen Sie den **Zweiggerätetyp** für das IPSec-Gerät und die Zentrale oder das Rechenzentrum aus, die bzw. das Sie zum Einrichten des Tunnels mit Prisma Access verwenden möchten.
3. Wählen Sie für die **IP-Adresse des Zweiggeräts** entweder eine **statische IP**-Adresse aus, die den Tunnelendpunkt identifiziert, oder eine **dynamische** IP-Adresse.

   Wenn Sie die **IP-Adresse des Zweiggeräts** auf **Dynamisch**setzen, müssen Sie auch die IKE-ID für die Zentrale oder das Rechenzentrum (**IKE Lokale Identifikation**) oder für Prisma Access (**IKE Peer-Identifikation**) hinzufügen, um die Authentifizierung der IPSec-Peers zu ermöglichen.

   Da Sie erst dann über die Werte verfügen, die Sie für die Prisma Access-IKE-ID (**IKE Peer-Identifikation**) verwenden sollten, wenn die Dienstverbindung vollständig bereitgestellt ist, ist es meist sinnvoll, die IKE-ID für die Zentrale oder das Rechenzentrum (**IKE Lokale Identifikation**) festzulegen und nicht die Prisma Access-IKE-ID.

**STEP 6 |** Aktivieren Sie die **Tunnelüberwachung**.

Geben Sie eine **Ziel-IP**-Adresse für die Tunnelüberwachung im Netzwerk der Zentrale oder des Rechenzentrums für Prisma Access ein, um zu ermitteln, ob der Tunnel aktiv ist. Wenn das IPSec-Gerät in der Zweigstelle eine richtlinienbasierte Lösung verwendet, geben Sie die zugehörige **Proxy-ID** ein.

Die von Ihnen eingegebene IP-Adresse für die Tunnelüberwachung wird automatisch zur Liste der Zweigstellensubnetzwerke hinzugefügt.

**STEP 7 |** **Speichern** Sie die Tunneleinstellungen.

**STEP 8 |** Um Routing- und Quality-of-Service-Einstellungen hinzuzufügen oder anzupassen, rufen Sie **Workflows** > **Prisma Access-Einrichtung** > **Dienstverbindungen**und **Dienstverbindung hinzufügen** auf. **Richten Sie** die **Routing**- oder **QoS**-Einstellungen ein oder **bearbeiten Sie sie**.

**STEP 9 |** Konfigurieren Sie statische Routen.

1. Wenn Sie statische Routen verwenden, um den Datenverkehr zu und von der Zentrale oder zum oder vom Rechenzentrum weiterzuleiten, wählen Sie **Hinzufügen** aus, um die IP-Subnetze oder IP-Adressen hinzuzufügen, die Sie am Standort der Zweigstelle sichern möchten.

   Wenn Sie Änderungen an den IP-Subnetzen im Netzwerk Ihrer Zentrale oder Ihres Rechenzentrums vornehmen, müssen Sie die statischen Routen manuell aktualisieren.

 ©2025 Palo Alto Networks, Inc.

**STEP 10 |** Konfigurieren Sie das dynamische Routing.

1. Wenn beim dynamischen Routing der Zentrale oder dem Subnetz des Rechenzentrums die Informationen mitgeteilt werden sollen, wählen Sie die Option **BGP für dynamisches Routing aktivieren** aus.
2. (Optional) Wählen Sie einen Wert für **MRAI-Timer** aus.

   Das BGP-Routing bietet einen Timer namens *Minimum Route Advertisement Interval (MRAI)*, den Sie verwenden können, um die BGP-Routingkonvergenz in Ihrem Netzwerk anzupassen. MRAI dient zur Ratenbegrenzung von Aktualisierungen auf Zielbasis und die BGP-Router warten mindestens die konfigurierte MRAI-Zeit ab, bevor sie eine Mitteilung für dasselbe Präfix senden. Eine kleinere Zahl ermöglicht eine schnellere Konvergenzzeit, erzeugt jedoch mehr Mitteilungen in Ihrem Netzwerk. Eine höhere Zahl verringert die Anzahl der Mitteilungen, die gesendet werden können, kann aber auch die Routingkonvergenz verlangsamen. Sie entscheiden, welche Anzahl Sie in Ihr Netzwerk einfügen wollen, um das optimale Gleichgewicht zwischen schnellerer Routingkonvergenz und weniger Mitteilungen zu erreichen.

   Konfigurieren Sie einen MRAI-Bereich zwischen 1 und 600 Sekunden, wobei der Standardwert 30 Sekunden beträgt.
3. Um die Anzahl der über BGP an Ihr Customer Premises Equipment (CPE) gesendeten IP-Subnetzmitteilungen für mobile Benutzer zu verringern, geben Sie an, dass Prisma Access die Subnetze vor der Mitteilung zusammenfassen soll. Wählen Sie hierzu **Mobile Benutzerrouten vor dem Mitteilen zusammenfassen** aus.

   Standardmäßig kündigt Prisma Access die IP-Adresspools der mobilen Benutzer in Blöcken von /24 Subnetzen an; wenn Sie sie zusammenfassen, kündigt Prisma Access den Pool basierend auf dem von Ihnen angegebenen Subnetz an. Beispiel: Prisma Access teilt einen öffentlichen, mobilen IP-Pool für Benutzer mit der Angabe 10.8.0.0/20 unter Verwendung des Subnetzes /20 mit, anstatt den Pool in die Subnetze 10.8.1.0/24, 10.8.2.0/24, 10.8.3.0/24 usw. zu unterteilen, bevor sie mitgeteilt werden. Durch die Zusammenfassung dieser Ankündigungen kann die Anzahl der in den CPE-Routingtabellen gespeicherten Routen reduziert werden. Sie können z. B. die Zusammenfassung von IP-Pools mit Cloud-VPN-Gateways (Virtual Private Gateways (VGWs) oder Transit Gateways (TGWs)) verwenden, die eine begrenzte Anzahl von Routen akzeptieren können.
4. (Optional) Damit Prisma Access eine Mitteilung für das Remote-Netzwerk über die Standardroute mithilfe von eBGP erstellt, wählen Sie **Standardroute mitteilen** aus. Vergewissern Sie sich, dass für Ihr Netzwerk keine andere Standardroute vorhanden ist, die von BGP angekündigt wurde, da es sonst zu Routingproblemen in Ihrem Netzwerk kommen kann.
5. (Optional) Wenn Sie ein sekundäres WAN konfiguriert haben und die Peer-Adresse für den sekundären (Backup-)BGP-Peer ändern müssen, dann wählen Sie **Anderen BGP-Peer für sekundären Tunnel verwenden** aus und geben Sie einen eindeutigen Peer und optional eine lokale IP-Adresse für das sekundäre WAN ein.
6. Um eine Community von Dienstverbindungen zu den ausgehenden Präfixen von den eBGP-Peers auf dem Customer Premises Equipment (CPE) hinzuzufügen, setzen

 ©2025 Palo Alto Networks, Inc.

Sie **No-Export-Community hinzufügen** auf **Aktiviert – Ausgang**. Diese Funktion ist standardmäßig auf **Deaktiviert** eingestellt.

Wählen Sie nicht **Aktiviert – Eingang** oder **Aktiviert – Beide** aus, da diese Optionen nicht unterstützt werden.

7. (Optional) Wählen Sie **Routen nicht exportieren** aus, um zu verhindern, dass Prisma Access Routen an die Zentrale oder das Rechenzentrum weiterleitet.

   Standardmäßig teilt Prisma Access alle BGP-Routinginformationen einschließlich lokaler Routen und aller Präfixe mit, die von anderen Dienstverbindungen, Remote-Netzwerken und Subnetzen mobiler Benutzer empfangen werden. Aktivieren Sie dieses Kontrollkästchen, um Prisma Access daran zu hindern, BGP-Mitteilungen zu senden. Die empfangenen BGP-Informationen werden aber weiterhin verwendet, um Informationen zu Routen anderer BGP-Nachbarn zu erhalten.

   *Da Prisma Access keine BGP-Mitteilungen sendet, müssen Sie, wenn Sie diese Option auswählen, statische Routen auf dem lokalen Gerät konfigurieren, um Routen zurück zu Prisma Access einzurichten.*

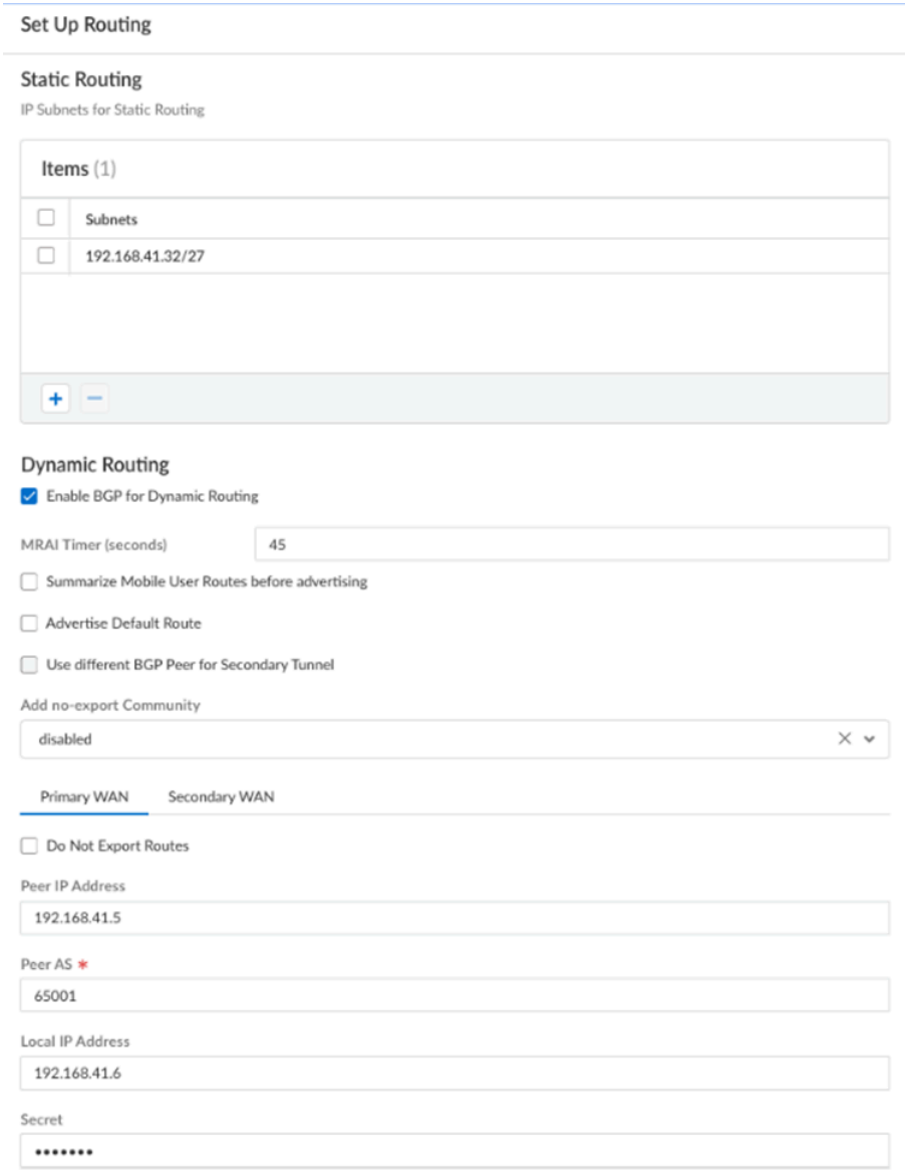
8. Geben Sie die **Peer-IP-Adresse** ein, die als Router-ID des eBGP-Routers im Netzwerk der Zentrale oder des Rechenzentrums zugewiesen wurde.
9. Geben Sie das **Peer-AS**, d. h. das autonome System (AS) für Ihr Netzwerk ein.

   Verwenden Sie eine RFC 6996-konforme private BGP-AS-Nummer.
10. Geben Sie die **lokale IP-Adresse** ein, die Prisma Access als lokale IP-Adresse für BGP verwendet.

    Eine lokale Adresse ist nur erforderlich, wenn Ihr Gerät in der Zentrale oder im Rechenzentrum diese Adresse für ein erfolgreiches BGP-Peering benötigt. Stellen Sie sicher, dass die angegebene Adresse nicht mit IP-Adressen im Infrastruktursubnetz oder in den Subnetzen des Remote-Netzwerks in Konflikt steht oder sich mit diesen überschneidet.
11. Geben Sie einen Wert für **Geheimer Schlüssel** ein, um die BGP-Peer-Kommunikation zu authentifizieren.

 ©2025 Palo Alto Networks, Inc.

12. Wählen Sie **Geheimen Schlüssel bestätigen** aus.

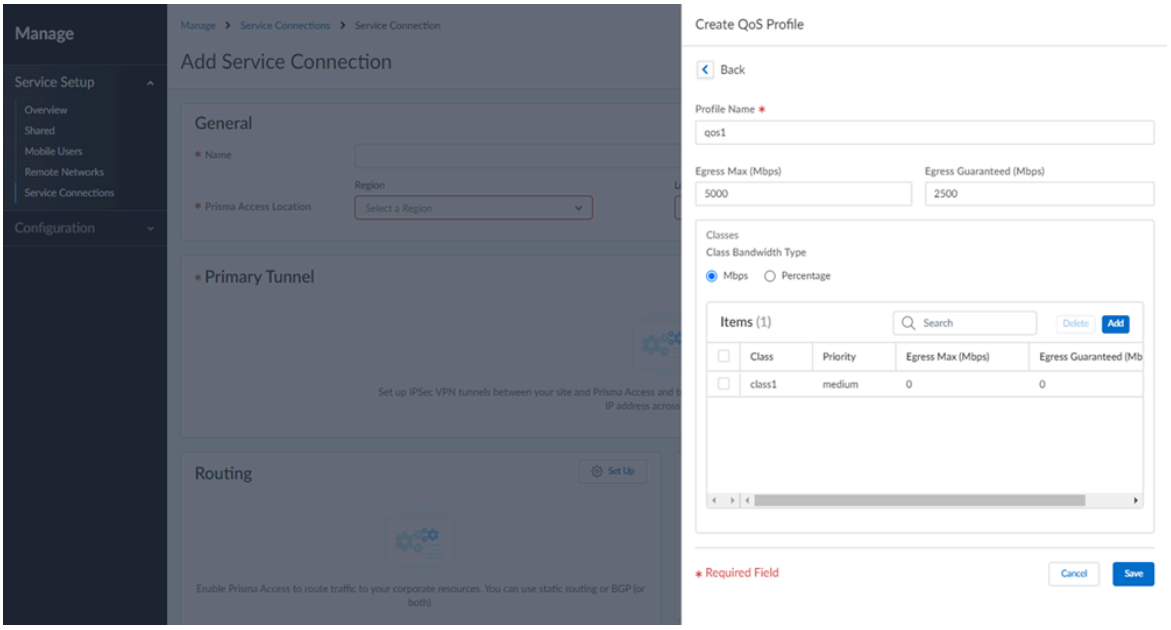



**STEP 11 |** (Optional) Konfigurieren Sie QoS.

Fügen Sie zunächst ein QoS-Profil hinzu, um die QoS-Klassen zu definieren, die den Datenverkehr zwischen der Zentrale oder dem Rechenzentrum und Prisma Access steuern. Anschließend erstellen Sie eine QoS-Richtlinienregel und fügen das Profil zur Regel hinzu,

 ©2025 Palo Alto Networks, Inc.

um für QoS den Abgleich des Datenverkehrs in der Zentrale oder im Rechenzentrum durchzusetzen.




1. Geben Sie einen Namen für Ihr **QoS-Profil** ein.
2. Wählen Sie **Neu erstellen** aus.
3. Legen Sie unter **Ausgang maximal**den maximalen Durchsatz (in Mbit/s) für den Datenverkehr fest, der die Dienstverbindung der Zentrale oder des Rechenzentrums verlässt.

   Sie können einen Wert bis zur maximal lizenzierten Bandbreite Ihrer Zentrale oder Ihres Rechenzentrums angeben.
4. Legen Sie die garantierte Bandbreite als **Ausgang garantiert** (in Mbit/s) fest.

   Für den Datenverkehr, der den Wert für „Garantierter Ausgang“ überschreitet, wird zwar das beste Ergebnis angestrebt, kann jedoch nicht garantiert werden. Sollte die garantierte Bandbreite nicht vollständig genutzt werden, steht der verbleibende Rest für den gesamten Datenverkehr zur Verfügung.
5. Definieren Sie jede QoS-**Klasse** und fügen Sie sie einer Richtlinienregel hinzu.

   Eine QoS-Klasse bestimmt die Priorität und Bandbreite für Datenverkehr, der einer QoS-Richtlinienregel entspricht. In einem einzigen QoS-Profil sind bis zu acht QoS-Klassen

 ©2025 Palo Alto Networks, Inc.

definierbar. Sofern nicht anders konfiguriert, wird Datenverkehr, der keiner QoS-Klasse entspricht, die Klasse 4 zugewiesen.

6. Konfigurieren Sie die **Priorität** einer QoS-Klasse.

   Zu den Prioritäten gehören „Echtzeit“, „Hoch“, „Mittel“ oder „Niedrig“.

7. Konfigurieren Sie den Wert für **Ausgang maximal**.

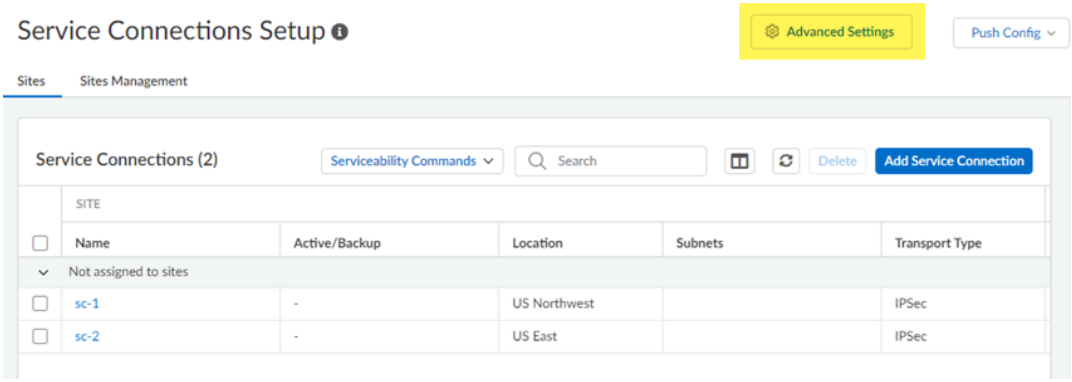
   Der maximale Ausgangswert für eine QoS-Klasse darf bzw. die kombinierten maximalen Ausgangswerte für mehrere QoS-Klassen dürfen den maximalen Ausgangswert für das QoS-Profil nicht überschreiten.

8. Konfigurieren Sie den Wert für **Ausgang garantiert**.

   Die der QoS-Klasse zugewiesene garantierte Bandbreite ist nicht für diese Klasse reserviert; ungenutzte Bandbreite bleibt für den gesamten Datenverkehr verfügbar. Für den Klassendatenverkehr, der den Wert für „Ausgang garantiert“ überschreitet, wird zwar das beste Ergebnis angestrebt, kann jedoch nicht garantiert werden.

 ©2025 Palo Alto Networks, Inc.

**STEP 12 |** Konfigurieren Sie **Erweiterte Einstellungen** für Ihre Dienstverbindung.




1. Geben Sie die **BGP-Routingpräferenz** an, die für Dienstverbindungen verwendet werden soll.

   Sie können Netzwerkeinstellungen festlegen, um den Datenverkehr über die Dienstverbindung entweder über das Netzwerk Ihres Unternehmens oder über das Prisma Access-Netzwerk zu verarbeiten.

   - **Standard** – Prisma Access verwendet im internen Netzwerk das Standardrouting.
   - **Hot-Potato-Routing** – Prisma Access leitet den Datenverkehr über die Dienstverbindung so schnell wie möglich an das WAN Ihres Unternehmens weiter.

   *Die Änderung der Routingmethode für die Prisma Access-Dienstverbindung erfordert ein gründliches Verständnis der Topologie und der Routinggeräte Ihres Unternehmens sowie ein Verständnis der Funktionsweise des Prisma Access-Routings. Wir empfehlen Ihnen, Routing für Dienstverbindungsverkehr sorgfältig zu lesen, bevor Sie die standardmäßige Routingmethode ändern.*
2. **Statische Routen zurückziehen, wenn der IPSec-Tunnel für die Dienstverbindung oder das Remote-Netzwerk ausgefallen ist**, wenn Prisma Access statische Routen entfernen soll, wenn ein Tunnel ohne Backup-Tunnel ausfällt.

   Prisma Access entfernt die Route in folgenden Situationen:

   - Der primäre Tunnel fällt aus und es gibt keinen sekundären Tunnel.
   - Wenn ein primärer und ein sekundärer Tunnel konfiguriert sind, aber beide ausfallen.

   Sie können diese Änderung nicht anwenden, wenn die Tunnelüberwachung nicht aktiviert ist.
3. Konfigurieren Sie für die Dienstverbindungen die Verwendung des **Backbone-Routings**.

   Standardmäßig erfordert das Prisma Access-Backbone, dass Sie einen symmetrischen Netzwerkpfad für den Datenverkehr haben, der über eine Dienstverbindung vom Standort des Rechenzentrums oder der Zentrale zurückgesendet wird. Wenn Sie ECMP oder einen anderen Lastausgleichsmechanismus für Dienstverbindungen von Ihrem CPE verwenden möchten, können Sie asymmetrische Flüsse über das Prisma Access-Backbone aktivieren.

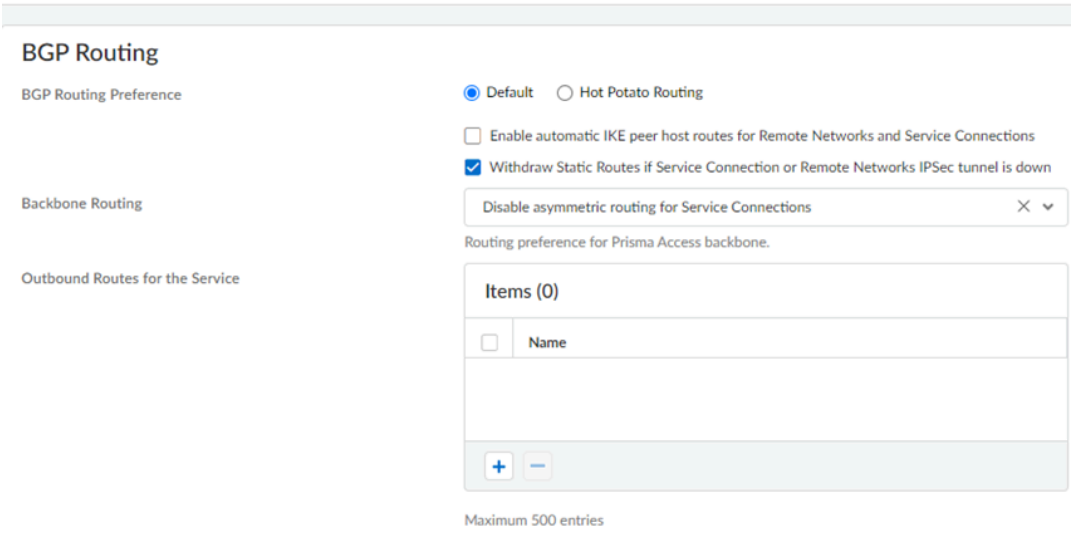
   - Wählen Sie **Asymmetrisches Routing für Dienstverbindungen deaktivieren** aus, um einen symmetrischen Datenfluss über das Backbone der Dienstverbindungen anzufordern.

 ©2025 Palo Alto Networks, Inc.

- Wählen Sie **Asymmetrisches Routing für Dienstverbindungen zulassen** aus, um Prisma Access einen asymmetrischen Datenfluss über das Backbone der Dienstverbindungen zu erlauben.
- Wenn Sie mehrere Dienstverbindungen zu einem Standort haben, können Sie den Lastausgleich in Ihrer Prisma Access-Bereitstellung nutzen, indem Sie **Asymmetrisches Routing und Lastverteilung über Dienstverbindungen zulassen** (Standardeinstellung) auswählen. Der Lastausgleich erfolgt jedoch auf Best-Effort-Basis und schlägt fehl, wenn eine der Dienstverbindungen ausfällt.

  Wenn Sie **Asymmetrisches Routing und Lastverteilung über Dienstverbindungen zulassen** auswählen, aktiviert Prisma Access die Netzwerkredundanz zwischen den GlobalProtect-Portalen und -Gateways sowie den Dienstverbindungen. Diese Funktionalität bietet redundante Netzwerkpfade zwischen der Datenebene der mobilen Benutzer und den Dienstverbindungen an verschiedenen Compute-Standorten. Durch die Aktivierung der Redundanz erhalten Benutzer einen zuverlässigeren Zugriff auf die Ressourcen, die hinter den Dienstverbindungen in einem Rechenzentrum oder in der Zentrale stehen. Da für den Zugriff mobiler Benutzer auf Ressourcen aus Remote-Netzwerken eine Dienstverbindung erforderlich ist, ist auch der Zugriff auf Ressourcen an Remote-Netzwerkstandorten für Benutzer zuverlässiger.

4. (Optional) **Geben Sie Outboundrouten für den Dienst** an, indem Sie bis zu 500 Präfixe hinzufügen, für die Prisma Access statische Routen für alle Dienstverbindungen und Remote-Netzwerkverbindungen hinzufügt. Prisma Access leitet den Datenverkehr dann über das Internet zu diesen Präfixen weiter.




## Weitere IKE-Optionen

Basierend auf dem von Ihnen ausgewählten IPSec-Gerätetyp stellt Prisma Access einen empfohlenen Satz von Chiffren und eine Schlüssellebensdauer für den IKE-Phase-1-Schlüsselaustauschprozess zwischen dem Gerät in Ihrer Zentrale oder Ihrem Rechenzentrum sowie Prisma Access bereit. Sie können die empfohlenen Einstellungen verwenden oder sie nach Bedarf an Ihre Umgebung anpassen.

 ©2025 Palo Alto Networks, Inc.

- Wählen Sie eine **IKE-Protokollversion** aus, die von Ihrem IPSec-Gerät und Prisma Access für die IKE-Verhandlung verwendet werden soll.

  Wenn Sie **Nur-IKEv1-Modus** auswählen, kann Prisma Access für die Verhandlung nur das IKEv1-Protokoll verwenden. Wenn Sie **Nur-IKEv2-Modus** auswählen, kann Prisma Access für die Verhandlung nur das IKEv2-Protokoll verwenden. Wenn Sie **Bevorzugter IKEv2-Modus** auswählen, verwendet Prisma Access das IKEv2-Protokoll nur, wenn Ihr IPSec-Gerät auch IKEv2 unterstützt. Wenn Ihr IPSec-Gerät IKEv2 nicht unterstützt, greift Prisma Access auf die Verwendung des IKEv1-Protokolls zurück.

- Fügen Sie ein **IKEv1-Verschlüsselungsprofil** hinzu, um die IKE-Verschlüsselungseinstellungen anzupassen, die die Verschlüsselungs- und Authentifizierungsalgorithmen definieren, die für den Schlüsselaustauschprozess in IKE Phase 1 verwendet werden.

  Prisma Access verwendet automatisch ein standardmäßiges IKE-Verschlüsselungsprofil basierend auf dem **Zweiggerätetyp**, der zum Erstellen dieses Tunnels verwendet wird.

  - **Verschlüsselung** – Geben Sie den Verschlüsselungsalgorithmus an, der in der IKE-SA-Verhandlung verwendet wird.

    Prisma Access unterstützt die folgenden Verschlüsselungsalgorithmen: 3des (168 Bit), aes-128-cbc (128 Bit), aes-192-cbc (192 Bit), aes-256-cbc (256 Bit), und DES (56 Bit). Sie können auch null (keine Verschlüsselung) auswählen.
  - **Authentifizierung** – Geben Sie den Authentifizierungsalgorithmus an, der in der IKE-SA-Verhandlung verwendet wird.

    Prisma Access unterstützt die folgenden Authentifizierungsalgorithmen: sha1 (160 Bit), sha256 (256 Bit), sha384 (384 Bit), sha512 (512 Bit) und md5 (128 Bit). Sie können auch null (keine Authentifizierung) auswählen.
  - **DH-Gruppe** – Geben Sie die DH-Gruppen (Diffie-Hellmann) an, die zum Generieren symmetrischer Schlüssel für IKE in der IKE-SA-Verhandlung verwendet werden. Der DH-Algorithmus (Diffie-Hellman) verwendet den privaten Schlüssel einer Partei und den öffentlichen Schlüssel der anderen, um ein geteiltes Geheimnis zu erstellen, also einen verschlüsselten Schlüssel, den beide VPN-Tunnel-Peers gemeinsam verwenden.

    Prisma Access unterstützt folgende DH-Gruppen: Gruppe 1 (768 Bit), Gruppe 2 (1.024 Bit – Standard), Gruppe 5 (1.536 Bit), Gruppe 14 (2.048 Bit), Gruppe 19 (256-Bit, Gruppe elliptischer Kurven) und Gruppe 20 (384 Bit, Gruppe elliptischer Kurven). Für die stärkste Sicherheit wählen Sie die Gruppe mit der höchsten Zahl aus.
  - **Lebensdauer** – Geben Sie die Einheit und die Dauer an, für die der IKE-Phase-1-Schlüssel gültig ist (der Standardwert ist 8 Stunden). Bei IKEv1 wird die Sicherheitszuordnung (Security Association – SA) nicht aktiv erneut verschlüsselt, bevor die Schlüssellebensdauer abläuft. Die IKEv1-Phase-1-Neuverschlüsselung wird nur ausgelöst, wenn die SA abläuft. Bei IKEv2 muss die SA vor Ablauf der Schlüssellebensdauer neu verschlüsselt werden. Wenn die SA nach dem Ablauf nicht neu verschlüsselt wird, muss die SA mit dem Erstellen eines neuen Phase-1-Schlüssels beginnen.
  - **IKEv2-Authentifizierung mehrfach** – Geben Sie den Wert an, der mit der Schlüssellebensdauer multipliziert wird, um die Authentifizierungsanzahl zu bestimmen (Bereich ist 0–50; Standardwert ist 0). Die Authentifizierungsanzahl gibt an, wie oft der Sicherheitsverarbeitungsknoten die IKEv2-IKE-SA-Neuverschlüsselung durchführen kann,

 ©2025 Palo Alto Networks, Inc.

bevor die erneute IKEv2-Authentifizierung gestartet werden muss. Mit dem Standardwert 0 kann die Funktion zur erneuten Authentifizierung deaktiviert werden.

- Aktivieren Sie den **IKE Passivmodus**, damit Prisma Access nur auf IKE-Verbindungen reagiert und diese nicht initiiert.

- **IKE NAT-Traversal** ist standardmäßig aktiviert.

  Dies bedeutet, dass die UDP-Kapselung in IKE- und UDP-Protokollen verwendet wird, sodass sie NAT-Geräte (Network Address Translation) passieren können, die sich zwischen den IPSec-VPN-Tunnelendpunkten befinden.

## Weitere IPSec-Optionen

Basierend auf dem von Ihnen ausgewählten IPSec-Gerätetyp bietet Prisma Access einen empfohlenen Satz von Einstellungen für das IPSec-Protokoll und die Einstellungen zur Schlüssellebensdauer an, um Daten innerhalb des IPSec-Tunnels zwischen Ihrem IPSec-Gerät und Prisma Access in IKE Phase 2 für die Sicherheitszuordnung (Security Association – SA) zu sichern. Sie können die empfohlenen Einstellungen verwenden oder sie nach Bedarf an Ihre Umgebung anpassen.

- Passen Sie das **IPSec-Verschlüsselungsprofil** an, um zu definieren, wie Daten innerhalb des Tunnels gesichert werden, wenn Auto Key IKE während IKE Phase 2 automatisch Schlüssel für die IKE-SAs generiert.

  Prisma Access konfiguriert automatisch ein standardmäßiges IPSec-Verschlüsselungsprofil basierend auf dem Anbieter des **Zweiggerätetyps**. Sie können entweder das Standardprofil verwenden oder ein benutzerdefiniertes Profil erstellen.

  - **IPSec-Protokoll** – Sichern Sie die Daten, die den VPN-Tunnel durchqueren. Das **ESP**-Protokoll (Encapsulating Security Payload) verschlüsselt die Daten, authentifiziert die Quelle und überprüft die Datenintegrität. Das **AH**-Protokoll (Authentication Header) authentifiziert die Quelle und überprüft die Datenintegrität.

    Wenn Sie **ESP** als IPSec-Protokoll verwenden, geben Sie auch den bei der IPSec-SA-Verhandlung verwendeten **Verschlüsselungsalgorithmus** an.

    Prisma Access unterstützt die folgenden Verschlüsselungsalgorithmen: aes-256-gcm (256 Bit), aes-256-cbc (256 Bit), aes-192-cbc (192 Bit), aes-128-gcm (128 Bit), aes-128-cbc (128 Bit), 3des (168 Bit) und DES (56 Bit). Sie können auch null (keine Verschlüsselung) auswählen.

- **Authentifizierung** – Geben Sie den Authentifizierungsalgorithmus an, der in der IPSec-SA-Verhandlung verwendet wird.

  Prisma Access unterstützt die folgenden Authentifizierungsalgorithmen: sha1 (160 Bit), sha256 (256 Bit), sha384 (384 Bit), sha512 (512 Bit) und md5 (128 Bit). Wenn Sie das IPSec-Protokoll auf „ESP“ setzen, können Sie auch „Keine“ (keine Authentifizierung) auswählen.

 ©2025 Palo Alto Networks, Inc.

- **DH-Gruppe** – Geben Sie die DH-Gruppen (Diffie-Hellman) für IKE in der IPSec-SA-Verhandlung (Security Association) an.

  Prisma Access unterstützt folgende DH-Gruppen: Gruppe 1 (768 Bit), Gruppe 2 (1.024 Bit – Standard), Gruppe 5 (1.536 Bit), Gruppe 14 (2.048 Bit), Gruppe 19 (256-Bit, Gruppe elliptischer Kurven) und Gruppe 20 (384 Bit, Gruppe elliptischer Kurven). Für die stärkste Sicherheit wählen Sie die Gruppe mit der höchsten Zahl aus. Wenn Sie den Schlüssel, den Prisma Access während der IKE-Phase 1 erstellt, nicht erneuern möchten, wählen Sie **no-pfs** (kein perfektes Weiterleitungsgeheimnis) aus. Wenn Sie diese Option auswählen, verwendet Prisma Access den aktuellen Schlüssel wieder für die IPSec-SA-Verhandlung.

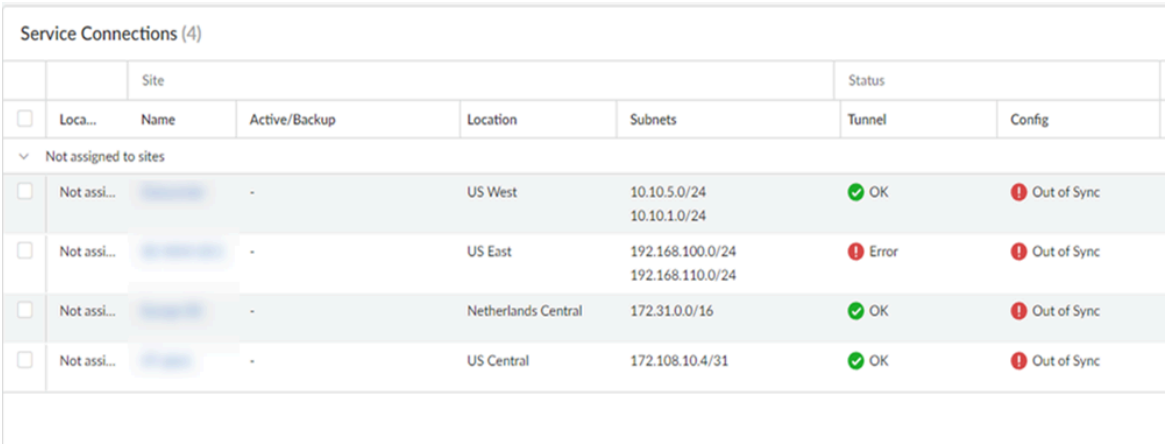
- **Lebensdauer** – Geben Sie die Einheit und Zeitspanne an, für die der ausgehandelte Schlüssel gültig ist (Standardwert ist 1 Stunde).

- **Lebensgroß** – Geben Sie die Einheit und Zeitdauer an, die der Schlüssel zur Verschlüsselung verwenden kann.

## Dienstverbindungsstatus verifizieren

Um zu überprüfen, ob die Dienstverbindung erfolgreich eingerichtet wurde, wählen Sie **Workflows** > **Prisma Access-Einrichtung** > **Dienstverbindungen** und überprüfen Sie, ob der **Status OK** ist.

Wenn der Status nicht **OK** ist, bewegen Sie den Mauszeiger über das Statussymbol, um etwaige Fehler anzuzeigen.




Im Bereich **Standorte** können Sie alle eingebundenen Dienstverbindungen zusammen mit dem zugehörigen Status und weiteren Details anzeigen.

**Standort**

- **Name** – Der Name der Dienstverbindung.
- **Aktiv/Backup** – Die aktiven und die Backup-Standorte der Dienstverbindung.
- **Subnetze** – Die zugewiesenen Infrastruktursubnetze der Dienstverbindung.

**Status**

- **Tunnel** – Der Betriebsstatus der Verbindung zwischen Prisma Access und Ihrer Dienstverbindung.

 ©2025 Palo Alto Networks, Inc.

- **Konfiguration** – Der Status der letzten Übertragung Ihrer Konfiguration an den Dienst. Wenn die lokale Konfiguration und die Konfiguration in der Cloud übereinstimmen, lautet der Konfigurationsstatus **Synchron**. Wenn Sie lokal eine Änderung vorgenommen und die Konfiguration noch nicht in die Cloud übertragen haben, wird möglicherweise der Status **Nicht synchron** angezeigt. Bewegen Sie den Mauszeiger über die Statusanzeige, um detailliertere Informationen zu erhalten. Nach dem Festschreiben und Übertragen der Konfiguration auf Prisma Access ändert sich der Konfigurationsstatus in **Synchron**.

**Prisma Access**

- **Standort** – Der Standort, an dem die Dienstverbindung bereitgestellt wird.
- **Dienst-IP** – Die IP-Adresse der Dienstverbindung.
- **EBGP-Router** – Die IP-Adresse des EBGP-Routers in der Dienstverbindung.

**Links**

- **BGP IPv4** – Der Status des BGP-IPv4-Routings in der Dienstverbindung.
- **BGP IPv6** – Der Status des BGP-IPv6-Routings in der Dienstverbindung.
- **IPSec-Tunnel** – Der IPSec-Tunnel Ihrer Dienstverbindung. Der erste IPSec-Tunnel, den Sie einrichten, ist der **(Primäre)** Tunnel. Wenn Sie einen zweiten IPSec-Tunnel eingerichtet haben, wird dieser zum **(Sekundären)** Tunnel.
- **Peer-IP-Adresse** – Die Gateway-IP-Adresse der Dienstverbindung.

## Konfigurieren einer Dienstverbindung in Prisma Access (Panorama)

Führen Sie die folgenden Schritte aus, um eine Dienstverbindung für Prisma Access Panorama so zu konfigurieren, dass der Zugriff auf private Apps oder interne Unternehmensressourcen ermöglicht wird.

*Verwenden Sie die CLI nicht, um Dienstverbindungen einzubinden und zu konfigurieren. Wenn Sie die CLI für das Onboarding von Dienstverbindungen benötigen, wenden Sie sich an Ihr Team von Palo Alto Networks.*

**STEP 1 |** Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Dienstverbindung** aus.

**STEP 2 |** Fügen Sie durch Auswahl von **Hinzufügen** einem Ihrer Unternehmensnetzwerkstandorten eine neue Dienstverbindung hinzu.

**STEP 3 |** Geben Sie unter **Name** einen Namen für den Unternehmensstandort an.

**STEP 4 |** Wählen Sie den **Standort** aus, der Ihrem Standort am nächsten liegt.

In diesem Abschnitt finden Sie eine Liste der Prisma Access-Standorte.

Standorte, die mit zwei Sternchen gekennzeichnet sind, sind **Lokale Zonen**. Diese Standorte platzieren Compute-, Speicher-, Datenbank- und Infrastrukturdienste in der Nähe großer Bevölkerungs- und Industriezentren; sie haben jedoch auch einige Einschränkungen. Um eine lokale Zone hinzuzufügen, wenden Sie sich an Ihren Ansprechpartner bei Palo Alto Networks.

 ©2025 Palo Alto Networks, Inc.

**STEP 5 |** Wählen Sie eine neue Konfiguration für einen **IPSec-Tunnel** aus oder fügen Sie eine solche Konfiguration hinzu, um auf die Firewall, den Router oder das SD-WAN-Gerät am Unternehmensstandort zuzugreifen:

- Wenn Sie eine vorhandene **IPSec-Tunnel**-Konfiguration verwenden, wählen Sie diese im Dropdown-Menü aus. Beachten Sie, dass der Tunnel, den Sie für jede Netzwerkverbindung erstellen, Prisma Access mit dem IPSec-fähigen Gerät an jedem Unternehmensstandort verbindet. Die Peer-Adressen in der IKE-Gateway-Konfiguration müssen für jeden Tunnel eindeutig sein. Sie können jedoch einige der anderen allgemeinen Konfigurationselemente wie z. B. Verschlüsselungsprofile wiederverwenden.

  *Der von Ihnen ausgewählte IPSec-Tunnel darf nur den automatischen Schlüsselaustausch und IPv4 verwenden. Darüber hinaus müssen Sie sicherstellen, dass die Namen des IPSec-Tunnels, des IKE-Gateways und des Verschlüsselungsprofils maximal 31 Zeichen lang sein dürfen.*

- So erstellen Sie eine neue IPSec-Tunnel-Konfiguration:

  Klicken Sie auf **Neuer IPSec-Tunnel**, ordnen Sie ihm unter **Name** einen Namen zu und konfigurieren Sie die Einstellungen für IKE-Gateway, IPSec-Verschlüsselungsprofil und Tunnelüberwachung.

- Wenn das IPSec-fähige Gerät in Ihrer Zentrale oder am Standort des Rechenzentrums richtlinienbasiertes VPN verwendet:

  Wählen Sie auf der Registerkarte **Proxy-IDs** die Option **Hinzufügen** aus, um eine Proxy-ID hinzuzufügen, die den auf Ihrem lokalen IPSec-Gerät konfigurierten Einstellungen entspricht. Auf diese Weise können Sie sicherstellen, dass Prisma Access erfolgreich einen IPSec-Tunnel mit Ihrem lokalen Gerät einrichten kann.

- So erkennen und neutralisieren Sie Replay-Angriffe:

  Behalten Sie die Auswahl von **Replay-Schutz aktivieren** bei.

- So erhalten Sie die ursprünglichen ToS-Informationen:

  Wählen Sie **ToS-Header kopieren** aus, um den ToS-Header (Type of Service) vom inneren IP-Header in den äußeren IP-Header der gekapselten Pakete zu kopieren.

- So aktivieren Sie die Tunnelüberwachung für die Dienstverbindung:

  Wählen Sie **Tunnelüberwachung** aus:

  - Geben Sie eine **Ziel-IP**-Adresse ein.

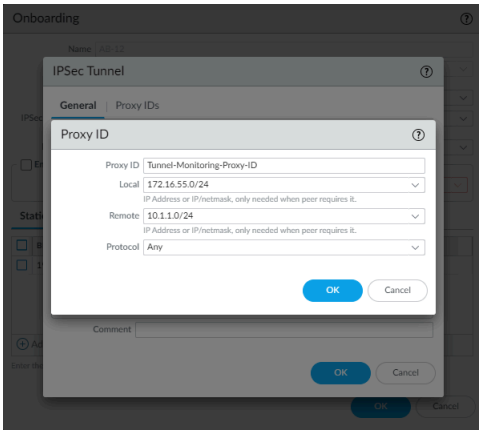
    Geben Sie eine IP-Adresse in Ihrer Zentrale oder Ihrem Rechenzentrum an, an die Prisma Access ICMP-Ping-Anfragen zur IPSec-Tunnelüberwachung senden kann. Stellen Sie sicher, dass diese Adresse für ICMP im gesamten Prisma Access-Infrastruktursubnetz erreichbar ist.

  - Wenn Sie die Tunnelüberwachung mit einem Peer-Gerät verwenden, das mehrere Proxy-IDs verwendet, geben Sie eine **Proxy-ID** an oder fügen Sie eine **Neue Proxy-ID**

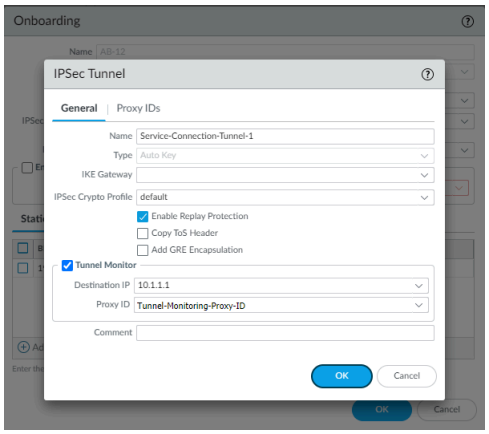
 ©2025 Palo Alto Networks, Inc.

hinzu, die den Zugriff des Infrastruktursubnetzes auf den Standort ermöglicht, an dem sich Ihre Zentrale oder Ihr Rechenzentrum befindet.

Die folgende Abbildung zeigt eine Proxy-ID mit dem Subnetz der Dienstinfrastruktur (172.16.55.0/24 in diesem Beispiel) als **lokales** IP-Subnetz und dem Subnetz der Zentrale oder des Rechenzentrums (10.1.1.0/24 in diesem Beispiel) als **Remote**-Subnetz.




Die folgende Abbildung zeigt, wie die von Ihnen erstellte Proxy-ID auf die Konfiguration der Tunnelüberwachung angewendet wird, indem sie im Feld **Proxy-ID** angegeben wird.



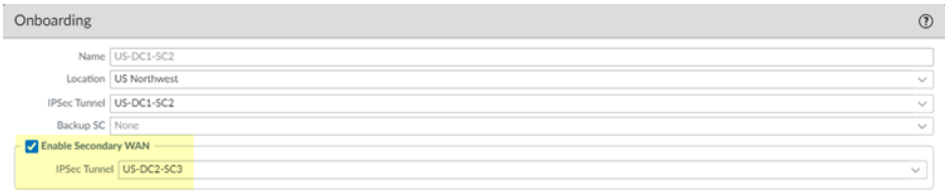

*Sie müssen auf Ihrem CPE eine statische Route zur IP-Adresse der Tunnelüberwachung konfigurieren, damit die Tunnelüberwachung fehlerfrei ausgeführt werden kann. Um die Ziel-IP-Adresse für die Tunnelüberwachung von Ihrem Rechenzentrum oder Ihrer Zentrale zu Prisma Access zu suchen, wählen Sie **Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** aus. Klicken Sie dann auf das Optionsfeld **Dienstinfrastruktur** und suchen Sie die **IP-Adresse der Tunnelüberwachung**.*

**STEP 6 |** Nur BGP- und Hot-Potato-Routing-Bereitstellungen – Wählen Sie eine Dienstverbindung aus, die als bevorzugte Backupeinheit (**Backup-SC**) verwendet werden soll.

Sie können jede bereits hinzugefügte Dienstverbindung auswählen. Prisma Access verwendet im Falle eines Verbindungsausfalls die von Ihnen ausgewählte **Backup-SC** als bevorzugte Dienstverbindung. Durch Auswahl einer Backup-Dienstverbindung (Backup-SC) können Probleme aufgrund asymmetrischen Routings verhindert werden, wenn Sie mehr als zwei

 ©2025 Palo Alto Networks, Inc.

Dienstverbindungen eingebunden haben. Diese Auswahl ist nur im Hot-Potato-Routing-Modus verfügbar.




**STEP 7 |** Wenn Sie an diesem Standort über eine sekundäre WAN-Verbindung verfügen, wählen Sie **Sekundäres WAN aktivieren** aus. Wählen Sie dann einen **IPSec-Tunnel** auf dieselbe Weise aus oder konfigurieren Sie ihn auf die gleiche Weise, die Sie zum Einrichten des primären IPSec-Tunnels verwendet haben.

Wenn die primäre WAN-Verbindung ausfällt, erkennt Prisma Access den Ausfall und richtet über die sekundäre WAN-Verbindung einen Tunnel zur Zentrale oder zum Standort des Rechenzentrums ein. Wird die primäre WAN-Verbindung wieder aktiv, wird wieder zurück zur primären Verbindung gewechselt.

Die Konfiguration eines sekundären WAN wird in den nachfolgenden Bereitstellungen nicht unterstützt:

- Wenn Ihr sekundäres WAN im Aktiv-Aktiv-Modus mit dem primären IPSec-Tunnel eingerichtet wird.
- Wenn Ihr Customer Premises Equipment (CPE) in einer ECMP-Konfiguration (Equal Cost Multipath) mit dem primären und sekundären IPSec-Tunnel eingerichtet wird.

Wenn Sie statische Routen verwenden, beträgt die Tunnel-Failover-Zeit abhängig von Ihrem WAN-Anbieter weniger als 15 Sekunden ab dem Zeitpunkt der Erkennung.

Wenn Sie das BGP-Routing konfigurieren und die Tunnelüberwachung aktiviert haben, besteht die kürzeste Standardhaltezeit zur Feststellung eines Fehlers bei einem Sicherheitsparameterindex (SPI) über die Tunnelüberwachung. Hierbei werden alle Routen zu einem Peer entfernt, wenn ein Tunnelfehler festgestellt wird, der länger als 15 aufeinanderfolgende Sekunden anhält. Auf diese Weise ermittelt die Tunnelüberwachung das Verhalten der BGP-Routen. Wenn Sie die Tunnelüberwachung nicht konfigurieren, bestimmt der Haltetimer die Zeitspanne, für die der Tunnel inaktiv sein darf, bevor die Route entfernt wird. Prisma Access verwendet den standardmäßigen BGP-HoldTime-Wert von 90 Sekunden, der in RFC 4271 definiert ist. Hierbei handelt es sich um die maximal zulässige Wartezeit, nach deren Ablauf Prisma Access eine Route für einen inaktiven SPI entfernt. Wenn das Peer-BGP-Gerät eine kürzere konfigurierte Haltezeit hat, verwendet der BGP-Haltetimer den niedrigeren Wert.

Nach der erfolgreichen Installation des sekundären Tunnels hat die sekundäre Route so lange Vorrang, bis der primäre Tunnel wieder einsatzbereit ist. Wenn sowohl die primäre als auch die sekundäre Route aktiv sind, hat die primäre Route Vorrang.

*Wenn Sie einen anderen BGP-Peer für die sekundäre (Backup-)Verbindung verwenden, berücksichtigt Prisma Access die vom CPE angekündigten MED-Attribute (Multi-Exit Discriminator) nicht. Diese Einschränkung gilt, wenn Sie mehrere BGP-Peers für Remote-Netzwerkverbindungen oder Dienstverbindungen verwenden.*

 ©2025 Palo Alto Networks, Inc.

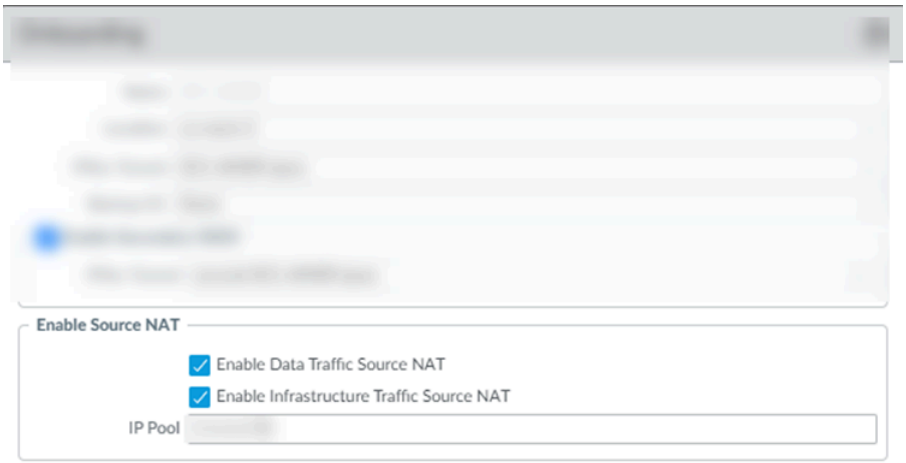
**STEP 8 |** (Optional) Aktivieren Sie die Quell-NAT für mobile Benutzer – GlobalProtect-IP-Pooladressen, IP-Adressen im Infrastruktursubnetz oder beides.

Sie können ein Subnetz an einer oder mehreren Dienstverbindungen angeben, die für den NAT-Datenverkehr zwischen mobilen Prisma Access-GlobalProtect-Benutzern und privaten Anwendungen und Ressourcen in einem Rechenzentrum verwendet werden.

- **Quell-NAT des Datenverkehrs aktivieren** – Führt die NAT für Adressen des IP-Adresspools mobiler Benutzer aus, sodass diese nicht ans Rechenzentrum mitgeteilt werden und nur die von Ihnen bei den Dienstverbindungen angegebenen Subnetze ans Rechenzentrum mitgeteilt und geroutet werden.
- **Quell-NAT des Infrastrukturdatenverkehrs aktivieren** – Führt die NAT für Adressen aus dem Infrastruktursubnetz aus, sodass diese nicht ans Rechenzentrum mitgeteilt werden und nur die von Ihnen bei den Dienstverbindungen angegebenen Subnetze im Rechenzentrum mitgeteilt und geroutet werden.
- **Benutzer-ID** – Wird diese Option ausgewählt, verwendet Prisma Access diese Dienstverbindung zur Identitätsweitergabe.

  ***Verwaltung der Umverteilung von Benutzer-IDs*** *– In bestimmten Fällen sind bei der Umverteilung von Benutzer-IDs in besonders umfangreichen Prisma Access-Bereitstellungen detaillierte Kontrollen erforderlich. Mithilfe der Umverteilungsverwaltung für Benutzer-IDs können Sie das standardmäßige Identitätsumverteilungsverhalten für bestimmte Dienstverbindungen manuell deaktivieren, indem Sie das Häkchen in der Spalte* ***Benutzer-ID*** *entfernen und dann bestimmte Dienstverbindungen auswählen, die für die Identitätsweitergabe verwendet werden sollen. Für die meisten Konfigurationen ist dieser Arbeitsschritt nicht erforderlich. Wenden Sie sich an den Support von Palo Alto Networks, um diese Funktionalität zu aktivieren.*
- **IP-Pool** – Geben Sie den IP-Adresspool an, der zum Ausführen von NAT im IP-Adresspool für mobile Benutzer und/oder im Infrastruktursubnetz verwendet wird.

  Verwenden Sie ein privates IP-Subnetz (RFC 1918) oder ein geeignetes Subnetz, das in Ihrer Routingdomäne routingfähig ist und sich nicht mit dem GlobalProtect-IP-Adresspool der mobilen Benutzer oder dem Infrastruktursubnetz überschneidet. Geben Sie ein Subnetz zwischen /25 und /32 ein.



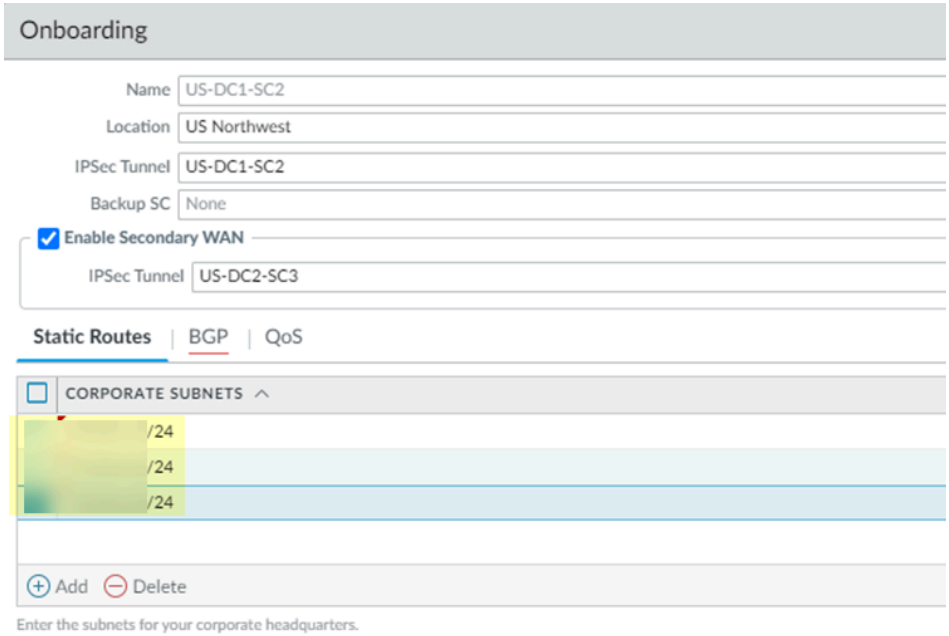

 ©2025 Palo Alto Networks, Inc.

**STEP 9 |** Aktivieren Sie das Routing zu den Subnetzwerken oder einzelnen IP-Adressen am Unternehmensstandort, auf den die Benutzer Zugriff benötigen.

Prisma Access verwendet diese Informationen, um Anforderungen an den richtigen Standort weiterzuleiten. Die Netzwerke an den einzelnen Standorten dürfen sich nicht gegenseitig oder mit IP-Adresspools überschneiden, die Sie für die Dienstinfrastruktur oder für Prisma Access für IP-Pools der Benutzer bestimmt haben. Sie können **Statische Routen**, **BGP** oder eine Kombination dieser beiden Komponenten konfigurieren.

So konfigurieren Sie **Statische Routen**:

1. Klicken Sie auf der Registerkarte **Statische Routen** auf **Hinzufügen** und geben Sie die Subnetzadresse (z. B. 172.168.10.0/24) oder die individuelle IP-Adresse einer Ressource wie einem DNS-Server (z. B. 10.32.5.1/32) ein, auf die Ihre Remote-Benutzer Zugriff benötigen.
2. Wiederholen Sie diesen Arbeitsschritt für alle Subnetze oder IP-Adressen, auf die Prisma Access an diesem Standort zugreifen können muss.




Um **BGP** zu konfigurieren:

1. Wählen Sie auf der Registerkarte **BGP** die Option **Aktivieren** aus.

   Wenn Sie BGP aktivieren, legt Prisma Access den Time-to-Live-Wert (TTL) für externe BGP (eBGP) auf 8 fest, um alle zusätzlichen Hops aufzunehmen, die zwischen der Prisma

 ©2025 Palo Alto Networks, Inc.

Access-Infrastruktur und dem CPE (Customer Premises Equipment) auftreten können, das die eBGP-Verbindung abschließt.

*Prisma Access akzeptiert keine BGP-Standardroutenmitteilungen für Dienstverbindungen oder Remote-Netzwerkverbindungen.*

2. (Optional) Wählen Sie eine der folgenden Optionen aus:

   - Um den ausgehenden Präfixen von den eBGP-Peers im Customer Premises Equipment (CPE) eine **No-Export**-Community für Corporate Access Nodes (Dienstverbindungen) hinzuzufügen, legen Sie für **No-Export-Community hinzufügen** die Einstellung **Aktiviert – Ausgang** fest. Diese Funktionalität ist standardmäßig auf **Deaktiviert** eingestellt.

     Verwenden Sie diese Funktionalität nicht im Hot-Potato-Routing-Modus.

   - Um zu verhindern, dass der Prisma Access-BGP-Peer Routen in das Netzwerk Ihrer Organisation weiterleitet. **Teilen Sie Prisma Access Routes nicht mit**.

     Standardmäßig teilt Prisma Access alle BGP-Routinginformationen einschließlich lokaler Routen und aller Präfixe, die es von anderen Dienstverbindungen, Remote-Netzwerken und den Subnetzen mobiler Benutzer erhält, mit. Wählen Sie dieses Kontrollkästchen aus, um zu verhindern, dass Prisma Access BGP-Mitteilungen sendet, aber weiterhin die erhaltenen BGP-Informationen verwendet, um festzustellen, welche Routen von anderen BGP-Nachbarn verwendet werden.

     *Da Prisma Access keine BGP-Mitteilungen sendet, wenn Sie diese Option auswählen, müssen Sie statische Routen auf dem lokalen Gerät konfigurieren, um Routen zu erstellen, mit denen zu Prisma Access zurückgekehrt werden kann.*

   - Um die Anzahl der IP-Subnetzmitteilungen für mobile Benutzer über BGP an die Geräte Ihrer Kunden vor Ort (CPE) zu reduzieren, geben Sie für Prisma Access an, dass die Subnetze zusammengefasst werden sollen, bevor diese mitgeteilt werden. Wählen Sie hierzu **Mobile Benutzerrouten vor dem Mitteilen zusammenfassen** aus.

     Standardmäßig teilt Prisma Access die IP-Adresspools für mobile Benutzer in Blöcken von /24 Subnetzen mit; wenn Sie sie zusammenfassen, teilt Prisma Access den Pool basierend auf dem von Ihnen angegebenen Subnetz mit. Beispiel: Prisma Access teilt einen öffentlichen mobilen IP-Pool für Benutzer mit der Angabe 10.8.0.0/20 unter Verwendung des Subnetzes /20 mit, anstatt den Pool in die Subnetze 10.8.1.0/24, 10.8.2.0/24, 10.8.3.0/24 usw. zu unterteilen, bevor sie mitgeteilt werden. Durch die Zusammenfassung dieser Ankündigungen kann die Anzahl der in den CPE-Routingtabellen gespeicherten Routen reduziert werden. Sie können z. B. die IP-Poolzusammenfassung mit Cloud-VPN-Gateways (Virtual Private Gateways (VGWs) oder Transit Gateways (TGWs)) verwenden, die eine begrenzte Anzahl von Routen akzeptieren können.

     *Wenn Sie das Hot-Potato-Routing aktiviert haben und die Routenzusammenfassung aktivieren, stellt Prisma Access keine AS-PATHs mehr voran, was möglicherweise zu asymmetrischem Routing führen kann. Stellen Sie sicher, dass Ihr Rückkehrdatenverkehr vom Rechenzentrum oder der Zentrale eine symmetrische Rückführung garantiert, bevor Sie die Routenzusammenfassung mit Hot-Potato-Routing aktivieren.*

 ©2025 Palo Alto Networks, Inc.

3. (Optional) Wählen Sie einen Wert für **MRAI-Timer** aus.

   Das BGP-Routing bietet einen Timer namens *Minimum Route Advertisement Interval (MRAI)*, den Sie verwenden können, um die BGP-Routingkonvergenz in Ihrem Netzwerk anzupassen. MRAI dient zur Ratenbegrenzung von Aktualisierungen auf Zielbasis und die BGP-Router warten mindestens die konfigurierte MRAI-Zeit ab, bevor sie eine Mitteilung für dasselbe Präfix senden. Eine kleinere Zahl ermöglicht eine schnellere Konvergenzzeit, erzeugt jedoch mehr Mitteilungen in Ihrem Netzwerk. Eine höhere Zahl verringert die Anzahl der Mitteilungen, die gesendet werden können, kann aber auch die Routingkonvergenz verlangsamen. Sie bestimmen die Anzahl, die Sie in Ihr Netzwerk einfügen möchten, um die beste Balance zwischen schnellerer Routingkonvergenz und weniger Mitteilungen zu erzielen.

   Konfigurieren Sie einen MRAI-Bereich zwischen 1 und 600 Sekunden mit einem Standardwert von 30 Sekunden.
4. Geben Sie die IP-Adresse ein, die als Router-ID des eBGP-Routers im Netzwerk des Rechenzentrums bzw. der Zentrale zugewiesen wurde, für das Sie diese Dienstverbindung als **Peer-Adresse** konfigurieren.
5. Geben Sie das **Peer-AS** ein, bei dem es sich um das autonome System (AS) handelt, zu dem der virtuelle Firewall-Router oder BGP-Router im Netzwerk Ihres Rechenzentrums bzw. Ihrer Zentrale gehört.
6. (Optional) Geben Sie eine Adresse ein, die Prisma Access als lokale IP-Adresse für BGP verwendet.

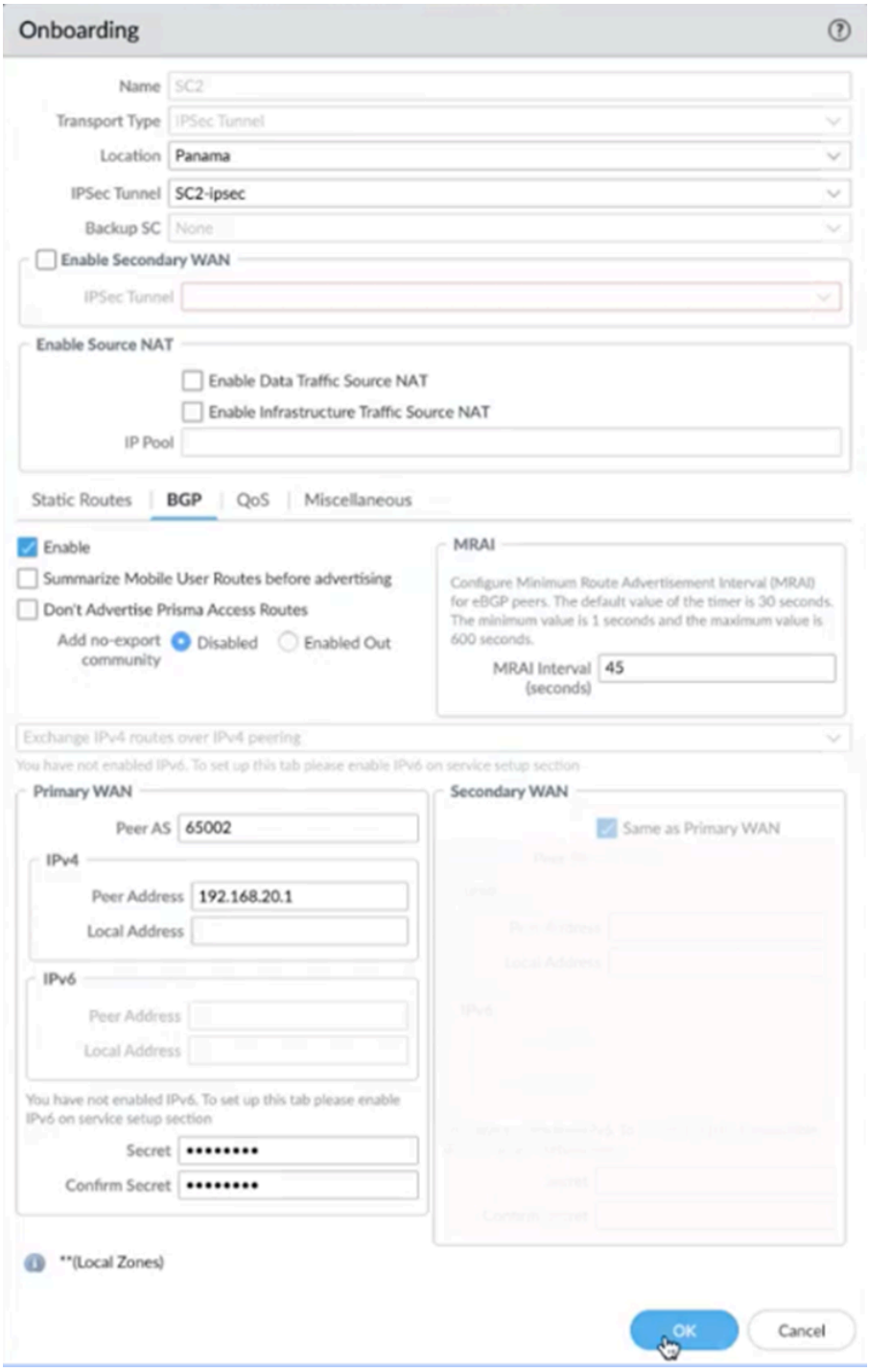
   Die Angabe einer **lokalen Adresse** ist nützlich, wenn das Gerät auf der anderen Seite der Verbindung (z. B. ein virtuelles privates Gateway von Amazon Web Service (AWS)) eine bestimmte lokale IP-Adresse für das BGP-Peering benötigt, um erfolgreich arbeiten zu können. Stellen Sie sicher, dass die von Ihnen angegebene Adresse nicht mit IP-Adressen im Infrastruktursubnetz oder in den Subnetzen in der Dienstverbindung in Konflikt steht oder sich mit diesen überschneidet.

   *Sie müssen eine statische Route auf Ihrem CPE zur **lokalen Adresse** von BGP konfigurieren.*

   Wenn Sie IPV6-Unterstützung für Ihre Dienstverbindung verwenden, können Sie **IPv6**-Adressen sowie **IPv4**-Adressen konfigurieren. Des Weiteren müssen Sie die IPv6-Vernetzung weltweit in Ihrer Prisma Access-Infrastruktur aktivieren, bevor Sie die IPv6-Adressierung verwenden können.

 ©2025 Palo Alto Networks, Inc.

7. (Optional) Geben Sie eine **geheime** Passphrase ein und bestätigen Sie diese, um die BGP-Peer-Kommunikation zu authentifizieren.




**STEP 10 |** (Optional) Wenn Sie ein **Sekundäres WAN** konfiguriert haben und die **Peer-Adresse** oder den Wert für **Lokale Adresse** für den sekundären (Backup-)BGP-Peer ändern müssen, dann

 ©2025 Palo Alto Networks, Inc.

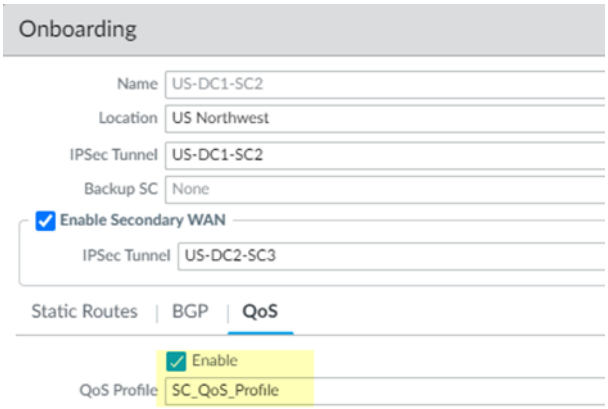
nehmen Sie die Auswahl von **Identisch mit primärem WAN** zurück und geben Sie einen eindeutigen Peer und optional eine lokale IP-Adresse für das sekundäre WAN ein.

In einigen Bereitstellungen (z. B. bei der Verwendung von BGP für das Peering mit einem AWS-VPN-Gateway) kann der BGP-Peer für das primäre und das sekundäre WAN unterschiedlich sein. In diesen Szenarien können Sie einen anderen BGP-Peer für das sekundäre WAN festlegen.

*Bei BGP-Bereitstellungen mit sekundären WANs legt Prisma Access sowohl für den primären als auch den sekundären Tunnel den Status **AKTIV**fest, befolgt jedoch das normale BGP-Aktiv-Backup-Verhalten für den Netzwerkverkehr. Prisma Access legt den primären Tunnel als aktiv fest und sendet und empfängt Datenverkehr nur durch diesen Tunnel. Wenn der primäre Tunnel ausfällt, erkennt Prisma Access den Fehler mithilfe von BGP-Regeln, legt den sekundären Tunnel als aktiv fest und verwendet zum Senden und Empfangen von Datenverkehr nur den sekundären Tunnel.*

**STEP 11 |** (Optional) Aktivieren Sie **Quality of Service** für die Dienstverbindung und geben Sie ein QoS-Profil an oder fügen Sie ein **Neues QoS-Profil** hinzu.

Sie können QoS-Profile erstellen, um den QoS-Datenverkehr für Remote-Netzwerkverbindungen und Dienstverbindungen zu regeln und diese Profile auf Datenverkehr anzuwenden, den Sie mit PAN-OS-Sicherheitsrichtlinien und/oder mit einem lokalen Gerät markiert haben. Weitere Einzelheiten finden Sie unter QoS für Remote-Netzwerke.



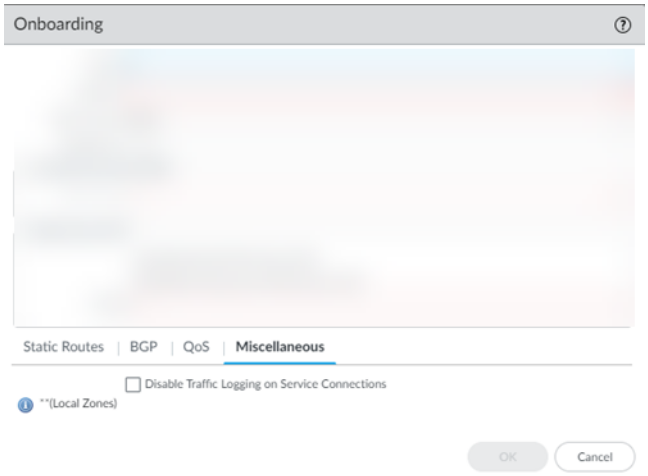

**STEP 12 |** (Optional) Konfigurieren Sie unter **Verschiedenes** weitere Einstellungen.

1. (Optional) **Deaktivieren Sie die Protokollierung des Datenverkehrs auf Dienstverbindungen**, um die Protokollierung auf den Dienstverbindungen für Ihre Prisma Access-Bereitstellung zu deaktivieren.

   Wenn die Mehrzahl der von den Dienstverbindungen protokollierten Datenverkehrsflüsse asymmetrisch ist, sollten Sie möglicherweise die Dienstverbindungsprotokollierung deaktivieren, um den Verbrauch von Strata Logging Service-Protokollspeicher zu reduzieren. Wenn Ihre Bereitstellung keine

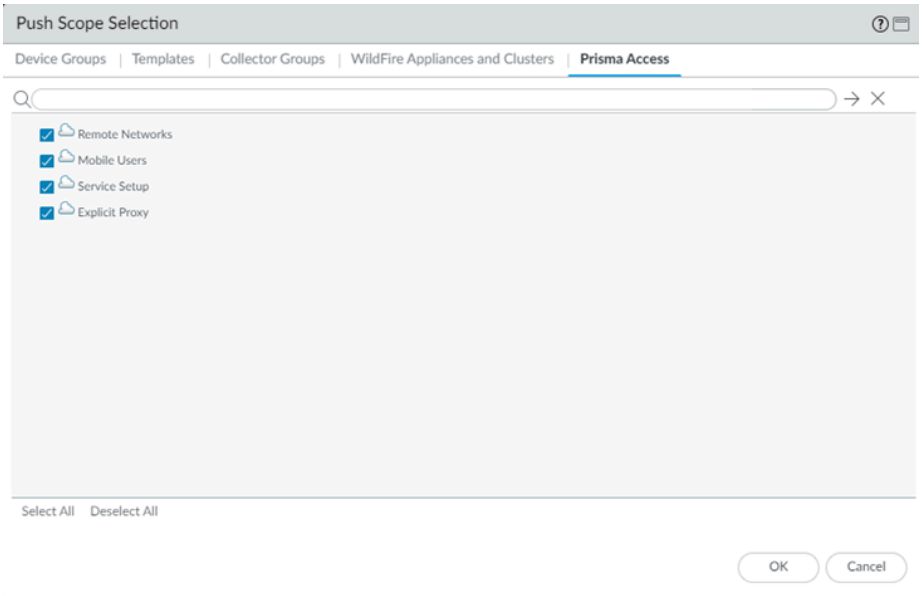
 ©2025 Palo Alto Networks, Inc.

asymmetrischen Datenverkehrsflüsse über die Dienstverbindungen aufweist, müssen Sie die Protokollierung nicht deaktivieren.




**STEP 13 |** Schreiben Sie Ihre Änderungen in Panorama fest und übertragen Sie die Konfigurationsänderungen an Prisma Access.

1. Klicken Sie auf **Commit** > **Commit und Push**.
2. **Bearbeiten Sie Auswahlen** und stellen Sie auf der Registerkarte **Prisma Access** sicher, dass **Diensteinrichtung** im **Übertragungsumfang** ausgewählt ist. Klicken Sie anschließend auf **OK**.




3. Klicken Sie auf **Commit und Push**.

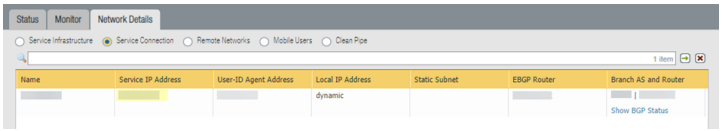
**STEP 14 |** Fügen Sie weitere Dienstverbindungen hinzu, indem Sie Schritt 2 bis Schritt 11 wiederholen.


©2025 Palo Alto Networks, Inc.

**STEP 15 |** Konfigurieren Sie den oder die IPSec-Tunnel von Ihrem IPSec-fähigen Gerät im Unternehmensnetzwerk zurück zu Prisma Access.

1. Um die IP-Adresse des Tunnels in Prisma Access zu ermitteln, wählen Sie **Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** aus. Klicken Sie dann das Optionsfeld **Dienstverbindung** und notieren Sie die **Dienst-IP-Adresse** und die für den Standort.

   Die **Dienst-IP-Adresse** ist die öffentlich zugängliche Adresse, mit der Sie eine Verbindung herstellen müssen, wenn Sie den Tunnel von Ihrem IPSec-fähigen Gerät zurück zur Dienstverbindung erstellen.



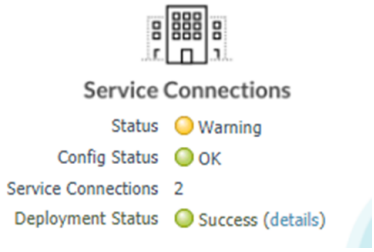

2. Konfigurieren Sie auf Ihrem IPSec-fähigen Gerät am Unternehmensstandort einen IPSec-Tunnel, der eine Verbindung zur **Dienst-IP-Adresse** in Prisma Access herstellt, und schreiben Sie die Änderung auf diesem Gerät mit Commit fest, damit der Tunnel eingerichtet werden kann.

## Dienstverbindungsstatus verifizieren

Um zu überprüfen, ob die Dienstverbindung erfolgreich eingerichtet wurde, wählen Sie **Panorama > Cloud Services > Status > Status** aus und überprüfen dann, ob für den Status **OK** angegeben wird.

*Wenn Sie eine Dienstverbindung mit Platzhalterwerten erstellt haben, um die Kommunikation zwischen mobilen Benutzern und Benutzern in Remote-Netzwerken zu ermöglichen, müssen Sie den Status der Dienstverbindung nicht überprüfen.*

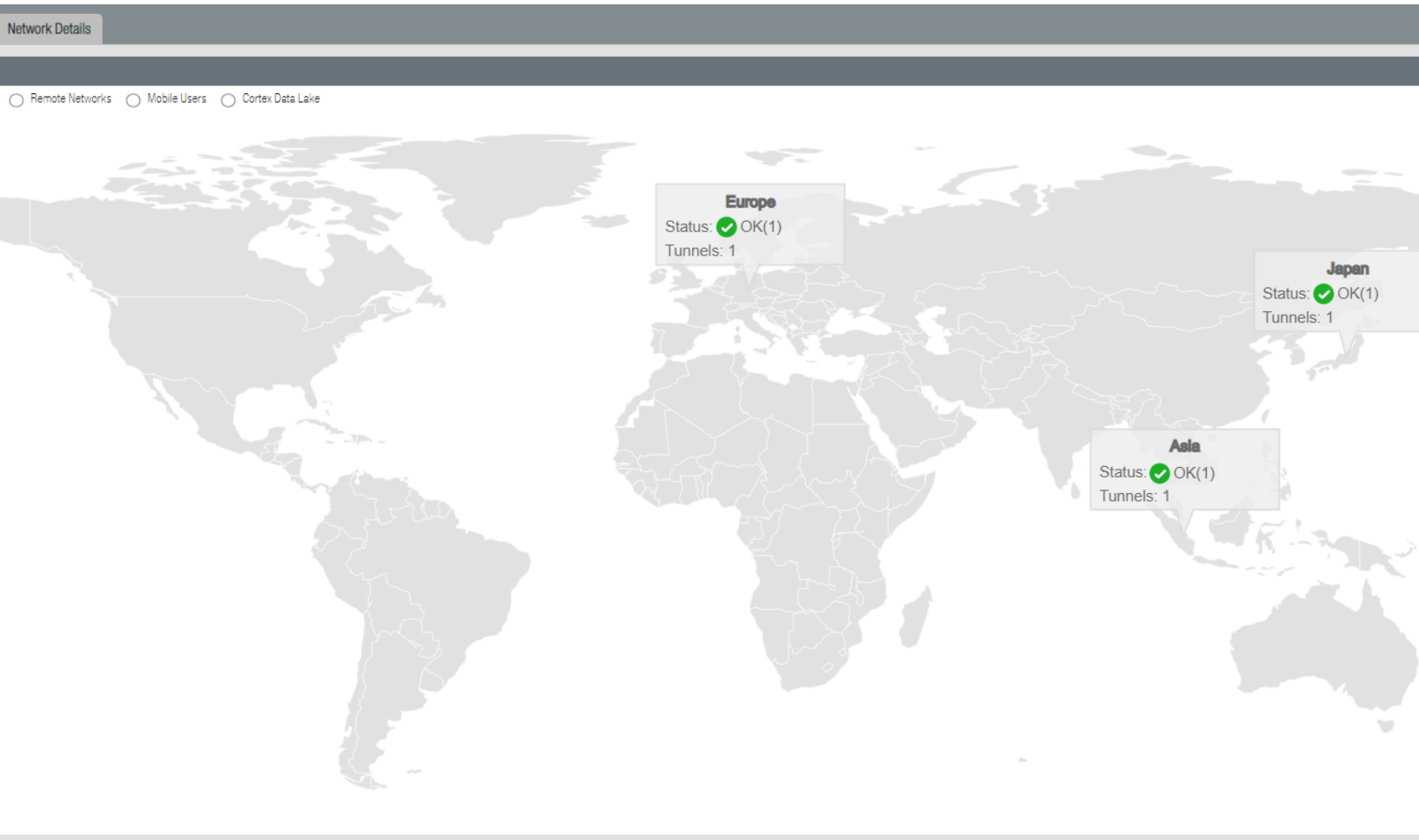
Im Bereich **Bereitstellungsstatus** können Sie den Fortschritt der Onboarding- und Bereitstellungsaufträgen verfolgen, bevor sie abgeschlossen sind. Außerdem erhalten Sie weitere Informationen zum Status abgeschlossener Jobs.



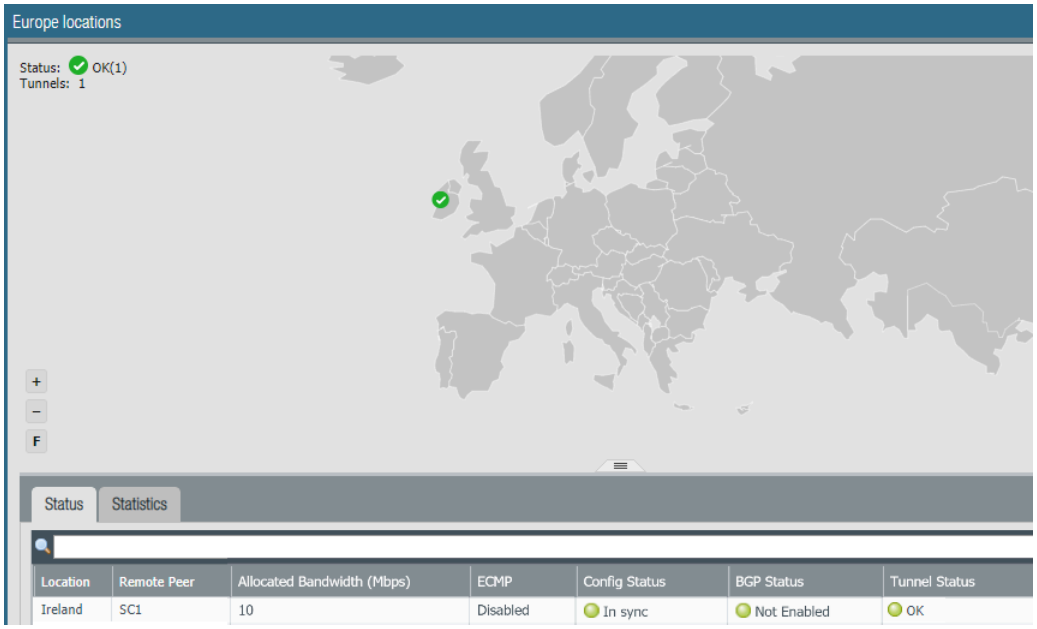

Wenn der Status nicht **OK** lautet, bewegen Sie den Mauszeiger über das Statussymbol, um Fehler anzuzeigen.

Um eine grafische Darstellung der Dienstverbindung zusammen mit Statusdetails anzuzeigen, wählen Sie auf der Registerkarte **Überwachen** die Option **Dienstverbindung** aus.

 ©2025 Palo Alto Networks, Inc.




Wählen Sie eine Region aus, um weiterführende Details zu dieser Region abzufragen.




Klicken Sie auf die Registerkarten unter der Karte, um weitere Informationen zu den Dienstverbindungen anzuzeigen.

 ©2025 Palo Alto Networks, Inc.

Registerkarte **Status**:

- **Standort** – Der Standort, an dem Ihre Dienstverbindung bereitgestellt wird.
- **Remote-Peer** – Der Unternehmensstandort, zu dem diese Dienstinfrastruktur einen IPSec-Tunnel einrichtet.
- **Zugewiesene Bandbreite** – Die Anzahl der zugewiesenen Dienstverbindungen multipliziert mit 300 Mbit/s.

  Diese Anzahl spiegelt nicht die verfügbare Dienstverbindungsbandbreite wider.

  *Während jede Dienstverbindung etwa 1 Gb/s Durchsatz bereitstellt, hängt der tatsächliche Durchsatz von mehreren Faktoren ab, darunter:*

  - *Datenverkehrsmix (z.B. Rahmengröße)*
  - *Latenz und Paketverlust zwischen der Dienstverbindung und der Zentrale oder dem Rechenzentrum*
  - *Leistungsgrenzen der Dienstanbieter*
  - *Leistungsgrenzen für Kundenabschlussgeräte*
  - *Sonstiger Datenverkehr des Kunden im Rechenzentrum*
- **ECMP** – Wenn Sie für diese Dienstverbindung einen Equal Cost Multipath (ECMP) konfiguriert haben. Da ECMP nicht für Dienstverbindungen verwendet wird, lautet dieser Status **Deaktiviert**.
- **Konfigurationsstatus** – Der Status Ihrer letzten Übertragungsaktion für die Konfiguration an den Dienst. Wenn die lokale Konfiguration und die Konfiguration in der Cloud übereinstimmen, lautet der Konfigurationsstatus **Synchron**. Wenn Sie lokal eine Änderung vorgenommen und die Konfiguration noch nicht in die Cloud übertragen haben, wird möglicherweise der Status **Nicht synchron** angezeigt. Bewegen Sie den Mauszeiger über die Statusanzeige, um detailliertere Informationen zu erhalten. Nach dem Festschreiben und Übertragen der Konfiguration auf Prisma Access ändert sich der Konfigurationsstatus in **Synchron**.
- **BGP-Status** – Zeigt Informationen zum BGP-Status zwischen der Firewall oder dem Router am Standort Ihres Unternehmens bzw. der Zentrale und Prisma Access an, wo die Dienstverbindung eingerichtet wird. Obwohl der Status beim Durchlaufen der verschiedenen BGP-Status nur kurz angezeigt wird (**Inaktiv**, **Aktiv**, **Offen Senden**, **Offen Anstehend**, **Offen Bestätigen**), wird der BGP-Status meist angezeigt:
  - **Verbinden** – Der Router im Rechenzentrum bzw. der Zentrale versucht, die BGP-Peer-Beziehung zu Prisma Access herzustellen.
  - **Eingerichtet** – Die BGP-Peer-Beziehung wurde eingerichtet.

  In diesem Feld wird auch angezeigt, ob sich die BGP-Verbindung in einem Fehlerzustand befindet:

  - **Warnung** – Seit mehr als acht Minuten wurde der BGP-Status nicht aktualisiert. Dies kann auf einen Ausfall der Firewall hindeuten.
  - **Fehler** – Der BGP-Status ist unbekannt.

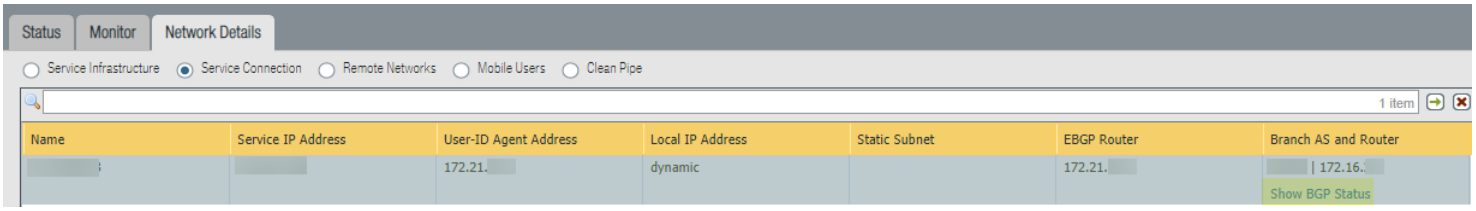
 ©2025 Palo Alto Networks, Inc.

- **Tunnelstatus** – Der Betriebsstatus der Verbindung zwischen Prisma Access und Ihrer Dienstverbindung.

Registerkarte **Statistiken**:

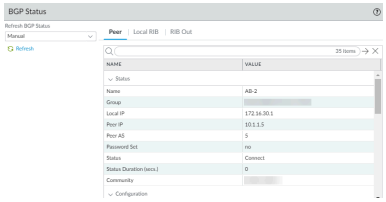
- **Standort** – Der Standort, an dem Ihre Dienstverbindung bereitgestellt wird.
- **Remote-Peer** – Der Unternehmensstandort, zu dem die Dienstverbindung einen IPSec-Tunnel einrichtet.
- **Eingangsbandbreite (Mbit/s)** – Die Bandbreite vom Standort der Zentrale/des Rechenzentrums bis zu Prisma Access.
- **Höchste Eingangsbandbreite (Mbit/s)** – Die Spitzenlast vom Standort der Zentrale/des Rechenzentrums in den Cloud-Dienst.
- **Ausgangsbandbreite (Mbit/s)** – Die Bandbreite von Prisma Access bis zum Standort der Zentrale/des Rechenzentrums.
- **Höchste Eingangsbandbreite (Mbit/s)** – Die Spitzenlast von Prisma Access bis zum Standort der Zentrale/des Rechenzentrums.
- **QoS** – Wählen Sie diese Schaltfläche aus, um ein Grafikdiagramm anzuzeigen, das eine Echtzeitstatistik und eine historische QoS-Statistik einschließlich der Anzahl der gelöschten Pakete pro Klasse anzeigt. Dieses Diagramm wird nur für Dienstverbindungen oder Remote-Netzwerkverbindungen angezeigt, bei denen QoS aktiviert ist.

Wenn Sie BGP konfiguriert haben, können Sie dessen Status überprüfen, indem Sie **Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Dienstverbindung** > **BGP-Status anzeigen**auswählen.




Der Dialog für den BGP-Status wird angezeigt. Diese Tabelle enthält folgende Informationen:

- **Peer** – Routinginformationen für den BGP-Peer, einschließlich Status, Gesamtzahl der Routen, Konfigurations- und Laufzeitstatistiken sowie Zähler. Die Gesamtzahl der Routen wird im Bereich **bgpAfiIpv4-unicast Counters** in den Feldern **Gesamtwert eingehend** und **Gesamtwert ausgehend** angezeigt.

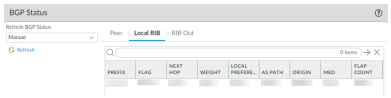



- **Lokale RIB** – BGP-Routen, die Prisma Access lokal nutzt. Prisma Access wählt diese Informationen aus der BGP-RIB-Eingabetabelle aus, in der die von benachbarten Netzwerkgeräten gesendeten Informationen gespeichert werden, wendet lokale BGP-

 ©2025 Palo Alto Networks, Inc.

Importrichtlinien und -Routingentscheidungen an und speichert die lokalen RIB-Informationen in der Routinginformationsbasis (RIB).

Beachten Sie, dass nur die ersten 256 Einträge angezeigt werden. Um zusätzliche Einträge anzuzeigen, geben Sie im Feld „Filter“ ein Subnetz oder eine IP-Adresse ein und klicken Sie dann auf „Filter anwenden“, um eine Teilmenge der Routingeinträge bis zur maximalen Anzahl von 256 anzuzeigen.




- **RIB Ausgehend** – Routinginformationen, die Prisma Access über BGP-Aktualisierungsnachrichten an seine Peers mitteilt.

 ©2025 Palo Alto Networks, Inc.

# Aktivieren Sie den Zugriff zwischen mobilen Benutzern und Remote-Netzwerken mithilfe einer Dienstverbindung.

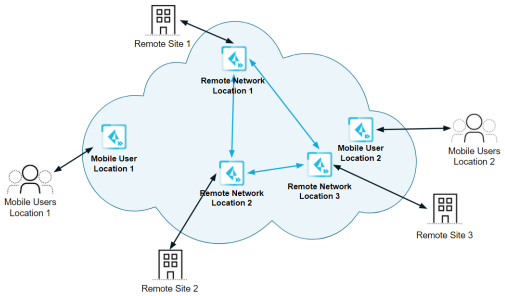
| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz, die Net Interconnect für Site-to-Site- und User-to-Site-Zugriff umfasst |

**Fügen** Sie zum Konfigurieren einer Dienstverbindung zum Verbinden mobiler Benutzer und Remote-Netzwerke eine Dienstverbindung mit den folgenden Werten hinzu:

- Geben Sie eine **Region** an, die sich in der Nähe Ihrer mobilen Benutzer befindet.
- **Fügen Sie** einen**IPSec-Tunnel** und ein **IKE-Gateway** mit Platzhalterwerten hinzu.
- Fügen Sie den Platzhalter **Unternehmens-Subnetze** hinzu.

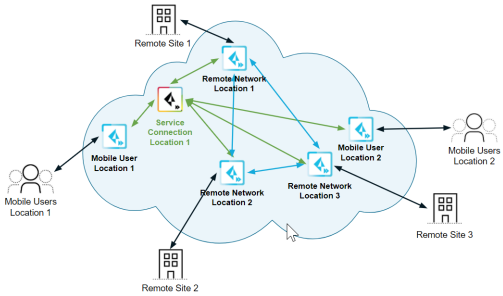
  Da Prisma Access keinen Datenverkehr durch diesen Tunnel leitet, ist jeder Wert gültig, der nicht mit anderen konfigurierten Subnetzen kollidiert oder sich mit ihnen überschneidet.

Das folgende Beispiel zeigt eine Prisma Access-Bereitstellung mit mobilen Benutzern in verschiedenen geografischen Gebieten und Remote-Netzwerken. Die Remote-Netzwerkverbindungen sind in einem Mesh-Netzwerk in der Prisma Access-Infrastruktur verbunden. Die mobilen Benutzer können sich jedoch nicht mit den Remote-Netzwerken verbinden. Zudem ist es mobilen Benutzern in unterschiedlichen geografischen Gebieten auch nicht möglich, ohne eine Dienstverbindung eine Verbindung zueinander herzustellen.

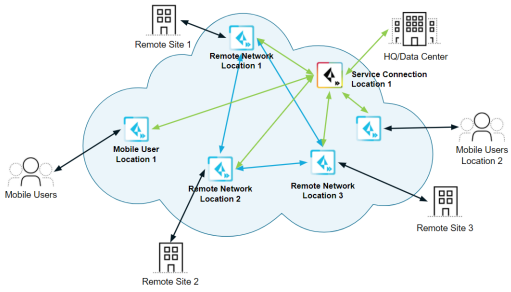



Nachdem Sie eine Dienstverbindung hinzugefügt haben, verbindet diese die mobilen Benutzer und die Remote-Netzwerke in einem Hub-and-Spoke-Netzwerk.

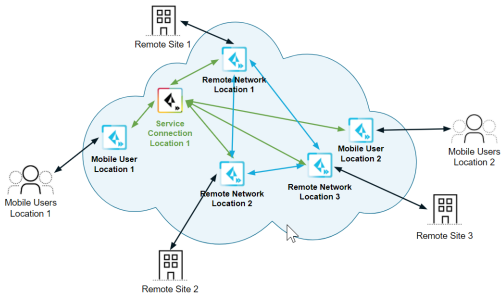
 ©2025 Palo Alto Networks, Inc.




Außerdem ist eine solche Dienstverbindung sinnvoll, wenn die Dienstverbindung weit von den mobilen Benutzern entfernt ist. Die folgende Abbildung zeigt ein Beispiel für diese Netzwerkbereitstellung.




Das Hinzufügen einer zweiten Dienstverbindung, die näher an den mobilen Benutzern liegt, schafft ein effizienteres Netzwerk zwischen den mobilen Benutzern und Remote-Netzwerken.




 ©2025 Palo Alto Networks, Inc.

# Hinweise zu dynamischem Routing für Dienstverbindungen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

## Funktionsweise: Routing von Dienstverbindungsverkehr

Prisma Access verwendet BGP für dynamisches Routing und die BGP-Pfadauswahl, um Routen in der Routentabelle zu installieren. Wenn Prisma Access Datenverkehr über Dienstverbindungen an Ihre Zentrale oder Ihr Rechenzentrum leitet, verwendet es Routingmethoden, die diesen Datenverkehr effektiv leiten. Prisma Access verwendet ein Standardroutingmodell, das für die meisten Netzwerkbereitstellungen entwickelt wurde. Allerdings sind nicht alle Netzwerke einer Organisation gleich. Sie können mit Prisma Access einen anderen Modus für das Dienstverbindungsrouting auswählen, um eine breitere Palette von Bereitstellungen zu ermöglichen. In den folgenden Abschnitten wird auf die von Prisma Access verwendeten BGP-Routingmethoden sowie die Faktoren eingegangen, die im Netzwerk Ihrer Organisation vor der Änderung der Prisma Access-Standardmethode für das Routing von Dienstverbindungen zu berücksichtigen sind.

*Das Ändern der Prisma Access-Methode für das Routing von Dienstverbindungen erfordert ein gründliches Verständnis der Topologie und der Routinggeräte Ihrer Organisation sowie ein Verständnis der Funktionsweise des Prisma Access-Routings, wie in diesem Abschnitt beschrieben. Wir empfehlen Ihnen, diesen Abschnitt sorgfältig zu lesen, bevor Sie die standardmäßige Routingmethode ändern.*

Prisma Access unterstützt statisches und dynamisches Routing mit BGP für Dienstverbindungen und Remote-Netzwerkverbindungen. In diesem Abschnitt wird davon ausgegangen, dass Sie BGP-Routing für Ihre Prisma Access-Bereitstellungen verwenden. Wenn Sie BGP-Routing auswählen, erhält das Netzwerk Ihrer Organisation BGP-Informationen von Prisma Access.

### Routingmodi für Dienstverbindungen

Mit Prisma Access können Sie aus folgenden Routingmodi wählen:

- Standardrouting – Dies ist das aktuelle von Prisma Access verwendete Routingmodell.

  Verwenden Sie diesen Routingmodus, wenn Prisma Access die besten BGP-Pfadauswahlmechanismen verwenden soll, ohne die BGP-Attribute anpassen zu müssen. In diesem Modus berücksichtigt Prisma Access jedes Attribut, das von dem Customer Premises Equipment (CPE) angekündigt wird.

 ©2025 Palo Alto Networks, Inc.

- Hot-Potato-Routing – Prisma Access leitet den Datenverkehr so schnell wie möglich an das Netzwerk Ihrer Organisation weiter.

  Verwenden Sie diese Routingmethode, wenn das Netzwerk Ihrer Organisation die meisten Routingentscheidungen treffen soll.

## Prisma Access-Standardrouting

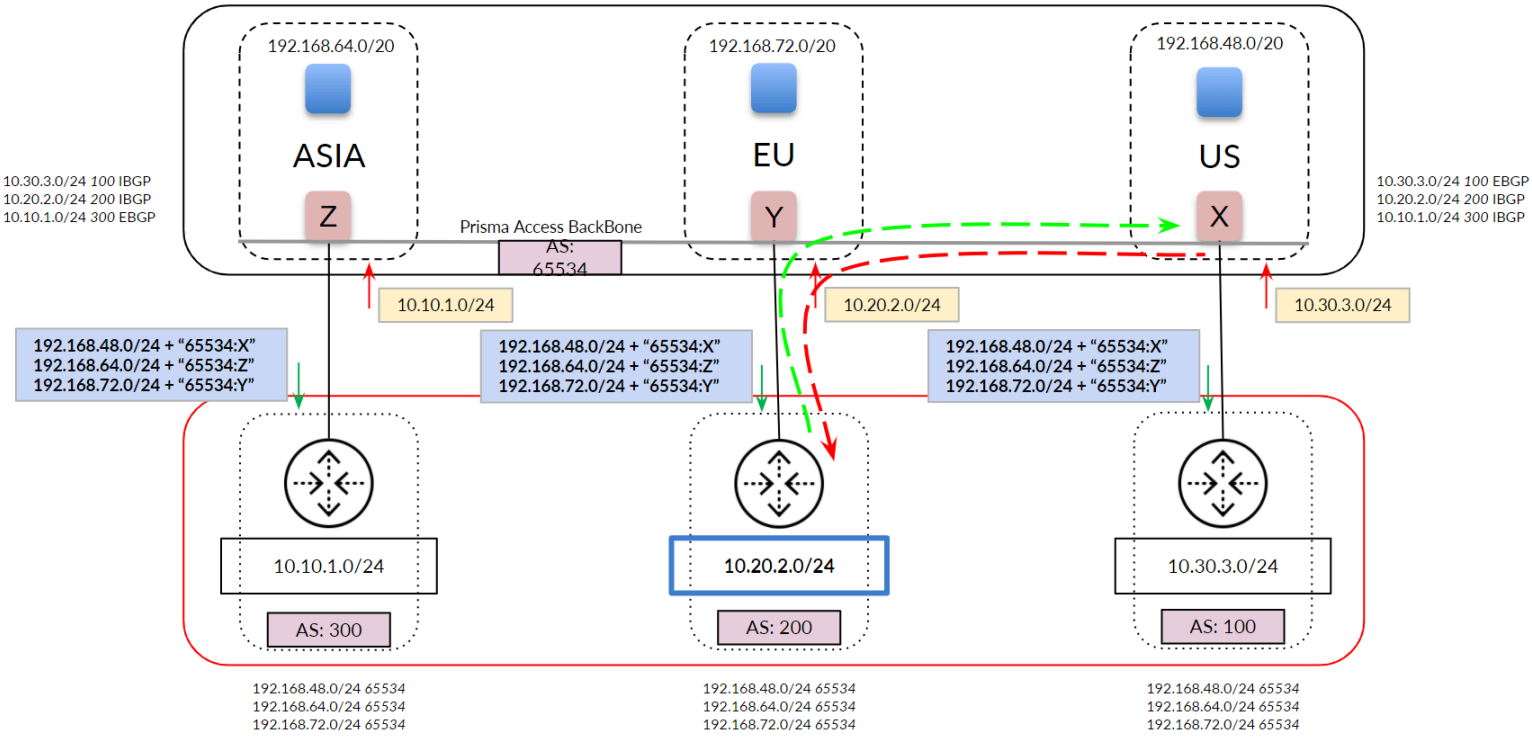
In der folgenden Abbildung ist ein Beispiel für das Prisma Access-Routing von Dienstverbindungsverkehr im Standardroutingmodus dargestellt. Das Netzwerk der Organisation verfügt über drei separate Netzwerke in drei Rechenzentren. Ein Backbone, das die Netzwerke verbindet, ist nicht vorhanden. Im Standardroutingmodus werden in den drei Netzwerken mobile Benutzerpools gleichermaßen angekündigt, wie unten in der Abbildung dargestellt.

Beachten Sie Folgendes: Wenn Prisma Access Routen mobiler Benutzer ankündigt, kündigt es vorher die /20 Subnetze mobiler Benutzer in /24-Chunks an, wenn Präfixe von den Gateways verbraucht werden.

Beachten Sie, wie Prisma Access BGP-Routenankündigungen verwendet:

- Prisma Access passt die BGP-Standardattribute für angekündigte Routen mobiler Benutzer nicht an (Prisma Access ergänzt die Routenankündigungen um seine AS-Anzahl).
- Prisma Access kündigt Routen mobiler Benutzer an und fügt BGP-Community-Werte in den Routen hinzu, die es über die Dienstverbindung ankündigt. In der folgenden Abbildung ist eine Bereitstellung für mobile Benutzer mit drei Dienstverbindungen und drei verschiedenen IP-Adressblöcken dargestellt, die angegeben wurden für: `192.168.64.0/20` für die Region **Asien, Australien und Japan**, `192.168.72.0/20` für die Region **Afrika, Europa und Naher Osten** und `192.168.48.0/20` für die Region **Nordamerika und Südamerika**. Prisma Access teilt diese Strecken in Block /24 ein und kündigt sie mit der Prisma Access-AS-Nummer **65534** an, fügt aber den Ankündigungen auch die BGP-Community-Werte an (**Z** für Asien, **Y** für EU und **X** für US). Diese Routen sind in der Mitte der Abbildung dargestellt. Auf diese Weise können Sie Dienstverbindungen in Ihrem Netzwerk auch dann unterscheiden, wenn Prisma Access ihnen dieselbe AS-Nummer zuweist.

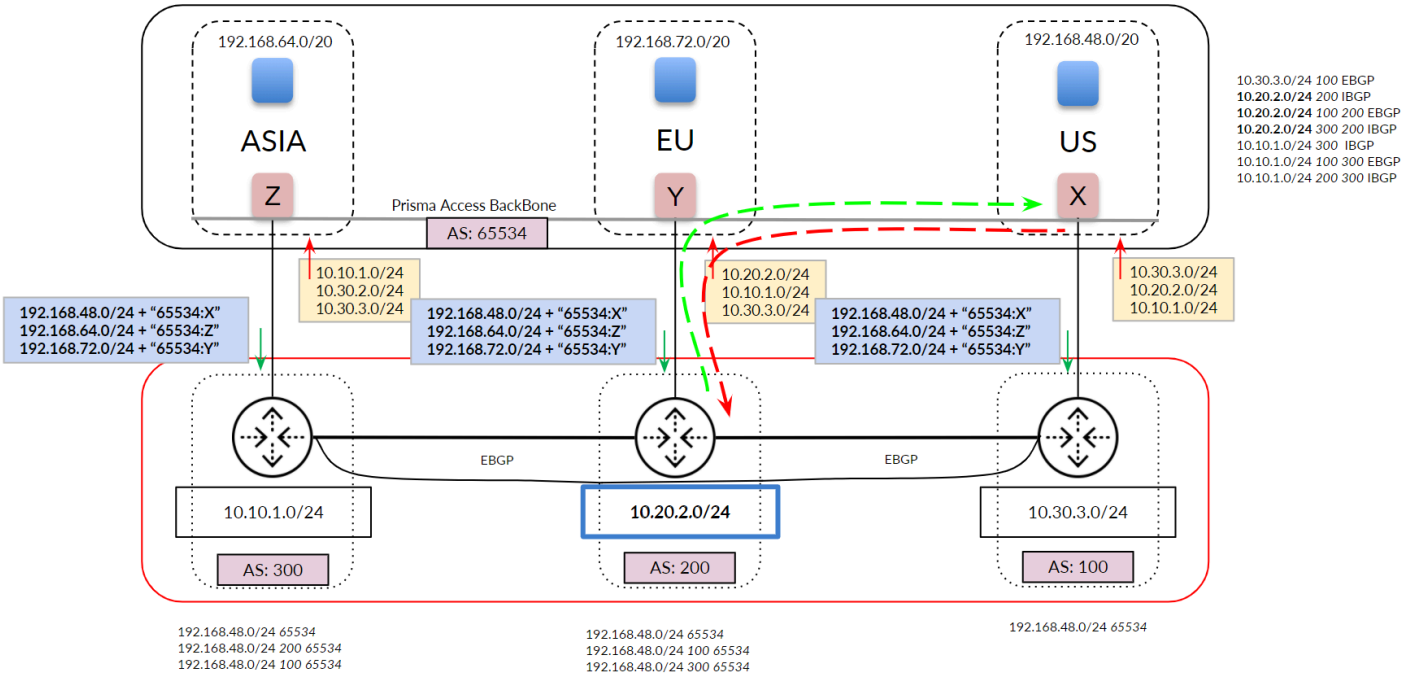
 ©2025 Palo Alto Networks, Inc.




In der folgenden Abbildung ist ein gängigeres Netzwerk mit einem vollständig vermaschten eBGP-Backbone dargestellt. Oben rechts sind die Routen abgebildet, von denen Prisma Access über das Netzwerk Ihrer Organisation erfahren hat. Beachten Sie die zusätzlichen Routen, von denen Prisma Access über das Prisma Access-Backbone (iBGP) und das Backbone (eBGP) Ihrer Organisation erfahren hat.

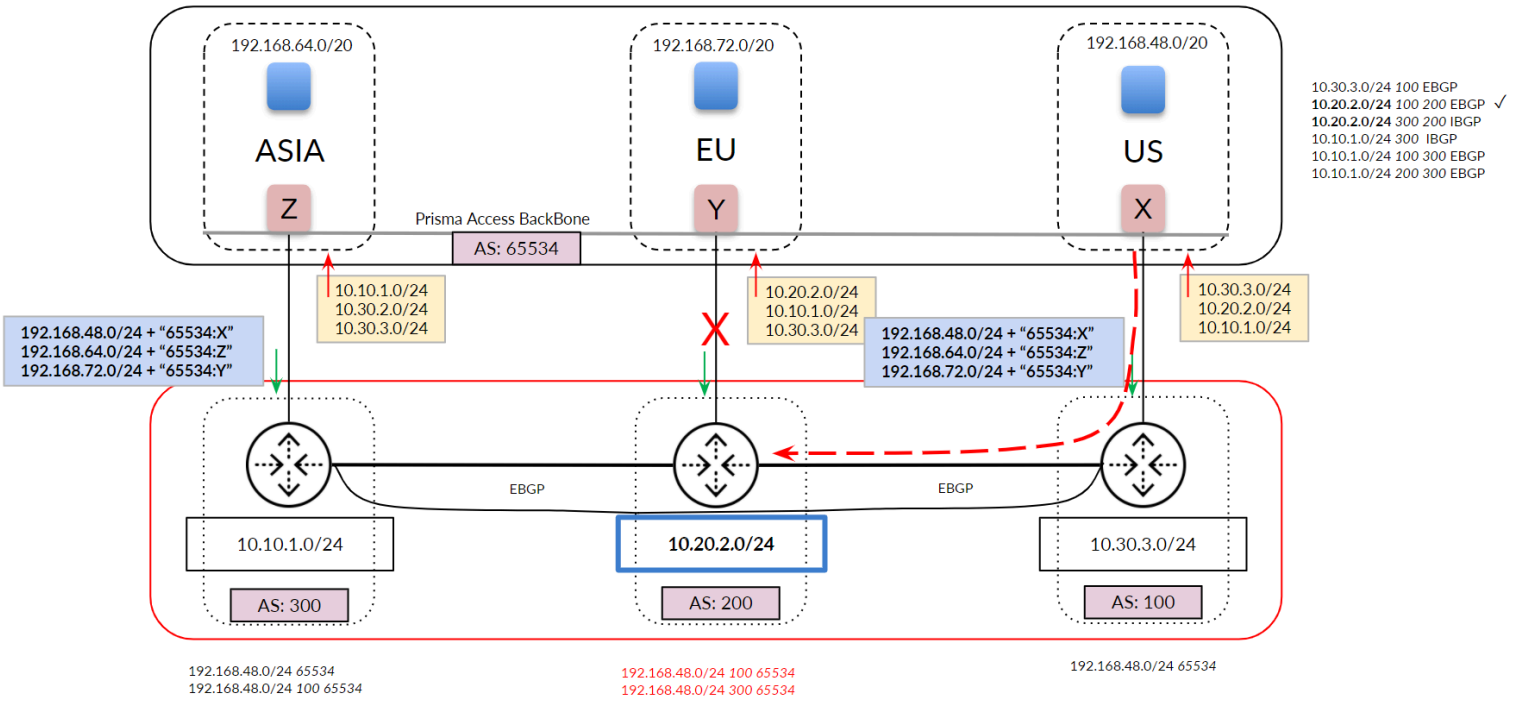
Für den Datenverkehr zwischen mobilen Benutzern in der Region **Nordamerika und Südamerika** (im Diagramm „US“) und dem Rechenzentrum in der Region **Afrika, Europa und Naher Osten** Ihrer Organisation (im Diagramm „EU“) wählt Prisma Access den Pfad über die EU-Dienstverbindung, da Routen mit kürzerem AS-Pfad bevorzugt werden.

 ©2025 Palo Alto Networks, Inc.




Bei Bereitstellungen mit einem vollständig vermaschten eBGP-Backbone kann es zu Asymmetrien kommen, wenn Prisma Access ein bestimmtes Rechenzentrum aufgrund eines ISP/CPE-Fehlers im Rechenzentrum des Kunden nicht erreichen kann. Die folgende Abbildung zeigt, was geschehen könnte, wenn die Verbindung zur EU-Dienstverbindung ausfällt. Ihr Netzwerk erkennt den Ausfall der Verbindung und erstellt eine neue Routentabelle für AS 200. Datenverkehr von der US-Dienstverbindung zu AS 200 nutzt den Pfad über AS 100, da die eBGP-Route für Ihr Backbone zwischen AS 200 und AS 100 gegenüber der iBGP-Route zwischen der EU- und der US-Dienstverbindung vorgezogen wird. Es ist jedoch nicht garantiert, dass der zurückfließende Datenverkehr über denselben Pfad weitergeleitet wird, weil das lokale CPE beide Pfade (rot dargestellt) auswählen kann, um den Datenverkehr zurückzugeben.

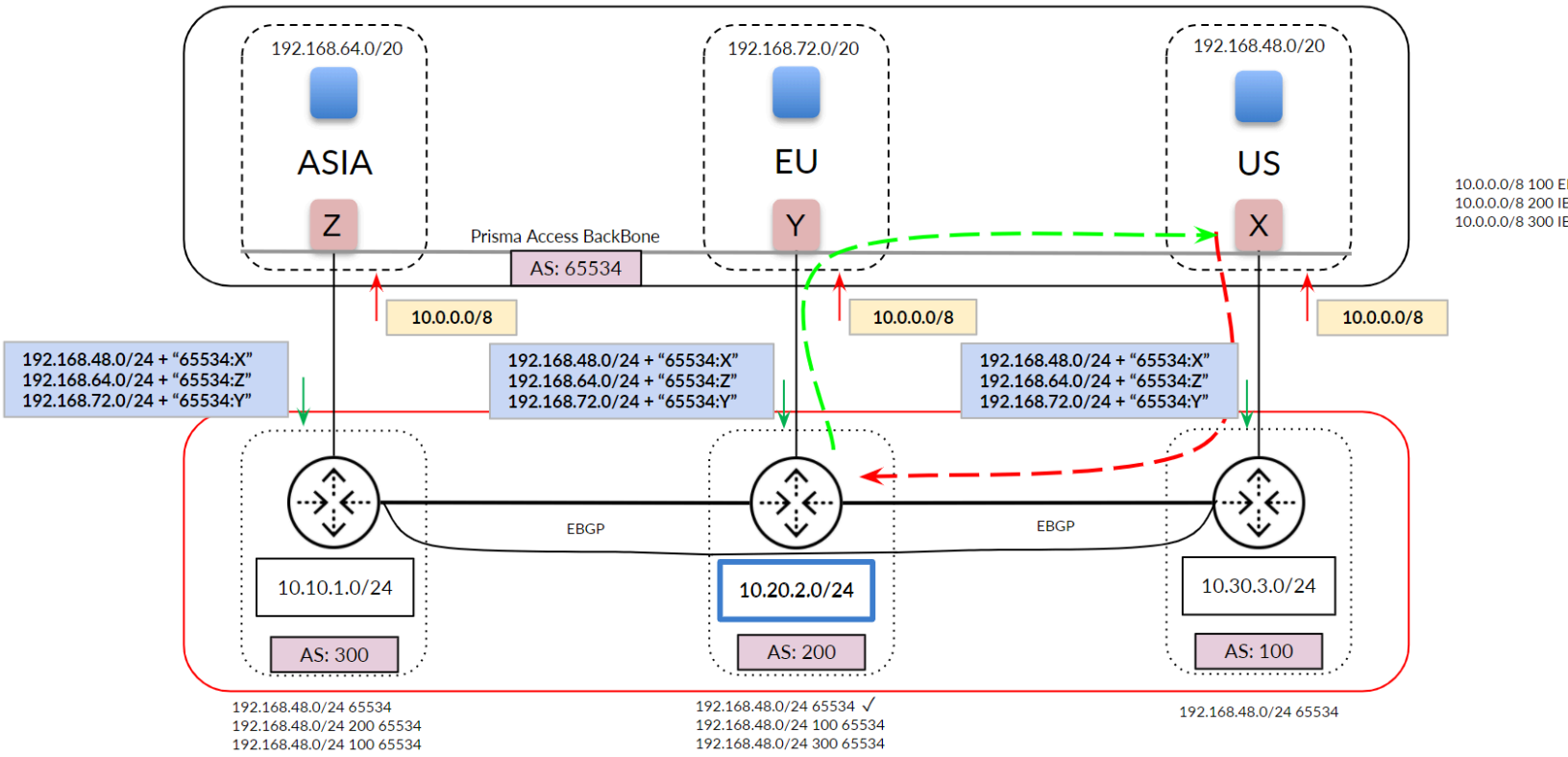
 ©2025 Palo Alto Networks, Inc.




In den obigen Beispielen ist ein Netzwerk dargestellt, dessen Routen nicht aggregiert wurden (d. h., Sie haben vor dem Senden der BGP-Routenankündigung an Prisma Access keine Routenzusammenfassung durchgeführt). Das folgende Beispiel zeigt ein Netzwerk, das seine Routen vor dem Senden an Prisma Access auf 10.0.0.0/8 zusammenfasst. Wenn Sie Standardrouting auswählen, kann diese Konfiguration zu Problemen durch asymmetrisches Routing führen, da Prisma Access aus den zusammengefassten Routen nicht den richtigen Rückgabepfad ermitteln kann.

*Wenn Ihre Prisma Access-Bereitstellung über Remote-Netzwerke verfügt, empfiehlt Palo Alto Networks, keine Routenzusammenfassung für Dienstverbindungen zu verwenden. Die Routenzusammenfassung für Dienstverbindungen ist nur für Bereitstellungen für mobile Benutzer bestimmt.*

 ©2025 Palo Alto Networks, Inc.




Wenn Sie die Routenaggregation für mobile Benutzer verwenden, empfehlen wir dringend, das Hot-Potato-Routing anstelle des Standardroutings zu aktivieren. Hier leitet Prisma Access den Datenverkehr so schnell wie möglich an das Netzwerk Ihrer Organisation weiter. Darüber hinaus empfehlen wir Ihnen, für jede Dienstverbindung eine Backup-Dienstverbindung (**Backup-SC**) auszuwählen, wie im folgenden Abschnitt beschrieben, um ein deterministisches Routingverhalten zu erzielen.

## Hot-Potato-Routing

Wenn Sie **Hot-Potato-Routing** auswählen, leitet Prisma Access den an Dienstverbindungen/Rechenzentren gebundenen Datenverkehr so schnell wie möglich aus seinem internen Netzwerk.

Beim Hot-Potato-Routing stellt Prisma Access den AS-Pfad (AS-PATH) den von Gateways gesendeten BGP-Präfixankündigungen voran. Diese Voranstellung wird ausgeführt, wenn die Präfixe aus der Dienstverbindung heraus den lokalen CPEs Ihrer Organisation angekündigt werden. Prisma Access stellt die AS-Pfade so voran, dass Ihr CPE den primären und sekundären Tunneln die richtige Präferenz gibt, sodass bei Ausfall des primären Tunnels Ihr CPE den sekundären Tunnel als Backup wählt.

Wenn Sie eine andere IP-Adresse für den sekundären BGP-Peer (das Backup) angegeben haben, fügt Prisma Access weitere Voranstellungen basierend auf dem Tunneltyp hinzu, wie in der folgenden Tabelle aufgeführt.

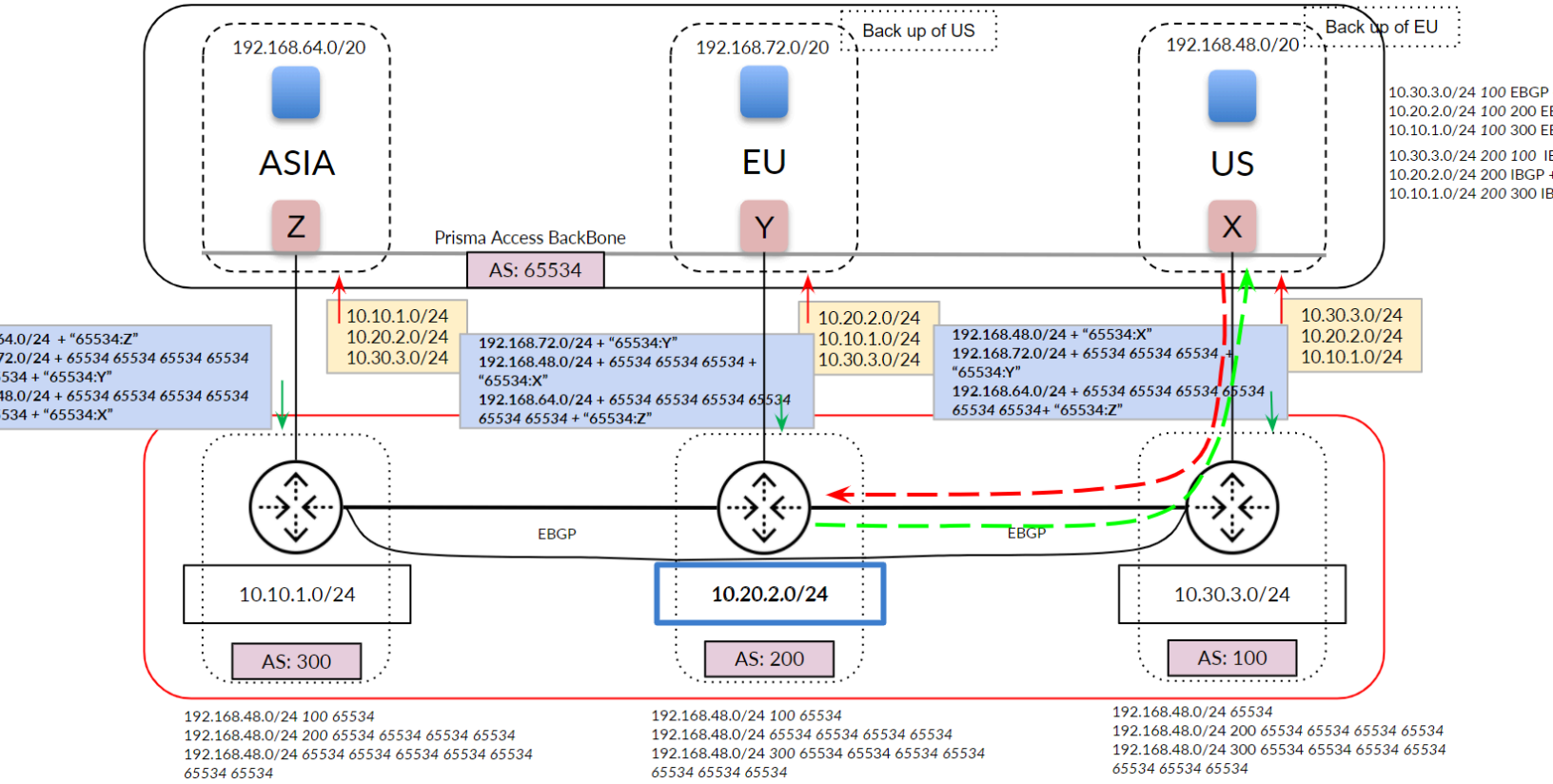
 ©2025 Palo Alto Networks, Inc.

| Präfixtyp | Typ des Dienstverbindungstunnels | Anzahl der AS-Pfad-Voranstellun | Gesamtzahl der AS-Pfade, die auf dem CPE angezeigt werden |
|---|---|---|---|
| Gateway-Präfixe von der primären Dienstverbindung | Primäre oder sekundäre Tunnel mit gleicher BGP-Peer-IP-Adresse | 0 | 1 |
| Gateway-Präfixe von der Backup-Dienstverbindung | Primäre oder sekundäre Tunnel mit gleicher BGP-Peer-IP-Adresse | 3 | 4 |
| Gateway-Präfixe von allen anderen Dienstverbindungen | Primäre oder sekundäre Tunnel mit gleicher BGP-Peer-IP-Adresse | 6 | 7 |
| Gateway-Präfixe von der primären Dienstverbindung | Sekundärer Tunnel mit einer anderen BGP-Peer-IP-Adresse | 1 | 2 |
| Gateway-Präfixe von der Backup-Dienstverbindung | Sekundärer Tunnel mit einer anderen BGP-Peer-IP-Adresse | 4 | 5 |
| Gateway-Präfixe von allen anderen Dienstverbindungen | Sekundärer Tunnel mit einer anderen BGP-Peer-IP-Adresse | 7 | 8 |

Geben Sie eine **Backup-Dienstverbindung** an, damit Prisma Access diese Dienstverbindung als Backup verwendet, sollte eine Dienstverbindung fehlschlagen.

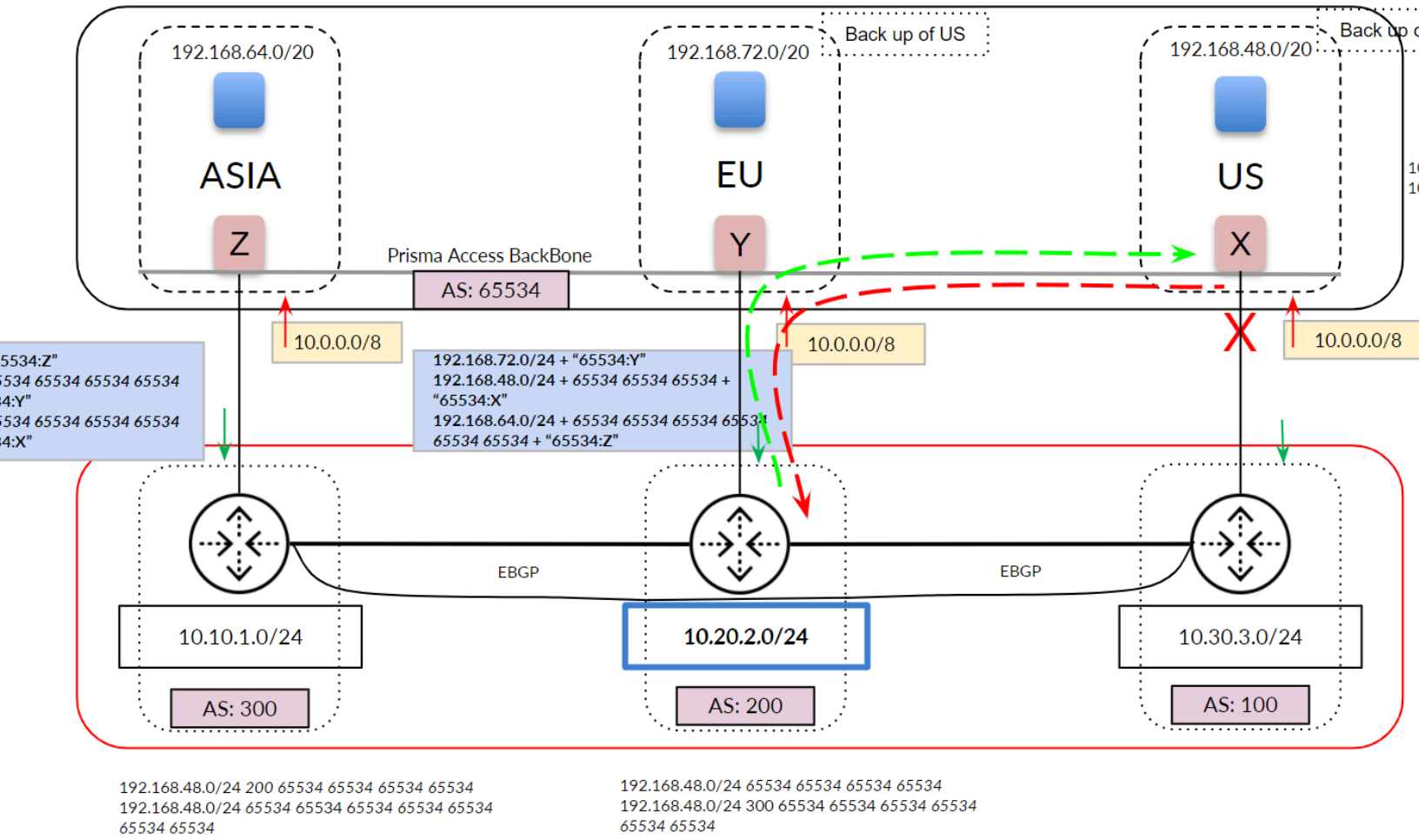
In der folgenden Abbildung ist eine Hot-Potato-Routing-Konfiguration für den Datenverkehr zwischen der US-Dienstverbindung und AS 200 dargestellt, wobei die EU-Dienstverbindung als **Backup-Dienstverbindung** der US-Dienstverbindung konfiguriert ist. Mithilfe von Hot-Potato-Routing sendet Prisma Access den Datenverkehr von seinem nächstgelegenen Ausgangspfad über die US-Dienstverbindung. Der zurückfließende Datenverkehr nimmt den gleichen Pfad über AS 100, da dieser Pfad einen kürzeren AS-Pfad zum Pool der mobilen Benutzer am US-Standort hat. Prisma Access stellt den AS-Pfad seinen Präfixankündigungen voran, abhängig davon, ob es sich bei dem Tunnel um einen primären Tunnel oder einen Backup-Tunnel handelt oder ob er weder als primärer Tunnel noch als Backup-Tunnel verwendet wird.

 ©2025 Palo Alto Networks, Inc.



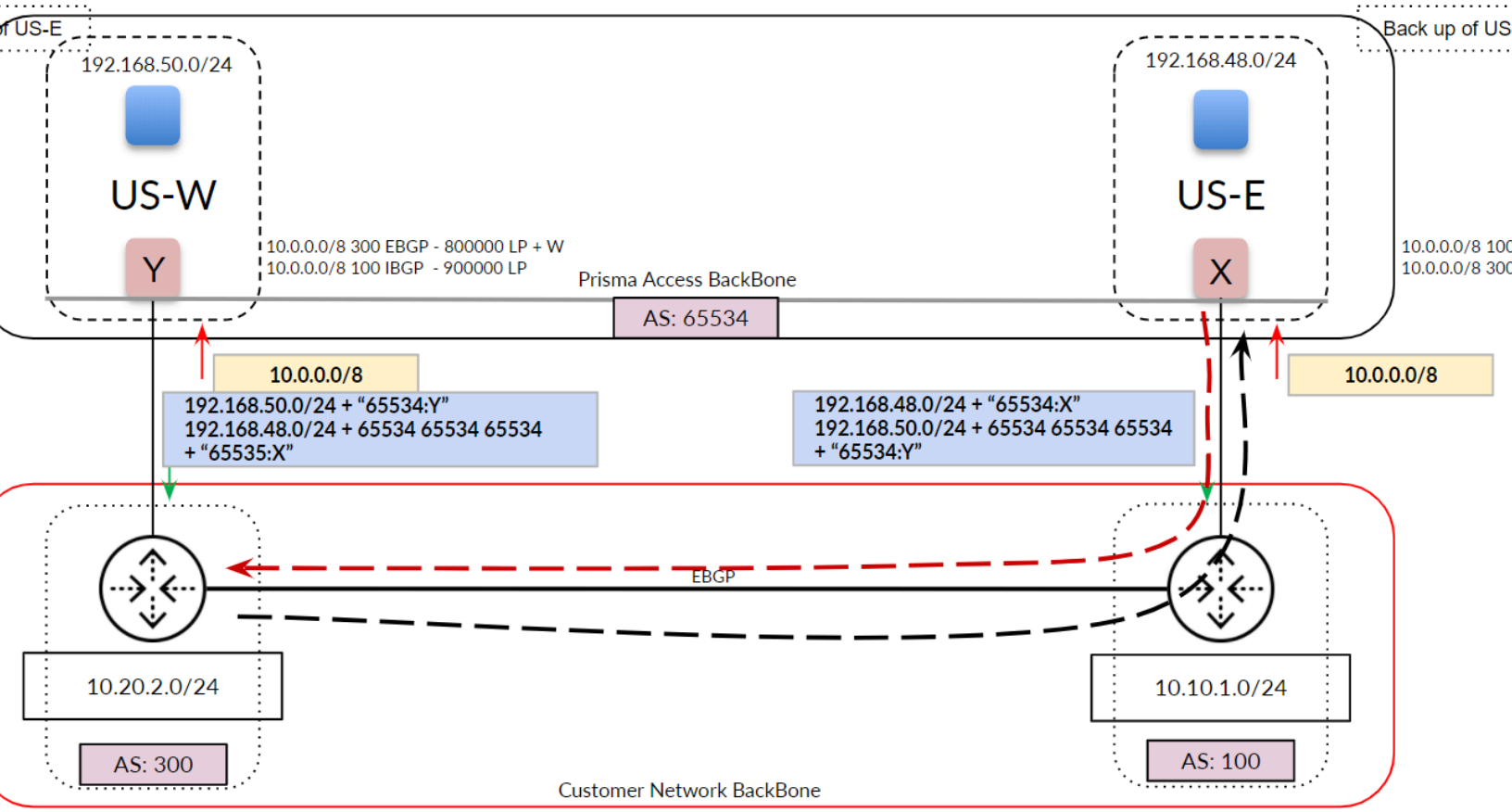

Da Sie eine Backup-Dienstverbindung eingerichtet haben, sendet das Hot-Potato-Routing den Datenverkehr auf kürzestem Weg über die EU-Dienstverbindung hinaus, wenn die US-Dienstverbindung ausfällt. Dieses Routingszenario gilt auch für Netzwerke, die eine Routenaggregation verwenden.

 ©2025 Palo Alto Networks, Inc.




Sie können auch Backup-Dienstverbindungen für mehrere Dienstverbindungen in einer Region verwenden. Die folgende Abbildung zeigt eine Prisma Access-Bereitstellung mit zwei Dienstverbindungen in der Region Nordamerika. In diesem Fall geben Sie die **Backup-Dienstverbindung** US-E für die Dienstverbindung US-W an und umgekehrt, um symmetrisches Routing zu gewährleisten.

 ©2025 Palo Alto Networks, Inc.




 ©2025 Palo Alto Networks, Inc.

# Prisma Access ZTNA-Connector

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access Version 4.0<br>❑ ZTNA-Connector-Add-on-Lizenz<br>Die Essential-Lizenz mit der Add-on-Lizenz umfasst acht ZTNA-Connectors, 100 FQDNs und vier IP-Subnetzfunktionen.<br>Die Advanced-Lizenz mit der Add-on-Lizenz umfasst 40 ZTNA-Connectors, 300 FQDNs und 1.024 IP-Subnetzfunktionen.<br>Die Premiumlizenz mit der Add-on-Lizenz umfasst 200 ZTNA-Connectors, 4.000 FQDNs und 1.024 IP-Subnetzfunktionen.<br>❑ Wenn Sie die ZTNA-Connector-Add-on-Lizenz nicht erwerben, beinhalten die Prisma Access-Lizenzen vier Konnektoren, 40 FQDNs und vier IP-Subnetze. Diese Funktionalität wird bereitgestellt, um ZTNA-Connectors in Ihrer Umgebung zu testen. |

Mit dem ZTNA-Connector (Zero Trust Network Access) können Sie einfach und sicher eine Verbindung zwischen Prisma Access und den privaten Apps Ihres Unternehmens herstellen. ZTNA-Connector bietet mobilen Benutzern und Benutzern in Zweigstellen über einen automatisierten sicheren Tunnel Zugriff auf Ihre privaten Apps. Da der ZTNA-Connector die Tunnel automatisch einrichtet, müssen Sie IPSec-Tunnel und das Routing zum Rechenzentrums- oder Zentralenstandort, zu öffentlichen Cloud-Standorten und Partnernetzwerken, in denen sich Ihre privaten Apps befinden, nicht manuell einrichten.

Die von Ihnen bereitgestellten ZTNA-Connector-VMs stellen automatisch eine Verbindung zum nächstgelegenen Prisma Access-Standort her, um so die bestmögliche Latenz zu gewährleisten. Außerdem skalieren Sie den Bandbreitenzugriff auf bis zu 2 Gbit/s pro Konnektor und 8 Gbit/s pro Konnektorgruppe.

Prisma Access verweigert standardmäßig jeglichen Zugriff, und ein Administrator muss den Zugriff auf eine Ressource mithilfe einer Richtlinienregel, die auf unseren patentierten Konstrukten User-ID, App-ID und Device-ID basiert, explizit zulassen, sodass Sie die Angriffsfläche und die Sicherheitsrisiken reduzieren können. Sobald eine Verbindung zugelassen ist, wird kontinuierlich überprüft, ob diese Verbindung vertrauenswürdig ist. Des Weiteren wird kontinuierlich überprüft, ob Sicherheitsbedrohungen vorliegen und ob Datenlecks aufgetreten sind. Darüber hinaus

werden die privaten IP-Adressen Ihrer Anwendungen nicht offengelegt, wenn Sie den Prisma Access-ZTNA-Connector verwenden.

 ©2025 Palo Alto Networks, Inc.

# ZTNA-Connector-Komponenten

- **Konnektoren** – Konnektoren sind die virtuellen Maschinen, über die Tunnel zu Prisma Access erstellt werden. ZTNA-Connector automatisiert das Tunnelmanagement, ohne dass Sie IPSec- und IKE-Einstellungen angeben müssen. Sie binden Konnektoren in VMs ein, die Sie in einen Cloud-Dienst (Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure) oder in einen virtuellen Server (VMware ESXi) oder in eine Kernel-basierte virtuelle Maschine (KVM)) integrieren. Palo Alto Networks empfiehlt, die VM im selben Subnetz wie die eingebundene Anwendung für Prisma Access bereitzustellen. Sie können auch ein anderes Subnetz angeben, sofern vom Konnektor aus eine Route zu den Anwendungen besteht.

  Nachdem Sie die Konnektor-VM bereitgestellt haben, verwaltet Prisma Access die VM und stellt darüber hinaus Optionen zum Upgrade der VM-Version bereit. Nach der Installation der ZTNA-Connector-VM erkennt sie den nächstgelegenen Prisma Access-Standort und initiiert einen sicheren IPSec-Tunnel zu Prisma Access.
- **Konnektorgruppen** – Eine Konnektorgruppe ist eine logische Gruppierung von Konnektoren und Apps. Durch das Hinzufügen mehrerer Konnektoren zu einer Konnektorgruppe bieten Sie Tunnelredundanz und eine erhöhte Bandbreite für die Apps innerhalb der Gruppe. Jede Konnektorgruppe unterstützt bis zu vier Konnektoren.

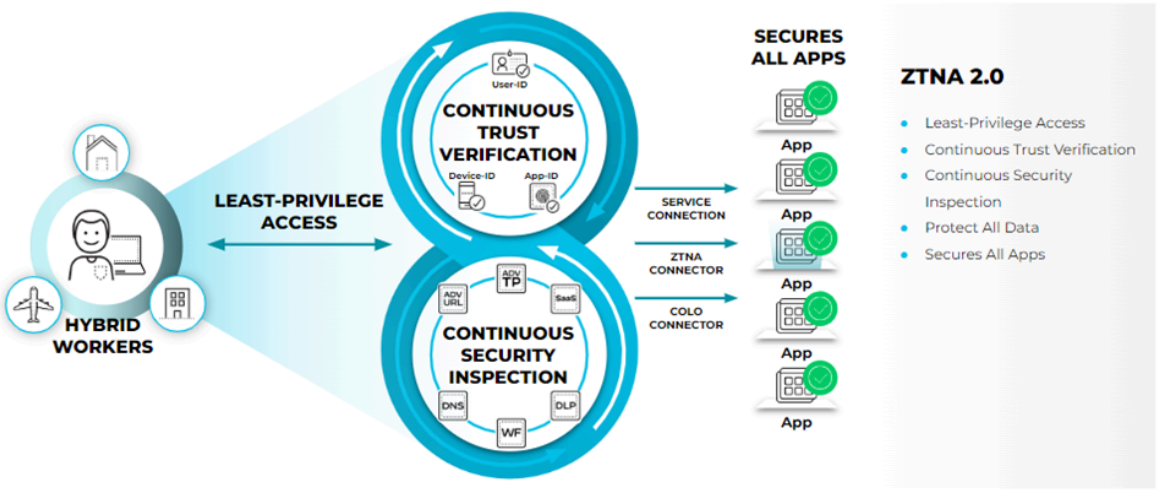
  Wenn Sie mithilfe unterschiedlicher Konnektoren Zugriff auf bestimmte Apps gewähren möchten, platzieren Sie die Konnektoren in separaten Gruppen.
- **Ziele** – Die privaten Apps, die ZTNA-Connector in Prisma Access einbindet. Sie können bestimmte Apps definieren, auf die Sie Zugriff gewähren möchten, indem Sie FQDN (**FQDN-Ziele**), Platzhalter (**Platzhalterziele**) oder IP-Adressen oder Subnetze verwenden, in denen sich die Apps befinden. Alternativ hierzu können die Apps von ZTNA-Connector auch automatisch erkannt werden, indem Sie sie von einem mit CIE verbundenen IdP abrufen.

 ©2025 Palo Alto Networks, Inc.

# Anwendungsfälle für ZTNA-Connector

Verwenden Sie ZTNA-Connector in diesen Szenarien:

- **Verbindung zu privaten Apps herstellen** – Verwenden Sie den ZTNA-Connector für den gesamten vom Client initiierten Datenverkehr, der eine Verbindung zu privaten Apps herstellt.



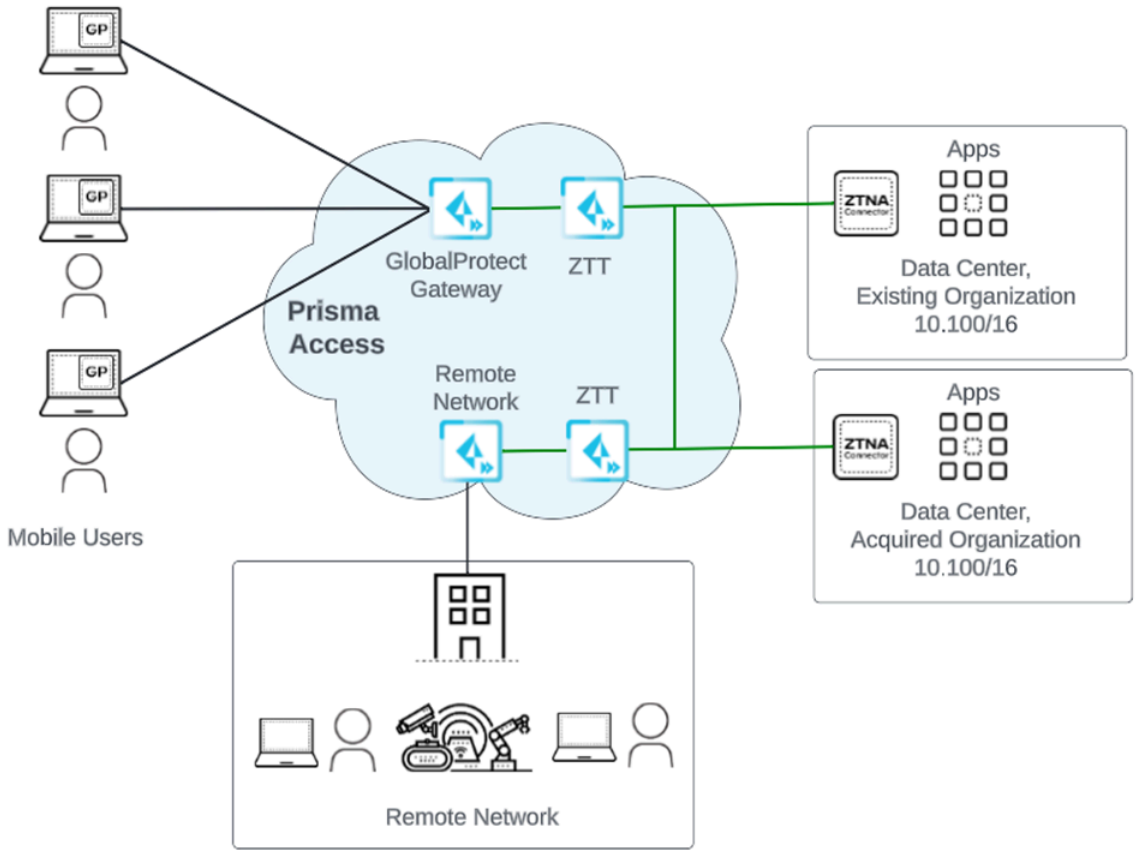

- **Überlappende private Netzwerke** – Wenn Sie Netzwerkadministrator in einem großen Unternehmen sind, das eine andere Organisation übernommen oder mit ihr fusioniert hat, verwenden zwei Netzwerke möglicherweise Adressbereiche, die sich überschneiden (z. B. der private Netzwerk-Adressraum gemäß RFC 1918). Wenn Sie Ihren Benutzern Zugriff auf Apps gewähren wollen, die in überlappenden Netzwerken gehostet werden, dann können Routing und NAT-Konfiguration sehr aufwendig werden. ZTNA-Connector vereinfacht den App-Zugriff in überlappenden Netzwerken, indem Sie mithilfe von FQDNs, FQDN-Platzhaltern und IP-Subnetzen eine Verbindung zu Apps herstellen können, ohne dass Sie das IP-Routing konfigurieren müssen.

  ZTNA-Connector bietet Ihren Benutzern sicheren Zugriff auf private Apps mithilfe von ZTNA-Connector Tunnel Terminators (ZTTs).

  Wenn Sie einen ZTNA-Connector in einer Rechenregion aktivieren, werden automatisch ZTT-Knoten eingebunden. Der ZTNA-Connector bildet automatisch IPSec-Tunnel mit ZTTs. ZTT-Knoten in einer Region bleiben 24 Stunden lang aktiv, nachdem alle Konnektoren in dieser Region gelöscht wurden. Wenn innerhalb von 24 Stunden, nachdem alle Konnektoren in derselben Region gelöscht wurden, ein neuer Konnektor bereitgestellt wird, verwendet er den

 ©2025 Palo Alto Networks, Inc.

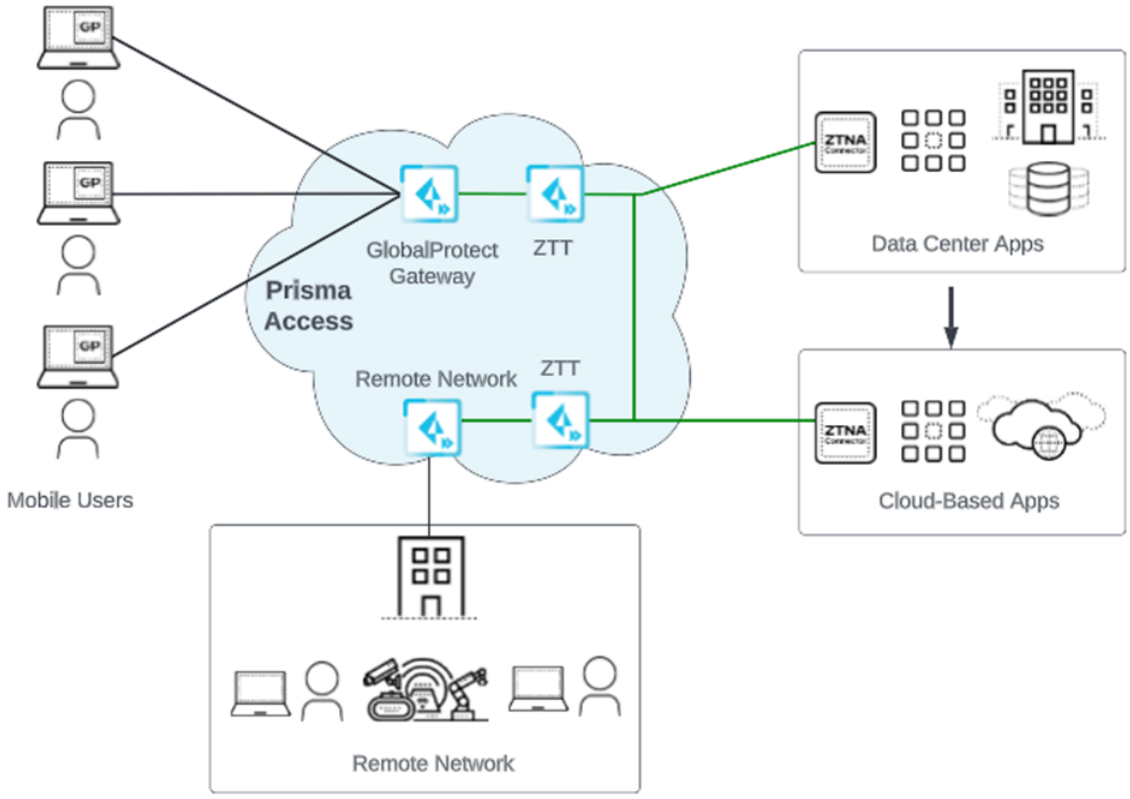
vorhandenen ZTT erneut. Wenn erst nach Ablauf von 24 Stunden ein neuer ZTNA-Connector aktiviert wird, dann wird ein neuer ZTT erstellt.




- **Migration vom Rechenzentrum zur Cloud** – Wenn Ihr Unternehmen Ihre lokalen Apps in die Cloud migriert (und dazu entweder Ihre vorhandenen lokalen Anwendungen mithilfe von „Lift and Shift“ migriert oder Cloud-native Apps entwickelt), können Sie Apps in Cloud-VPCs in AWS, GCP, Azure oder anderen Cloud-Anbietern hosten. Wenn Sie Hunderte oder Tausende

 ©2025 Palo Alto Networks, Inc.

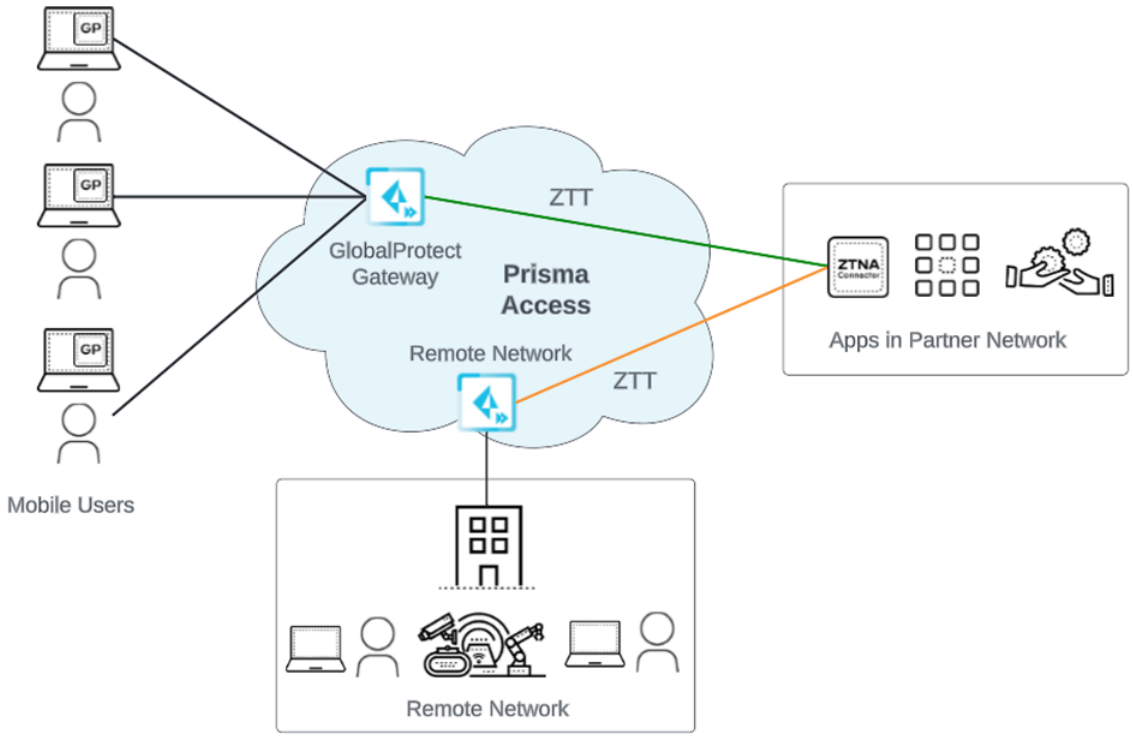
von VPCs haben, kann ZTNA-Connector den Prozess der Bereitstellung des über die Cloud bereitgestellten App-Zugriffs beschleunigen.




- **Zugriff auf Anwendungen in Geschäftspartnernetzwerken** – Einige Unternehmen greifen auf Apps zu, die in den Netzwerken ihrer Geschäftspartner gehostet werden. Die Verwendung von Dienstverbindungen zum Verbinden dieser Apps erfordert ein manuelles Routing und die

 ©2025 Palo Alto Networks, Inc.

NAT-Konfiguration. Mit dem ZTNA-Connector können Sie eine Verbindung zu diesen Apps herstellen, ohne die IP-Routing-Konfiguration manuell durchführen zu müssen.




 ©2025 Palo Alto Networks, Inc.

# Unterstützte Anwendungsfälle für Dienstverbindungen und ZTNA-Connector

Der ZTNA-Connector ist kein Ersatz für Dienstverbindungen. Er kann Dienstverbindungen ergänzen oder mit diesen koexistieren, sodass Sie private Apps flexibel schützen können. Wenn Sie bereits Dienstverbindungen bereitgestellt haben, können Sie diese weiterhin verwenden, es sei denn, Sie möchten zu einem anderen Anwendungszugriffsmodell wechseln. Die folgende Tabelle zeigt die unterstützten und nicht unterstützten Anwendungsfälle für Dienstverbindungen oder ZTNA-Connector. Ein Häkchen gibt an, dass der Anwendungsfall unterstützt wird; ein Bindestrich (–) bedeutet, dass er nicht unterstützt wird.

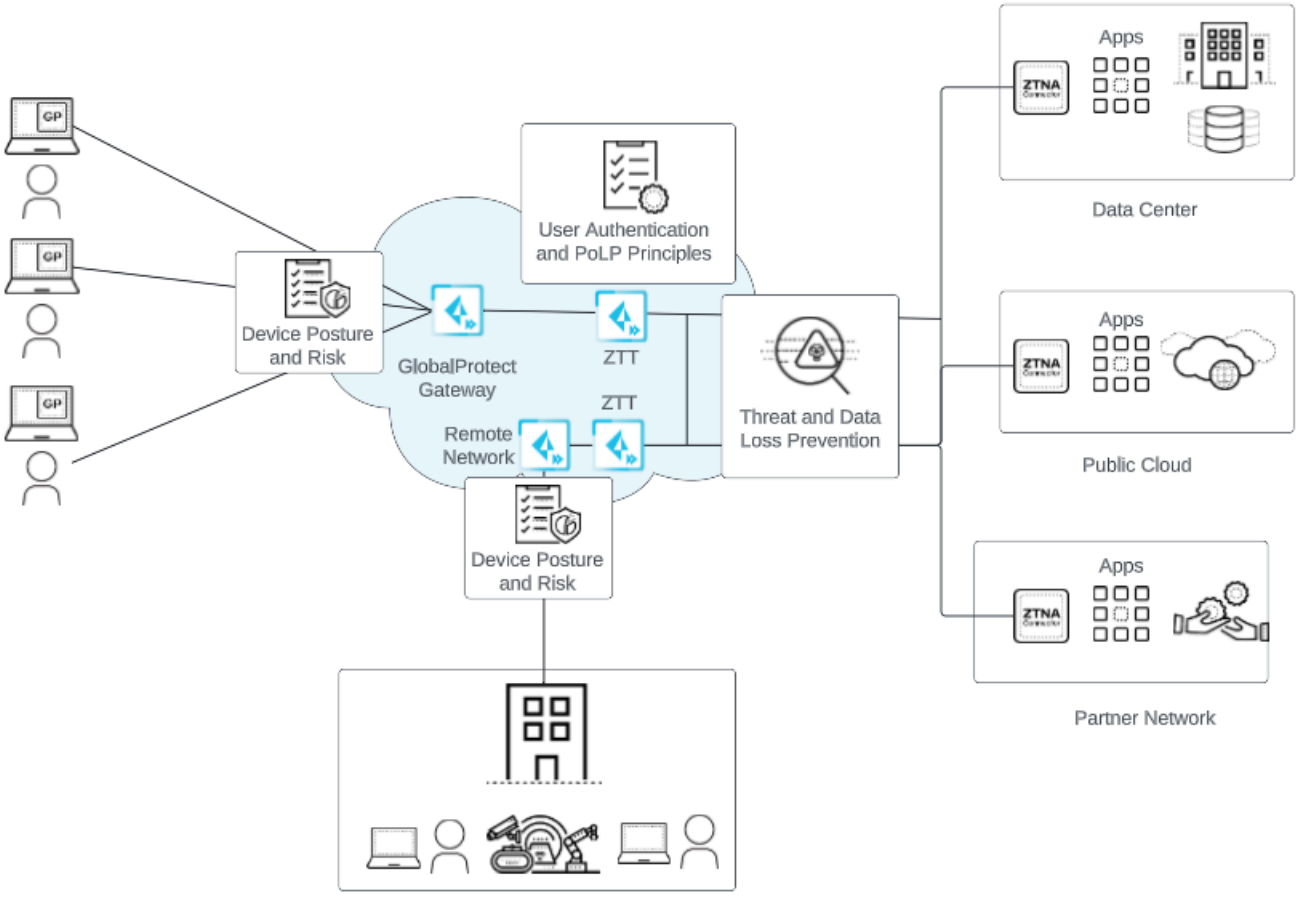
| Anwendungsfall | Unterstützung für ZTNA-Connector | Unterstützung für Dienstverbindung |
|---|---|---|
| Zugriff auf Anwendungen in überlappenden Netzwerken | √ | - |
| Zugriff auf alle Ports und Protokolle für vom Client initiierten Anwendungsverkehr | √ | √ |
| Automatische Tunneleinrichtung zu Prisma Access | √ | - |
| Automatische Prisma Access-Standortermittlung | √ | - |
| Automatische Skalierung von Prisma Access-Standorten für einen Durchsatz von bis zu 10 Gbit/s | √ | - |
| Zugriff auf private Apps mithilfe von IP-Adressen und Subnetzen | √ | √ |
| Vom Server initiierter Datenverkehr (z. B. ein Remote-Helpdesk), der eine Verbindung zu einem verwalteten Gerät (GlobalProtect für mobile Benutzer oder Remote-Netzwerk) herstellt. | - | √ |
| Anwendungen oder Dienste, die eine eindeutige Client-IP-Adresse benötigen | √ | √ |
| Zugriff auf Anwendungen mit dynamischen Ports (z. B. FTP Active-Modus oder VoIP) | - | √ |
| Hybridbereitstellungen mit lokalen Next-Generation Firewalls, bei denen auf der Benutzer-ID basierende Richtlinienregeln angewendet werden | √ | √ |


©2025 Palo Alto Networks, Inc.

# Prinzipien von ZTNA-Connector 2.0

Mit ZTNA-Connector können Sie Ihre privaten Apps mithilfe der folgenden ZTNA-Connector 2.0-Prinzipien mit Prisma Access verbinden:

- **Gerätestatus und Risiko** – Mithilfe von Richtlinienregeln, die auf der Benutzer-ID in Prisma Access basieren, können Sie einen Status für Benutzer und Geräte (sowohl mobile Benutzer als auch IoT-Geräte) definieren, um den unbefugten Zugriff auf die privaten Apps zu verhindern. Sie können auch gemeinsame Richtlinienregeln zwischen ZTNA-Connector und Prisma Access erstellen.
- **Benutzerauthentifizierung und Zugriff nach dem Least-Privilege-Prinzip** – Mithilfe von Benutzerauthentifizierungs- und Richtlinienregeln, die auf Benutzern oder Gruppen basieren, können Sie das Least-Privilege-Prinzip (PoLP) implementieren, um Benutzern Zugriff auf die Apps zu gewähren, die sie benötigen, während der Zugriff auf Apps, die sie nicht benötigen, blockiert wird.
- **Schutz vor Bedrohungen und Datenverlust** – Prisma Access und ZTNA-Connector verwenden erweiterte Sicherheitsfunktionen wie Advanced Threat Prevention, Advanced URL Filtering, SaaS Security, Advanced WildFire und Enterprise DLP, um sicherzustellen, dass Ihre privaten Apps und App-Daten sicher sind.




 ©2025 Palo Alto Networks, Inc.

# Anforderungen und Richtlinien für ZTNA-Connector

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access Version 4.0<br>❑ ZTNA-Connector-Add-on-Lizenz<br>Die Essential-Lizenz mit der Add-on-Lizenz umfasst acht ZTNA-Connectors, 100 FQDNs und vier IP-Subnetzfunktionen.<br>Die Advanced-Lizenz mit der Add-on-Lizenz umfasst 40 ZTNA-Connectors, 300 FQDNs und 1.024 IP-Subnetzfunktionen.<br>Die Premiumlizenz mit der Add-on-Lizenz umfasst 200 ZTNA-Connectors, 4.000 FQDNs und 1.024 IP-Subnetzfunktionen.<br>❑ Wenn Sie die ZTNA-Connector-Add-on-Lizenz nicht erwerben, beinhalten die Prisma Access-Lizenzen vier Konnektoren, 40 FQDNs und vier IP-Subnetze. Diese Funktionalität wird bereitgestellt, um ZTNA-Connectors in Ihrer Umgebung zu testen. |

Bevor Sie ZTNA-Connector konfigurieren, überprüfen Sie, ob Sie die Anforderungen und Beschränkungen des Konnektors sowie die Richtlinien verstanden haben, die Sie bei der Bereitstellung befolgen sollten.

## Unterstützte Versionen und Anforderungen von Prisma Access

- Prisma Access Version 4.0 mit einem kompatiblen SaaS-Agent.

  Aktualisieren Sie alle Prisma Access-Versionen vor 4.0, einschließlich aller Innovation-Versionen, mindestens auf Version 4.0.

  Für Prisma Access ist mindestens Version 5.0 erforderlich, wenn Sie FQDN-Platzhalter oder IP-Subnetze für den Zugriff auf Apps verwenden möchten. Zusätzlich ermöglicht Prisma Access Version 5.0 die Nutzung der Diagnosetools „Dump Overview“, „Packet Capture“ und „Tech Support“.
- Sie müssen für Ihre Konnektor-Versionen ein Upgrade auf mindestens 6-2-2-ztna-connector-b1 durchführen, um die Funktionalität von Version 5.0 nutzen zu können.

 ©2025 Palo Alto Networks, Inc.

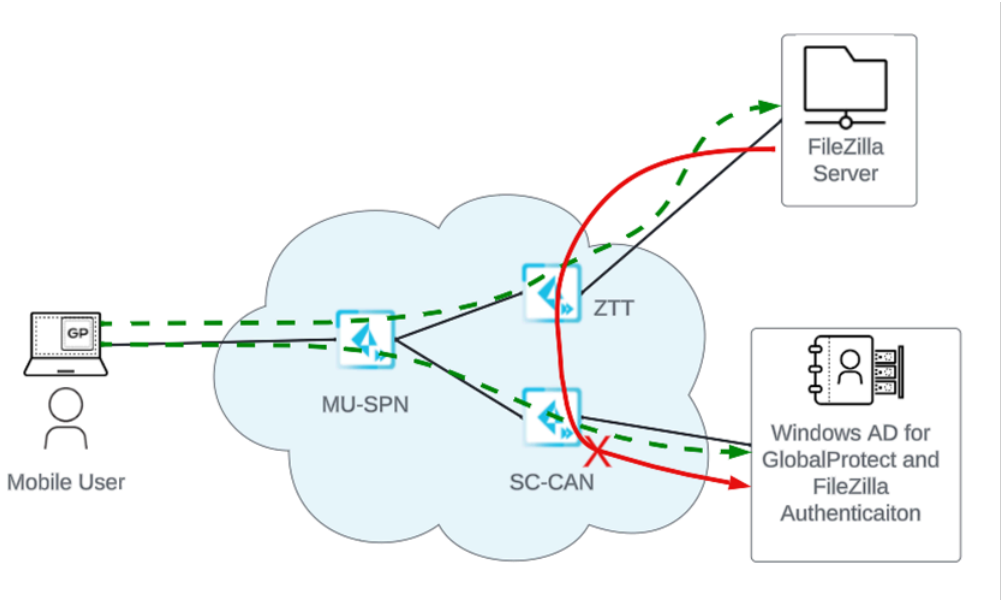
- Führen Sie für Prisma Access (Managed by Panorama) ein Upgrade des Cloud Services-Plug-ins auf mindestens Version 4.0 durch. Führen Sie ein Upgrade auf das neueste Cloud Services-Plug-in durch, um die neuesten Funktionen freizuschalten.

## App-Unterstützung

ZTNA-Connector bietet Zugriff auf Ihren gesamten privaten App-Datenverkehr. Dabei gelten jedoch die folgenden Ausnahmen:

- ZTNA-Connector bietet keine Unterstützung für:
  - Vom Rechenzentrum ausgehender Datenverkehr (z. B. SCCM- oder Remote-Helpdesk-Datenverkehr).
  - Weitergabe der Benutzer-ID.
  - Anwendungen, die Port-Hopping durchführen (z. B. VoIP oder Active Mode FTP).
  - ALG-Apps (Application-Level-Gateway) wie Active Mode FTP und SIP.
  - Die Windows-integrierte Authentifizierung für Anwendungen (wie etwa NTLM oder Kerberos) wird nur unterstützt, wenn Sie die Domänencontroller und Ressourcen des Rechenzentrums als IP-Adresssubnetze einbinden. SAML, OAuth und LDAP werden unterstützt.
  - Die Kommunikation zwischen Apps hinter einer Dienstverbindung und Apps hinter ZTNA-Connector.

    Beispielsweise hosten Sie einen Windows-AD-Server (Active Directory) hinter einer Dienstverbindung (da AD-Server hinter ZTNA-Connector nicht unterstützt werden) und einen FTP-Server (Filezilla) hinter ZTNA-Connector. Wenn der FTP-Server gegenüber dem Windows AD-Server authentifiziert werden muss, schlägt die Authentifizierung fehl, da Sie Prisma Access nicht als Backbone zwischen dem Service Connection Corporate Access Node (SC-CAN) und dem Tunnel Terminator von ZTNA-Connector (ZTT) verwenden können.




 ©2025 Palo Alto Networks, Inc.

# Einschränkungen bei Features und Funktionalität

Beachten Sie beim Einrichten und Konfigurieren einer ZTNA-Connector-Bereitstellung die folgenden Einschränkungen:

- Verwenden Sie keine Sonderzeichen wie z. B. < > ! @ # $ % ^ & und chinesische, japanische oder koreanische Zeichen in ZTNA-Objektnamen.
- Die folgenden Funktionen werden bei der Standardbereitstellung von Prisma Access nicht unterstützt. Wenden Sie sich an Ihr Palo Alto Networks-Team, um sie aktivieren zu lassen:
  - Verwenden Sie RFC 6598-Adressen für Ihre Prisma Access-Infrastruktur-IP-Adressen mit ZTNA-Connector
- **Richtlinien für Konnektorgruppen** – Beachten Sie beim Hinzufügen von Konnektorgruppen die folgenden Empfehlungen:
  - Alle Apps in einer einzelnen Konnektorgruppe sollten denselben DNS-Server für die DNS-Auflösung verwenden.
  - Wenn Sie auf Apps aus einem Rechenzentrum oder der Zentrale eines Standorts zugreifen, sollten alle Apps in der Konnektorgruppe aus demselben Rechenzentrum oder derselben Zentrale stammen.
  - Fügen Sie in einer einzigen Konnektorgruppe keine Konnektoren aus zwei oder mehr Regionen hinzu. Alle Konnektoren in einer Konnektorgruppe sollten sich in derselben Region befinden.
  - Ab Prisma Access Version 5.01 können Sie bis zu vier Konnektorgruppen pro FQDN-Ziel oder Platzhalterziel angeben (Version 5.0 und frühere Versionen unterstützen eine Konnektorgruppe pro FQDN-Ziel oder Platzhalterziel). Achten Sie beim Zuweisen von Konnektorgruppen auf Basis des FQDN-Ziels oder Platzhalterziels darauf, dass Sie derselben App nicht mehr als vier Konnektoren pro Region zuweisen.

    Sie haben beispielsweise dieselbe App (entweder ein FQDN-Ziel oder ein Platzhalterziel) vier Konnektorgruppen zugewiesen. Jede Gruppe verfügt über einen einzelnen Konnektor und alle Konnektoren befinden sich in derselben Region. Diese Konfiguration ist akzeptabel, da Sie in einer einzelnen Region nicht mehr als vier Konnektoren pro App zuweisen.

    Wenn Sie jedoch eine App (entweder ein FQDN-Ziel oder ein Platzhalterziel) drei Konnektorgruppen zuweisen, verfügt jede Gruppe über zwei Konnektoren und alle Konnektoren befinden sich in derselben Region. Dies ist eine ungültige Konfiguration, weil Sie einer bestimmten App in einer einzigen Region sechs Konnektoren zuweisen.
- Bestimmte ZTNA-Connectors wie etwa AWS-basierte Konnektoren oder Azure-basierte Konnektoren, unterstützen die Autoskalierung, wobei AWS oder Azure die Netzwerkbandbreitennutzung auf den Konnektoren überwacht und die Kapazität automatisch anpasst, um die App-Leistung aufrechtzuerhalten. Wenn die Netzwerkbandbreitennutzung an den Konnektoren sinkt, lösen AWS oder Azure ein automatisches Scale-in aus. Wenn in ZTNA-Connector ein Scale-in erfolgt, werden vorhandene Sitzungen mit langer Laufzeit, die vom für das Scale-in markierten ZTNA-Connector verwaltet werden, vorzeitig beendet. Dieses Verhalten hat keine Auswirkungen auf neue Datenverkehrssitzungen, die nach dem Scale-in initiiert werden. Bei Sitzungen mit langer Laufzeit wie beispielsweise SSH oder RDP beendet ZTNA-Connector die Sitzung während des Scale-ins, sodass Sie die Sitzung erneut verbinden müssen.

 ©2025 Palo Alto Networks, Inc.

# Überlegungen zu Skalierung und Durchsatz

ZTNA-Connector unterstützt die folgenden Maximalwerte:

- 4.096 Anwendungen pro Mandant über alle Konnektorgruppen hinweg
- 200 Konnektoren pro Mandant
- 512 Anwendungen pro Konnektorgruppe
- 4 Konnektoren pro Konnektorgruppe
- 200.000 gleichzeitige Sitzungen pro Konnektor

  *Jeder Konnektor kann 200.000 gleichzeitige Verbindungen unterstützen. Eine Konnektorgruppe kann maximal vier Konnektoren für bis zu 800.000 gleichzeitige Verbindungen pro Konnektorgruppe haben.*
- 26 Rechenregionen
- 1 Gbit/s Durchsatz pro Konnektor, mit maximal 10 Gbit/s pro Prisma Access-Compute-Standort

# Unterstützte Umgebungen für das Anwendungshosting

Sie können Ihre ZTNA-Connector-VMs in den folgenden Rechenzentrumsumgebungen mit den angegebenen Mindestanforderungen bereitstellen:

| Cloud-Anbieter | Instanzgröße | CPU-Größe | Größe des Arbeitsspeichers | Festplattengröße |
|---|---|---|---|---|
| Amazon AWS | m5.xlarge pro Region | 4 vCPUs | 16 GB | 40 GB |
| Google Cloud Platform (GCP) | n2-standard-4 pro Region | 4 vCPUs | 16 GB | 40 GB |
| Microsoft Azure | Standard_D4_v3 pro Region | 4 vCPUs | 16 GB | 40 GB |
| KVM | Verwendet qcow-Image | 4 vCPUs | 16 GB | 40 GB |
| Hyper-V | Verwendet VHD-Image | 4 vCPUs | 8 GB Arbeitsspeicher pro VM | 40 GB |
| VMware ESXi | Verwendet OVA-Image. Unterstützt auf vSphere und direkt auf ESXi-Hosts | 4 vCPUs pro VM | 8 GB Arbeitsspeicher pro VM | 40 GB Festplatte (Thick Provisioned) |

 ©2025 Palo Alto Networks, Inc.

| Cloud-Anbieter | Instanzgröße | CPU-Größe | Größe des Arbeitsspeichers | Festplattengröße |
|---|---|---|---|---|
| Für VMware ESXi werden vMotion, VM-Snapshots oder Migrationen für Konnektor-VMs nicht unterstützt.<br>Für KVM werden Livemigrationen und Snapshots auf Konnektor-VMs nicht unterstützt. | | | | |

*Es liegt in Ihrer Verantwortung, die VMs zu hosten und sicherzustellen, dass sie eine Verbindung zum Internet herstellen können.*

AWS, GCP und Azure verfügen über ZTNA-Connectors, die Sie in ihren jeweiligen Marketplaces erwerben können. Sie können die VMware ESXi-OVA-Datei (Open Virtualization Application) und die KVM-qcow-Datei vom Palo Alto-Kunden-Support-Portal herunterladen.

## Netzwerkanforderungen

Die folgenden Netzwerkanforderungen ermöglichen die Konnektivität zwischen ZTNA-Connector und Prisma Access:

- Nachdem Sie ZTNA-Connector aktiviert haben, Prisma Access erfolgt die Einrichtung eines DNS-Proxys für DNS-Anfragen mithilfe von DNS-Regeln, die für Remote-Netzwerke und GlobalProtect für mobile Benutzer eingerichtet wurden.
- Die UDP-Nutzlastgröße, einschließlich Header, sollte auf dem Pfad zum ZTNA-Anwendungsserver die MTU-Größe von 1.300 Byte nicht überschreiten. Palo Alto Networks empfiehlt, Pakete auf oder unter dieser MTU-Größe zu halten.
- Lassen Sie den ausgehenden UDP-Port 4500 und UDP 500 von der IP-Adresse der WAN-Schnittstelle (Port 1) für IPSec- und IKE-Konnektivität zum ZTNA Tunnel Terminator (ZTT) zu. Wenn Sie die Aktivierung einer ausgehenden UDP-Verbindung über die Ports 500 und 4500 auf eine einzelne IP-Adresse beschränken möchten, aktivieren Sie sie für die **PA-Dienst-IP**-Adresse (unter **Workflows** > **ZTNA-Connector** > **Konnektoren**) des ZTNA-Connectors.




- Wenn der ZTNA-Connector eine öffentliche IP-Adresse für seine Internetschnittstelle verwendet, müssen Sie eine IP/50 Encapsulating Security Payload (ESP) zulassen.
- Lassen Sie ausgehenden Datenverkehr vom TCP-Port 443 über die IP-Adresse der WAN-Schnittstelle (Port 1) mit HTTPS-Konnektivität zu den ZTNA-Connector-Controllern zu.
- Der ZTNA-Connector konfiguriert sowohl die Prisma Access-ZTT-Seite des IPSec-Tunnels als auch die ZTNA-Connector-Seite automatisch. Die für die DH-Gruppe/Verschlüsselung/Hash für IKE und ESP konfigurierten Algorithmen sind: ecp384/aes256/sha512.
- Beenden Sie den IPSec-Tunnel, den der ZTNA-Connector erstellt und für den Zugriff auf die privaten Apps verwendet, nicht.
- (Nur Bereitstellungen für GlobalProtect für mobile Benutzer) Wenn Sie eine Anwendung zum ersten Mal in ZTNA-Connector einbinden, müssen Sie die GlobalProtect-App aktualisieren, damit mobile Benutzer die aktualisierte DNS-Serverkonfiguration erhalten. Wenn Sie eine

 ©2025 Palo Alto Networks, Inc.

Anwendung aus ZTNA-Connector entfernt haben, müssen Sie die GlobalProtect-App aktualisieren, damit mobile Benutzer die aktualisierte DNS-Serverkonfiguration erhalten können.

- Wenn sich zwischen dem ZTNA-Connector und der privaten App eine Firewall befindet, muss die Firewall den Zugriff auf die App vom ZTNA-Connector aus zulassen (d. h., Sie müssen der privaten App den Zugriff auf die aufgelösten IP-Adressen, Protokolle und Ports des App-Servers erlauben).

  Darüber hinaus müssen Sie zulassen, dass das Protokoll (TCP oder ICMP), das Sie für das Anwendungsziel konfiguriert haben, eine Zustandsprüfung für die App durchführt. Die Konnektoranwendung prüft den App-Server, um zu ermitteln, ob dieser Zugriff auf die App gewähren kann. Sie können den Probentyp für das Anwendungsziel auf **tcp ping**, **icmp ping**oder **none** (keine Probe) setzen. Wenn Sie **tcp ping** angeben, muss die Firewall den TCP-Zugriff auf die App zulassen. Wenn Sie **icmp ping** angeben, muss die Firewall ICMP-Echoanfragen und -antworten für die App zulassen.
- Vergewissern Sie sich, dass Sie ICMP in Ihrem Rechenzentrum zugelassen haben, bevor Sie die Diagnosetools „Ping“ und „Traceroute“ verwenden. In bestimmten Cloud-Umgebungen ist ICMP aus Sicherheitsgründen nicht zulässig. In diesem Fall zeigen diese Tools keine Aktivität.

  Das Diagnosetool „Traceroute“ verwendet auch zufällige UDP-Ports. Sie müssen daher alle UDP- und ICMP-Fehlerantworten zulassen, damit das Tool „Traceroute“ funktioniert.
- Stellen Sie sicher, dass Sie DNS-Einträge auf den lokalen Schnittstellen konfiguriert haben, damit ZTNA-Connector die App-FQDNs auflösen kann, und dass ZTNA-Connector auf den DNS-Server über UDP-Port 53 (für die DNS-Auflösung verwendeter Port) zugreifen kann.
- (ZTNA-Connector Version 5.0 und höher) Stellen Sie sicher, dass Sie in Ihrem Netzwerk Sicherheitsregeln konfiguriert haben, die es ZTNA-Connectors erlauben, Anwendungstests in Ihrem Rechenzentrum durchzuführen. ZTNA-Connectors verwenden die Schnittstellen-IP-Adresse ihres Rechenzentrums als Quell-IP-Adresse der Anwendung, die die Anwendungsserver prüft. Wenn die Anwendungsprüfung erfolgreich verlaufen ist, lautet der Anwendungsstatus **Aktiv** und Benutzersitzungen zu ZTNA-Connector haben dieselbe Schnittstellen-IP-Adresse für das Rechenzentrum wie die Quell-IP-Adresse. Wenn die Anwendungsprüfung fehlgeschlagen ist, lautet der Anwendungsstatus **Inaktiv**. In diesem Fall können Sie die Diagnosetools „ping“ und „tcp ping“ verwenden, um die Verbindungen zur Anwendung zu testen.
- Wenn Sie in Ihrem Netzwerk gemeinsam genutzte RFC 6598-Adressen verwenden, müssen Sie IP-Adressblöcke angeben, die ZTNA-Connector für das Routing zwischen Prisma Access und Ihren Konnektoren und zwischen Prisma Access und Ihren privaten Apps verwenden kann.

 ©2025 Palo Alto Networks, Inc.

- Wenn Sie die Liste der IP-Adressen und FQDNs einschränken müssen, die Sie den Zulassungslisten Ihrer Organisation hinzufügen wollen, fügen Sie die in Zuzulassende IP-Adressen und FQDNs für ZTNA-Connector aufgelisteten hinzu.

  Wenn Sie beispielsweise einen ZTNA-Connector in den USA einrichten, fügen Sie die folgenden URLs zu den Zulassungslisten Ihrer Organisation hinzu:

  - https://controller.cgnx.net
  - https://locator.cgnx.net
  - https://controller.hood.cgnx.net
  - https://vmfg.hood.cgnx.net
  - https://sdwan-stats-hood-us.cgnx.net
  - time.nist.gov (für NTP)
  - 0.cloudgenix.pool.ntp.org (für NTP)
  - 1.cloudgenix.pool.ntp.org (für NTP)
  - 2.cloudgenix.pool.ntp.org (für NTP)
  - 3.cloudgenix.pool.ntp.org (für NTP)

  *Beschränken Sie die DNS-Auflösung der vorherigen FQDNs auf die IPv4-Auflösung. Der ZTNA-Connector unterstützt das Herstellen einer Verbindung zu den Controller-FQDNs über IPv6 nicht.*

- Deaktivieren Sie die SSL-Entschlüsselung für Sitzungen mit den Controllern.

## Zuzulassende IP-Adressen und FQDNs für ZTNA-Connector

Um eine reibungslose Funktion des ZTNA-Connectors sicherzustellen, fügen Sie Ihren Zulassungslisten die folgenden URLs und IP-Adressen hinzu.

| Name des Dienstes | Port | Richtung | Quellschnittstelle Internetprotokoll | Ziel- und IP-Adressen |
|---|---|---|---|---|
| ZTNA-Connector-Zugriff auf Prisma Access | 443 | Ausgehend | ZTNA-Connector-WAN-Port | https://controller.cgnx.net<br>Adresse: 52.8.93.87<br>Adresse: 52.8.25.40<br>https://locator.cgnx.net<br>Adresse: 13.56.217.238<br>Adresse: 13.56.201.169<br>hood:<br>52.40.98.31<br>34.218.98.185<br>sugarloaf:<br>18.200.102.82 |

 ©2025 Palo Alto Networks, Inc.

| Name des Dienstes | Port | Richtung | Quellschnittstelle Internetprotokoll | Ziel- und IP-Adressen |
|---|---|---|---|---|
| | | | | 18.200.135.33<br>faber:<br>18.139.242.53<br>54.255.61.109<br>https://vmfg.cgnx.net<br>Adresse: 52.53.122.104<br>Adresse: 52.53.102.7<br>https://controller.elcapitan.cgnx.net<br>Adresse: 52.8.93.87<br>Adresse: 52.8.25.40<br>https://vmfg.elcapitan.cgnx.net<br>Adresse: 52.53.122.104<br>Adresse: 52.53.102.7<br>https://controller.hood.cgnx.net<br>Adresse: 52.32.167.5<br>Adresse: 54.70.168.33<br>https://vmfg.hood.cgnx.net<br>Adresse: 50.112.136.184<br>Adresse: 34.210.34.87<br>https://controller.sugarloaf.cgnx.net<br>Adresse: 108.128.176.192<br>Adresse: 18.200.144.58<br>https://vmfg.sugarloaf.cgnx.net<br>Adresse 99.81.179.99<br>Adresse 99.80.52.255<br>https://sdwan-stats-hood-us.cgnx.net<br>https://sdwan-stats-elcapitan-us.cgnx.net<br>https://sdwan-stats-hood-jp.cgnx.net |


©2025 Palo Alto Networks, Inc.

| Name des Dienstes | Port | Richtung | Quellschnittstelle Internetprotokoll | Ziel- und IP-Adressen |
|---|---|---|---|---|
| | | | | https://sdwan-stats-elcapitan-jp.cgnx.net<br>https://sdwan-stats-hood-sg.cgnx.net<br>https://sdwan-stats-elcapitan-sg.cgnx.net<br>https://sdwan-stats-hood-au.cgnx.net<br>https://sdwan-stats-elcapitan-au.cgnx.net<br>https://sdwan-stats-hood-in.cgnx.net<br>https://sdwan-stats-elcapitan-in.cgnx.net<br>https://sdwan-stats-hood-ca.cgnx.net<br>https://sdwan-stats-elcapitan-ca.cgnx.net<br>https://sdwan-stats-sugarloaf-eu.cgnx.net<br>https://sdwan-stats-sugarloaf-de.cgnx.net<br>https://sdwan-stats-sugarloaf-uk.cgnx.net<br>https://controller.bowfell.cgnx.net<br>Adresse: 13.41.243.90<br>Adresse: 18.171.17.23<br>https://vmfg.bowfell.cgnx.net<br>Adresse: 52.56.35.36<br>Adresse: 52.56.224.242<br>https://controller.faber.cgnx.net<br>Adresse: 52.74.47.220<br>Adresse: 13.251.109.27<br>https://vmfg.faber.cgnx.net |

 ©2025 Palo Alto Networks, Inc.

| Name des Dienstes | Port | Richtung | Quellschnittstelle Internetprotokoll | Ziel- und IP-Adressen |
|---|---|---|---|---|
| | | | | Adresse: 18.142.153.59<br>Adresse: 52.74.58.219<br>http://controller.townsend.cgnx.net<br>Adresse: 13.55.31.41<br>Adresse: 3.106.168.215<br>https://vmfg.townsend.cgnx.net<br>Adresse: 52.64.177.240<br>Adresse: 13.55.164.51<br>https://sdwan-stats-faber-sg.cgnx.net<br>https://sdwan-stats-bowfell-uk.cgnx.net<br>https://sdwan-stats-townsend-au.cgnx.net |
| NTP | 123 | Ausgehend | ZTNA-Connector WAN- und LAN-Ports | time.nist.gov<br>0.cloudgenix.pool.ntp.org<br>1.cloudgenix.pool.ntp.org<br>2.cloudgenix.pool.ntp.org<br>3.cloudgenix.pool.ntp.org |
| DNS | 53 | Ausgehend | ZTNA-Connector WAN- und LAN-Ports | DNS-Server des Kunden oder Anbieters |

## Zertifikatverwaltung

Um das nötige Vertrauen zwischen Parteien in einer sicheren Kommunikationssitzung zu gewährleisten, verwendet Prisma Access digitale Zertifikate. Jedes Zertifikat enthält einen kryptografischen Schlüssel zum Verschlüsseln von Klartext bzw. Entschlüsseln von verschlüsseltem Text. Jedes Zertifikat enthält außerdem eine digitale Signatur zur Authentifizierung der Identität des Ausstellers. Der Aussteller muss in der Liste der vertrauenswürdigen Zertifizierungsstellen (CAs) der authentifizierenden Partei aufgeführt sein. Optional verifiziert die authentifizierende Partei, dass der Aussteller das Zertifikat nicht widerrufen hat. Prisma Access verwendet Zertifikate, um Funktionen wie Entschlüsselung und Authentifizierung zu sichern und die Kommunikation zwischen allen Clients, Servern, Benutzern und Geräten sicherzustellen, die eine Verbindung zu Ihrem Netzwerk herstellen.

 ©2025 Palo Alto Networks, Inc.

Richten Sie für Anwendungen, die in ZTNA-Connector eingebunden wurden, Ihre Zertifikate ein, fügen Sie Zertifizierungsstellen hinzu und definieren Sie Zertifikatsprüfungen mithilfe der Prisma Access-Zertifikatverwaltung.

 ©2025 Palo Alto Networks, Inc.

# ZTNA-Connector aktivieren

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access Version 4.0<br>❑ ZTNA-Connector-Add-on-Lizenz<br>Die Essential-Lizenz mit der Add-on-Lizenz umfasst acht ZTNA-Connectors, 100 FQDNs und vier IP-Subnetzfunktionen.<br>Die Advanced-Lizenz mit der Add-on-Lizenz umfasst 40 ZTNA-Connectors, 300 FQDNs und 1.024 IP-Subnetzfunktionen.<br>Die Premiumlizenz mit der Add-on-Lizenz umfasst 200 ZTNA-Connectors, 4.000 FQDNs und 1.024 IP-Subnetzfunktionen.<br>❑ Wenn Sie die ZTNA-Connector-Add-on-Lizenz nicht erwerben, beinhalten die Prisma Access-Lizenzen vier Konnektoren, 40 FQDNs und vier IP-Subnetze. Diese Funktionalität wird bereitgestellt, um ZTNA-Connectors in Ihrer Umgebung zu testen. |

Bevor Sie einen ZTNA-Connector einrichten können, müssen Sie ihn innerhalb von Prisma Access aktivieren. Bevor Sie ZTNA-Connector aktivieren, führen Sie Folgendes aus:

- Überprüfen Sie die Anforderungen und Richtlinien für ZTNA-Connector.
- Identifizieren Sie Ihre Anwendungs-IP- und Connector-IP-Adressblöcke. Sie müssen einen separaten Adresspool reservieren, der für die interne Nutzung innerhalb von Prisma Access reserviert werden kann, um den Datenverkehr zu den Konnektoren und privaten Anwendungen zu leiten, die Sie einbinden möchten. Prisma Access löst die FQDNs der Anwendungen, die Sie in ZTNA-Connector einbinden, in die IP-Adressen im Anwendungs-IP-Adressblock auf. Ebenso verwendet Prisma Access den Connector-IP-Adressblock, um den Datenverkehr vom Remote-Netzwerk oder von mobilen Benutzern zum entsprechenden ZTNA-Connector zu leiten.

  Sie sollten mindestens ein /16-Subnetz für den Adresspool reservieren. Verwenden Sie RFC 1918- oder RFC 6598-Adressen. Anstelle von RFC 6598 können Sie einen RFC 1918-Adresspool während der Einrichtung von ZTNA-Connector angeben. Sie können jedoch den Adresspooltyp nicht zurück in RFC 6598 ändern, nachdem Sie RFC 1918 angegeben haben.
- Strata Cloud Manager
- Panorama

 ©2025 Palo Alto Networks, Inc.

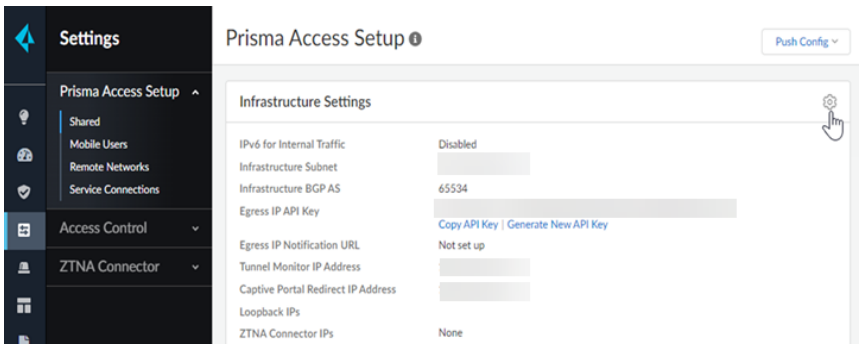
# ZTNA-Connector aktivieren (Strata Cloud Manager)

Verwenden Sie den folgenden Workflow, um einen ZTNA-Connector in Cloud-verwaltetem Prisma Access zu aktivieren.

**STEP 1 |** Konfigurieren Sie die IP-Adressblöcke, mit denen Prisma Access intern den Datenverkehr an den ZTNA-Connector und die privaten Apps weiterleitet, die Sie einbinden.

Sie müssen separate IP-Adressblöcke für Ihre Konnektoren und Ihre Anwendungen definieren und die Blöcke dürfen sich nicht untereinander, mit dem Subnetz der Prisma Access-Infrastruktur oder mit Ihrem GlobalProtect-IP-Adresspool überschneiden.

- Wählen Sie **Workflows** > **Prisma Access-Einrichtung** > **Prisma Access** > **Infrastruktureinstellungen** aus.




- Fügen Sie **Anwendungs-IP-Blöcke von ZTNA-Connector** hinzu.

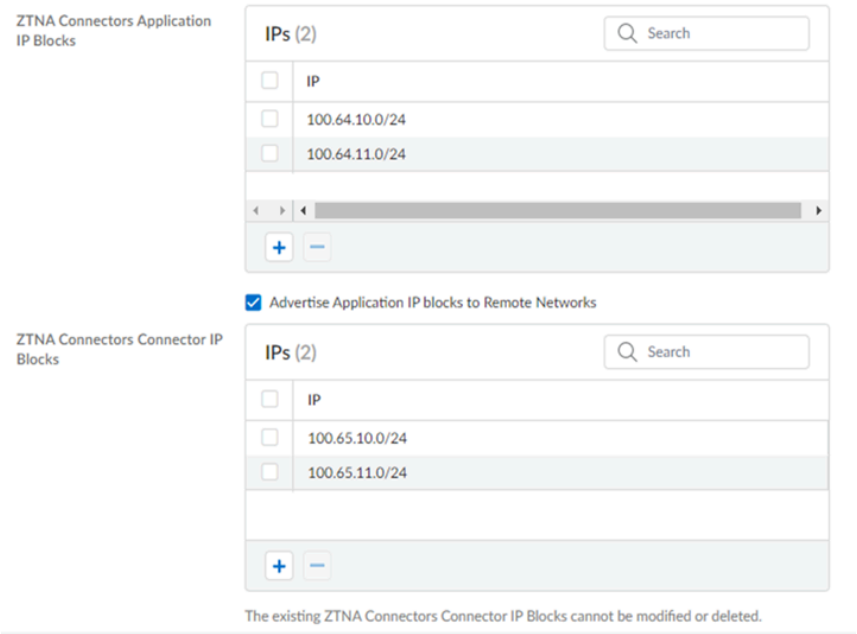
  Sie können je nach Bereitstellung einen einzelnen Anwendungs-IP-Block oder mehrere Blöcke hinzufügen. Geben Sie z. B. 100.64.10.0/24 und 100.64.11.0/24 ein. Sie

 ©2025 Palo Alto Networks, Inc.

können auch **Anwendungs-IP-Blöcke für Remote-Netzwerke ankündigen**, um Remote-Netzwerkzugriff bereitzustellen.

- Fügen Sie **Connector-IP-Blöcke von ZTNA-Connector** hinzu, mit denen Prisma Access intern den Datenverkehr zwischen mobilen Benutzern, Remote-Netzwerken und den Connector-VMs in Ihren Rechenzentren weiterleitet.

  Sie können je nach Bereitstellung einen einzelnen Connector-IP-Block oder mehrere Blöcke hinzufügen. Geben Sie z. B. 100.65.10.0/24 und 100.65.11.0/24 ein.

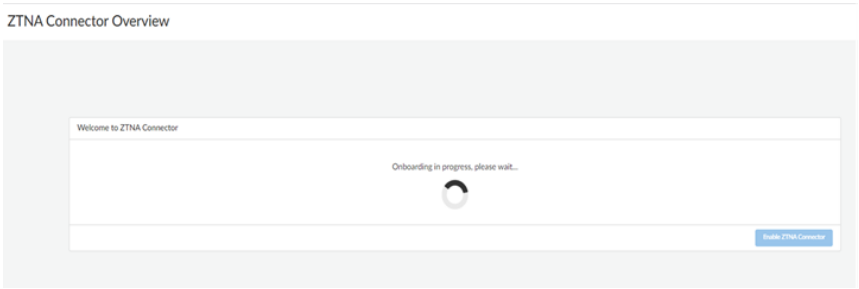



- Klicken Sie auf **Speichern**, um die Konfiguration des IP-Adressblocks zu speichern, und dann auf **Commit** und übertragen Sie die Konfiguration per Push.

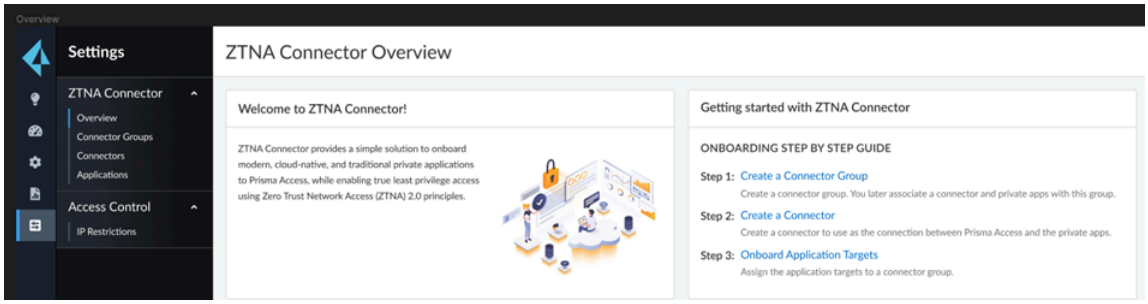
 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Starten Sie den ZTNA-Connector über Strata Cloud Manager.

- Wählen Sie **Workflows** > **ZTNA-Connector** aus.
- Prisma Access beginnt mit der Einrichtung der Infrastruktur für den ZTNA-Connector. Dies kann einige Minuten dauern.




- Wenn das Onboarding abgeschlossen ist, wird die Übersicht über ZTNA-Connector angezeigt.



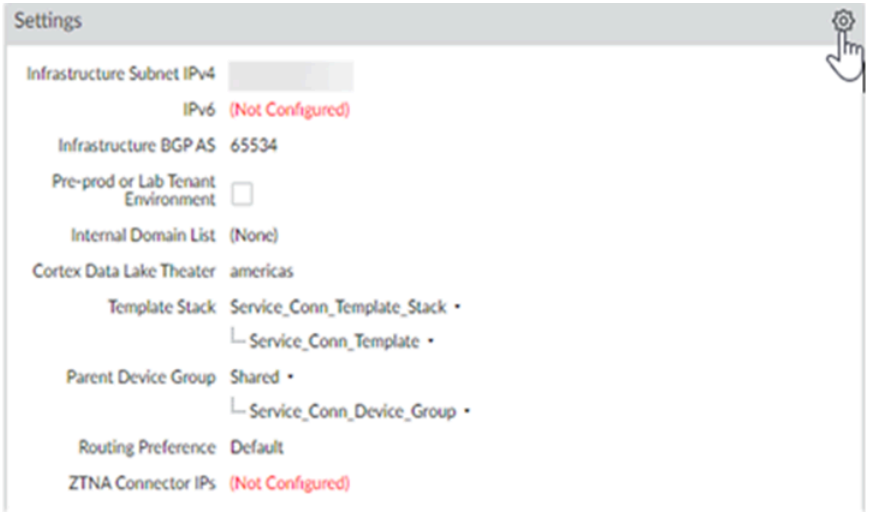

# ZTNA-Connector aktivieren (Panorama)

Verwenden Sie den folgenden Workflow, um einen ZTNA-Connector in Prisma Access (Managed by Panorama) zu aktivieren.

 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** Konfigurieren Sie die IP-Adressblöcke, mit denen Prisma Access intern den Datenverkehr an den ZTNA-Connector und die privaten Apps weiterleitet, die Sie einbinden.

- Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Diensteinrichtung** aus und **bearbeiten** Sie die **Einstellungen**.

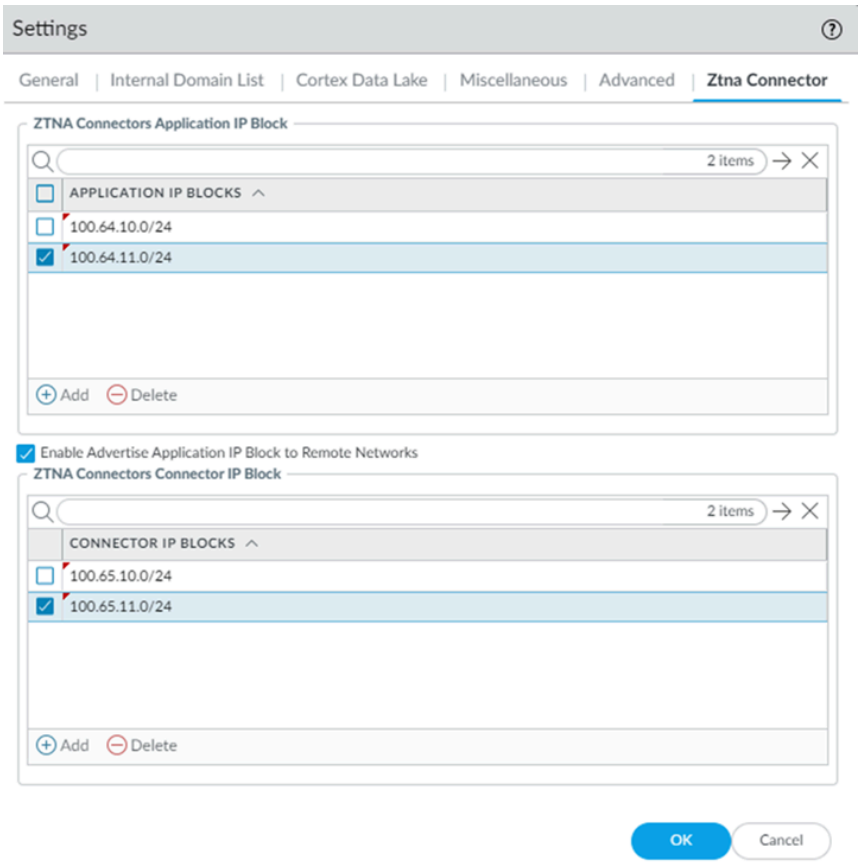



- **Fügen** Sie auf der Registerkarte **ZTNA-Connector** einen **Anwendungs-IP-Block** hinzu.

  Sie können je nach Bereitstellung einen einzelnen Anwendungs-IP-Block oder mehrere Blöcke hinzufügen. Geben Sie z. B. 100.64.10.0/24 und 100.64.11.0/24 ein. Sie können auch **Anwendungs-IP-Blöcke für Remote-Netzwerke ankündigen** aktivieren.
- Legen Sie die **Connector-IP-Blöcke** fest, mit denen Prisma Access den Datenverkehr zwischen mobilen Benutzern, Remote-Netzwerken und den Connector-VMs in Ihren Rechenzentren intern weiterleitet.

  Sie können je nach Bereitstellung einen einzelnen Connector-IP-Block oder mehrere Blöcke hinzufügen. Geben Sie z. B. 100.65.10.0/24 und 100.65.11.0/24 ein.

 ©2025 Palo Alto Networks, Inc.

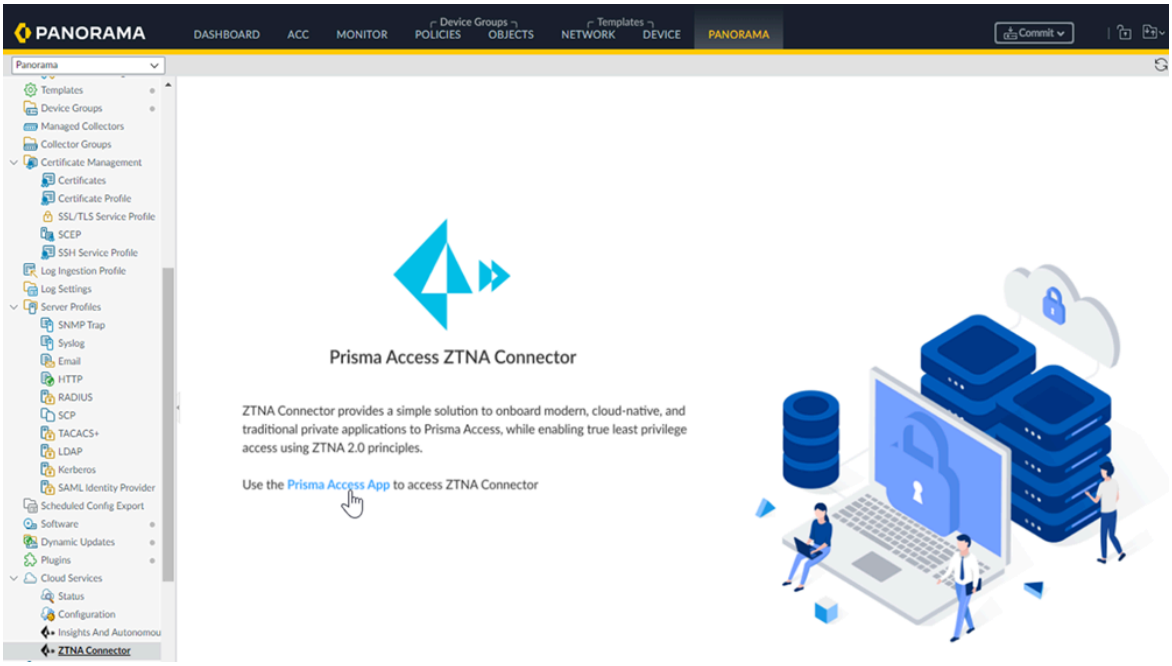



- Klicken Sie auf **OK**, um die Konfiguration des IP-Adressblocks zu speichern, und dann auf **Commit** und übertragen Sie die Konfiguration per Push.

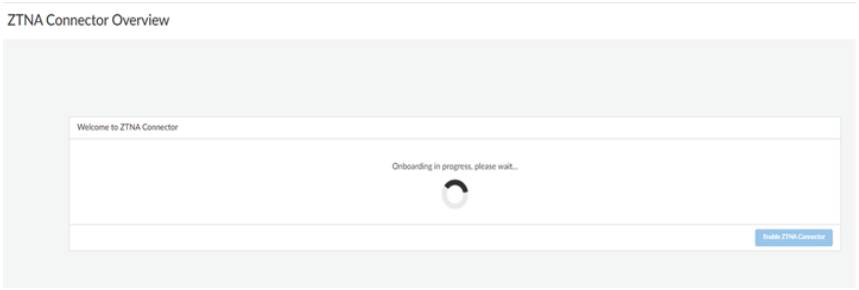
 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Starten Sie ZTNA-Connector über das Cloud Services-Plug-in auf Panorama.

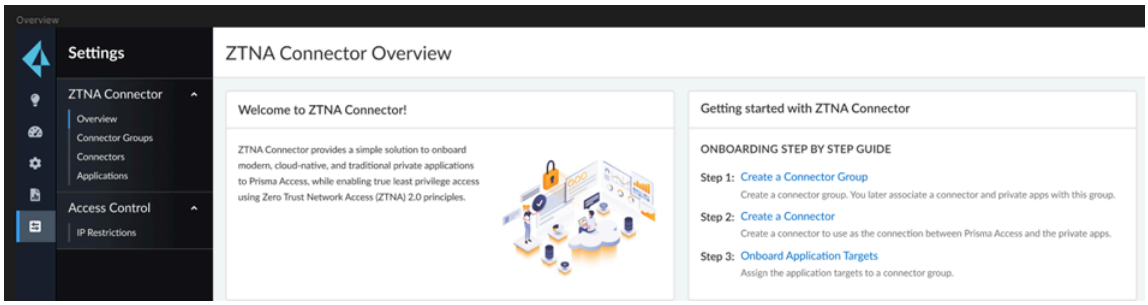
- Wählen Sie**Panorama** > **Cloud Services** > **ZTNA-Connector** aus.
- Klicken Sie auf Strata Cloud Manager, um ZTNA-Connector in Strata Cloud Manager auf dem Hub zu starten.




- Wählen Sie in Strata Cloud Manager **Einstellungen** > **ZTNA-Connector** aus.
- Prisma Access beginnt mit der Einrichtung der Infrastruktur für den ZTNA-Connector. Dies kann einige Minuten dauern.




- Wenn das Onboarding abgeschlossen ist, wird die Übersicht über ZTNA-Connector angezeigt.




 ©2025 Palo Alto Networks, Inc.

# ZTNA-Connector konfigurieren

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access Version 4.0<br>❑ ZTNA-Connector-Add-on-Lizenz<br>Die Essential-Lizenz mit der Add-on-Lizenz umfasst acht ZTNA-Connectors, 100 FQDNs und vier IP-Subnetzfunktionen.<br>Die Advanced-Lizenz mit der Add-on-Lizenz umfasst 40 ZTNA-Connectors, 300 FQDNs und 1.024 IP-Subnetzfunktionen.<br>Die Premiumlizenz mit der Add-on-Lizenz umfasst 200 ZTNA-Connectors, 4.000 FQDNs und 1.024 IP-Subnetzfunktionen.<br>❑ Wenn Sie die ZTNA-Connector-Add-on-Lizenz nicht erwerben, beinhalten die Prisma Access-Lizenzen vier Konnektoren, 40 FQDNs und vier IP-Subnetze. Diese Funktionalität wird bereitgestellt, um ZTNA-Connectors in Ihrer Umgebung zu testen. |

Nach dem ZTNA-Connector aktivieren können Sie mit der Einrichtung der ZTNA-Connector-Komponenten beginnen:

**STEP 1 |** Identifizieren Sie Ihre IP-Adressblöcke für Anwendungen und Konnektoren und fügen Sie die IP-Adressblöcke in Prisma Access hinzu.

*Beachten Sie die folgende Empfehlung für die IP-Adressblöcke:*

- *Vergeben Sie für jede Anwendung eine eigene IP-Adresse.*
- *Weisen Sie jedem Konnektor mindestens einen /27-IP-Adressblock (mindestens 32 IP-Adressen pro Konnektor) zu.*
- *Weisen Sie jeder Konnektorgruppe eine eindeutige IP-Adresse zu.*

*Sie können je nach Bedarf weitere Konnektoren oder Anwendungsblöcke hinzufügen.*

Wenn Sie in Ihrem Netzwerk RFC 6598-Adressen verwenden, müssen Sie einen separaten RFC 6598-IP-Adresspool reservieren, der intern in Prisma Access genutzt wird, um

 ©2025 Palo Alto Networks, Inc.

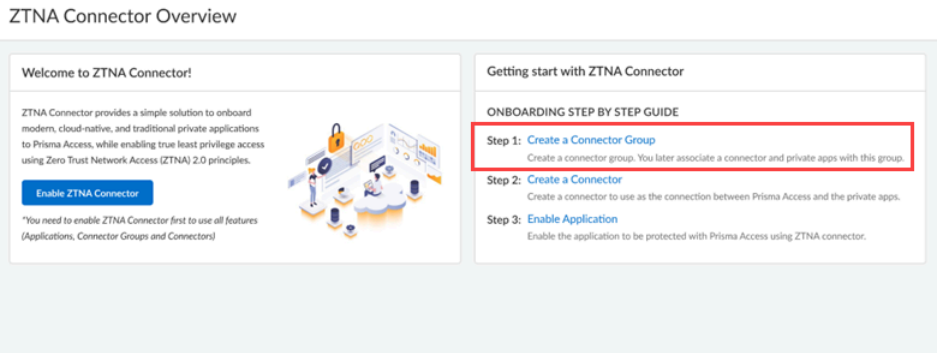
Datenverkehr an die Konnektoren und privaten Anwendungen weiterzuleiten, die Sie einbinden werden.

**STEP 2 |** Erstellen Sie eine Konnektorgruppe.

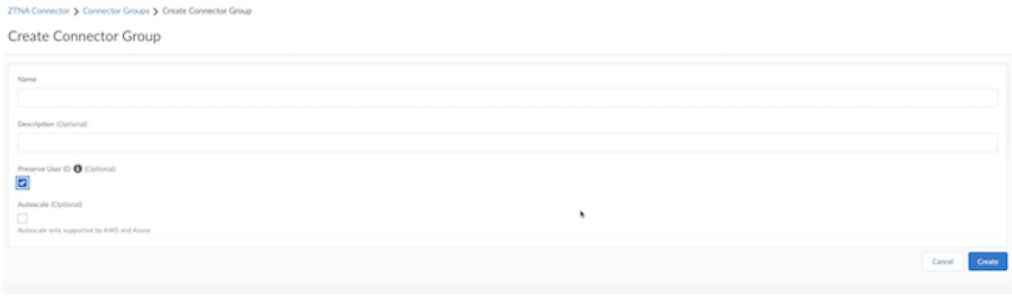
Konnektorgruppen sind logische Gruppierungen von Konnektoren und Anwendungen. Es gibt viele verschiedene Möglichkeiten, Anwendungen und Konnektoren zu gruppieren. Sie können Konnektoren zur Erreichung von Redundanz an verschiedenen geografischen Standorten gruppieren. Alternativ hierzu können Sie mehrere Konnektoren im selben Rechenzentrum erstellen, um den Durchsatz zu erhöhen. Zur Vereinfachung der Richtlinienverwaltung können Sie Anwendungen, die von denselben Benutzergruppen verwendet werden, zu Gruppen zusammenfassen. Erstellen Sie zunächst Ihre Konnektorgruppen und fügen Sie dann die Konnektoren und Anwendungen den Gruppen hinzu.

Wiederholen Sie diesen Schritt, um alle Konnektorgruppen zu erstellen, die Sie zum Gruppieren Ihrer Konnektoren und Anwendungen benötigen.

1. Wählen Sie**Workflows** > **ZTNA-Connector** und dann **Übersicht** oder **Konnektorgruppen** und **Konnektorgruppe erstellen** aus.




2. Ordnen Sie der Konnektorgruppe unter **Name** einen Namen zu, aktivieren Sie **Benutzer-ID beibehalten** und geben Sie optional eine **Beschreibung** an.




3. (Optional) Wenn sich Ihr Rechenzentrum in Azure oder AWS befindet und Sie die Funktionalität für die Autoskalierung verwenden möchten, wählen Sie **Autoskalierung** aus. Wenn Sie diese Funktionalität aktiviert haben, müssen Sie keinen Konnektor erstellen.
4. **Erstellen** Sie eine Konnektorgruppe.

 ©2025 Palo Alto Networks, Inc.

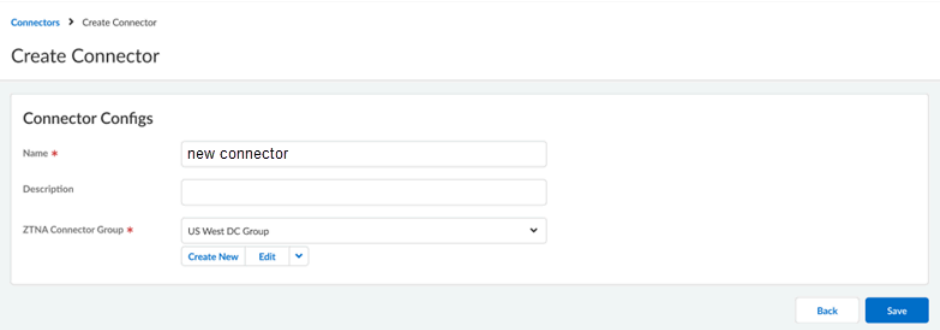
**STEP 3 |** *Erstellen Sie einen Konnektor und fügen Sie ihn einer Konnektorgruppe nur dann hinzu, wenn Sie eine nicht automatisch skalierbare Konnektorgruppe auswählen.*

Erstellen Sie Konnektoren und fügen Sie sie der Konnektorgruppe hinzu.

Konnektoren repräsentieren die in Ihren Rechenzentren ausgeführten VMs, die eine Verbindung zu Prisma Access herstellen. Sie müssen den Konnektor innerhalb von Prisma Access erstellen und den bereitgestellten geheimen Schlüssel/Schlüssel verwenden, um die entsprechende Konnektor-VM in Ihr Rechenzentrum einzubinden.

Wiederholen Sie diesen Schritt, um so viele Konnektoren zu erstellen, wie Sie benötigen, um die Apps für Ihr Rechenzentrum mit Prisma Access zu verbinden.

- Wählen Sie **Workflows** > **ZTNA-Connector** und dann **Übersicht** oder **Konnektoren** und **Konnektor erstellen** aus.
- Geben Sie unter **Name** einen Namen für den Konnektor ein.




- (Optional) Fügen Sie eine **Beschreibung** für den Konnektor hinzu.
- Wählen Sie die **Konnektorgruppe** aus, der Sie Ihren Konnektor hinzufügen möchten.

*Um das Routing zu vereinfachen und den schnellsten Zugriff auf die Server im Rechenzentrum zu gewährleisten, empfiehlt Palo Alto Networks, dass sich die Konnektoren und Server im selben Subnetz befinden.*

- **Erstellen** Sie den Konnektor.

*Um ZTNA-Connectors auf dem aktuellsten Stand zu halten, können Sie die Symbole ihrer Softwareversion in **ZTNA- Connector** > **Konnektorgruppen** aktualisieren, um den Status der Konnektoren anzuzeigen und zu sehen, ob ein Upgrade verfügbar ist.*

 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** Rufen Sie den Schlüssel und den geheimen Schlüssel ab, die Sie verwenden, um den Konnektor einzurichten.

Sie werden die Werte des Schlüssels und des geheimen Schlüssels verwenden, wenn Sie die VMs in einem späteren Schritt einrichten.

1. Autoskalierbare Konnektorgruppe – Führen Sie die im Folgenden aufgeführten Schritte aus:
   1. Rufen Sie **Workflows** > **ZTNA-Connector** > **Konnektorgruppen** auf.
   2. Wählen Sie im Bereich **Aktionen** Ihrer autoskalierbaren Konnektorgruppe die Option **Token kopieren** aus und kopieren Sie dann die Werte für **Schlüssel** und **Geheimer Schlüssel**.

      Sie verwenden den Schlüssel und den geheimen Schlüssel, um die Cloud-Instanz oder VM, die Sie mit dem Konnektor erstellen, einander zuzuweisen.
2. Nicht autoskalierbare Konnektorgruppe – Befolgen Sie die unten aufgeführten Schritte:
   - Wählen Sie **Workflows** > **ZTNA-Connector** > **Konnektoren** aus.
   - Wählen Sie den Konnektor aus, den Sie bereitstellen möchten.
   - Wählen Sie im Bereich **Aktionen** die Option **Token kopieren** aus und kopieren Sie dann die Werte für **Schlüssel** und **Geheimer Schlüssel**.

     Sie verwenden den Schlüssel und den geheimen Schlüssel, um die Cloud-Instanz oder VM, die Sie mit dem Konnektor erstellen, einander zuzuweisen.

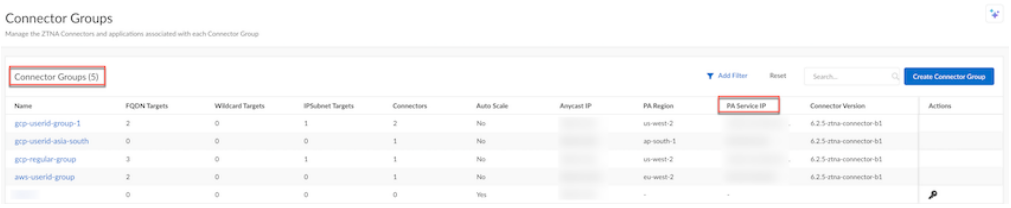



**STEP 5 |** Stellen Sie die VMs Ihres ZTNA-Connectors in Ihrem Rechenzentrum bereit.

**STEP 6 |** (Optional) Wählen Sie **Workflows** > **ZTNA-Connector** > **Konnektorgruppen** aus, notieren Sie sich die **PA-Dienst-IP**-Adresse der Konnektorgruppe und fügen Sie diese IP-Adresse den Zulassungslisten Ihrer Organisation hinzu.

*Die **PA-Dienst-IP** wird unter **Konnektorgruppen** erst angezeigt, nachdem Sie Ihren Konnektor eingebunden haben.*

Fügen Sie bei Bedarf diese IP-Adresse zu Ihren Zulassungslisten hinzu, damit Ihr Netzwerk den ZTNA-Connector-Datenverkehr übertragen und empfangen kann.




 ©2025 Palo Alto Networks, Inc.

**STEP 7 |** Fügen Sie die Ziele zu den Konnektorgruppen hinzu.

Richten Sie Ziele für den Zugriff auf die privaten Apps in den Rechenzentren über Ihre ZTNA-Connector-VMs ein. Sie können Ziele auf Basis von FQDN-Platzhaltern, FQDNs oder IP-Subnetzen hinzufügen; ZTNA-Connector übernimmt die Einrichtung der Netzwerk- und DNS-Einstellungen, die für Ihre mobilen Benutzer und die Benutzer in Zweigstellen erforderlich sind, um die Apps über Prisma Access sicher erreichen zu können.

1. Wählen Sie **Workflows** > **ZTNA-Connector** > **Anwendungsziele** aus.
2. Wählen Sie den Typ des Ziels aus, das Sie erstellen möchten.

   *Mit der Erweiterung für ein App-Onboarding ohne Commit dauert das Onboarding von Anwendungen jetzt weniger als eine Minute und ermöglicht so einen schnellen Zugriff auf die Anwendungen. Mit dieser Funktion können Sie auch eine größere Anzahl von Anwendungen einbinden.*

   ***Einschränkungen:***

   - *Sie können nicht denselben FQDN in mehreren Anwendungszielen (mit unterschiedlichem Port/Protokoll) hinzufügen.*
   - *Wenn Sie ein Platzhalterziel hinzufügen oder löschen, wird die Aktion „Commit“ auf MU oder RN ausgeführt, um DNS-Proxy-Weiterleitungsregeln hinzuzufügen oder zu löschen. Die anschließende platzhalterbasierte Anwendungserkennung von FQDNs, die mit dem Platzhalter übereinstimmen, erfordert jedoch keine zusätzlichen Commits, wodurch Sie Apps schnell einbinden und sofort auf sie zugreifen können.*

   *Um die Funktion für ein App-Onboarding ohne Commit zu aktivieren, müssen Sie das Prisma Access Dataplane auf Version 11.2.3 oder höher aktualisieren.*

- **Platzhalterziele** – Verwenden Sie einen Platzhalter (z. B. *.example.com) für das Ziel. Wenn Benutzer auf Standorte zugreifen, die mit dem Platzhalter übereinstimmen, werden diese Apps automatisch für den Zugriff über ZTNA-Connector für Ihre mobilen Benutzer und Remote-Netzwerkbenutzer eingebunden. Wenn Sie beispielsweise den Platzhalter *.example.com angeben und Benutzer auf die App unter app1.example.com zugreifen, erstellt ZTNA-Connector automatisch die Konfiguration, um diese untergeordnete App mit ihrem spezifischen FQDN, Protokoll und Port einzubinden.

  Wenn Benutzer mit einem Platzhalter auf eine App zugreifen (z. B. auf app1.example.com basierend auf dem Platzhalter *.example.com), wird die App erkannt und automatisch als **FQDN-Ziel** eingebunden.

  1. Rufen Sie **Platzhalterziele** und **Platzhalterziel erstellen** auf.
  2. Geben Sie unter **Name** einen eindeutigen Namen für das Ziel ein.
  3. Geben Sie die **Konnektorgruppe** ein, die dem Ziel zugeordnet werden soll.

     Die Gruppe muss dem Typ **FQDN/Platzhalter** entsprechen.

     Ab Prisma Access Version 5.0.1 können Sie mehrere Konnektorgruppen für Platzhalterziele und auch für FQDN-Ziele auswählen. Maximal können bis zu vier

 ©2025 Palo Alto Networks, Inc.

Konnektorgruppen pro Platzhalterziel oder FQDN-Ziel festgelegt werden. Verwenden Sie die Richtlinien, wenn Sie mehrere Konnektorgruppen pro Ziel auswählen.

4. Geben Sie den **Platzhalter** für das Ziel ein.

   Verwenden Sie bei der Eingabe das Format .example.com oder .my.example.com (die Benutzeroberfläche fügt implizit das Sternchen am Beginn des Platzhalters hinzu). Lassen Sie nicht alle Standorte zu, indem Sie den Platzhalter *.* angeben, beispielsweise example.*.com oder *.com.
5. Wählen Sie das **Protokoll** (**tcp**, **udp** oder beides) aus.
6. (Optional) Um das ICMP-Protokoll eines GlobalProtect-Benutzers für ein ZTNA-Connector-Rechenzentrum zu aktivieren, wählen Sie **ICMP-Protokoll zulassen** aus.
7. Wählen Sie den für die App zu verwendenden **Port** aus.

   Geben Sie einen einzelnen Port, mehrere Ports mit Kommas zwischen den Ports, einen Portbereich mit Bindestrichen oder eine Kombination dieser Optionen ein. Fügen Sie keine Leerzeichen nach den Kommas hinzu. Wählen Sie für den Port die Einstellung **Beliebig** aus, um mit allen von Ihnen angegebenen Ports übereinzustimmen, oder wählen Sie **Abgleichen** aus und geben Sie den Port oder die Ports ein, die abgeglichen werden sollen.

   Wenn Sie **beides** unter **Protokoll** ausgewählt haben, müssen Sie die Ports unter **TCP-Port** und **UDP-Port** hinzufügen.

   Wenn Sie im Feld **TCP-Port** unter **Erweiterte Einstellungen ICMP Ping** und **keiner** eingeben, wird **Probentyp** aktiviert.
8. Geben Sie abhängig vom ausgewählten Protokoll den **Probentyp TCP Ping**, **ICMP Ping** oder **keiner** ein.

   Wenn Sie **TCP Ping** auswählen, müssen Sie einen **Proben-Port** auswählen und einen einzelnen Port eingeben. Der Port muss nicht in dem Portbereich liegen, den Sie im Bereich **Port** und **Protokoll** eingegeben haben. Der ZTNA-Connector bestimmt die Erreichbarkeit der App, indem er einen TCP Ping vom Proben-Port zur aufgelösten IP-Adresse des FQDN durchführt. Wenn der Ping erfolgreich ist, wird die App als **Aktiv** eingestuft.

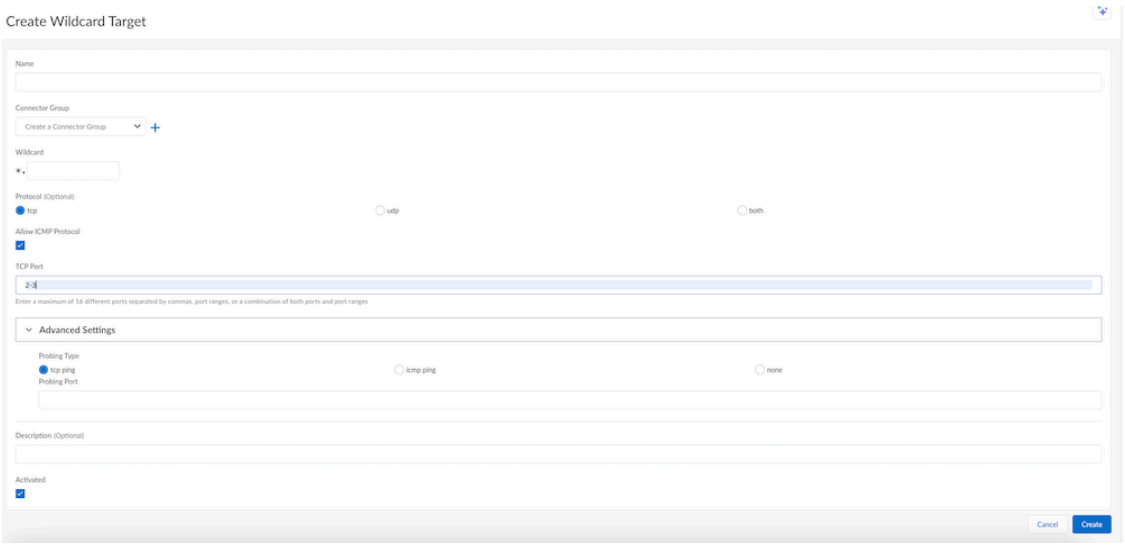
   Sie können den Proben-Port, den Sie während des Onboardings der Anwendung hinzugefügt haben, auch bearbeiten. Wenn der Proben-Port aktualisiert wird, startet ZTNA-Connector die TCP-Probenanwendung auf dem aktualisierten Port und der Anwendungsstatus wird entsprechend aktualisiert.

   Wenn Sie **ICMP Ping** auswählen, führt der ZTNA-Connector einen ICMP Ping an die aufgelöste IP-Adresse des FQDN aus. Wenn eine Antwort auf den ICMP Ping eingeht, wird die App als **Aktiv** eingestuft.

   Wenn Sie **keine** auswählen, wird keine Probe durchgeführt und die Anwendung wird immer als **Aktiv** markiert.

 ©2025 Palo Alto Networks, Inc.

9. Wählen Sie **Aktiviert** aus und **Erstellen** Sie das Ziel.




- **FQDN-Ziele** – Um ein Ziel für einen einzelnen FQDN zu erstellen, müssen Sie ein FQDN-Ziel erstellen.

  *Ab Prisma Access Version 5.0 führt der ZTNA-Connector für Konnektorgruppen mit Version 5.0 oder höher eine Anwendungsprobe durch, wenn ein Anwendungs-FQDN in mehrere private IP-Adressen aufgelöst wird. Auf diese Weise kann der Status aller aufgelösten IP-Adressen festgestellt und die Last beim FQDN-Zugriff auf mehrere aufgelöste IP-Adressen, die den Anwendungsstatus „Aktiv“ aufweisen, ausgeglichen werden.*

  Um ein FQDN-Ziel zu erstellen, rufen Sie **FQDN-Ziele** auf und **erstellen Sie das FQDN-Ziel**. Sie erstellen ein FQDN-Ziel genauso wie einen FQDN-Platzhalter und ersetzen den FQDN-Platzhalter durch einen einzelnen FQDN.

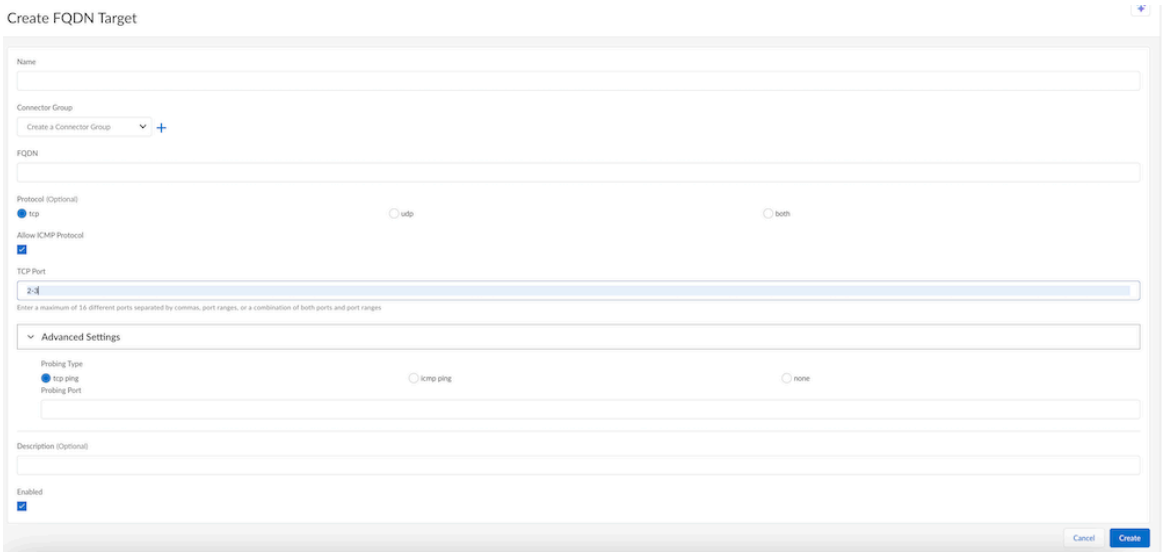
  Ab Prisma Access Version 5.0.1 können Sie mehrere Konnektorgruppen pro FQDN-Ziel sowie Platzhalterziele auswählen. Maximal können bis zu vier Konnektorgruppen pro FQDN-Ziel oder Platzhalterziele festgelegt werden. Verwenden Sie die Richtlinien, wenn Sie mehrere Konnektorgruppen pro Ziel konfigurieren möchten.

  Hier werden auch Anwendungen angezeigt, die anhand eines Platzhalterziels erkannt wurden. Wenn Benutzer auf Standorte zugreifen, die mit dem Platzhalter übereinstimmen, werden diese Apps automatisch für den Zugriff über ZTNA-Connector für Ihre mobilen Benutzer und Remote-Netzwerkbenutzer eingebunden. Wenn Benutzer beispielsweise durch Angabe des Platzhalters *.example.com auf die App unter app1.example.com zugreifen, fügt ZTNA-Connector diese App automatisch der Liste der FQDN-Ziele hinzu.

  Nachdem eine FQDN-Anwendung über ein übergeordnetes Platzhalterziel erkannt wurde, werden alle Änderungen am Platzhalterziel in der erkannten Anwendung nicht aktualisiert. Darüber hinaus wird für einen bereits erkannten FQDN keine erneute Erkennung durchgeführt. Wenn die Eigenschaften für die erkannte FQDN-Anwendung aktualisiert

 ©2025 Palo Alto Networks, Inc.

werden müssen, führen Sie eine manuelle Aktualisierung der erkannten Anwendung mit diesen Schritten durch.




- **IP-Subnetz** – Erstellen Sie ein Ziel auf Basis eines IP-Subnetzes, um Apps anhand von IP-Subnetzen anstelle von FQDNs zu suchen.

  1. Rufen Sie **IP-Subnetze** und dann **Subnetzregel erstellen** auf.
  2. Geben Sie unter **Name** einen eindeutigen Namen für das Ziel ein.
  3. Geben Sie die **Konnektorgruppe** ein, die dem Ziel zugeordnet werden soll.

     Die Gruppe muss den Typ **IP-Subnetz** aufweisen.
  4. Geben Sie die **IP-Subnetze** des Rechenzentrums an, auf die der Konnektor in der Gruppe den IP-Routingzugriff ermöglicht.

     Alle Konnektoren der Gruppe bieten Routingzugriff auf die angegebenen IP-Subnetze. Sie können eine einzelne IP-Adresse im Format 10.1.1.1/32, ein einzelnes Subnetz oder mehrere durch Kommas getrennte Subnetze auswählen. Geben Sie maximal 16 Subnetze ein.

     Das IP-Subnetz muss innerhalb der IP-Fabric des Mandanten geroutet werden können und die IP-Subnetze dürfen sich im Mandanten nicht mit anderen IP-Subnetzen überlappen. Hierzu gehören:

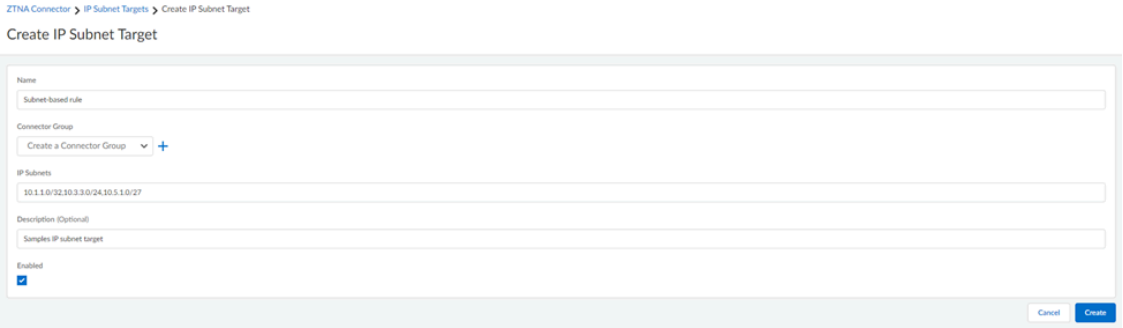
     - Andere routingfähige IP-Subnetze (einschließlich der IP-Subnetze mit vom Benutzer in Panorama konfigurierten statischen Routen), IP-Subnetze mit Routen, die von der

 ©2025 Palo Alto Networks, Inc.

Zweigstelle ans Remote-Netzwerk mitgeteilt werden, oder deren Routen, die vom Rechenzentrum zur Dienstverbindung mitgeteilt werden.

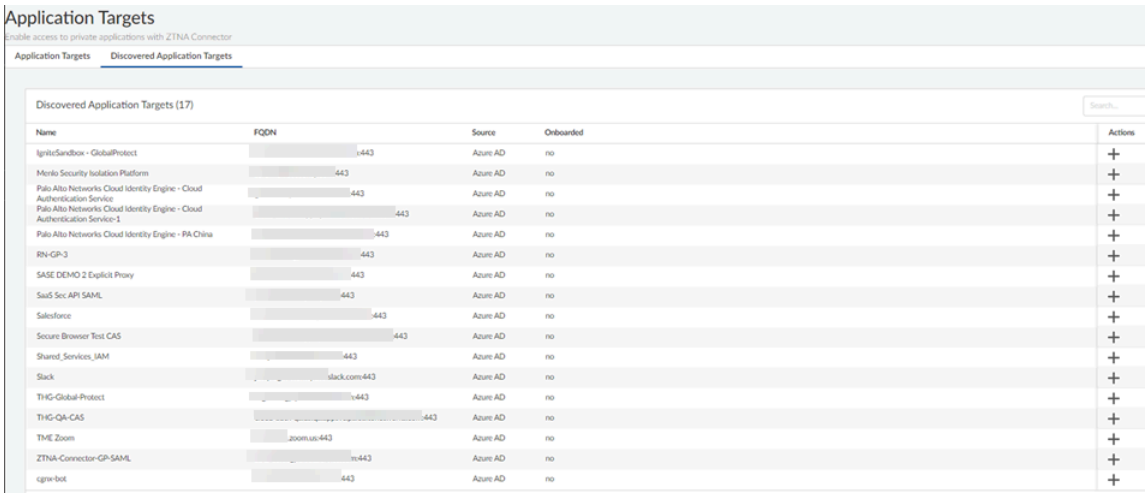
- ZTNA-FQDN-Anwendungs-IP-Subnetze
- ZTNA-Connector-IP-Subnetze
- IP-Adressen für Infrastruktursubnetze
- GlobalProtect-IP-Adresspools für mobile Benutzer

5. Wählen Sie **Aktiviert** aus und **erstellen** Sie das Ziel.




**STEP 8 |** Fügen Sie die Anwendungen, die von ZTNA-Connector automatisch erkannt werden, zur Konnektorgruppe hinzu.

1. Automatische Erkennung von Anwendungen mit Cloud Identity Engine einrichten
2. Wählen Sie **Workflows** > **ZTNA-Connector** > **Anwendungsziele** > **Erkannte Anwendungsziele** aus.




3. Klicken Sie unter **Aktionen** auf das Pluszeichen (+), um die Anwendung einer Konnektorgruppe hinzuzufügen.
4. Ordnen Sie der Anwendung unter **Name** einen eindeutigen Namen zu.
5. Wählen Sie die **ZTNA-Konnektorgruppe** aus, die der App zugeordnet werden soll.
6. Geben Sie den **Probentyp** ein (**TCP Ping**, **ICMP Ping** oder **keiner**).
   - Wenn Sie **TCP Ping** auswählen, wählen Sie auch einen **Proben-Port** aus. Der Port muss nicht in dem Portbereich liegen, den Sie im Bereich **Port** und **Protokoll**

 ©2025 Palo Alto Networks, Inc.

eingegeben haben. Wenn Sie als Probentyp **TCP Ping** auswählen, empfiehlt Palo Alto Networks, diesen Port auch als **Proben-Port** zu verwenden.

ZTNA-Connector ermittelt die Erreichbarkeit der App, indem es ein TCP-Ping-Signal vom Proben-Port zur aufgelösten IP-Adresse des FQDN absetzt. Wenn der Ping erfolgreich war, wird die App als **Aktiv** eingestuft.

- Sie können den Proben-Port, den Sie beim Onboarding der Anwendung hinzugefügt haben, auch bearbeiten. Wenn der Proben-Port aktualisiert wird, startet ZTNA-Connector die TCP-Probenanwendung auf dem aktualisierten Port und der Anwendungsstatus wird entsprechend aktualisiert.
- Wenn Sie **ICMP Ping** auswählen, führt ZTNA-Connector einen ICMP Ping zum FQDN aus. Wenn eine Antwort auf den ICMP Ping empfangen wird, setzt ZTNA-Connector den Status der Anwendung auf **Aktiv**.
- Wenn Sie **keine** auswählen, wird keine Probe durchgeführt und die Anwendung wird immer als **Aktiv** markiert.

7. Wählen Sie **Aktiviert** aus.
8. **Erstellen** Sie das Anwendungsziel.

**STEP 9 |** Erstellen Sie Sicherheitsrichtlinienregeln, um Benutzern den Zugriff auf die Apps in den Konnektoren zu ermöglichen.

**STEP 10 |** (Optional) Sie können ZTNA-Connectors anzeigen und überwachen, um festzustellen, welche Leistung Ihre ZTNA-Connectors und Konnektorgruppen erbringen.

**STEP 11 |** (Optional) Wenn beim Zugriff auf private Apps mit ZTNA-Connector Probleme auftreten, überprüfen Sie die App-Erreichbarkeit mithilfe der Diagnosetools Ping, Traceroute und Nslookup.

## Upgrade von ZTNA-Connectors

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access Version 4.0<br>❑ ZTNA-Connector-Add-on-Lizenz<br>Die Essential-Lizenz mit der Add-on-Lizenz umfasst acht ZTNA-Connectors, 100 FQDNs und vier IP-Subnetzfunktionen.<br>Die Advanced-Lizenz mit der Add-on-Lizenz umfasst 40 ZTNA-Connectors, 300 FQDNs und 1.024 IP-Subnetzfunktionen.<br>Die Premiumlizenz mit der Add-on-Lizenz umfasst 200 ZTNA-Connectors, 4.000 FQDNs und 1.024 IP-Subnetzfunktionen. |

 ©2025 Palo Alto Networks, Inc.

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| | ❑ Wenn Sie die ZTNA-Connector-Add-on-Lizenz nicht erwerben, beinhalten die Prisma Access-Lizenzen vier Konnektoren, 40 FQDNs und vier IP-Subnetze. Diese Funktionalität wird bereitgestellt, um ZTNA-Connectors in Ihrer Umgebung zu testen. |

Um die ZTNA-Connectors auf dem neuesten Stand zu halten, können Sie deren Softwareversion aktualisieren. Möglicherweise müssen Sie auch Ihre Konnektoren aktualisieren, um ein neues Feature oder eine neue Funktionalität zu unterstützen.

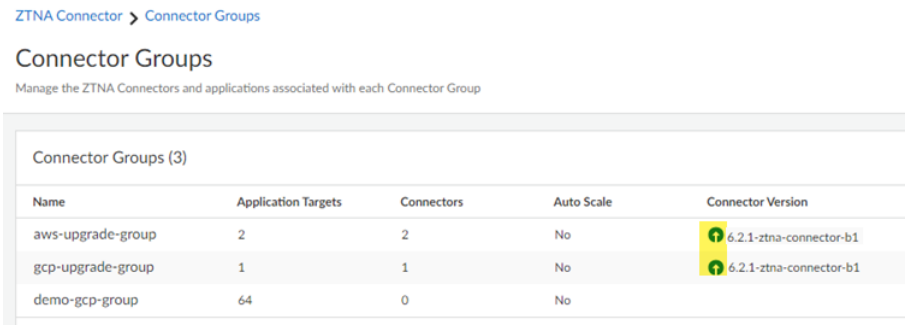
Wenn eine neue ZTNA-Connector-Version veröffentlicht wird, werden die Konnektoren in Ihrer Bereitstellung überprüft. Ist die veröffentlichte Version neuer als die vorhandene Version oder haben nicht alle Konnektoren in der Gruppe dieselbe Version, zeigen Symbole im Bereich „Konnektorgruppe“ an, dass ein Update verfügbar ist. Wenn Sie sich für ein Upgrade der Konnektoren entscheiden, haben Sie die Möglichkeit, die gesamte Gruppe zusammen zu aktualisieren. Beim Upgrade einer Gruppe werden automatisch alle Konnektoren in dieser Gruppe parallel aktualisiert. Für einzelne Konnektoren kann kein Upgrade durchgeführt werden.

*Das Upgrade eines ZTNA-Connectors dauert etwa 8 bis 10 Minuten. Während dieses Vorgangs wird der Konnektor neu gestartet. Palo Alto Networks empfiehlt, dass Sie ein Konnektor-Upgrade während einer Ausfallzeit oder eines geplanten Netzwerkausfalls planen.*

**STEP 1 |** Gehen Sie zu **ZTNA-Connector** > **Konnektorgruppen**. Grüne Pfeile zeigen an, dass ein Upgrade verfügbar ist.

Sie können nur ein Upgrade auf die neueste Imageversion durchführen, die für den Mandanten verfügbar ist.

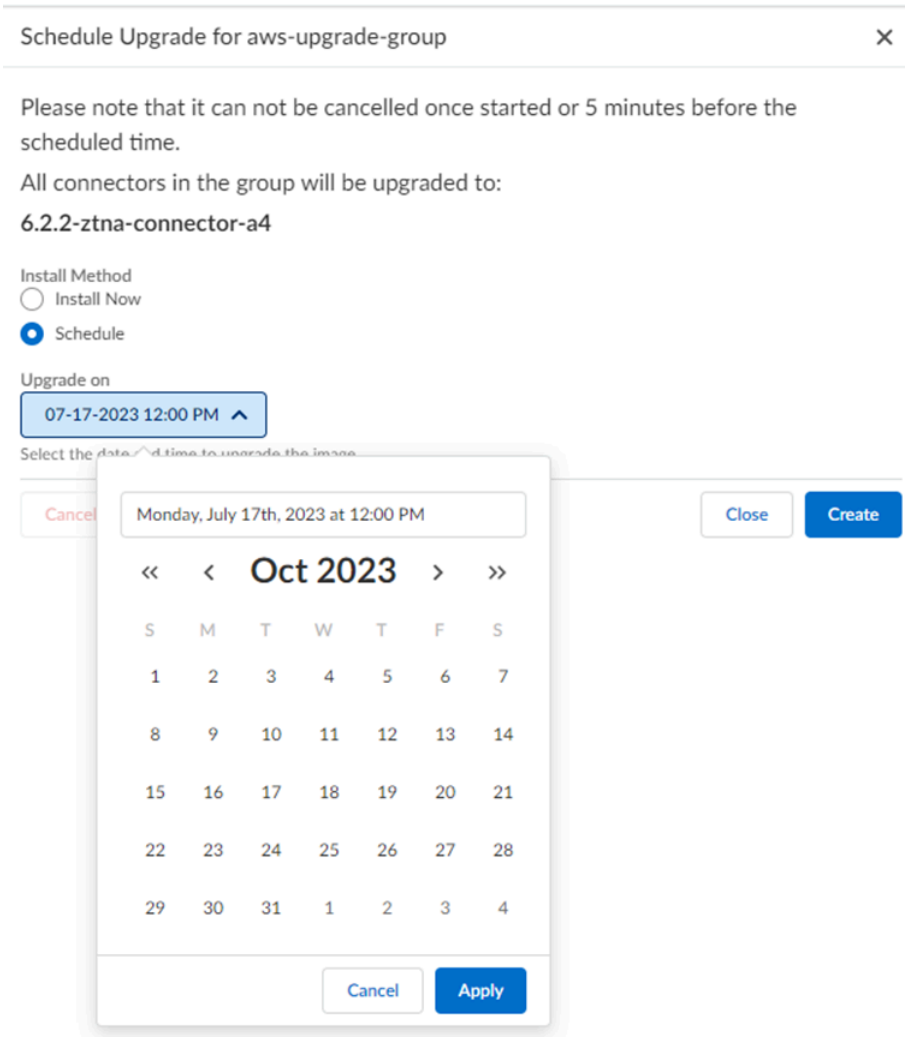
**STEP 2 |** Klicken Sie auf den grünen Pfeil neben der Konnektorgruppe.




 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Wählen Sie **Jetzt installieren** aus, um das Upgrade sofort durchzuführen, oder wählen Sie **Zeitplan** aus und geben Sie eine Uhrzeit und ein Datum für das Upgrade an. Die angezeigte Zeit ist die lokale Zeitzone des Administrators, der die ZTNA-Benutzeroberfläche verwendet.

Bis zu fünf Minuten vor Beginn können Sie ein **geplantes Upgrade abbrechen**.




**STEP 4 |** Überprüfen Sie den Status der Konnektoren über das Symbol unter **Konnektor-Version**.

| Symbol | Beschreibung |
|---|---|
|  | Ein Upgrade ist verfügbar. |
|  | Das Upgrade ist geplant. |
|  | Das Upgrade wurde gestartet und wird ausgeführt. |

 ©2025 Palo Alto Networks, Inc.

| Symbol | Beschreibung |
|---|---|
| Kein Symbol (es wird nur die Konnektor-Version angezeigt)<br>6.1.1-ztna-connector-a8 | Das Upgrade war erfolgreich. |
|  | Nicht alle Konnektoren wurden aktualisiert. |
|  | Das Upgrade ist fehlgeschlagen. |

## ZTNA-Connector-Diagnosetools

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access Version 4.0<br>❑ ZTNA-Connector-Add-on-Lizenz<br>Die Essential-Lizenz mit der Add-on-Lizenz umfasst acht ZTNA-Connectors, 100 FQDNs und vier IP-Subnetzfunktionen.<br>Die Advanced-Lizenz mit der Add-on-Lizenz umfasst 40 ZTNA-Connectors, 300 FQDNs und 1.024 IP-Subnetzfunktionen.<br>Die Premiumlizenz mit der Add-on-Lizenz umfasst 200 ZTNA-Connectors, 4.000 FQDNs und 1.024 IP-Subnetzfunktionen.<br>❑ Wenn Sie die ZTNA-Connector-Add-on-Lizenz nicht erwerben, beinhalten die Prisma Access-Lizenzen vier Konnektoren, 40 FQDNs und vier IP-Subnetze. Diese Funktionalität wird bereitgestellt, um ZTNA-Connectors in Ihrer Umgebung zu testen. |

Wenn Probleme beim Zugriff auf private Apps mit ZTNA-Connector auftreten, können Sie Tests über die ZTNA-Connector-Benutzeroberfläche durchführen, um das Problem mithilfe der folgenden Netzwerktools zu finden:

- Ping
- TCP Ping
- Traceroute

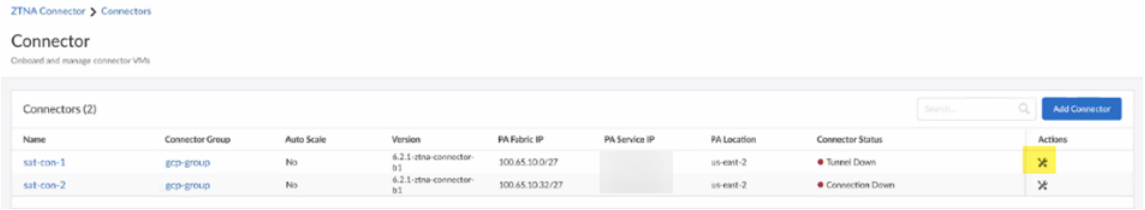
 ©2025 Palo Alto Networks, Inc.

- nslookup
- Dump-Übersicht
- Sie können auch Paketerfassungen vornehmen, um die Ursache von Problemen mit ZTNA-Connector zu ermitteln.

*Stellen Sie sicher, dass ICMP in Ihrem Netzwerk erlaubt ist, bevor Sie die Ping- und Traceroute-Tools verwenden. In einigen Cloud-Umgebungen ist ICMP aus Sicherheitsgründen nicht erlaubt. Diese Tools zeigen dann keine Aktivität an.*

**STEP 1 |** Gehen Sie zu **Workflows** > **ZTNA-Connector** > **Konnektoren**.

**STEP 2 |** Wählen Sie **Aktionen** > **Diagnose** für den Konnektor aus.



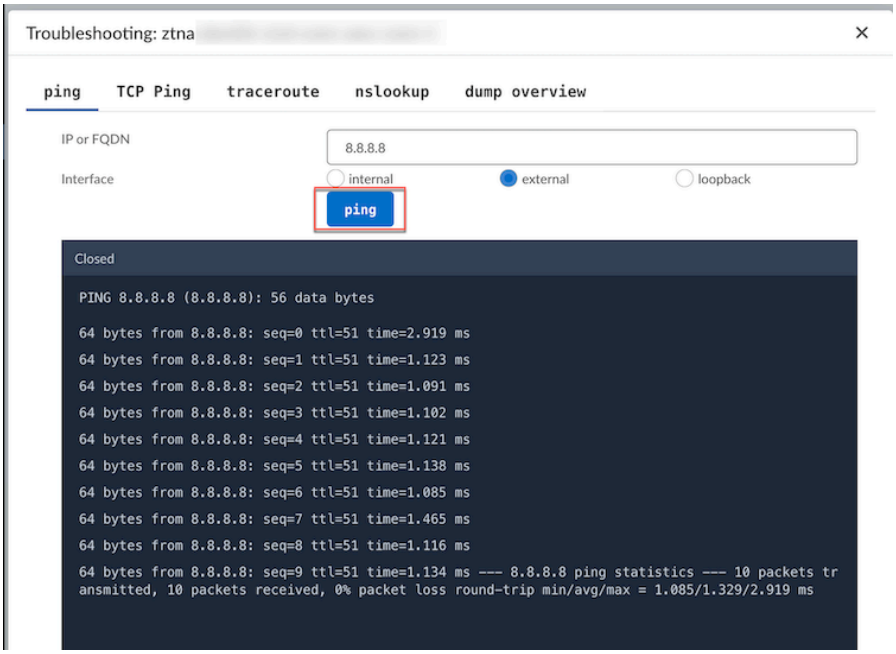

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Führen Sie die Diagnosetools Ping, TCP Ping, Traceroute oder Nslookup aus.

- **Ping**:
  1. Wählen Sie **die IP oder den FQDN** der Anwendung aus, die Sie erreichen möchten.
  2. Wählen Sie die **Schnittstelle** aus, über die Sie den Ping testen möchten.

     Wenn Sie Ihre VM mit einer zweiarmigen Bereitstellung konfiguriert haben, wählen Sie **intern** aus, um die LAN-Seite (Port 2) der VM zu überprüfen. Wenn Sie die WAN-Seite (Port 1) überprüfen möchten, wählen Sie **extern** aus.

     Bei einer einarmigen Bereitstellung wählen Sie entweder **intern** oder **extern**, da sowohl das WAN als auch das LAN zu Port 1 zuordnen.
  3. Wählen Sie **Ping** aus.

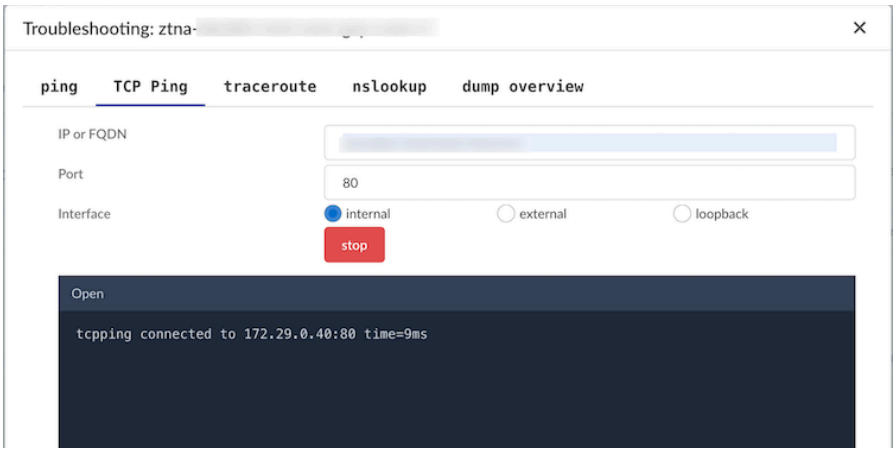
     Daraufhin wird die Ping-Ausgabe angezeigt.
  4. Wählen Sie zum Beenden des Tests die Option **Stopp** aus.
- **TCP Ping**:

  *Aktualisieren Sie den Konnektor auf die ZTNA-Connector-Version 6.2.5-b1. Wenn der Konnektor nicht mit dieser Version auf dem neuesten Stand ist, bietet die Strata Cloud Manager-Benutzeroberfläche **TCP Ping** nicht als Diagnosetool an.*

  1. Wählen Sie **die IP oder den FQDN** der Anwendung aus, die Sie erreichen möchten.
  2. Wählen Sie die **Schnittstelle** aus, über die Sie den Ping testen möchten.

     Wenn Sie Ihre VM mit einer zweiarmigen Bereitstellung konfiguriert haben, wählen Sie **intern** aus, um die LAN-Seite (Port 2) der VM zu überprüfen. Wenn Sie die WAN-Seite (Port 1) überprüfen möchten, wählen Sie **extern** aus.
  3. Wählen Sie **TCP Ping** aus.

 ©2025 Palo Alto Networks, Inc.

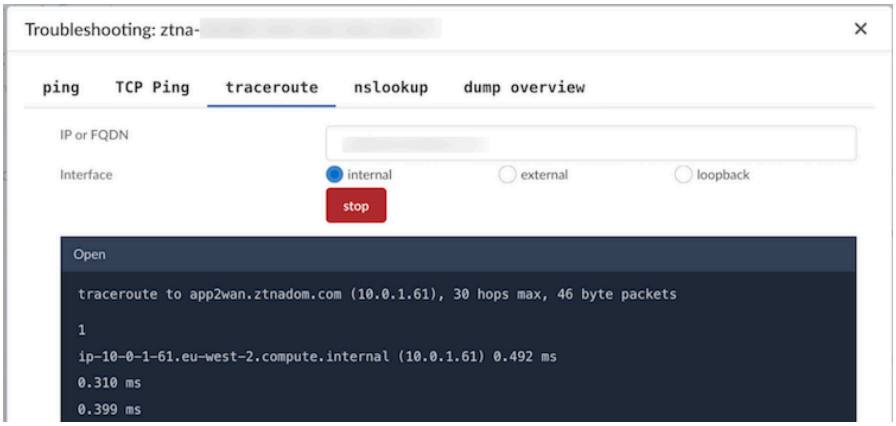



4. Wählen Sie zum Beenden des Tests die Option **Stopp** aus.

- **Traceroute**:

1. Wählen Sie **die IP oder den FQDN** der Anwendung aus, die Sie erreichen möchten.
2. Wählen Sie die **Schnittstelle** aus, über die Sie den Ping testen möchten.

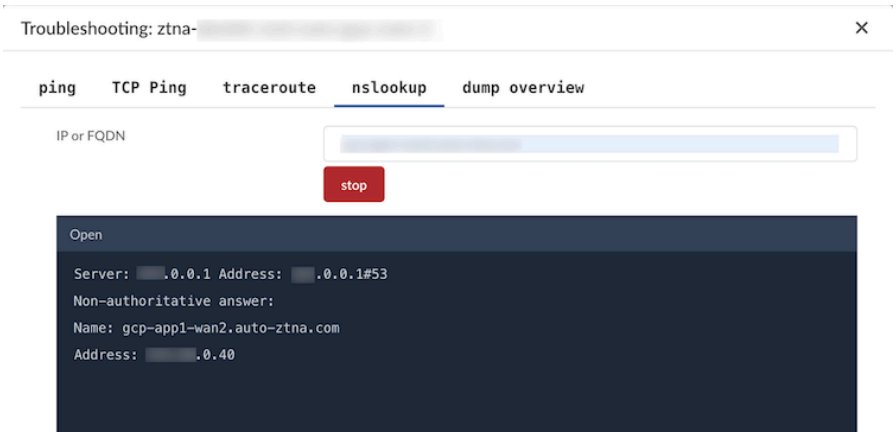
   Wenn Sie Ihre VM mit einer zweiarmigen Bereitstellung konfiguriert haben, wählen Sie **intern** aus, um die LAN-Seite (Port 2) der VM zu überprüfen. Wenn Sie die WAN-Seite (Port 1) überprüfen möchten, wählen Sie **extern** aus.
3. Wählen Sie **Traceroute** aus.
4. Wählen Sie zum Beenden des Tests die Option **Stopp** aus.




- **Nslookup**:

1. Wählen Sie **die IP oder den FQDN** der Anwendung aus, die Sie erreichen möchten.
2. Wählen Sie **Nslookup** aus.
3. Wählen Sie zum Beenden des Tests die Option **Stopp** aus.

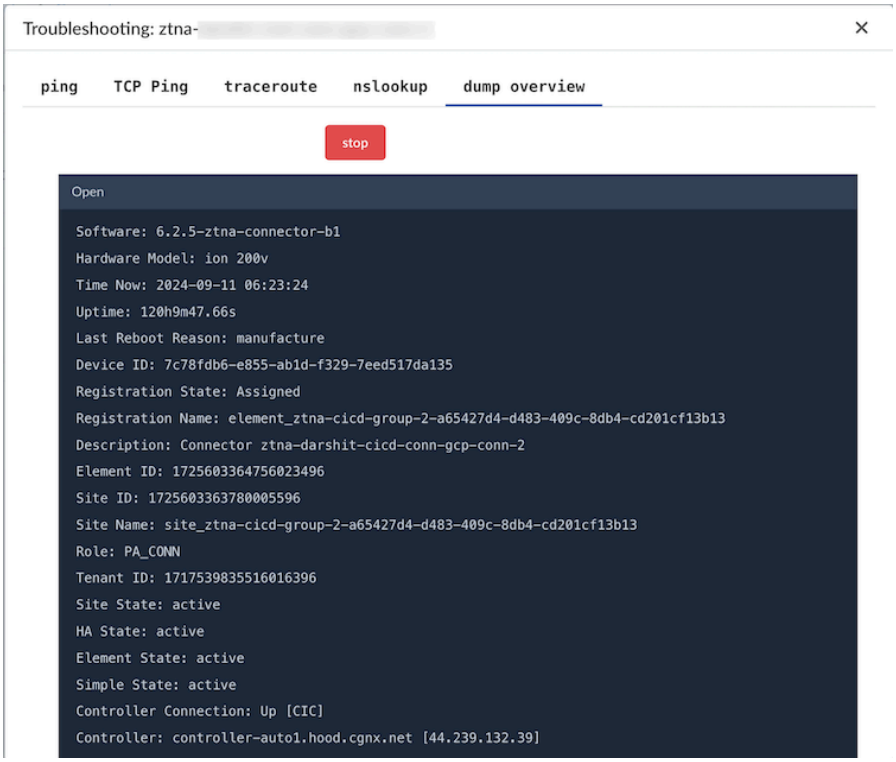
 ©2025 Palo Alto Networks, Inc.




- **Dump-Übersicht**:

  1. Klicken Sie auf **Start**, um einen Systemabdruck herunterzuladen, klicken Sie auf **Stopp**, um ihn zu stoppen.

     Die Dump-Übersicht enthält die Softwareversion, den Schnittstellen- und Verbindungsstatus sowie Informationen zur Konnektor-Identifizierung, die für die PANW-Fehlerbehebung erforderlich sind.




## Paketerfassungen

Wenn Sie Paketerfassungen zur Fehlerbehebung auf Netzwerkebene benötigen, können Sie Paketerfassungen vornehmen, die Netzwerkdaten von bestimmten Konnektoren erfassen. Sie können auch Pakete basierend auf bestimmten IP-Adressen oder Protokollen (z B. TCP) erfassen.

Paketerfassungen sind in folgenden Anwendungsfällen sinnvoll:

 ©2025 Palo Alto Networks, Inc.

- Bei Inaktivität Ihres Tunnels. Die Aufnahme der IKE-Verhandlung zwischen dem Konnektor und ZTT würde bei der Problemermittlung helfen. Wählen Sie in diesem Fall die **Internetschnittstelle** aus und verwenden Sie die IP-Adresse der Dienstverbindung als Quell- oder Zielschnittstelle.
- Wenn Ihre App ausfällt, können Sie das Probing der Apps überprüfen, indem Sie mittels tcpdump unter Angabe der IP-Adresse und des Ports des Servers sowie des Ports auf der Schnittstelle des Rechenzentrums eine Paketanalyse durchführen.
- Wenn die End-to-End-Datenebene nicht funktioniert, aber der Tunnel eine aktive Anwendung ist: In diesem Anwendungsfall wäre es vorteilhaft, mittels tcpdump den Benutzerverkehr auf dem IPSec-Tunnel zu analysieren, der für die Fabric-IP-Adresse der App bestimmt ist.

**STEP 1 |** Gehen Sie zu **Workflows** > **ZTNA-Connector** > **Konnektoren**.

**STEP 2 |** Wählen Sie **Paketerfassung** (die Lupe) für den Konnektor aus, den Sie beheben möchten.




**STEP 3 |** Wählen Sie die Schnittstelle aus, an der die Pakete erfasst werden sollen (**intern**, **extern** oder **Tunnel**).

**STEP 4 |** (Optional) Geben Sie die **Quell- oder Ziel-IPv4**-Adresse an, von der Pakete erfasst werden.

Wenn Sie diese Option angeben, werden nur Pakete von dieser IP-Adresse erfasst.

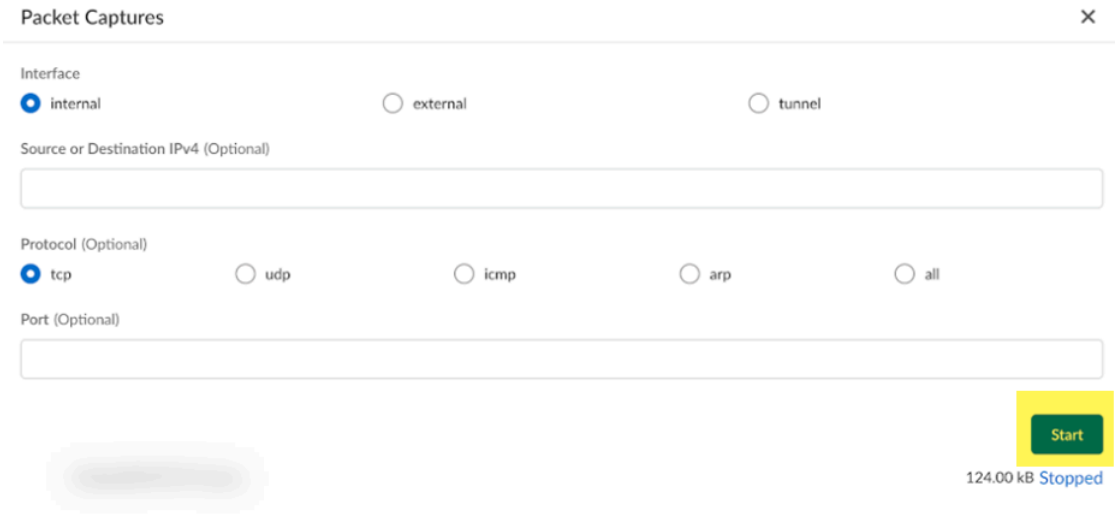
**STEP 5 |** (Optional) Wählen Sie den Typ der zu erfassenden Pakete aus.

Sie können Pakete eines bestimmten Protokolls auswählen, das erfasst werden soll (**tcp**, **udp**, **icmp** oder **arp**), oder **alle** auswählen, um alle Pakete zu erfassen.

**STEP 6 |** (Optional) Wählen Sie einen **Port** aus, von dem Pakete erfasst werden sollen.

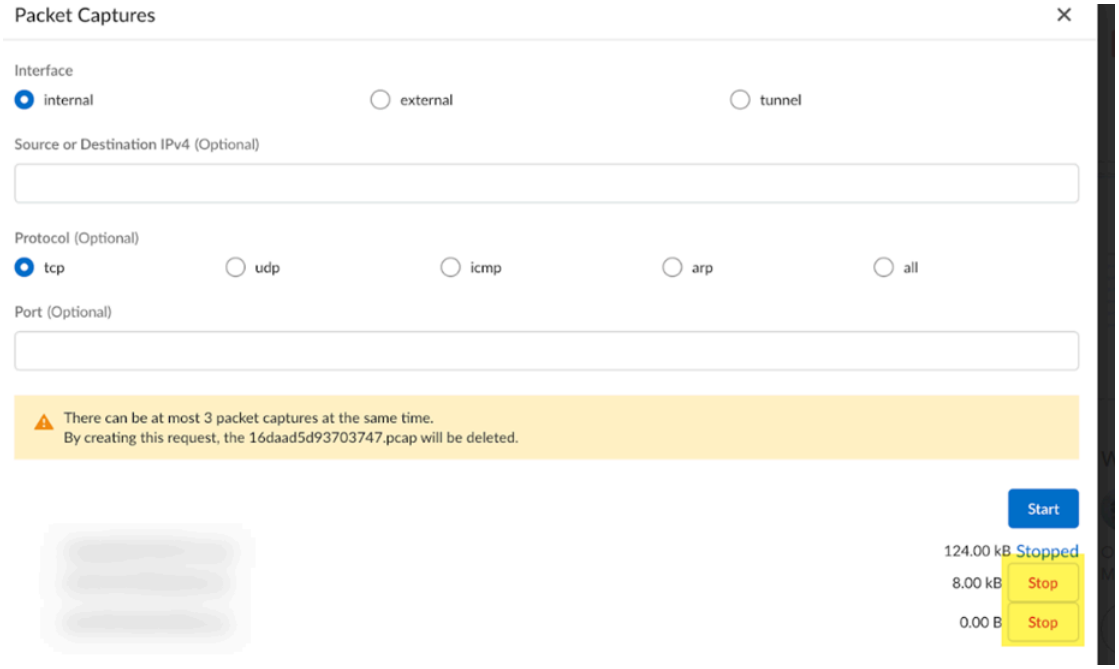
Wenn Sie diese Option angeben, werden nur Pakete von diesem Port erfasst.

**STEP 7 |** **Starten** Sie die Paketerfassungen.




 ©2025 Palo Alto Networks, Inc.

**STEP 8 |** Klicken Sie auf **Stopp**, um die Paketerfassung zu stoppen.




- Die maximale Dateigröße für Paketerfassungen beträgt 5 MB. Wenn Sie die Erfassungen nicht stoppen, bevor die maximale Größe erreicht ist, wird die Datei überschrieben.
- Auf einem Konnektor sind maximal drei gleichzeitige Paketerfassungen erlaubt. Wird eine vierte Sitzung initiiert, wird die erste laufende Sitzung abgebrochen.

## Sammeln von Dateien für den technischen Support

Die Datei „Technischer Support“ enthält Ihre Gerätekonfiguration, Systeminformationen und einige Protokolle (nicht zum Datenverkehr). Palo Alto Networks kann anfordern, dass Sie eine Datei für den technischen Support als Hilfe bei der Fehlerbehebung für ZTNA-Connector hochladen.

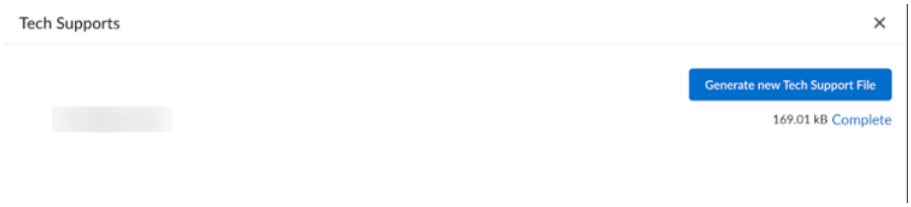
**STEP 1 |** Gehen Sie zu **Workflows** > **ZTNA-Connector** > **Konnektoren**.

**STEP 2 |** Wählen Sie **Technischer Support** (Handsymbol) für den Konnektor aus, den Sie beheben möchten.




 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** **Generieren Sie eine neue Datei für den technischen Support.**




**STEP 4 |** Wählen Sie **Abgeschlossen** aus, um die Datei für den technischen Support lokal herunterzuladen.

 ©2025 Palo Alto Networks, Inc.

# Connector-IP-Blöcke löschen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access Version 4.0<br>❑ ZTNA-Connector-Add-on-Lizenz<br>Die Essential-Lizenz mit der Add-on-Lizenz umfasst acht ZTNA-Connectors, 100 FQDNs und vier IP-Subnetzfunktionen.<br>Die Advanced-Lizenz mit der Add-on-Lizenz umfasst 40 ZTNA-Connectors, 300 FQDNs und 1.024 IP-Subnetzfunktionen.<br>Die Premiumlizenz mit der Add-on-Lizenz umfasst 200 ZTNA-Connectors, 4.000 FQDNs und 1.024 IP-Subnetzfunktionen.<br>❑ Wenn Sie die ZTNA-Connector-Add-on-Lizenz nicht erwerben, beinhalten die Prisma Access-Lizenzen vier Konnektoren, 40 FQDNs und vier IP-Subnetze. Diese Funktionalität wird bereitgestellt, um ZTNA-Connectors in Ihrer Umgebung zu testen. |

Sie können ZTNA-Connector aktivieren und die erforderlichen Connector-IP-Blöcke hinzufügen, mit denen Prisma Access intern den Datenverkehr zwischen mobilen Benutzern, Remote-Netzwerken und den Connector-VMs in Ihren Rechenzentren weiterleitet. Zuvor konnten Sie keine Änderungen an den Connector-IP-Blöcken nach deren Erstellung vornehmen. Jetzt können Sie jedoch die **Connector-IP-Blöcke** löschen oder aktualisieren. Gehen Sie wie erwähnt vor, um die Blöcke zu löschen oder zu aktualisieren.

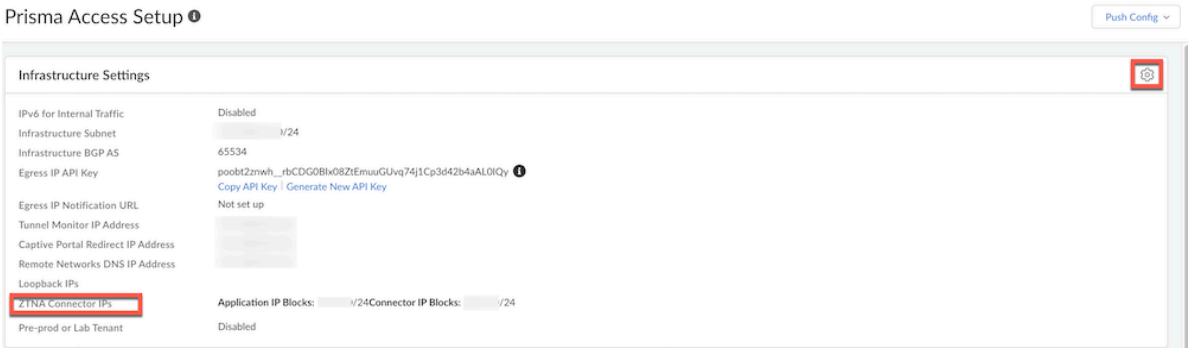
- Panorama
- Strata Cloud Manager

## Connector-IP-Blöcke löschen (Von der Cloud verwaltet)

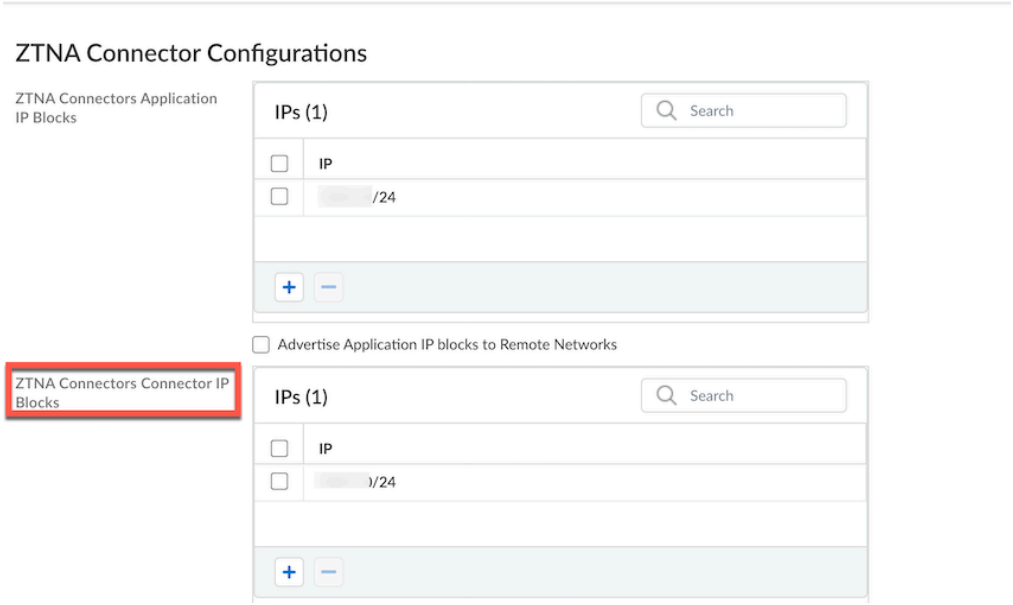
Führen Sie die folgenden Schritte aus, um die Connector-IP-Blöcke zu löschen.

 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** Gehen Sie zu **Workflows** > **Einrichtung Prisma Access** > **Prisma Access** > **Infrastruktureinstellungen** und klicken Sie auf das Zahnrad, um die **Einstellungen** zu bearbeiten.



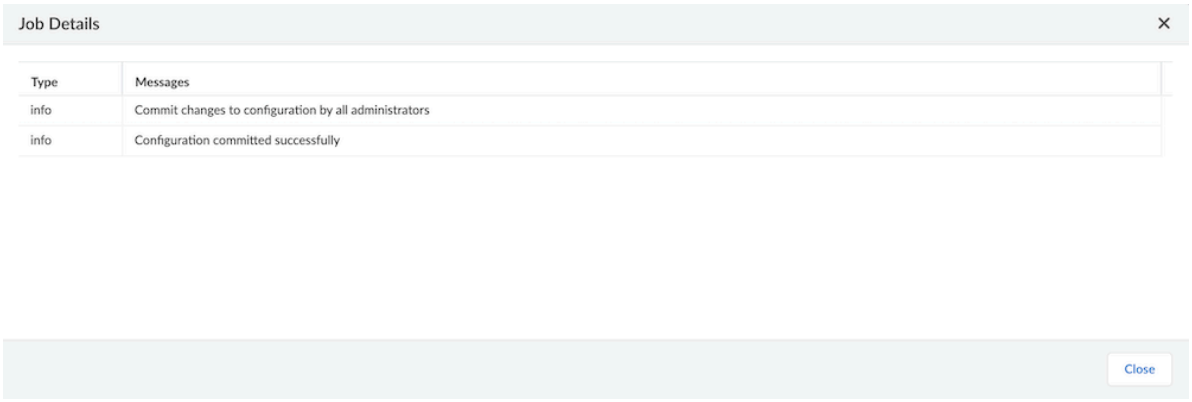

**STEP 2 |** Aktivieren Sie unter **ZTNA-Connector-Konfigurationen** > **Connector-IP-Blöcke von ZTNA-Connector** das Kontrollkästchen neben dem zu löschenden Connector-Block und klicken Sie auf **Speichern**.




 ©2025 Palo Alto Networks, Inc.

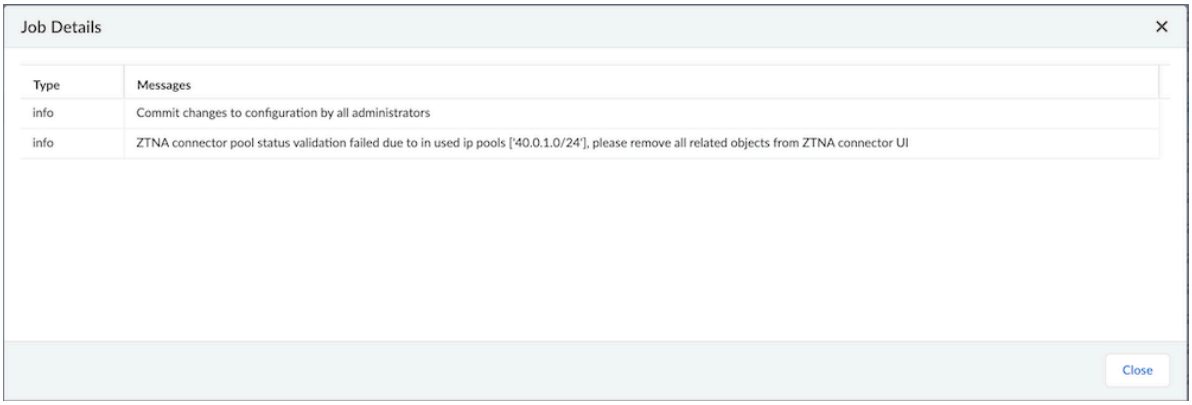
**STEP 3 |** Wählen Sie **Commit** aus und übertragen Sie die Konfigurationsänderung per Push.

Nach der Übergabe des Commits wird eine Meldung eingeblendet.




Wenn Sie ZTNA-Connector-Objekte wie Konnektoren, Anwendungen, Platzhalter und Konnektorgruppen erstellt haben und versuchen, den **Connector-IP-Block** zu löschen, ohne zuvor die ZTNA-Connector-Objekte zu löschen, schlägt die Aktion „Commit und Push“ fehl.

Löschen Sie in diesem Fall die ZTNA-Connector-Objekte, löschen Sie den erforderlichen **Connector-IP-Block** und führen Sie dann einen **Commit** durch. Der erste Commit schlägt fehl, aber der zweite wird übergeben.

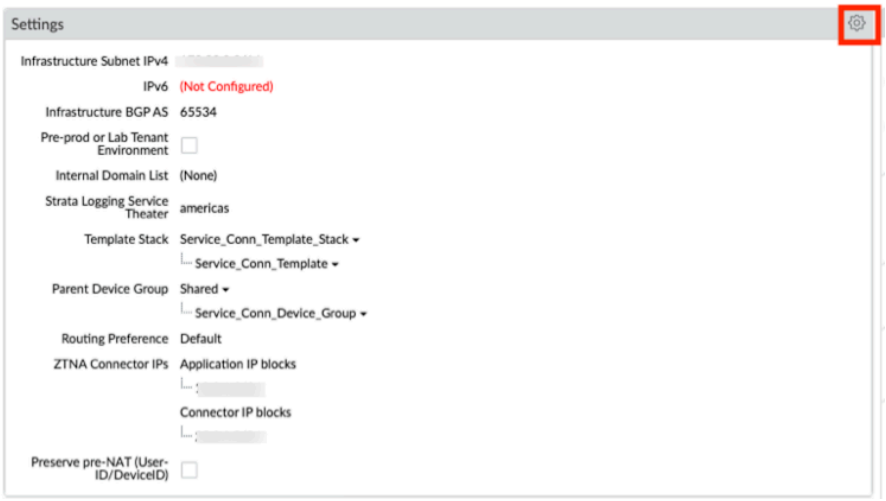



## Connector-IP-Blöcke löschen (Panorama)

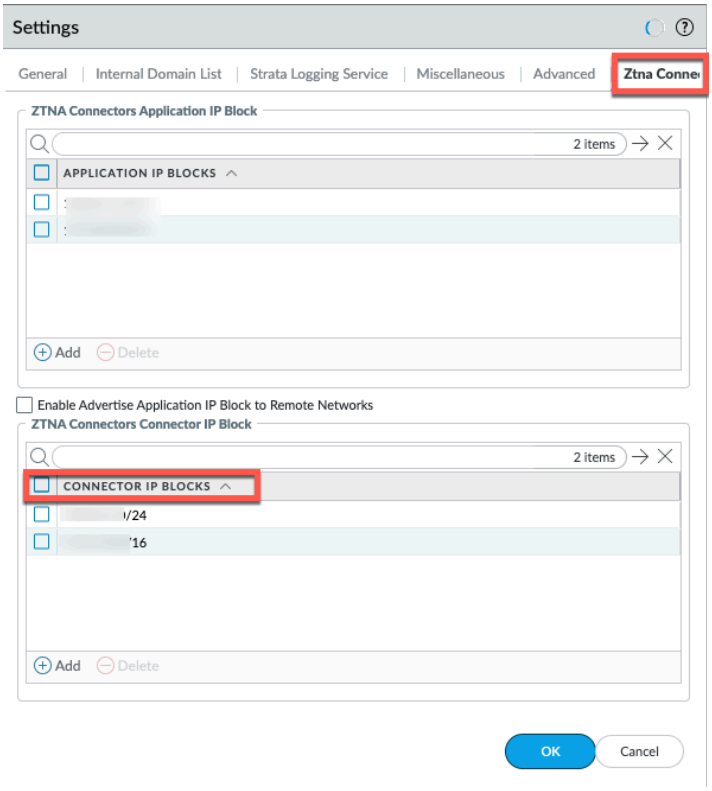
Führen Sie die folgenden Schritte aus, um die Connector-IP-Blöcke zu löschen.


©2025 Palo Alto Networks, Inc.

**STEP 1 |** Gehen Sie zu **Panorama** > **Cloud Services** > **Konfiguration** > **Diensteinrichtung** und klicken Sie auf das Zahnrad, um die **Einstellungen** zu bearbeiten.




**STEP 2 |** Wählen Sie **ZTNA-Connector** aus.

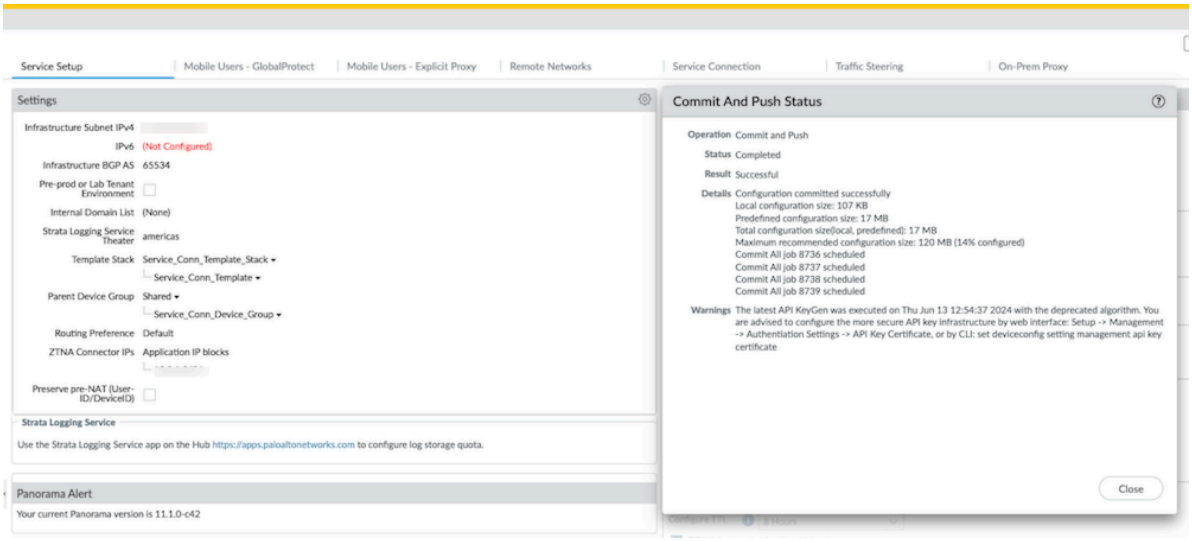



**STEP 3 |** Aktivieren Sie das Kontrollkästchen neben dem Connector-Block, den Sie löschen möchten, und klicken Sie auf **OK**, um die Konfiguration zu speichern.

 ©2025 Palo Alto Networks, Inc.

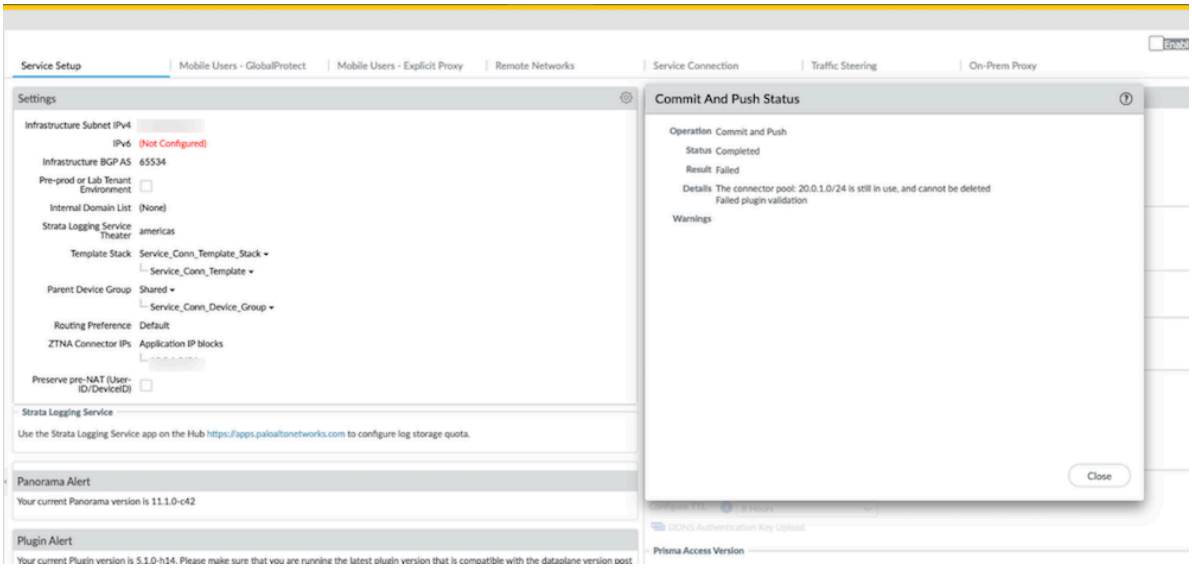
**STEP 4 |** Wählen Sie **Commit** aus und übertragen Sie die Konfigurationsänderung per Push.

Nach der Übergabe des Commits wird eine Meldung eingeblendet.




Wenn Sie zuvor ZTNA-Connector-Objekte wie Konnektoren, Anwendungen, Platzhalter und Konnektorgruppen erstellt haben und versuchen, den **Connector-IP-Block** zu löschen, ohne zuvor die ZTNA-Connector-Objekte zu löschen, schlägt die Aktion „Commit und Push“ fehl.

Löschen Sie in diesem Fall die ZTNA-Connector-Objekte, löschen Sie den erforderlichen **Connector-IP-Block** und führen Sie dann **Commit** und Push zweimal durch. Der erste Commit schlägt fehl, aber der zweite wird übergeben.




 ©2025 Palo Alto Networks, Inc.

# Automatische Erkennung von Anwendungen mit Cloud Identity Engine einrichten

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access Version 4.0<br>❑ ZTNA-Connector-Add-on-Lizenz<br>Die Essential-Lizenz mit der Add-on-Lizenz umfasst acht ZTNA-Connectors, 100 FQDNs und vier IP-Subnetzfunktionen.<br>Die Advanced-Lizenz mit der Add-on-Lizenz umfasst 40 ZTNA-Connectors, 300 FQDNs und 1.024 IP-Subnetzfunktionen.<br>Die Premiumlizenz mit der Add-on-Lizenz umfasst 200 ZTNA-Connectors, 4.000 FQDNs und 1.024 IP-Subnetzfunktionen.<br>❑ Wenn Sie die ZTNA-Connector-Add-on-Lizenz nicht erwerben, beinhalten die Prisma Access-Lizenzen vier Konnektoren, 40 FQDNs und vier IP-Subnetze. Diese Funktionalität wird bereitgestellt, um ZTNA-Connectors in Ihrer Umgebung zu testen. |

Damit ZTNA-Connector Anwendungen automatisch erkennt, die in Azure Active Directory oder Okta Directory definiert sind, müssen Sie Folgendes konfigurieren:

❑ Aktivieren Sie die Cloud Identity Engine im Hub und erstellen Sie Ihren ersten Mandanten.

Sie müssen **Unternehmensanwendungen sammeln** auswählen, wenn Sie Ihr Cloud-basiertes Verzeichnis in Azure oder Okta konfigurieren.

❑ Wählen Sie den Verzeichnistyp aus, auf den die Cloud Identity Engine zugreifen soll.

❑ Konfigurieren Sie ein Cloud-basiertes Verzeichnis, z. B. Azure Active Directory (Azure AD) oder Okta Directory, um mit der Cloud Identity Engine zu kommunizieren.

Die folgenden IdPs werden für die Verwendung mit Anwendungserkennung unterstützt:

- Azure AD
- Okta

 ©2025 Palo Alto Networks, Inc.

# Zielerkennung für private Anwendungen

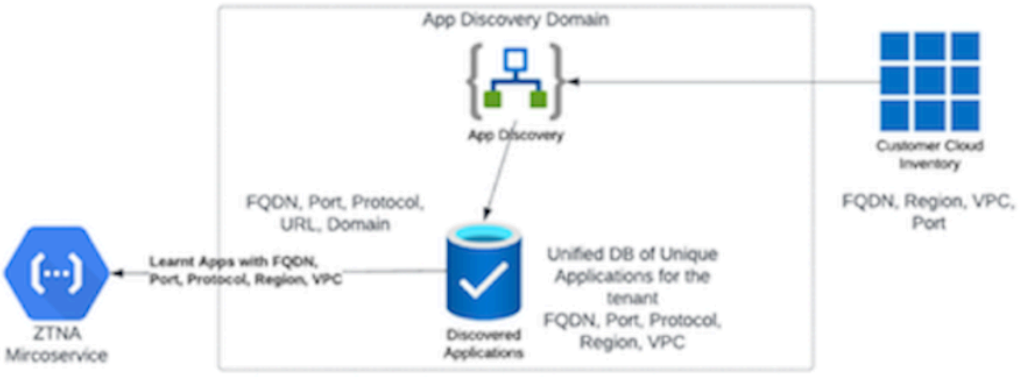
| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access Version 4.0<br>❑ ZTNA-Connector-Add-on-Lizenz<br>Die Essential-Lizenz mit der Add-on-Lizenz umfasst acht ZTNA-Connectors, 100 FQDNs und vier IP-Subnetzfunktionen.<br>Die Advanced-Lizenz mit der Add-on-Lizenz umfasst 40 ZTNA-Connectors, 300 FQDNs und 1.024 IP-Subnetzfunktionen.<br>Die Premiumlizenz mit der Add-on-Lizenz umfasst 200 ZTNA-Connectors, 4.000 FQDNs und 1.024 IP-Subnetzfunktionen.<br>❑ Wenn Sie die ZTNA-Connector-Add-on-Lizenz nicht erwerben, beinhalten die Prisma Access-Lizenzen vier Konnektoren, 40 FQDNs und vier IP-Subnetze. Diese Funktionalität wird bereitgestellt, um ZTNA-Connectors in Ihrer Umgebung zu testen. |

In einer modernen Netzwerkinfrastruktur werden Tausende von privaten Anwendungen lokal und in Multicloud-Rechenzentren bereitgestellt. Die Netzwerkteams wissen nicht, welche Anwendungen in ihrem Netzwerk oder in einem bestimmten Subnetz im Netzwerk ausgeführt werden, was zu fehlender Anwendungstransparenz führt.

Um einen sicheren Zugriff auf Anwendungen zu ermöglichen, müssen Sie den FQDN, den Port und die Anwendung manuell eingeben und sich der Abhängigkeit dieser Anwendung von den anderen Anwendungen bewusst sein.

Die Zielerkennung für private Anwendungen bietet eine Möglichkeit, die in der Cloud-Umgebung gehosteten Anwendungen zu ermitteln, und ermöglicht die Einbindung dieser Anwendungen in die ZTNA-Connector-Lösung. Dabei wird zudem eine Verbindung zum Netzwerk des Cloud-Anbieters hergestellt, die Erkennung durchgeführt und sie in der Datenbank gespeichert. Außerdem werden APIs für die verschiedenen Dienste bereitgestellt, um die erkannten Anwendungen abzurufen. Wenn der Benutzer nur über eine Dienstverbindung anstelle eines ZTNA-Connector verfügt, werden nur Anwendungsziele erkannt.

 ©2025 Palo Alto Networks, Inc.




Die Zielerkennung für private Anwendungen findet Folgendes:

- FQDN
- Port der Anwendung
- Protokoll der Anwendung

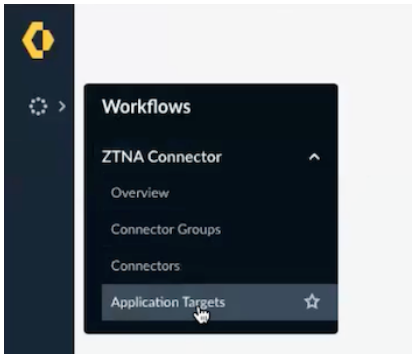
*Stellen Sie sicher, dass Sie Cloud Identity Engine (CIE) vor der Funktion zur Erkennung privater Anwendungen aktivieren.*

Führen Sie die folgenden Schritte aus, um ein Cloud-Konto, eine IAM-Rolle in AWS, hinzuzufügen und die Zielanwendungen zu erkennen.

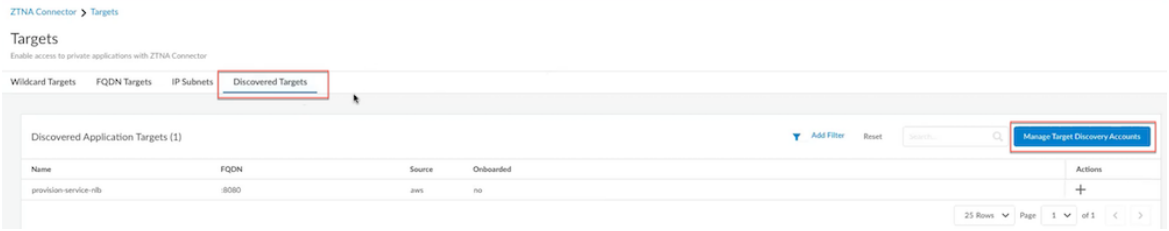
 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** Rufen Sie die CloudFormation-Vorlage (CFT) ab, um ein Cloud-Konto hinzuzufügen.

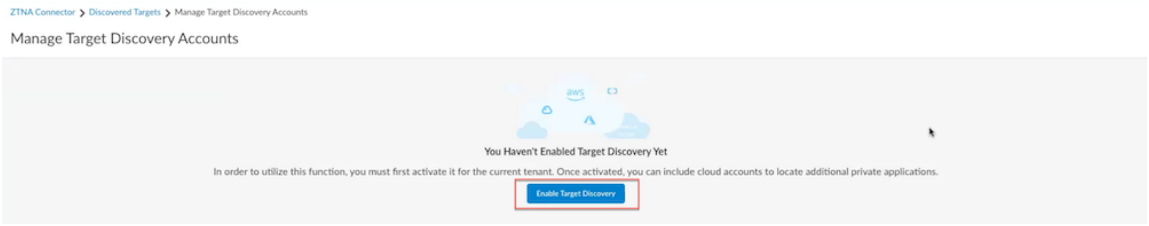
1. Navigieren Sie zu **Anwendungsziele**(**Workflows** > **ZTNA-Connector** > **Anwendungsziele**).



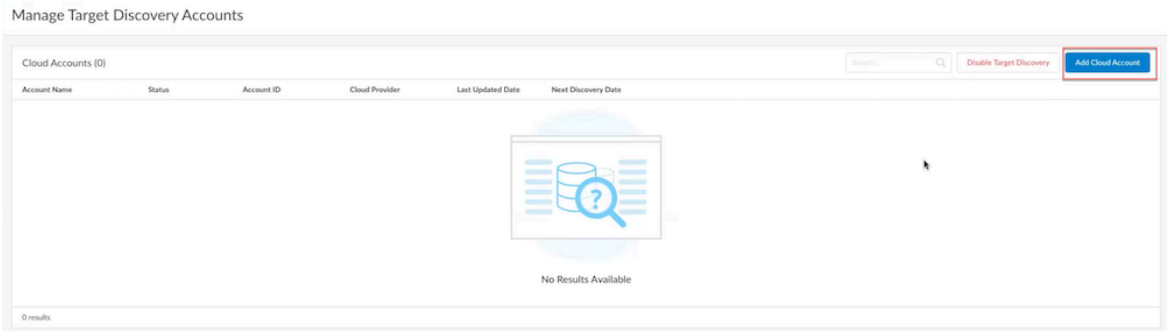

2. Wählen Sie auf der Seite **Anwendungsziele Gefundene Ziele** und dann **Zielerkennungskonten** aus.




3. Wählen Sie **Zielerkennung aktivieren** und dann **Aktivieren** aus.

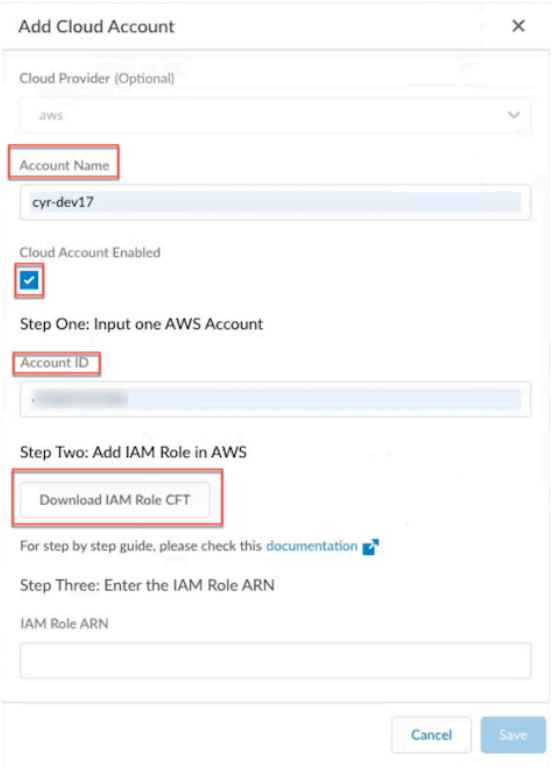



4. Wählen Sie auf der Seite **Zielerkennungskonten** die Option **Cloud-Konto hinzufügen** aus.



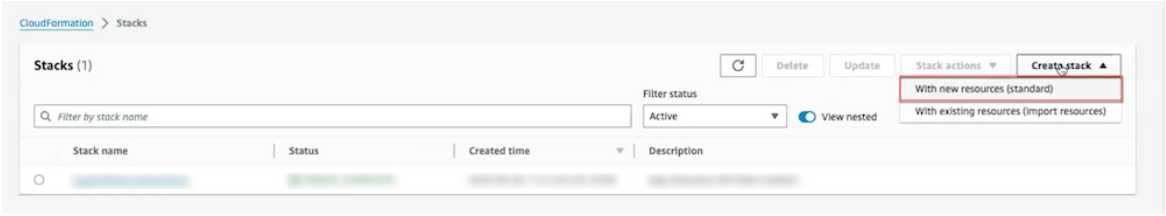

5. Fügen Sie den **Kontonamen** hinzu und klicken Sie auf das Kontrollkästchen unter **Cloud-Konto aktiviert**. Fügen Sie die **Konto-ID** von AWS hinzu und klicken Sie auf **CFT der IAM-Rolle herunterladen**, um die Datei herunterzuladen.

 ©2025 Palo Alto Networks, Inc.




**STEP 2 |** Erstellen Sie die IAM-Rolle in AWS.

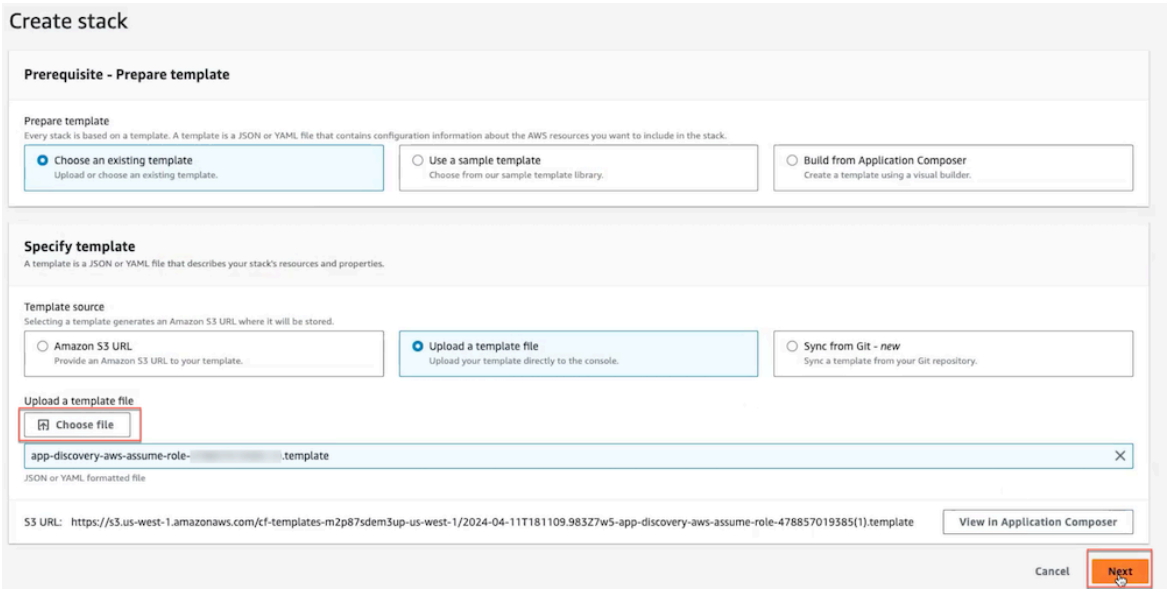
1. Navigieren Sie zur AWS-Anwendung, wählen Sie Ihr Konto und **Anmelden** aus.
2. Navigieren Sie zu **CloudFormation** > **Stacks** > **Stack erstellen** > **Mit neuen Ressourcen (Standard)**, um den Stack zu erstellen.



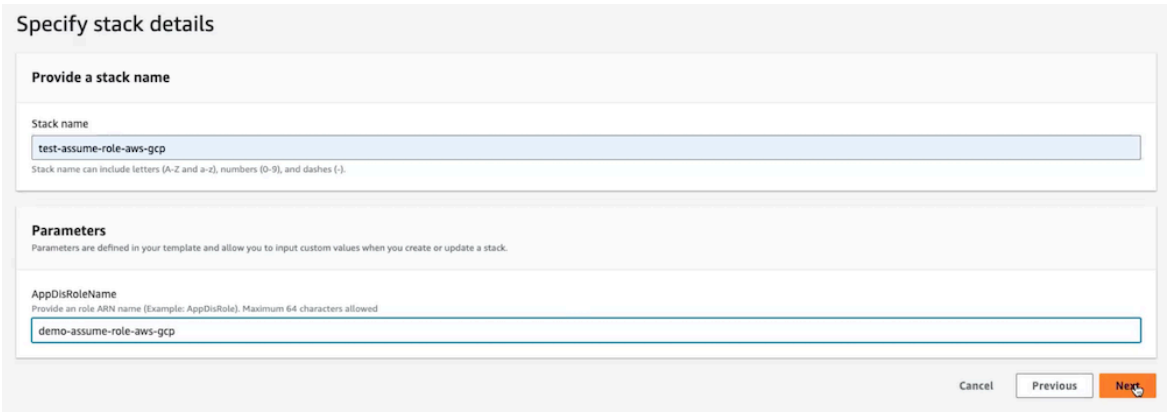

3. Wählen Sie auf der Seite **Stack erstellen** unter **Voraussetzung: Vorlage vorbereiten** die Option **Vorhandene Vorlage auswählen** aus. Wählen Sie unter **Vorlage angeben** die

 ©2025 Palo Alto Networks, Inc.

Option **Vorlagendatei hochladen** aus. Laden Sie die zuvor in Schritt 1 heruntergeladene Datei hoch und wählen Sie **Weiter** aus.




4. Fügen Sie **Stack-Name**, **AppDisRoleName** hinzu und wählen Sie **Weiter** aus.

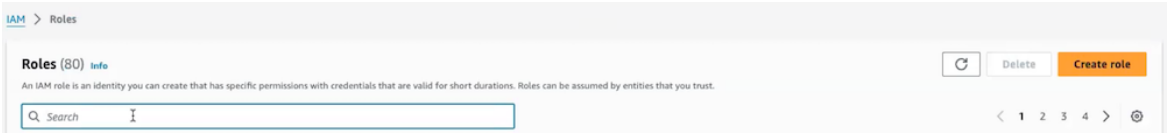



5. Nehmen Sie auf der Seite **Stack-Optionen** keine Aktualisierungen vor und wählen Sie **Weiter** aus.
6. Überprüfen Sie die Änderungen. Aktivieren Sie das Kontrollkästchen unter **Funktionen**, um die Erstellung von IAM-Ressourcen mit benutzerdefinierten Namen zu bestätigen, und wählen Sie dann **Übermitteln** aus.

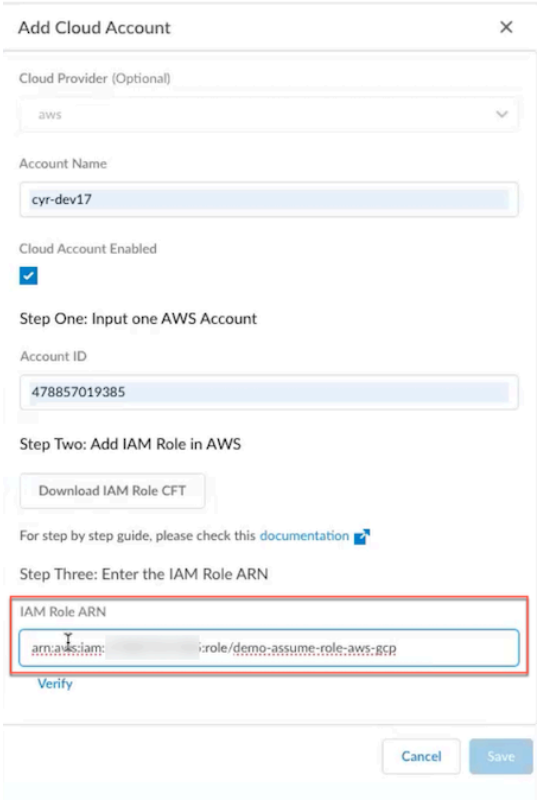



7. Navigieren Sie zu **IAM** > **Rollen** und suchen Sie nach dem von Ihnen definierten Rollennamen. Wählen Sie den Rollennamen aus und kopieren Sie den **ARN** für die Rolle.

 ©2025 Palo Alto Networks, Inc.



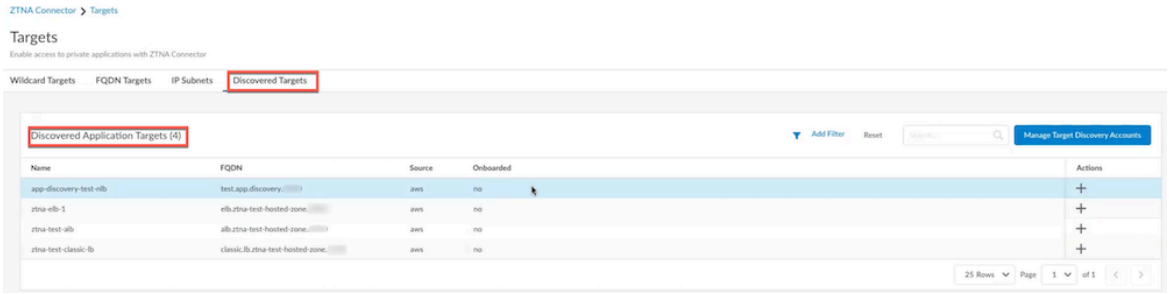

**STEP 3 |** Fügen Sie den ARN in das Textfeld **ARN der IAM-Rolle** ein und wählen Sie dann **Verifizieren** aus. Wenn der ARN verifiziert ist, wählen Sie **Speichern** aus.




*Wenn Sie einen falschen ARN in das Textfeld **ARN der IAM-Rolle** hinzufügen, schlägt die Verifizierung fehl und eine Fehlermeldung wird angezeigt.*

Nachdem Sie das Konto hinzugefügt haben, können Sie den Status, die Konto-ID und andere Details anzeigen. Der Aktualisierungszeitraum für die Erkennung beträgt 24 Stunden. Sie können demselben Mandanten auch mehrere Konten hinzufügen.

**STEP 4 |** Um die erkannten Apps zu identifizieren, wählen Sie **Gefundene Ziele** aus. Die Liste der identifizierten Anwendungen finden Sie unter **Erkannte Anwendungsziele**.

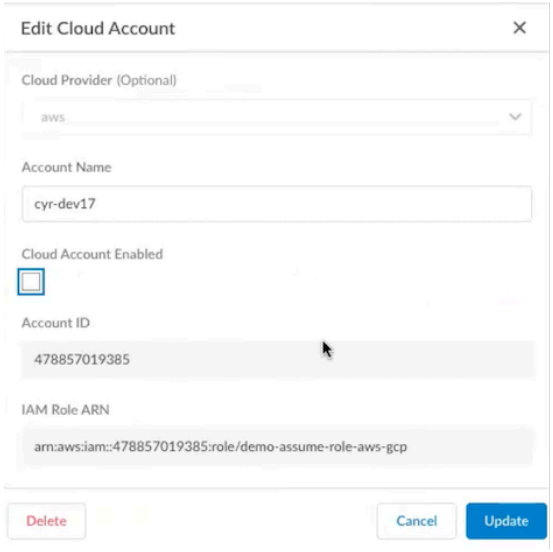



 ©2025 Palo Alto Networks, Inc.

**STEP 5 |** (Optional) Löschen Sie das Cloud-Konto.

Führen Sie folgende Schritte aus, um Ihr Cloud-Konto zu löschen und ein neues hinzuzufügen, ohne die Zielerkennung zu deaktivieren. Diese Schritte sind jedoch obligatorisch, wenn Sie die Zielerkennungsfunktion deaktivieren möchten.

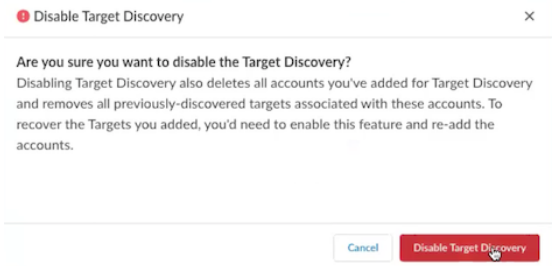
1. Klicken Sie unter **Zielerkennungskonten** auf den **Kontonamen** des Kontos, das Sie löschen möchten.
2. Deaktivieren Sie **Cloud-Konto aktiviert** und wählen Sie **Aktualisieren** aus. Wenn das Konto aktualisiert ist, wählen Sie **Löschen** aus. Das Konto wird gelöscht.




**STEP 6 |** (Optional) Deaktivieren Sie die Zielerkennung.

Stellen Sie sicher, dass alle Cloud-Konten gelöscht wurden, bevor Sie die Zielerkennung deaktivieren.

1. Wählen Sie **Zielerkennung** und dann **Zielerkennung deaktivieren** aus.




 ©2025 Palo Alto Networks, Inc.

# Sicherheitsrichtlinie für Apps mit ZTNA-Connector-Aktivierung

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access Version 4.0<br>❑ ZTNA-Connector-Add-on-Lizenz<br>Die Essential-Lizenz mit der Add-on-Lizenz umfasst acht ZTNA-Connectors, 100 FQDNs und vier IP-Subnetzfunktionen.<br>Die Advanced-Lizenz mit der Add-on-Lizenz umfasst 40 ZTNA-Connectors, 300 FQDNs und 1.024 IP-Subnetzfunktionen.<br>Die Premiumlizenz mit der Add-on-Lizenz umfasst 200 ZTNA-Connectors, 4.000 FQDNs und 1.024 IP-Subnetzfunktionen.<br>❑ Wenn Sie die ZTNA-Connector-Add-on-Lizenz nicht erwerben, beinhalten die Prisma Access-Lizenzen vier Konnektoren, 40 FQDNs und vier IP-Subnetze. Diese Funktionalität wird bereitgestellt, um ZTNA-Connectors in Ihrer Umgebung zu testen. |

ZTNA-Connector setzt keine Richtlinien durch, sondern ermöglicht eine reibungslose Erweiterung Ihrer bestehenden Prisma Access-Sicherheitsrichtlinie auf die Anwendungen, die für Prisma Access aktiviert werden. Dies bedeutet, dass Sie eine gemeinsame Richtlinie für alle Ihre Anwendungen und Rechenzentren verwenden können und Sie Ihre Sicherheitsrichtlinie nicht separat für Apps bearbeiten müssen, die in ZTNA-Connector eingebunden wurden.

Im Rahmen der Einrichtung von ZTNA-Connector müssen Sie jedoch sicherstellen, dass Ihre Sicherheitsrichtlinie folgende Voraussetzungen erfüllt:

**Zulassen des Datenverkehrs zwischen Prisma Access und ZTNA-Connector**

Befolgen Sie dazu die Anforderungen und Richtlinien für ZTNA-Connector, um sicherzustellen, dass ZTNA-Connector eine Verbindung zu Prisma Access herstellen kann.

**Benutzer können auf die Anwendungen hinter ZTNA-Connector zugreifen**

Um sicherzustellen, dass Ihre Benutzer auf ZTNA-Connector-Apps zugreifen können, befolgen Sie die hier aufgeführten Schritte für die Schnittstelle, die Sie zum Verwalten von Prisma Access verwenden.

 ©2025 Palo Alto Networks, Inc.

- Strata Cloud Manager
- Panorama

# Sicherheitsrichtlinie für Apps mit ZTNA-Connector-Aktivierung (Strata Cloud Manager)

Nachdem Sie Apps in ZTNA-Connector eingebunden haben, sollten Sie Richtlinienregeln einrichten, um den Zugriff für diese Apps zuzulassen und zu steuern. Das Verfahren zum Erstellen und Anwenden von Richtlinien unterscheidet sich abhängig davon, ob Ihre Apps durch Platzhalter, IP-Subnetze oder FQDNs definiert wurden.

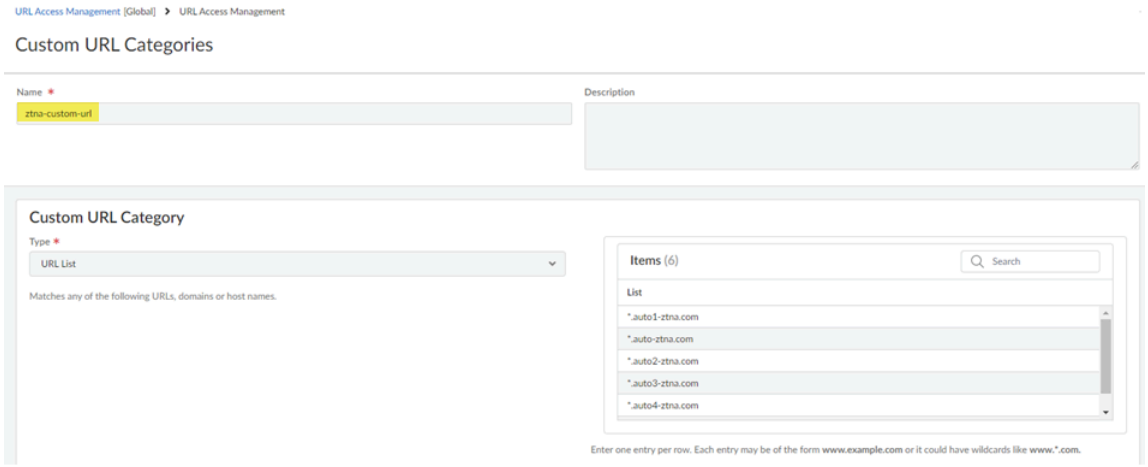
## Sicherheitsrichtlinie für platzhalterbasierte Apps

Für platzhalterbasierte Apps (**Einstellungen** > **ZTNA-Connector** > **Anwendungsziele** > **Platzhalterziele**) müssen Sie eine benutzerdefinierte URL-Kategorie erstellen. Dieser Kategorietyp setzt jedoch nur Richtlinien für HTTP- und HTTPS-Datenverkehr durch, wohingegen anderer Datenverkehr (wie SSH) nicht zulässig ist. Aus diesem Grund müssen Sie den Zugriff auf alle Apps vorübergehend zulassen, indem Sie den Datenverkehr über die Anwendungs-IP-Blöcke von ZTNA-Connector zulassen.

Nachdem ZTNA-Connector die FQDNs abgefragt hat, die auf Platzhaltern basieren, können Sie die Richtlinie deaktivieren, die den Datenverkehr über die Anwendungs-IP-Blöcke zulässt, und die Richtliniendurchsetzung basierend auf den abgefragten FQDNs anwenden.

**STEP 1 |** Erstellen Sie eine benutzerdefinierte URL-Kategorie und fügen Sie die Platzhalter-URLs der Kategorie hinzu.

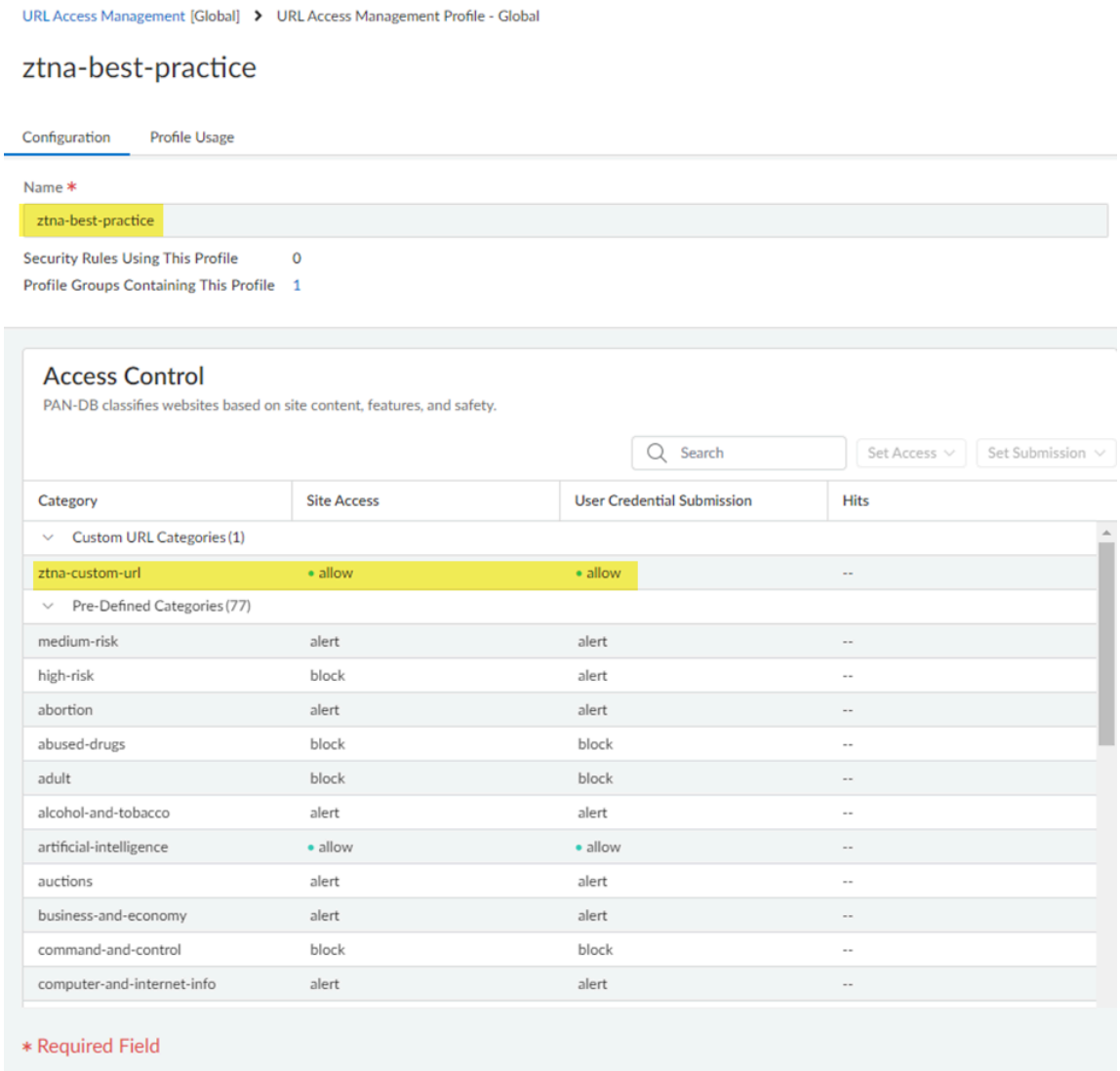
1. Rufen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Sicherheitsdienste** > **URL-Zugriffsverwaltung** auf.
2. Wählen Sie unter den benutzerdefinierten URL-Kategorien **Kategorie hinzufügen** aus.
3. Ordnen Sie der benutzerdefinierten URL-Kategorie einen aussagekräftigen **Namen** zu und wählen Sie als **Typ** die Option **URL-Liste** aus.
4. Fügen Sie unter **Elemente** die Platzhalter-URLs hinzu, die Sie in ZTNA-Connector erstellt haben.
5. **Speichern** Sie Ihre Änderungen.




 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Erstellen Sie ein URL-Zugriffsverwaltungs-Profil und fügen Sie ihm die von Ihnen erstellte, benutzerdefinierte URL-Kategorie hinzu.

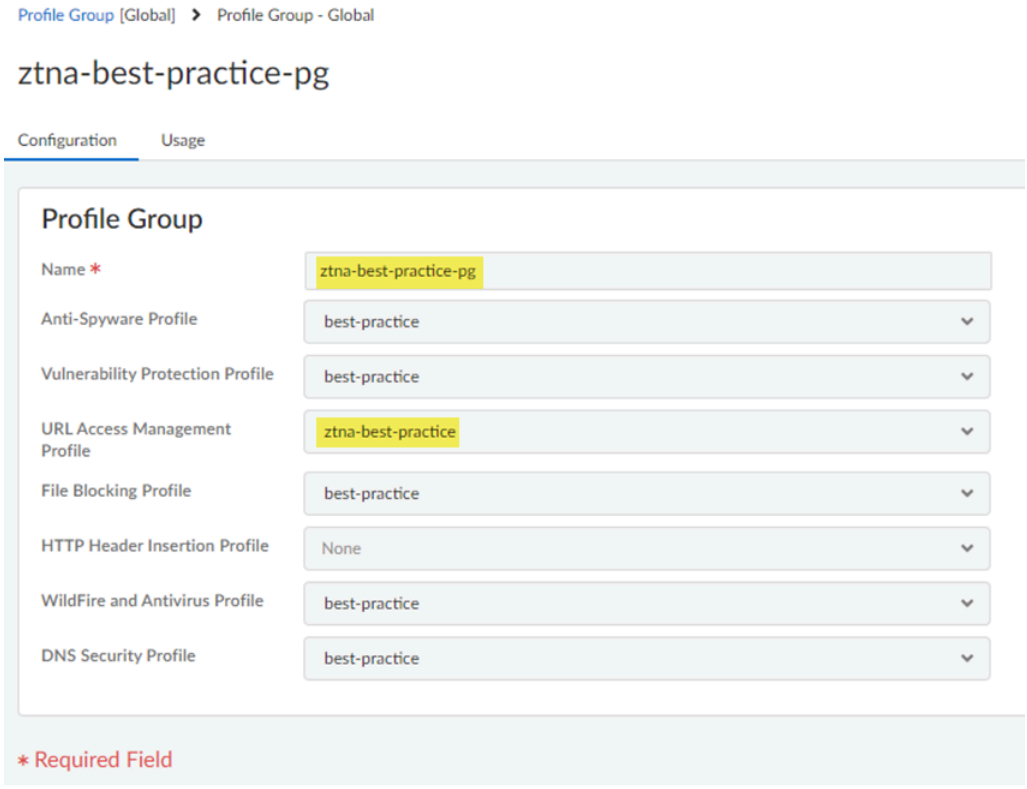
1. Wählen Sie im Bereich **URL-Zugriffsverwaltung** die Option **URL-Zugriffsverwaltung-Profile** aus.
2. Wählen Sie ein vorhandenes Profil aus, um es zu ändern, oder verwenden Sie **Profil hinzuzufügen**, um ein neues Profil hinzuzufügen.
3. Fügen Sie dem Profil die von Ihnen erstellte benutzerdefinierte URL-Kategorie hinzu.
4. Wählen Sie die folgenden Parameter aus:
   - **Standortzugriff**: Zulassen
   - **Übermittlung von Benutzeranmeldeinformationen**: Zulassen
5. **Speichern** Sie Ihre Änderungen.




 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Erstellen Sie eine Profilgruppe und fügen Sie der Gruppe das URL-Zugriffsverwaltungsprofil hinzu.

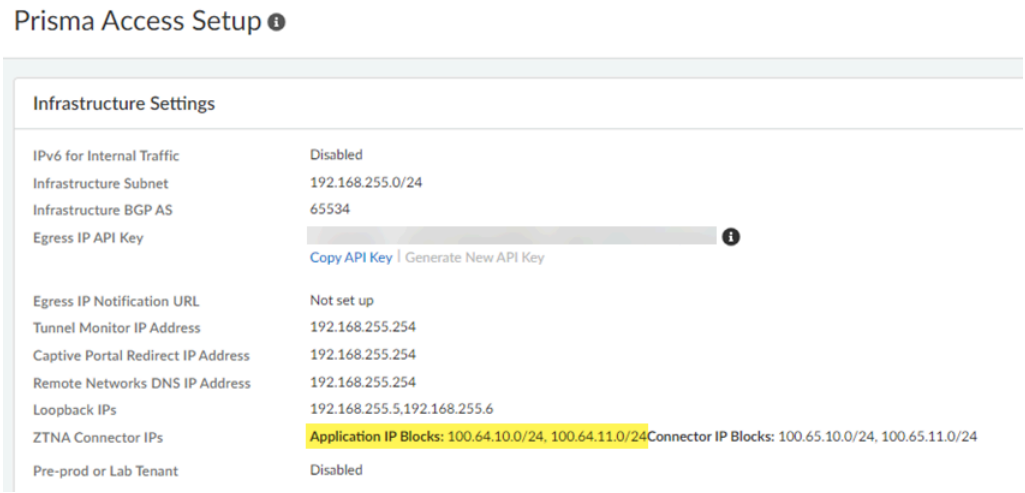
1. Rufen Sie **Konfiguration** > **NGFW und Prisma Access** > **Sicherheitsdienste** > **Profilgruppen** auf.
2. **Fügen Sie** eine Profilgruppe hinzu, die das von Ihnen erstellte URL-Zugriffsverwaltungs-Profil angibt.




 ©2025 Palo Alto Networks, Inc.

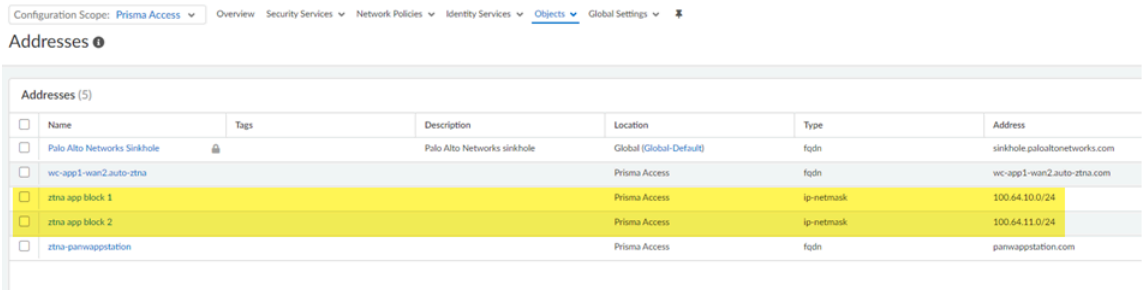
**STEP 4 |** Erstellen Sie eine Richtlinie, um die Profilgruppe und die IP-Adressen für die Anwendungs-IP-Blöcke von ZTNA-Connector zuzulassen.

1. Wählen Sie **Workflows** > **Prisma Access-Einrichtung** > **Prisma Access** > **Prisma Access-Einrichtung** aus und notieren Sie die **Anwendungs-IP-Blöcke** unter den IPs von ZTNA-Connector.

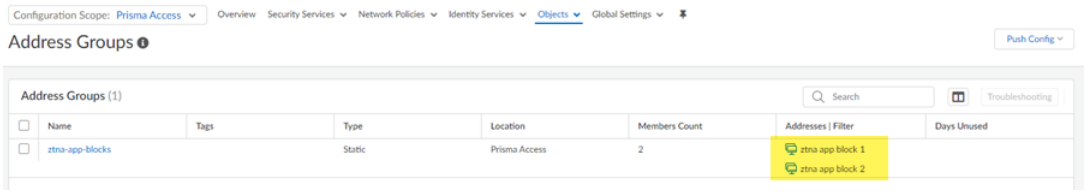



2. Rufen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Objekte** > **Adresse** > **Adressen** und dann **Hinzufügen** auf, um Adressobjekte basierend auf den abgerufenen IP-Adressen hinzuzufügen.

   Wenn Sie über IP-Subnetz-basierte Apps verfügen, erstellen Sie auch Adressobjekte für diese Subnetze.




3. Rufen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Objekte** > **Adresse** > **Adressgruppen** und dann **Hinzufügen** auf, um die von Ihnen erstellten Adressobjekte einer Adressgruppe hinzuzufügen.



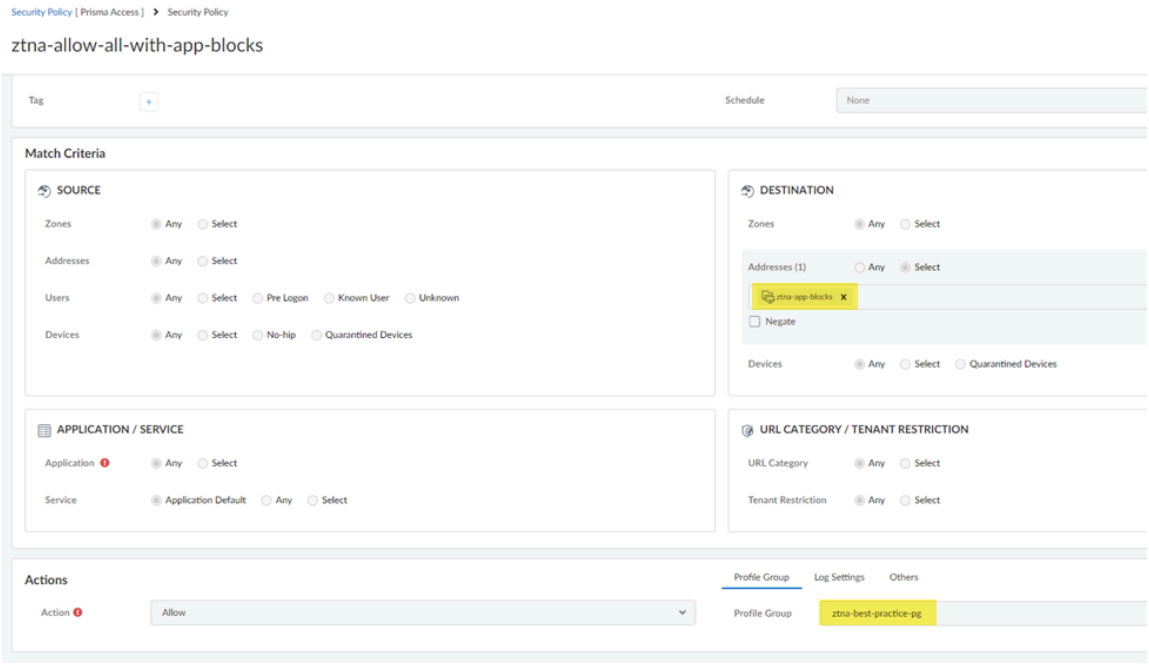

4. Wählen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Sicherheitsdienste** > **Sicherheitsrichtlinie** > **Vor-Regeln** und dann **Hinzufügen** aus, um eine Sicherheitsrichtlinie hinzuzufügen, mit der der Zugriff auf alle Anwendungs-IP-

 ©2025 Palo Alto Networks, Inc.

Adressblöcke zugelassen wird. Dabei werden die **Adressgruppe** und die **Profilgruppe** angegeben, die Sie in einem früheren Schritt erstellt haben.

Durch Hinzufügen dieser Sicherheitsrichtlinie kann der gesamte Datenverkehr aus platzhalterbasiertem App-Datenverkehr übergeben werden, während ZTNA-Connector die Apps basierend auf den Platzhaltern erkennt. Ohne die Regel, die Anwendungs-IP-Blöcke zuzulassen, können Benutzer nicht auf platzhalterbasierte Apps zugreifen.

Sie können diese Richtlinie beibehalten, bis ZTNA-Connector die platzhalterbasierten Apps erkennt. Anschließend können Sie diese Richtlinie deaktivieren und Sicherheitsrichtlinienregeln für jede der erkannten Apps hinzufügen.



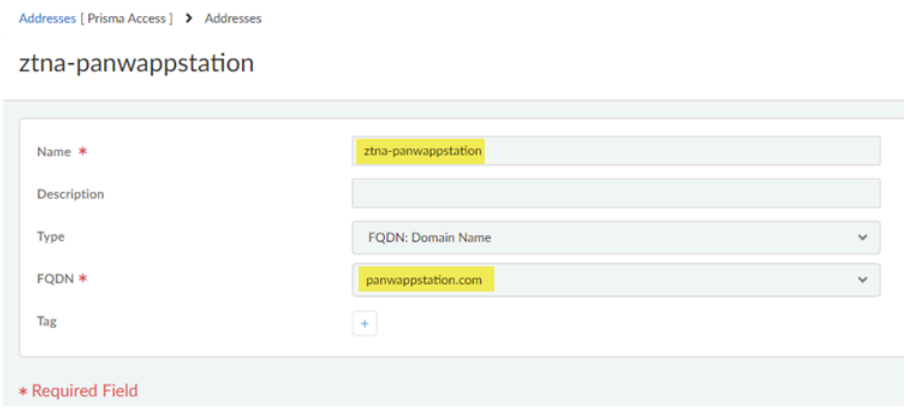

 ©2025 Palo Alto Networks, Inc.

**STEP 5 |** Nachdem ZTNA-Connector die Apps basierend auf Platzhaltern erkannt hat, konfigurieren Sie eine Sicherheitsrichtlinie für die Apps, die Sie mithilfe von FQDNs hinzugefügt haben.

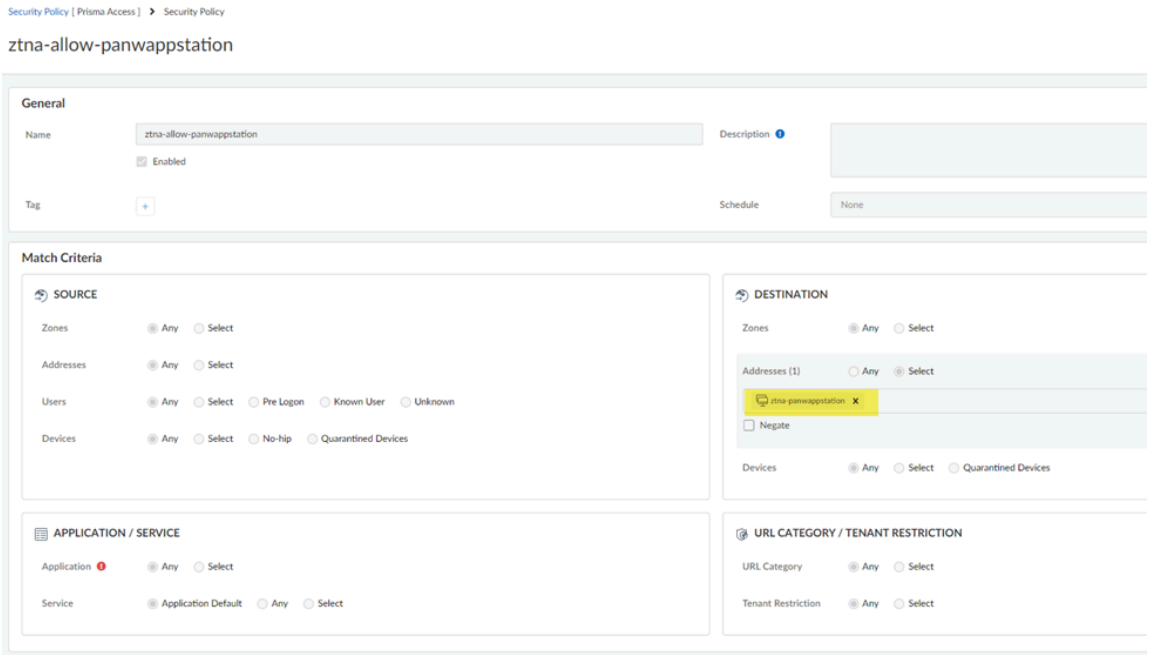
1. Rufen Sie dazu **Workflows** > **ZTNA-Connector** > **Anwendungsziele** > **FQDN-Ziele** auf und notieren Sie die von den Apps verwendeten FQDNs.
2. Erstellen Sie ein Adressobjekt für den FQDN (**Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Objekte** > **Adresse** > **Adressen**).

   Wählen Sie den Konfigurationsumfang **Prisma Access** aus.
3. Wählen Sie **Hinzufügen** aus, um ein Adressobjekt mit dem **Typ FQDN: Domänenname** hinzuzufügen, und geben Sie den **FQDN** der erkannten Anwendung ein.

   Geben Sie die FQDNs für die FQDN-Ziele ein.




4. Rufen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Sicherheitsdienste** > **Sicherheitsrichtlinie** > **Vor-Regeln** und dann **Hinzufügen** auf, um eine Sicherheitsrichtlinie hinzuzufügen, um den Zugriff auf die erkannten Apps zu ermöglichen.




 ©2025 Palo Alto Networks, Inc.

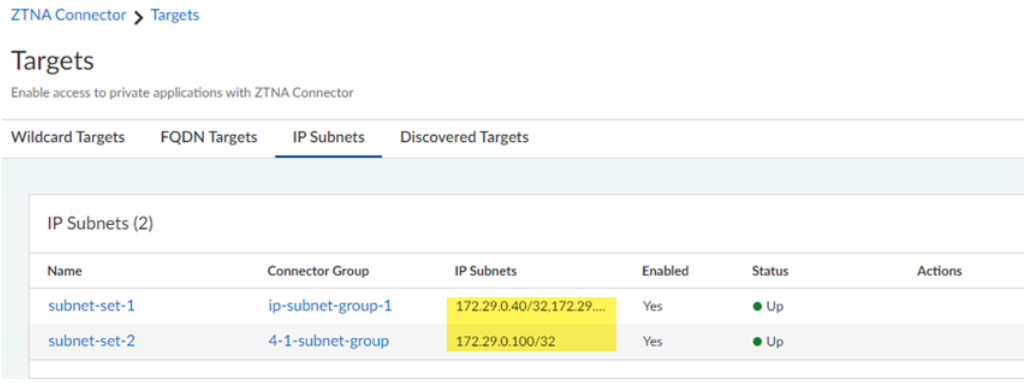
**STEP 6 |** Wählen Sie **Konfiguration übertragen** aus, um Ihre Konfigurationsänderungen zu speichern und zu übertragen.

**STEP 7 |** (Optional) Nachdem Sie die Sicherheitsrichtlinie auf Basis von FQDNs erstellt haben, entfernen Sie die Richtlinie auf Basis der IP-Anwendungsblöcke.

## Sicherheitsrichtlinie für Apps auf Basis des IP-Subnetzes

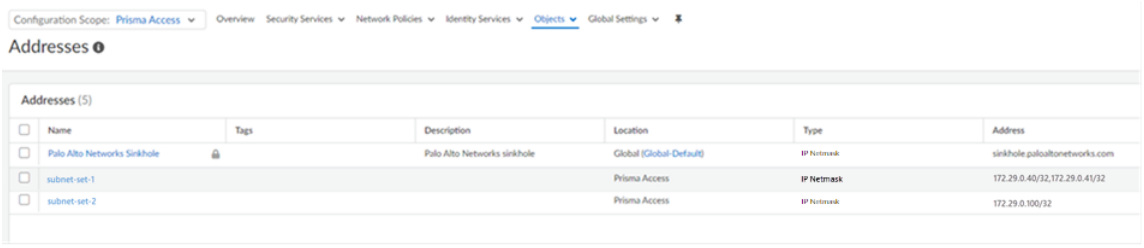
Wenn Sie ZTNA-Connector-Anwendungsziele basierend auf IP-Subnetzen erstellt haben (**Einstellungen** > **ZTNA-Connector** > **Konnektoren** > **Anwendungsziele** > **IP-Subnetze**), führen Sie die folgenden Schritte aus, um den Zugriff auf die Apps zuzulassen.

**STEP 1 |** Rufen Sie **Workflows** > **ZTNA-Connector** > **Anwendungsziele** > **IP-Subnetze** auf und notieren Sie die von den Apps verwendeten IP-Subnetze.

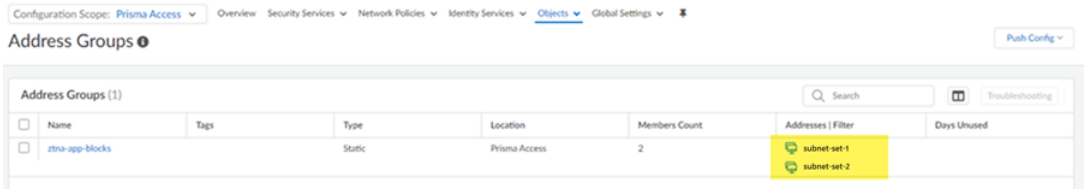



**STEP 2 |** Erstellen Sie eine Richtlinie, um die IP-Adressen für die IP-Subnetze zuzulassen, die für die Apps verwendet werden.

1. Rufen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Objekte** > **Adresse** > **Adressen** und dann **Hinzufügen** auf, um Adressobjekte basierend auf den abgerufenen IP-Adressen hinzuzufügen.



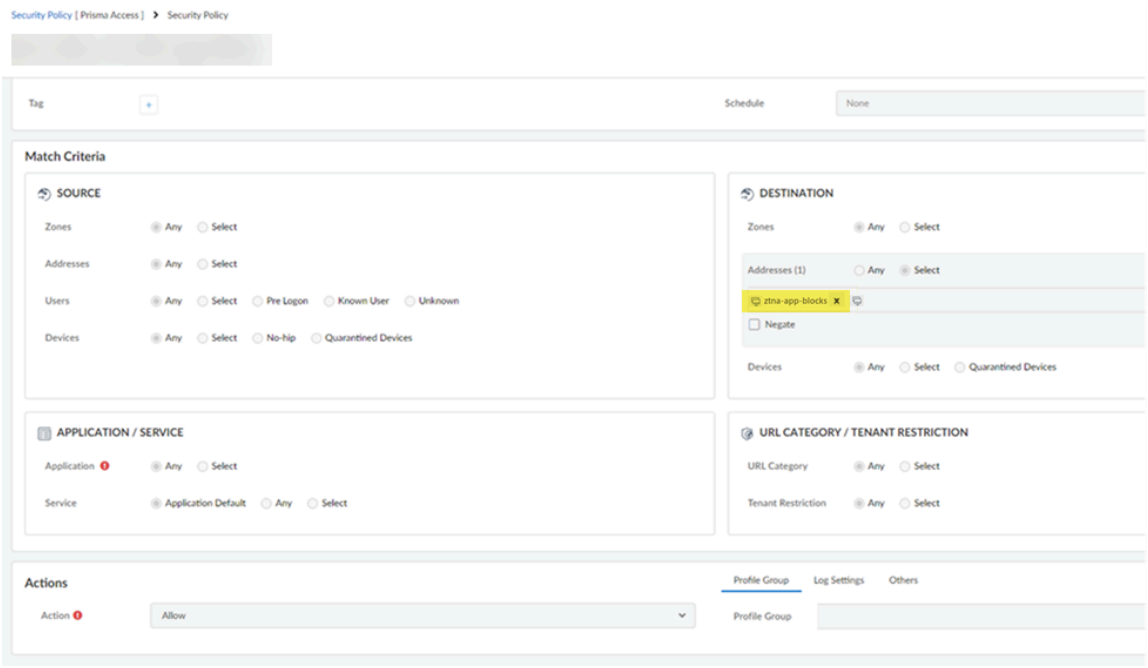

2. Rufen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Objekte** > **Adresse** > **Adressgruppen** und dann **Hinzufügen** auf, um die von Ihnen erstellten Adressen den Adressgruppen hinzuzufügen.




3. Wählen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Sicherheitsdienste** > **Sicherheitsrichtlinie** > **Vor-Regeln** und dann **Hinzufügen** aus,

 ©2025 Palo Alto Networks, Inc.

um eine Sicherheitsrichtlinie hinzuzufügen, um den Zugriff auf die IP-Subnetze für die Apps zu ermöglichen, wobei Sie die **Adressen** angeben, die Sie in einem früheren Schritt erstellt haben.




**STEP 3 |** Wählen Sie **Konfiguration übertragen** aus, um Ihre Konfigurationsänderungen zu speichern und zu übertragen.

## Sicherheitsrichtlinie für FQDN-basierte Apps

Wenn Sie Ziele basierend auf FQDNs hinzugefügt haben (**Einstellungen** > **ZTNA-Connector** > **Konnektoren** > **Anwendungsziele** > **FQDN-Ziele**), erstellen Sie ein Adressobjekt und eine Sicherheitsrichtlinie, um den Zugriff auf die Apps zu erlauben, indem Sie die folgenden Schritte ausführen.

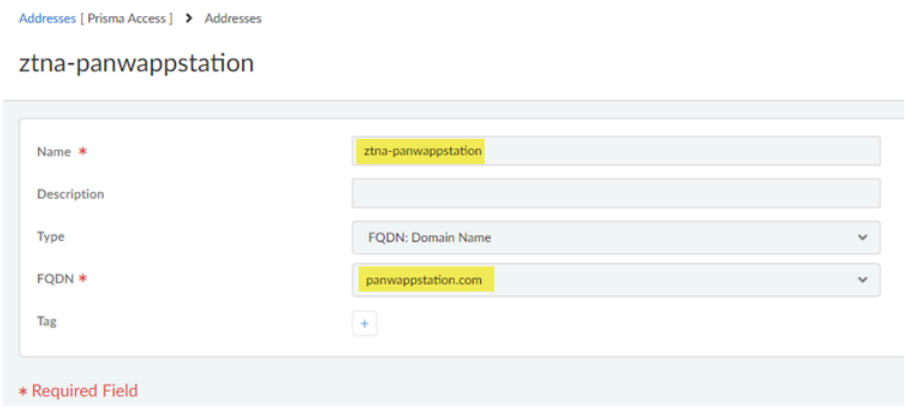
 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** Konfigurieren Sie eine Sicherheitsrichtlinie für die Apps, die Sie mithilfe von FQDNs hinzugefügt haben.

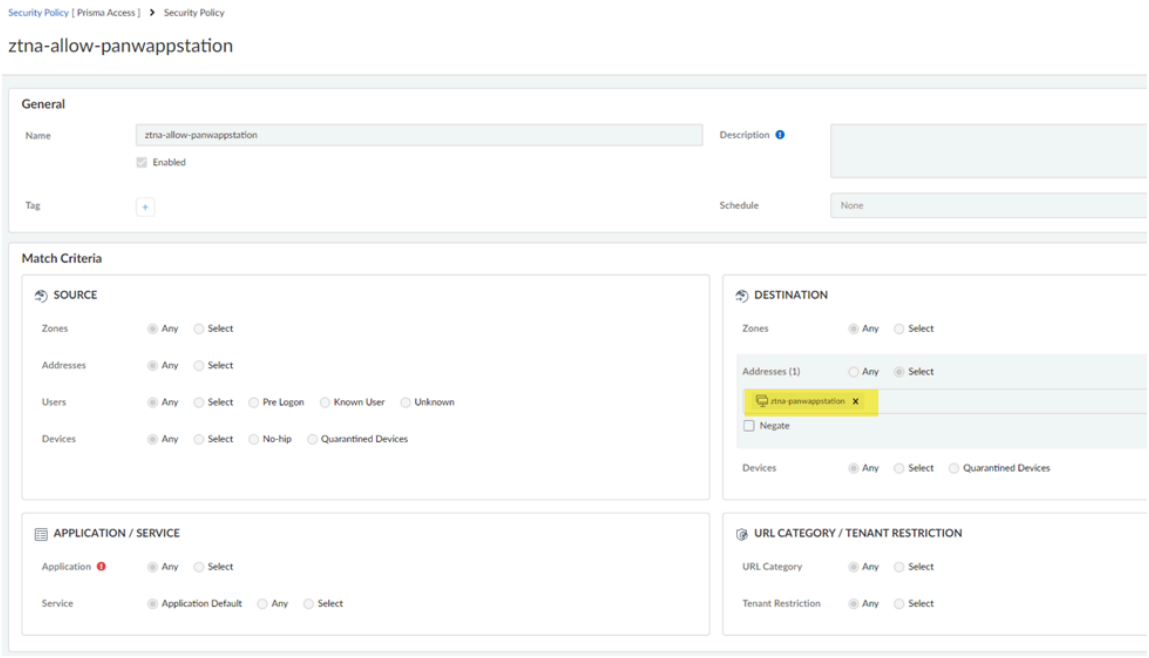
1. Rufen Sie dazu **Workflows** > **ZTNA-Connector** > **Anwendungsziele** > **FQDN-Ziele** auf und notieren Sie die von den Apps verwendeten FQDNs.
2. Erstellen Sie ein Adressobjekt für den FQDN (**Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Objekte** > **Adresse** > **Adressen**).

   Wählen Sie den Konfigurationsumfang **Prisma Access** aus.
3. Wählen Sie **Hinzufügen** aus, um ein Adressobjekt mit dem **Typ FQDN: Domänenname** hinzuzufügen, und geben Sie den **FQDN** der erkannten Anwendung ein.

   Geben Sie die FQDNs für alle erkannten Apps ein.




4. Optional Rufen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Sicherheitsdienste** > **Sicherheitsrichtlinie** > **Vor-Regeln** und **Hinzufügen** auf, um eine Sicherheitsrichtlinie hinzuzufügen, um den Zugriff auf die entdeckten Apps zu erlauben.




**STEP 2 |** Wählen Sie **Konfiguration übertragen** aus, um Ihre Konfigurationsänderungen zu speichern und zu übertragen.

 ©2025 Palo Alto Networks, Inc.

# Sicherheitsrichtlinie für Apps mit ZTNA-Connector-Aktivierung (Panorama)

Nachdem Sie Apps in ZTNA-Connector eingebunden haben, sollten Sie Richtlinienregeln einrichten, um den Zugriff für diese Apps zuzulassen und zu steuern. Das Verfahren zum Erstellen und Anwenden von Richtlinien unterscheidet sich abhängig davon, ob Ihre Apps durch Platzhalter, IP-Subnetze oder FQDNs definiert wurden.

## Sicherheitsrichtlinie für platzhalterbasierte Apps

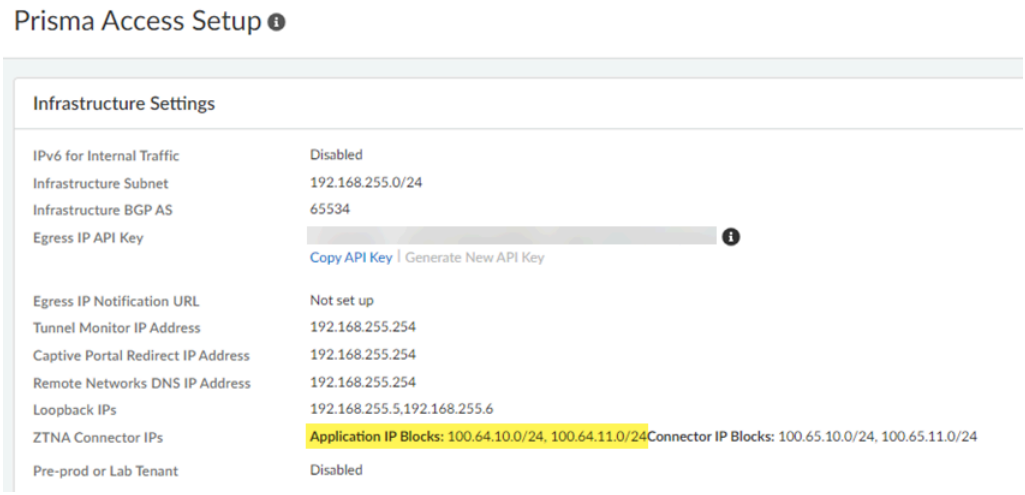
Für platzhalterbasierte Apps (**Einstellungen** > **ZTNA-Connector** > **Anwendungsziele** > **Platzhalterziele**) müssen Sie eine benutzerdefinierte URL-Kategorie erstellen. Dieser Kategorietyp setzt jedoch nur Richtlinien für HTTP- und HTTPS-Datenverkehr durch, wohingegen anderer Datenverkehr (wie SSH) nicht zulässig ist. Aus diesem Grund müssen Sie den Zugriff auf alle Apps vorübergehend zulassen, indem Sie den Datenverkehr über die Anwendungs-IP-Blöcke von ZTNA-Connector zulassen.

Nachdem ZTNA-Connector die FQDNs abgefragt hat, die auf Platzhaltern basieren, können Sie die Richtlinie deaktivieren, die den Datenverkehr über die Anwendungs-IP-Blöcke zulässt, und die Richtliniendurchsetzung basierend auf den abgefragten FQDNs anwenden.

 ©2025 Palo Alto Networks, Inc.

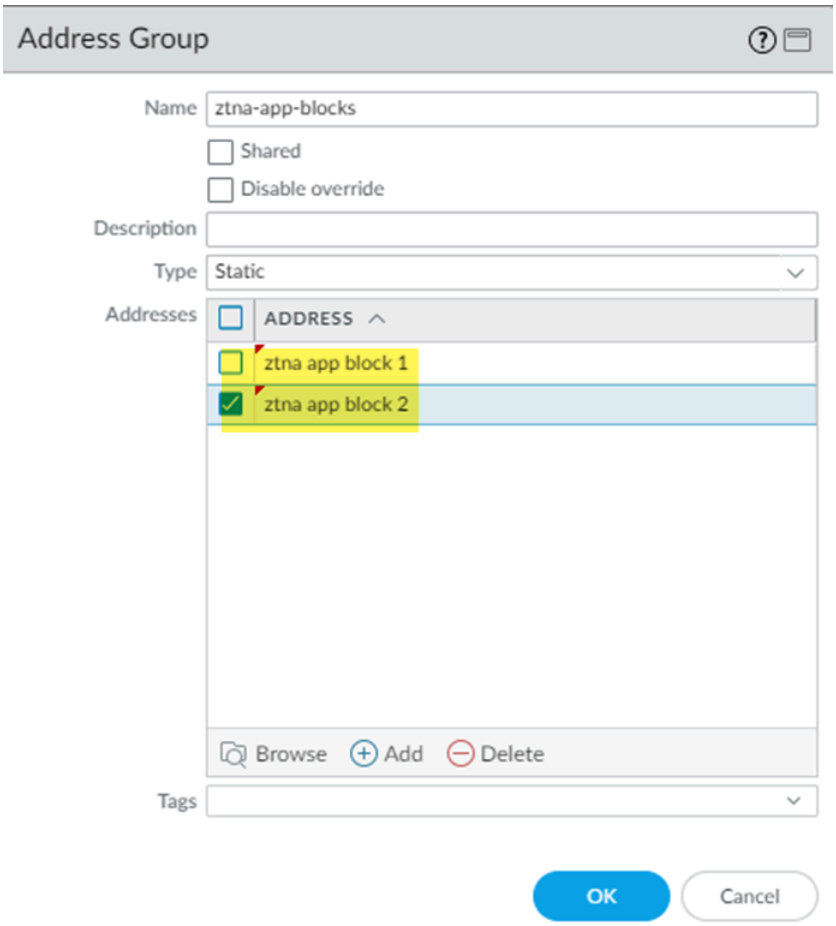
**STEP 1 |** Erstellen Sie eine Richtlinie, um die IP-Adressen für die Anwendungs-IP-Blöcke von ZTNA-Connector zuzulassen.

1. Wählen Sie in der Benutzeroberfläche von ZTNA-Connector **Workflows** > **Prisma Access-Einrichtung** > **Prisma Access** > **Prisma Access-Einrichtung** aus und notieren Sie die **Anwendungs-IP-Blöcke** unter den IPs von ZTNA-Connector.




2. Rufen Sie **Objekte** > **Adressen** und dann **Hinzufügen** auf, um Adressobjekte basierend auf den von Ihnen abgerufenen IP-Adressen hinzuzufügen.
3. Wählen Sie **Objekte** > **Adressgruppen** und dann **Hinzufügen** aus, um die von Ihnen erstellten Adressobjekte einer Adressgruppe hinzuzufügen.

 ©2025 Palo Alto Networks, Inc.



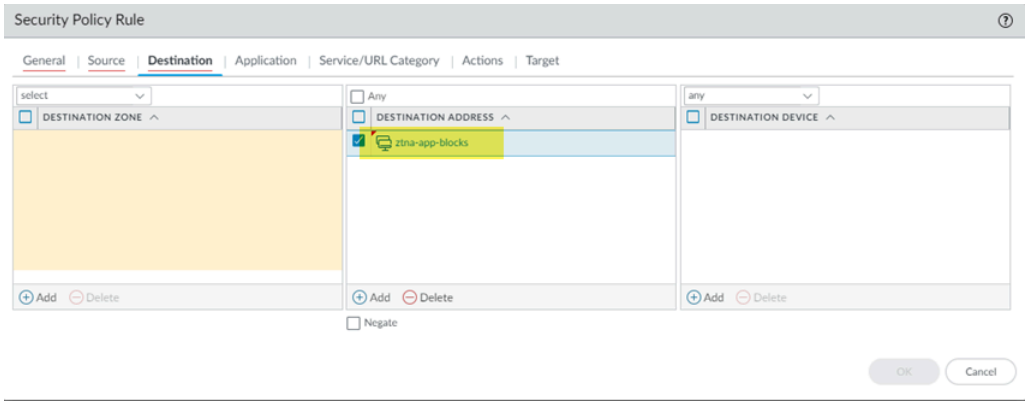

4. Wählen Sie **Richtlinien** > **Sicherheit** > **Vor-Regeln** und dann **Hinzufügen** aus, um eine Sicherheitsrichtlinie hinzuzufügen, um den Zugriff auf alle Anwendungs-IP-Adressblöcke zu erlauben, wobei Sie die **Adressgruppe** angeben, die Sie in einem früheren Schritt erstellt haben.

   Durch Hinzufügen dieser Sicherheitsrichtlinie kann der gesamte Datenverkehr aus platzhalterbasiertem App-Datenverkehr übergeben werden, während ZTNA-Connector

 ©2025 Palo Alto Networks, Inc.

die Apps basierend auf den Platzhaltern erkennt. Ohne die Regel, die Anwendungs-IP-Blöcke zuzulassen, können Benutzer nicht auf platzhalterbasierte Apps zugreifen.

Sie können diese Richtlinie beibehalten, bis ZTNA-Connector die platzhalterbasierten Apps erkennt. Anschließend können Sie diese Richtlinie deaktivieren und Sicherheitsrichtlinienregeln für jede der erkannten Apps hinzufügen.




**STEP 2 |** Nachdem ZTNA-Connector die Apps basierend auf Platzhaltern erkannt hat, konfigurieren Sie eine Sicherheitsrichtlinie für die Apps, die Sie mithilfe von FQDNs hinzugefügt haben.

1. Rufen Sie dazu **Workflows** > **ZTNA-Connector** > **Anwendungsziele** > **FQDN-Ziele** auf und notieren Sie die von den Apps verwendeten FQDNs.
2. Erstellen Sie ein Adressobjekt für den FQDN (**Objekte** > **Adressen**).

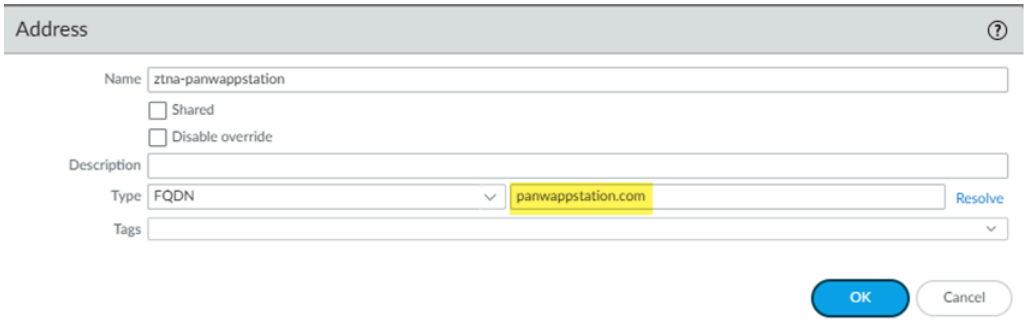
   Wählen Sie entweder die Gerätegruppe **Mobile_User_Device_Group** oder **Remote_Network_Device_Group** aus. Die Auswahl ist davon abhängig, ob mobile

 ©2025 Palo Alto Networks, Inc.

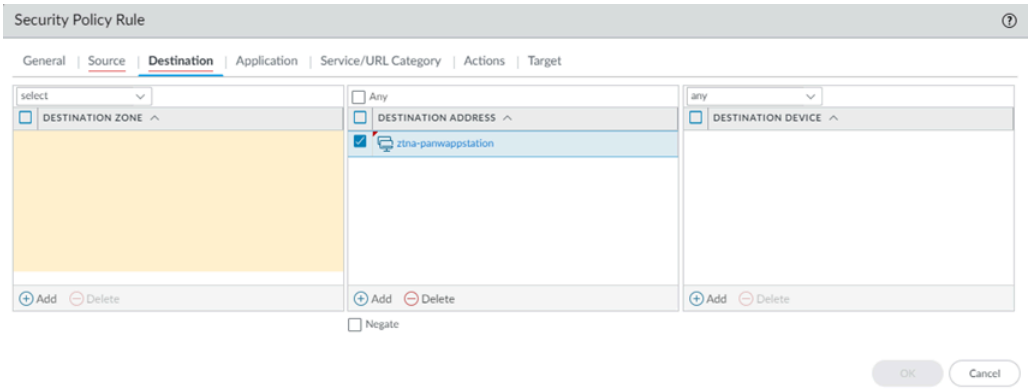
Benutzer oder Benutzer an Zweigstellenstandorten auf die privaten Apps hinter ZTNA-Connector zugreifen werden.

3. **Fügen Sie** ein Adressobjekt mit dem **Typ** des **FQDN** hinzu und geben Sie den **FQDN** der erkannten Anwendung ein.

   Geben Sie die FQDNs für die FQDN-Ziele ein.




4. Rufen Sie **Richtlinien** > **Sicherheit** > **Vor-Regeln** und dann **Hinzufügen** auf, um eine Sicherheitsrichtlinie hinzuzufügen, um den Zugriff auf die erkannten Apps zu erlauben.




**STEP 3 |** Führen Sie für Ihre Änderungen die Aktion **Commit und Push** aus.

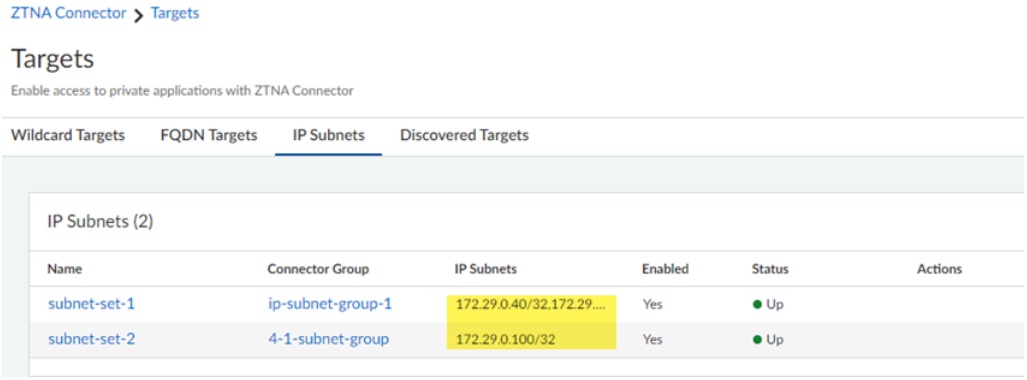
**STEP 4 |** (Optional) Nachdem Sie die Sicherheitsrichtlinie auf Basis von FQDNs erstellt haben, entfernen Sie die Richtlinie auf Basis der IP-Anwendungsblöcke.

## Sicherheitsrichtlinie für Apps auf Basis des IP-Subnetzes

Wenn Sie ZTNA-Connector-Anwendungsziele basierend auf IP-Subnetzen erstellt haben (**Einstellungen** > **ZTNA-Connector** > **Konnektoren** > **Anwendungsziele** > **IP-Subnetze**), führen Sie die folgenden Schritte aus, um den Zugriff auf die Apps zuzulassen.

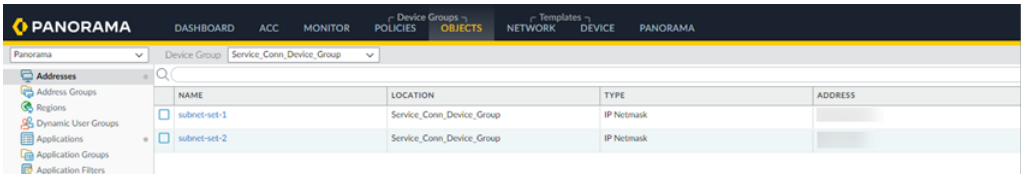

©2025 Palo Alto Networks, Inc.

**STEP 1 |** Rufen Sie **Workflows** > **ZTNA-Connector** > **Anwendungsziele** > **IP-Subnetze** auf und notieren Sie die von den Apps verwendeten IP-Subnetze.

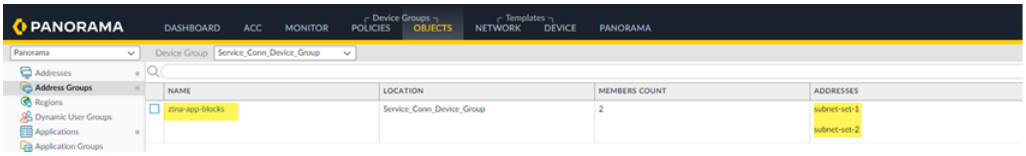



**STEP 2 |** Erstellen Sie eine Richtlinie, um die IP-Adressen für die IP-Subnetze zuzulassen, die für die Apps verwendet werden.

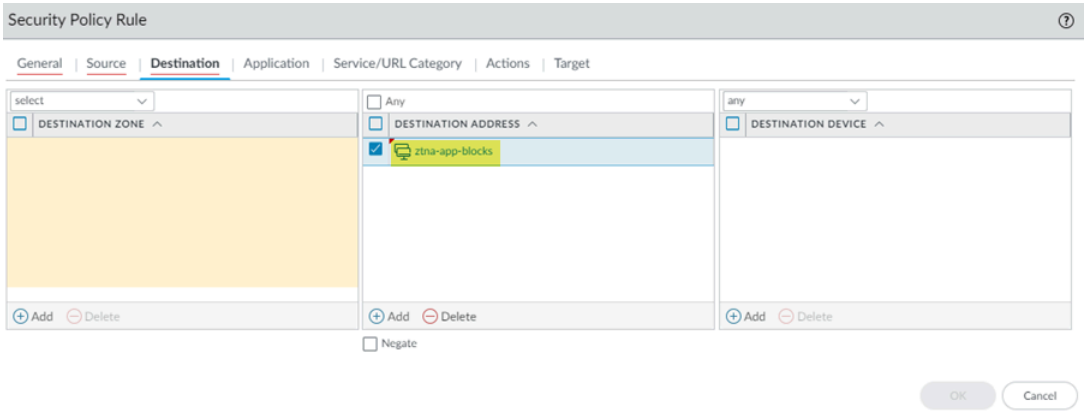
1. Rufen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Objekte** > **Adresse** > **Adressen** und dann **Hinzufügen** auf, um Adressobjekte basierend auf den abgerufenen IP-Adressen hinzuzufügen.




2. Wählen Sie **Objekte** > **Adressgruppen** und dann **Hinzufügen** aus, um die von Ihnen erstellten Adressen den Adressgruppen hinzuzufügen.




3. Wählen Sie **Richtlinien** > **Sicherheit** > **Vor-Regeln** und dann **Hinzufügen** aus, um eine Sicherheitsrichtlinie hinzuzufügen, um den Zugriff auf die IP-Subnetze für die Apps zu erlauben, wobei Sie die **Adressen** angeben, die Sie in einem früheren Schritt erstellt haben.




 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Wählen Sie **Konfiguration übertragen** aus, um Ihre Konfigurationsänderungen zu speichern und zu übertragen.

## Sicherheitsrichtlinie für FQDN-basierte Apps

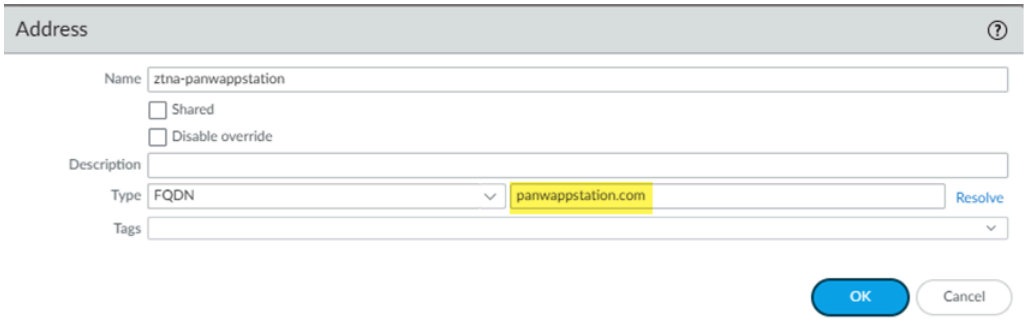
Wenn Sie Ziele basierend auf FQDNs hinzugefügt haben (**Einstellungen** > **ZTNA-Connector** > **Konnektoren** > **Anwendungsziele** > **FQDN-Ziele**), erstellen Sie ein Adressobjekt und eine Sicherheitsrichtlinie, um den Zugriff auf die Apps zu erlauben, indem Sie die folgenden Schritte ausführen.

**STEP 1 |** Konfigurieren Sie eine Sicherheitsrichtlinie für die Apps, die Sie mithilfe von FQDNs hinzugefügt haben.

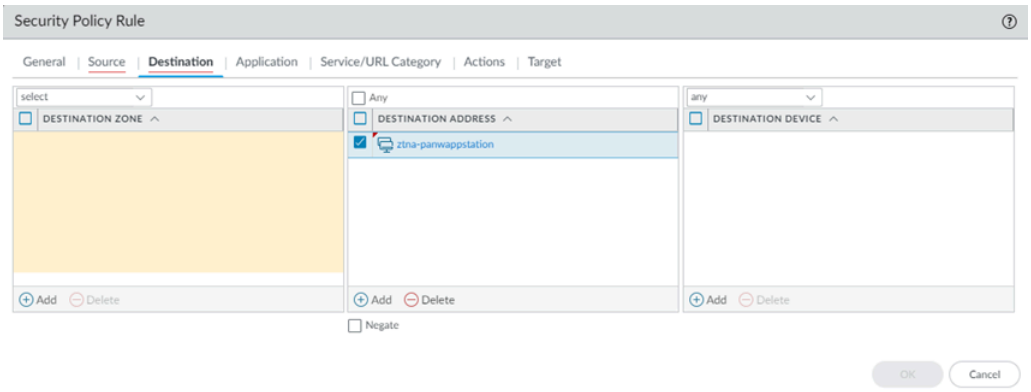
1. Rufen Sie dazu **Workflows** > **ZTNA-Connector** > **Anwendungsziele** > **FQDN-Ziele** auf und notieren Sie die von den Apps verwendeten FQDNs.
2. Erstellen Sie ein Adressobjekt für den FQDN (**Objekte** > **Adressen**).

   Wählen Sie entweder die Gerätegruppe **Mobile_User_Device_Group** oder **Remote_Network_Device_Group** aus. Die Auswahl ist davon abhängig, ob mobile Benutzer oder Benutzer an Zweigstellenstandorten auf die privaten Apps hinter ZTNA-Connector zugreifen werden.
3. **Fügen Sie** ein Adressobjekt mit dem **Typ** des **FQDN** hinzu und geben Sie den **FQDN** der erkannten Anwendung ein.

   Geben Sie die FQDNs für alle erkannten Apps ein.




4. Optional Rufen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Sicherheitsdienste** > **Sicherheitsrichtlinie** > **Vor-Regeln** und **Hinzufügen** auf, um eine Sicherheitsrichtlinie hinzuzufügen, um den Zugriff auf die entdeckten Apps zu erlauben.




 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Wählen Sie **Konfiguration übertragen** aus, um Ihre Konfigurationsänderungen zu speichern und zu übertragen.

 ©2025 Palo Alto Networks, Inc.

# ZTNA-Connector-VM in Ihr Rechenzentrum einbinden

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access Version 4.0<br>❑ ZTNA-Connector-Add-on-Lizenz<br>Die Essential-Lizenz mit der Add-on-Lizenz umfasst acht ZTNA-Connectors, 100 FQDNs und vier IP-Subnetzfunktionen.<br>Die Advanced-Lizenz mit der Add-on-Lizenz umfasst 40 ZTNA-Connectors, 300 FQDNs und 1.024 IP-Subnetzfunktionen.<br>Die Premiumlizenz mit der Add-on-Lizenz umfasst 200 ZTNA-Connectors, 4.000 FQDNs und 1.024 IP-Subnetzfunktionen.<br>❑ Wenn Sie die ZTNA-Connector-Add-on-Lizenz nicht erwerben, beinhalten die Prisma Access-Lizenzen vier Konnektoren, 40 FQDNs und vier IP-Subnetze. Diese Funktionalität wird bereitgestellt, um ZTNA-Connectors in Ihrer Umgebung zu testen. |

Nachdem Sie Ihre Konnektorgruppen, Konnektoren und Anwendungsziele in Prisma Access konfiguriert haben, müssen Sie die Connector-VM in Ihrem Rechenzentrum bereitstellen. Um das Onboarding von Konnektoren zu vereinfachen, sind Bereitstellungsvorlagen für jede Rechenzentrumsumgebung im Kunden-Support-Portal von Palo Alto Networks oder auf dem Cloud-Anbieter-Marktplatz verfügbar. Welche Vorlage Sie verwenden, hängt davon ab, ob Sie eine einarmige Bereitstellung oder eine zweiarmige Bereitstellung verwenden.

## Unterstützte ZTNA-Connector-Bereitstellungen

ZTNA-Connector initiiert die Verbindung zur öffentlichen IP-Adresse von Prisma Access in der Cloud, und Sie müssen keine Sicherheitsregeln für die Eingangsfirewall definieren. Da ZTNA-Connector die Verbindung jedoch initiiert, müssen Sie Ausgangsregeln hinzufügen, um ZTNA-Connector den Zugriff auf den Cloud-Controller und die IPSec-Verbindung zur Prisma Access-Dataplane zu gewähren. ZTNA-Connector leitet die Verbindung zur öffentlichen IP-Adresse von Prisma Access in der Cloud ein. Aus diesem Grund benötigen Sie die folgenden Ausgangsregeln, damit ZTNA-Connector einen IPSec-Tunnel zu Prisma Access erstellen kann:

- **Mit dem Internet verbunden** – Ausgehenden Datenverkehr für HTTPS (TCP 443) und IKE/IPSec (UDP 500 und 4500) zulassen.


©2025 Palo Alto Networks, Inc.

- **Mit dem Rechenzentrum verbunden** – Ausgehende Anwendungsports zulassen.

  Lassen Sie z. B. die Ausgangsanwendungsports HTTP (80) und HTTPS (443) zu. Bei diesen Beispielports handelt es sich um TCP-Ports. Wenn Ihr Rechenzentrum andere Ports verwendet, lassen Sie stattdessen diese Ports zu.

Sie können die Connector-VM in den folgenden Bereitstellungstopologien bereitstellen:

- **Einarmige Bereitstellung**

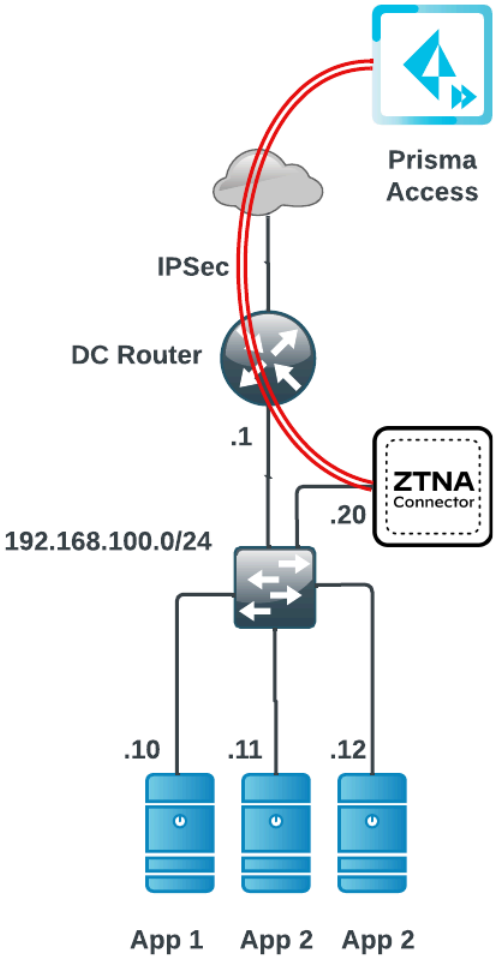
  *Einarmige Bereitstellungen werden nur in cloudnativen Umgebungen wie AWS, Azure oder GCP unterstützt. Für lokale Bereitstellungen wie ESXi oder eine Kernel-basierte virtuelle Maschine (KVM) oder Microsoft Hyper-V verwenden Sie die zweiarmige Bereitstellung.*

  In dieser Bereitstellung befindet sich Ihr ZTNA-Connector im Subnetz eines privaten Rechenzentrums mit Zugriff auf das Internet über einen Router im Rechenzentrum. Der

 ©2025 Palo Alto Networks, Inc.

Zugriff auf Anwendungen kann entweder lokal im selben Subnetz oder über den Router des Rechenzentrums erfolgen.

Im folgenden Diagramm ist eine Beispielbereitstellung des ZTNA-Connector-Netzwerks dargestellt, die eine einarmige Bereitstellung verwendet.




- **Zweiarmige Bereitstellung**

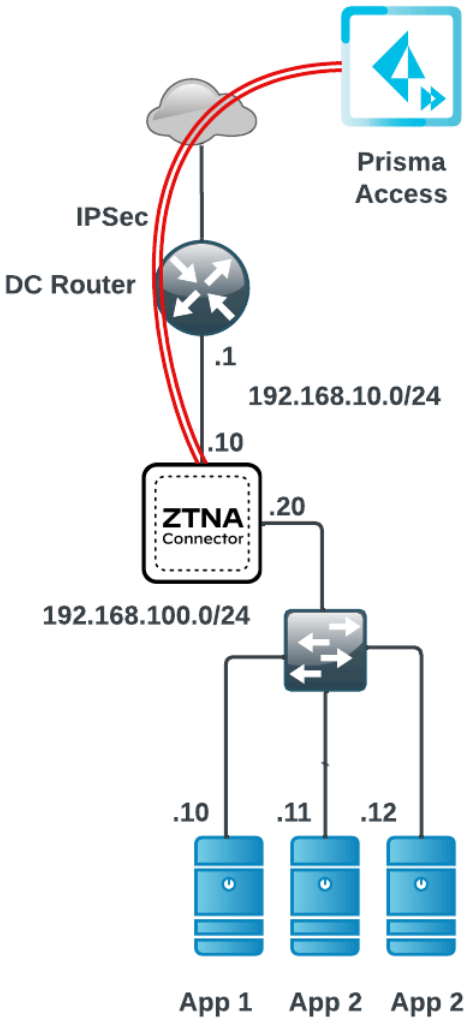
  Wenn Sie mehr Kontrolle über Ihre Sicherheitsregeln für ein- und ausgehenden Datenverkehr haben möchten oder wenn bei Ihnen eine lokale VM-Bereitstellung vorliegt, können Sie eine

 ©2025 Palo Alto Networks, Inc.

zweiarmige Bereitstellung verwenden, bei der eine Schnittstelle mit dem Internet und die andere mit dem Rechenzentrum verbunden ist.

*Wenn Sie IP-Adressen auf einem zweiarmigen Konnektor einrichten, stellen Sie sicher, dass Sie die IP-Adresszuweisungen für ZTNA-Connector ordnungsgemäß eingerichtet haben, bevor Sie die VM einschalten. Im folgenden Beispieldiagramm werden z. B. die IP-Adressen 192.168.10.10 und 192.168.10.20 verwendet. Richten Sie anhand dieser Beispieladressen die Ports auf ZTNA-Connector für 192.168.10.10 und 192.168.100.20 ein, da Prisma Access sonst die Apps im Rechenzentrum nicht über ZTNA-Connector erreichen kann. 192.168.10.10 und 192.168.100.20 sind Beispiel-IP-Adressen, und Sie müssen diese IP-Adressen nicht verwenden, damit die Bereitstellung funktioniert.*

Im folgenden Diagramm ist eine Beispielbereitstellung eines ZTNA-Connector-Netzwerks dargestellt, die eine zweiarmige Bereitstellung verwendet.

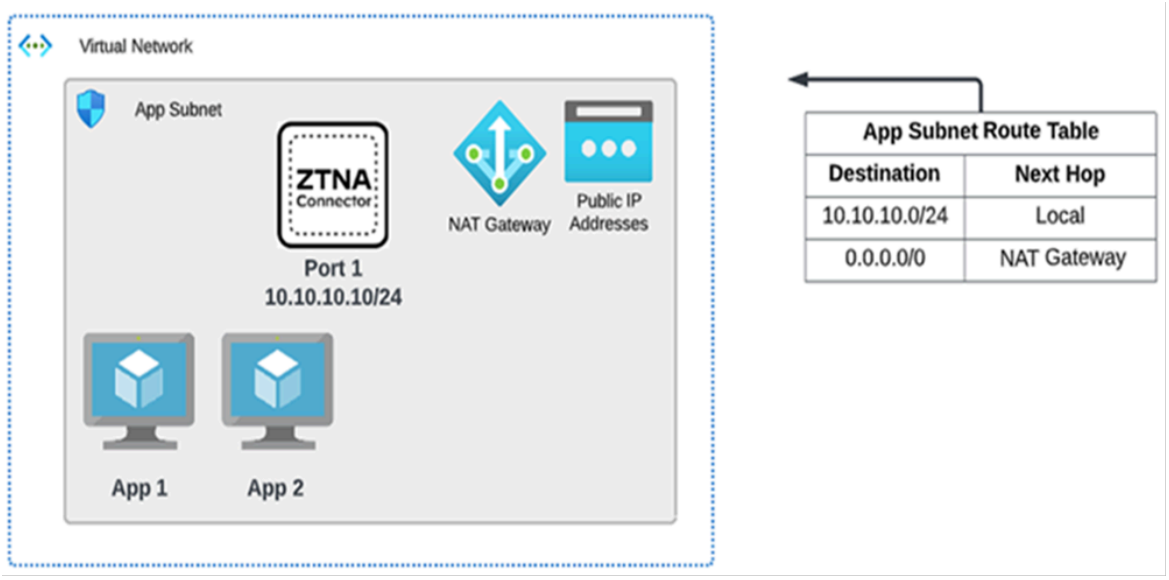



 ©2025 Palo Alto Networks, Inc.

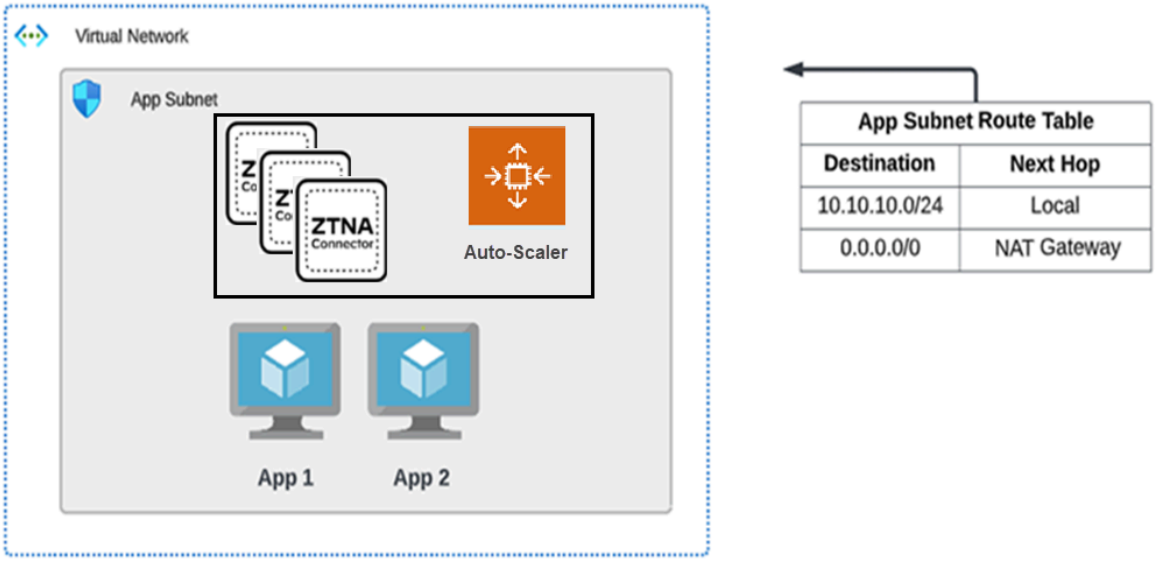
# Microsoft Azure-Bereitstellungen, die von ZTNA-Connector unterstützt werden

Die Prisma Access ZTNA-Connector-Netzwerkbereitstellung in Microsoft Azure unterstützt zwei Bereitstellungen und eine entsprechende Vorlage für jede Bereitstellung.

Im folgenden Diagramm ist eine Beispielbereitstellung für Prisma Access ZTNA-Connector in Azure dargestellt, die den einarmigen Modus mit NAT-Gateway verwendet.

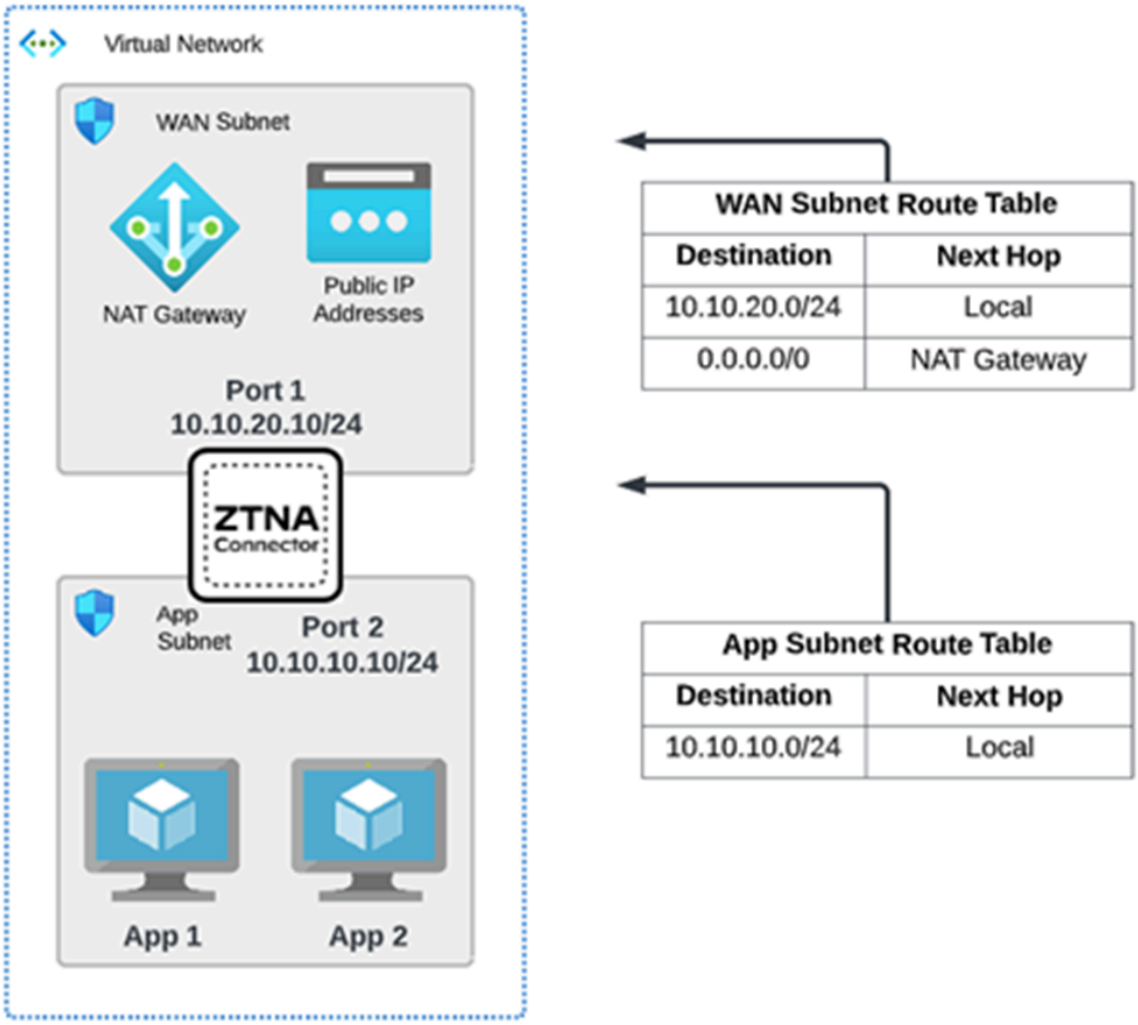



Im folgenden Diagramm ist eine Beispielbereitstellung für ZTNA-Connector in AWS dargestellt, die die einarmige Autoskalierung mit einem NAT-Gateway verwendet.



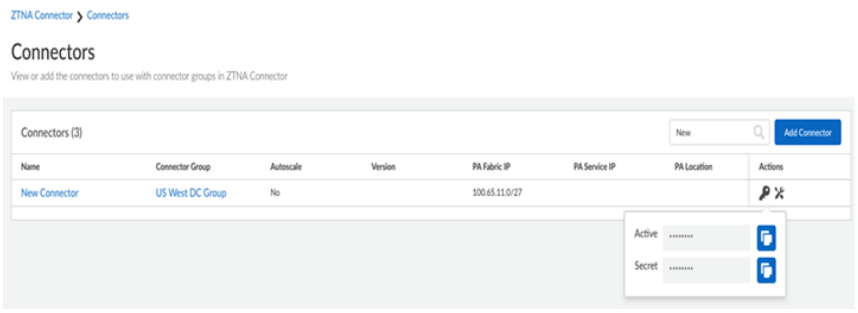

Im folgenden Diagramm ist eine Beispielbereitstellung für Prisma Access ZTNA-Connector in Azure dargestellt, die den zweiarmigen Modus mit einem NAT-Gateway verwendet.

 ©2025 Palo Alto Networks, Inc.



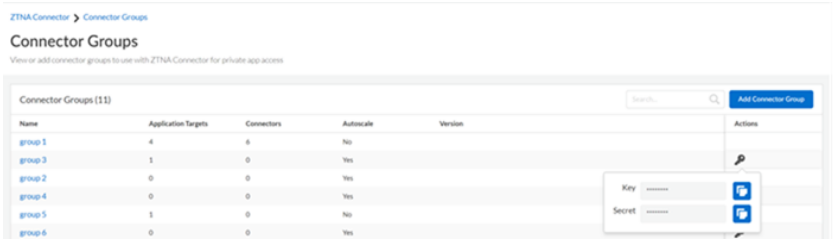

## ZTNA-Connector in Microsoft Azure einbinden

- Überprüfen Sie die Anforderungen und Richtlinien sowie die FQDNs und Ports, die Sie konfigurieren müssen, um ZTNA-Connector in Microsoft Azure zu verwenden.
- Rufen Sie auf der Prisma SASE-Plattform die Werte für den Schlüssel und den geheimen Schlüssel des Konnektors ab und kopieren Sie diese: Wählen Sie **Workflows** > **ZTNA-Connector** > **Konnektoren** aus, suchen Sie nach dem Konnektorobjekt, das Sie in Prisma Access erstellt haben, um es mit dieser VM zu verknüpfen, und wählen Sie **Token kopieren** aus. Kopieren Sie anschließend die Werte für **Schlüssel** und **Geheimer Schlüssel**.




 ©2025 Palo Alto Networks, Inc.

- Für die Bereitstellung **Prisma Access ZTNA-Connector – einarmig, Autoskalierung** müssen Sie die Werte für den Schlüssel und den geheimen Schlüssel der Konnektorgruppe abrufen und kopieren: Wählen Sie **Workflows** > **ZTNA-Connector** > **Konnektorgruppen** aus, suchen Sie nach dem Konnektorgruppen-Objekt, das Sie in Prisma Access erstellt haben, um es mit dieser VM zu verknüpfen, und wählen Sie **Token kopieren** aus. Kopieren Sie anschließend den **Schlüssel** und den **geheimen Schlüssel**.




Nachdem Sie alle Voraussetzungen erfüllt haben, gehen Sie wie folgt vor, um einen ZTNA Connector in Microsoft Azure einzubinden.

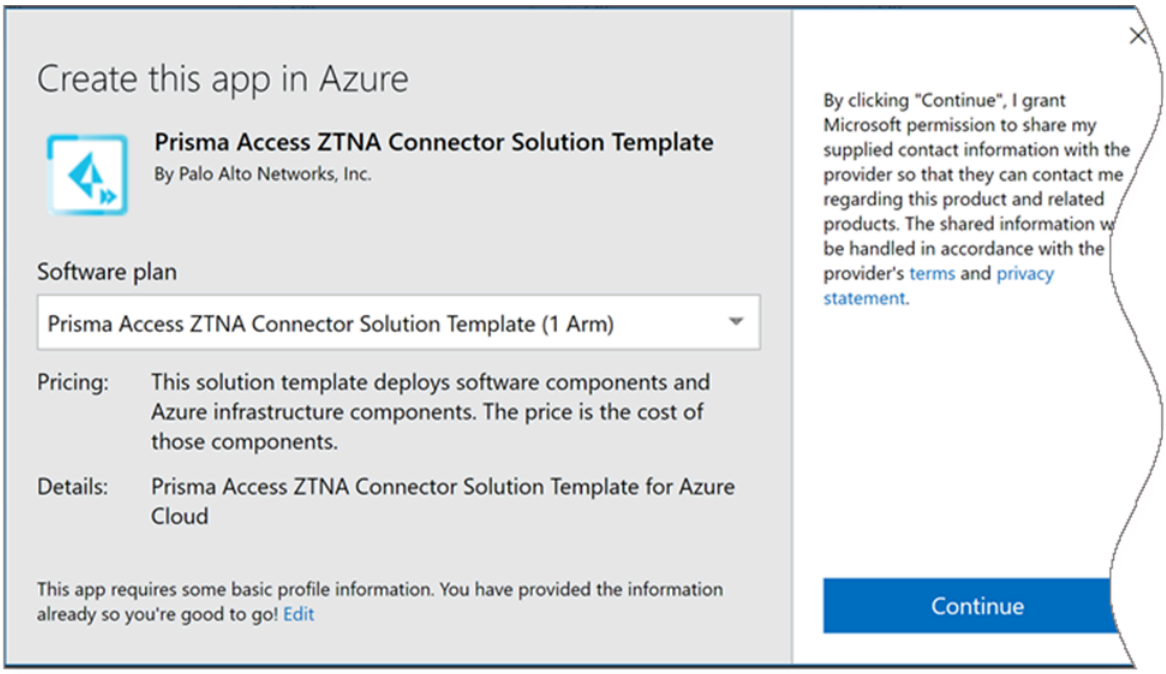
**STEP 1 |** Melden Sie sich bei Azure Marketplace an und suchen Sie nach **Prisma Access ZTNA-Connector**.

**STEP 2 |** Klicken Sie auf **Jetzt abrufen**.



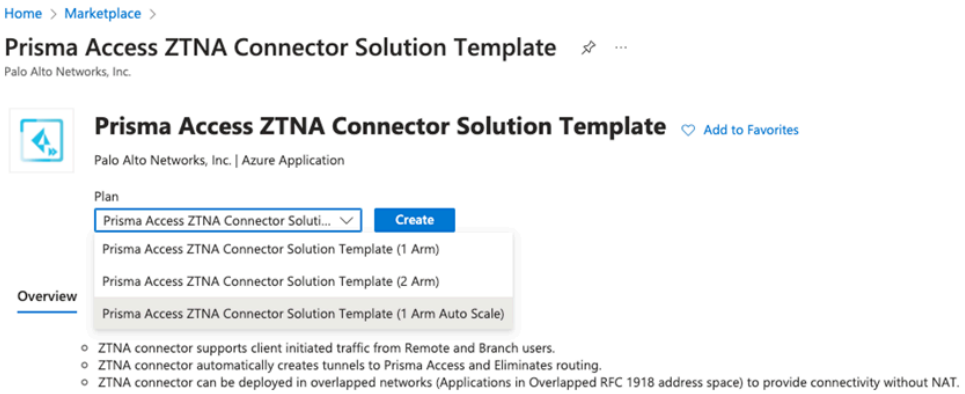

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Wählen Sie **Weiter** aus, um mit dem Erstellen fortzufahren.




**STEP 4 |** Wählen Sie den Softwareplan aus und wählen Sie **Erstellen** aus, um diese Anwendung in Azure zu erstellen:

- Vorlage für die Prisma Access ZTNA-Connector-Lösung (einarmig)
- Einarmigen ZTNA-Connector mit Autoskalierung in Microsoft Azure bereitstellen
- Vorlage für die Prisma Access ZTNA-Connector-Lösung (zweiarmig)



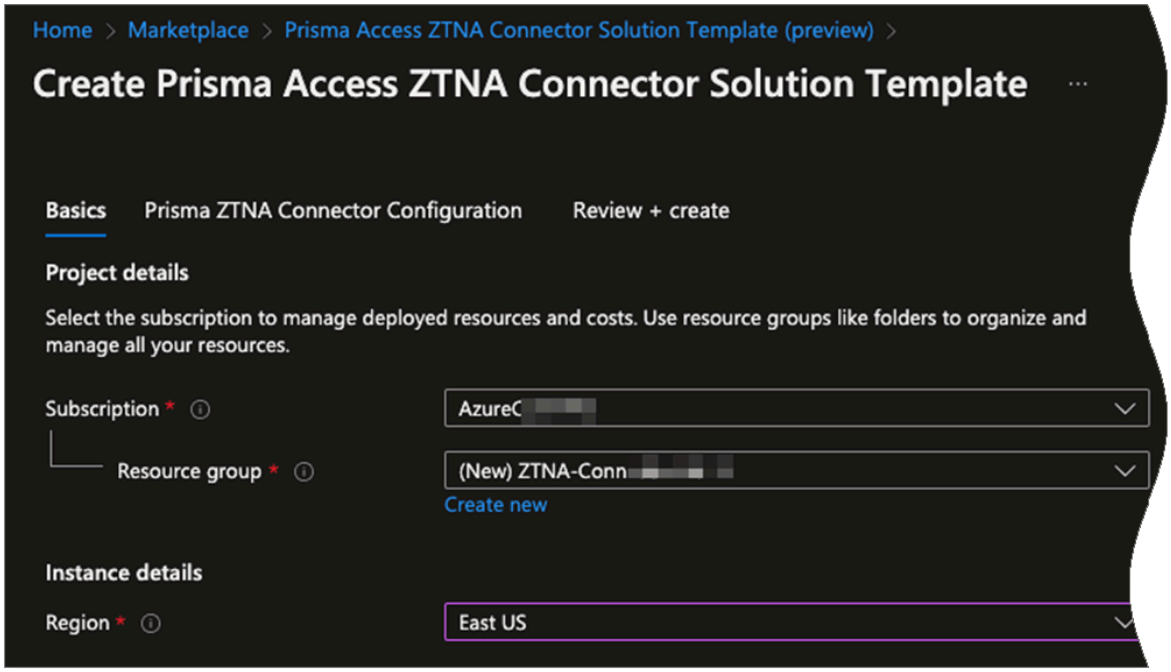

### Einarmigen ZTNA-Connector in Microsoft Azure bereitstellen

Gehen Sie wie folgt vor, um den einarmigen ZTNA-Connector in Microsoft Azure bereitzustellen:

 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** Konfigurieren Sie auf der Registerkarte **Grundlagen** Folgendes:

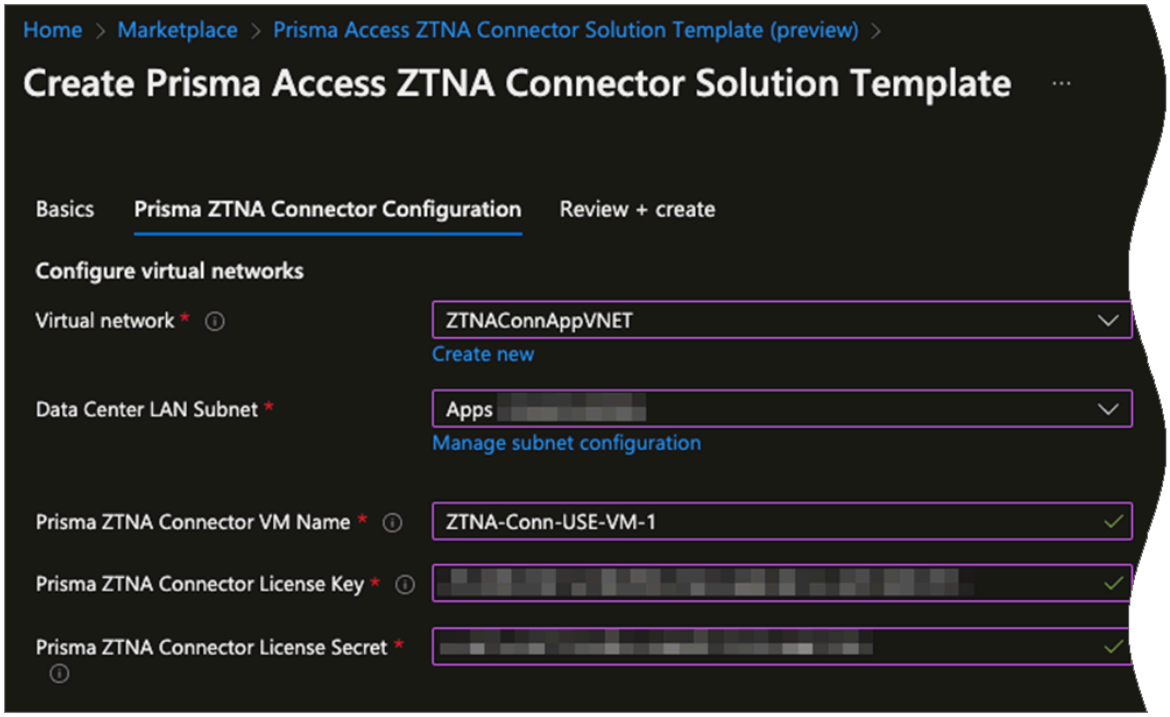
- Wählen Sie Ihr Azure-**Abonnement** aus, um bereitgestellte Ressourcen zu verwalten.
- Wählen Sie eine vorhandene **Ressourcengruppe** oder **Neu erstellen** aus.
- Wählen Sie eine Azure-**Region** aus, die für Ihren Standort relevant ist.
- Klicken Sie auf **Weiter: Prisma ZTNA-Connector-Konfiguration**.



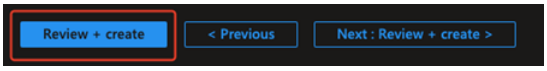

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Konfigurieren Sie ein virtuelles Netzwerk auf der Registerkarte **Prisma ZTNA-Connector-Konfiguration**:

- Erstellen Sie ein neues virtuelles Netzwerk oder wählen Sie ein vorhandenes **virtuelles Netzwerk** aus.
- Wählen Sie das **LAN-Subnetz des Rechenzentrums** aus, in dem Sie Anwendungen bereitgestellt haben, die für diesen Konnektor eingebunden werden sollen.
- Geben Sie den **Namen der VM des Prisma ZTNA-Connectors** ein.
- Geben Sie den **Lizenzschlüssel** und den **geheimen Lizenzschlüssel** von Prisma Access ZTNA-Connector ein, die Sie aus dem Prisma SASE-Portal abgerufen haben.



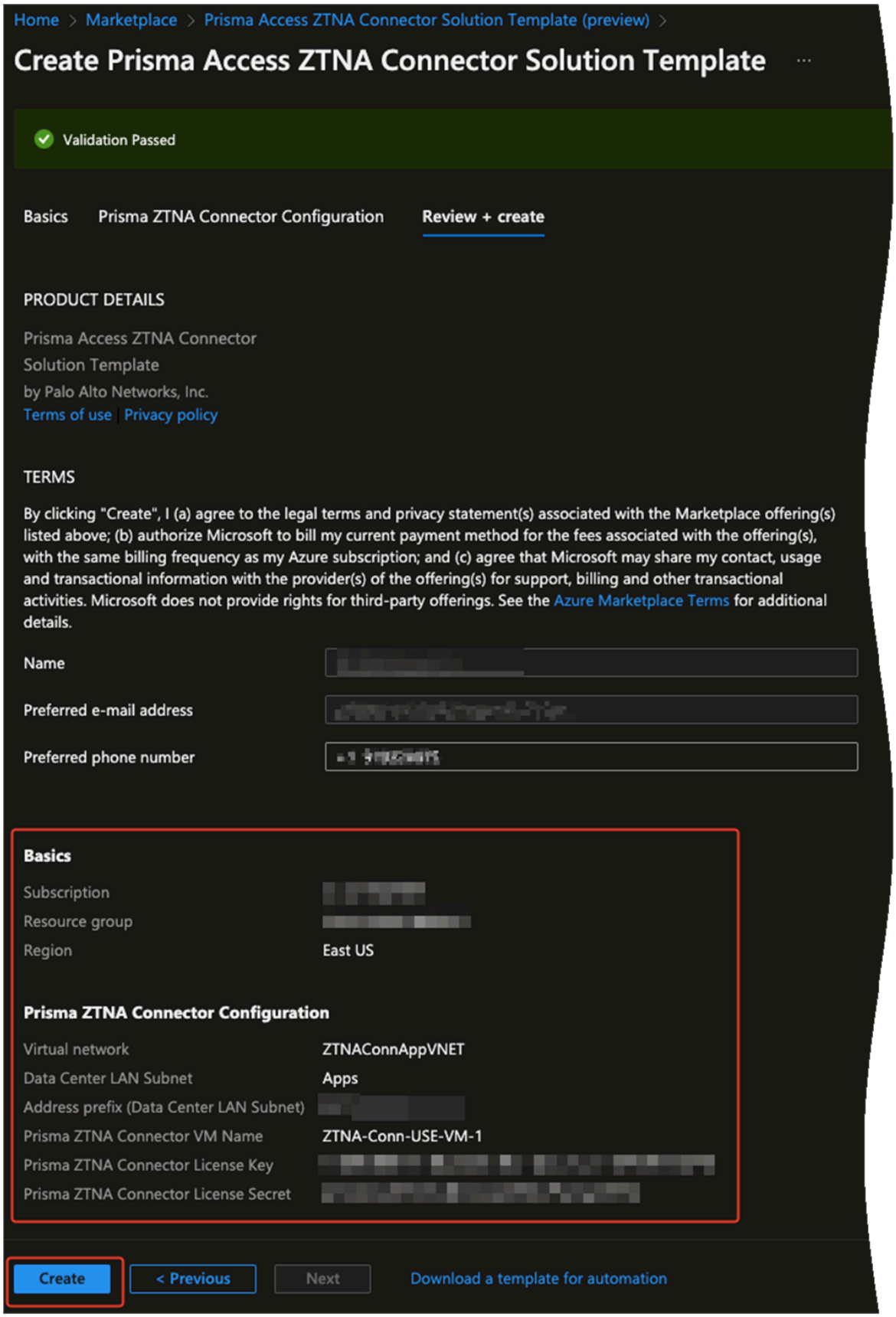

- Wählen Sie **Überprüfen + Erstellen** aus, um Ihre verwaltete Prisma ZTNA-Connector-Konfiguration zu überprüfen.




 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Bestätigen Sie die angegebenen Details und klicken Sie auf **Erstellen**, um die Bereitstellung der virtuellen Maschine zu starten.

 ©2025 Palo Alto Networks, Inc.



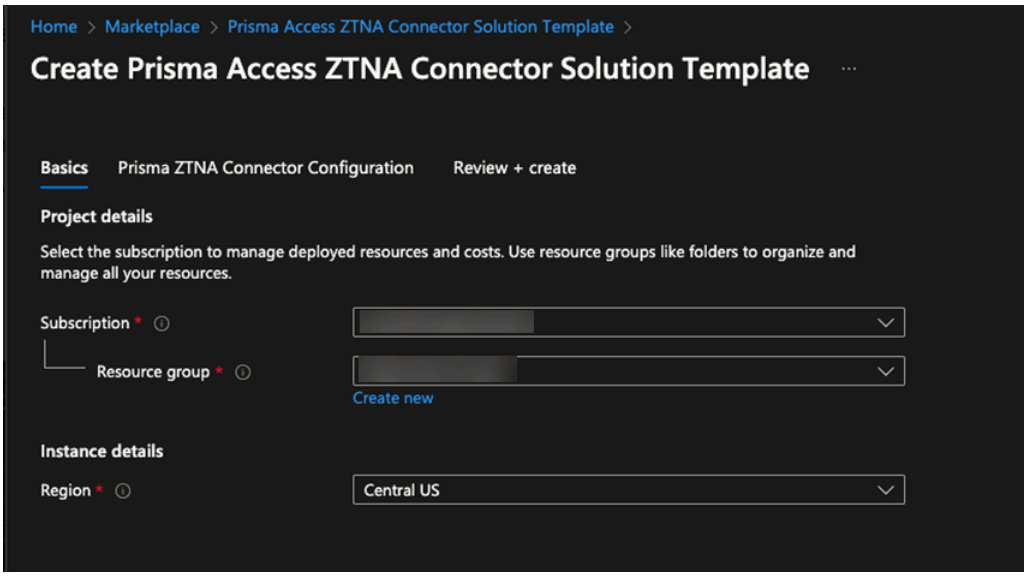

 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** Wählen Sie anschließend **Zur Ressource wechseln** aus.

### Einarmigen ZTNA-Connector mit Autoskalierung in Microsoft Azure bereitstellen

**STEP 1 |** Konfigurieren Sie auf der Registerkarte **Grundlagen** Folgendes:

- Wählen Sie Ihr Azure-**Abonnement** aus, um bereitgestellte Ressourcen zu verwalten.
- Wählen Sie eine vorhandene **Ressourcengruppe** oder **Neu erstellen** aus.
- Wählen Sie eine Azure-**Region** aus, die für Ihren Standort relevant ist.
- Klicken Sie auf **Weiter: Prisma ZTNA-Connector-Konfiguration**.

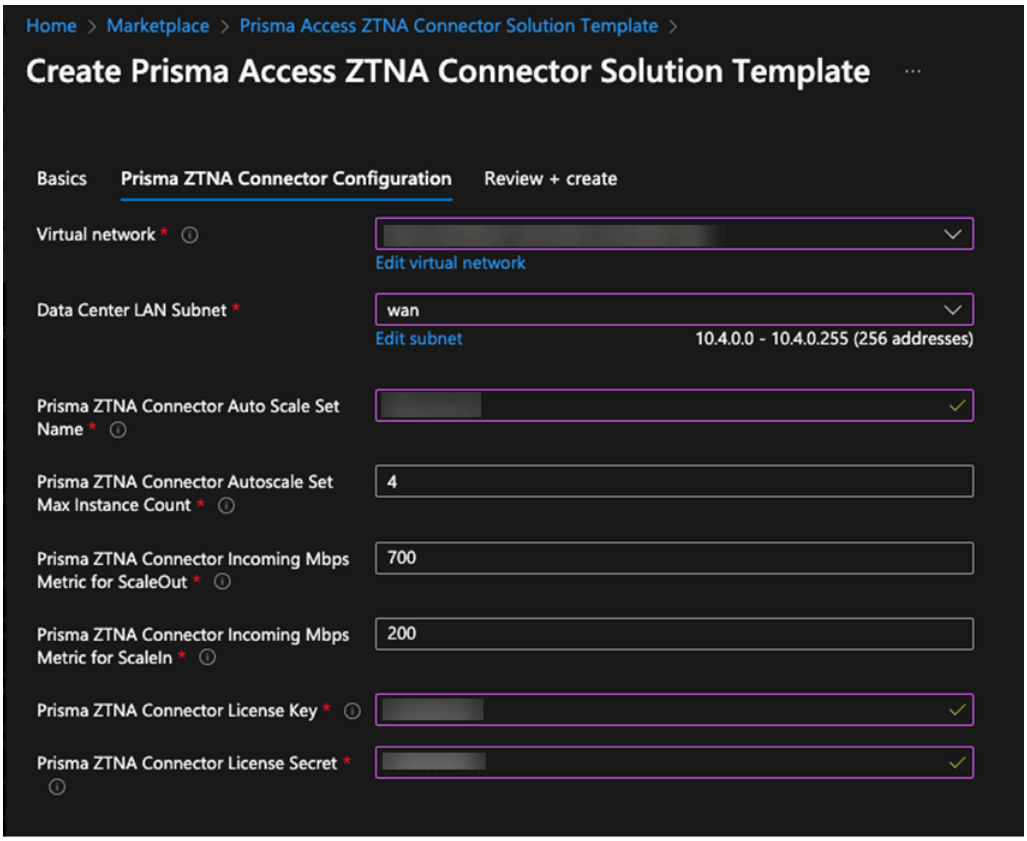



**STEP 2 |** Konfigurieren Sie ein virtuelles Netzwerk auf der Registerkarte **Weiter: Prisma ZTNA-Connector-Konfiguration**:

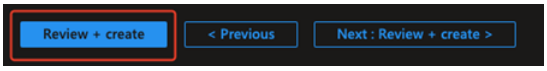
- Erstellen Sie ein neues **virtuelles Netzwerk** oder wählen Sie ein vorhandenes **virtuelles Netzwerk** aus.
- Wählen Sie das **LAN-Subnetz des Rechenzentrums** aus, in dem Sie Anwendungen bereitgestellt haben, die für diesen Konnektor eingebunden werden sollen.
- Geben Sie den **Namen des Satzes für den Prisma ZTNA-Connector mit Auto-Skalierung** ein, indem Sie den Namen des in Azure erstellten Skalierungssatzes angeben.
- Geben Sie die **Instanznummer des Satzes für den Prisma ZTNA-Connector mit Auto-Skalierung** ein. Es sind maximal vier ZTNA-Connectors in der Konnektorgruppe zulässig.
- Geben Sie die **Eingehende Mbit/s-Metrik des Prisma ZTNA-Connectors für ScaleOut** ein. Geben Sie einen Wert zwischen 100 und 1000 ein.
- Geben Sie die **Eingehende Mbit/s-Metrik des Prisma ZTNA-Connectors für ScaleIn** ein. Geben Sie einen Wert zwischen 1 und 500 ein.
- Geben Sie die Werte für den **Lizenzschlüssel des Prisma ZTNA-Connectors** und den **geheimen Lizenzschlüssel des Prisma ZTNA-Connectors** ein, die Sie aus dem Prisma SASE-

 ©2025 Palo Alto Networks, Inc.

Portal für die Connector-Gruppe abgerufen haben, in der Sie den Connector einbinden möchten.

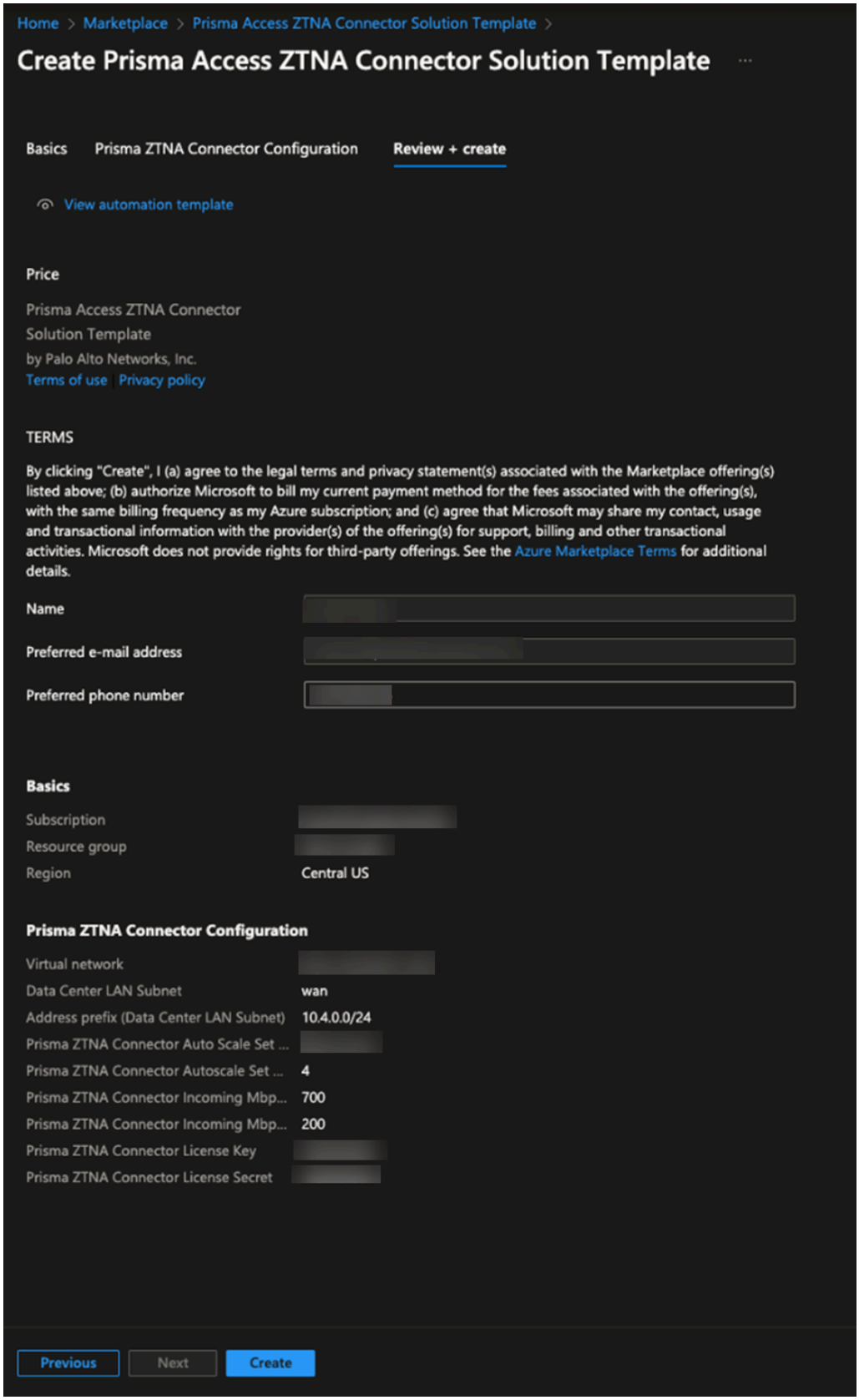



- Wählen Sie **Überprüfen + Erstellen** aus, um Ihre verwaltete Prisma ZTNA-Connector-Konfiguration zu überprüfen.



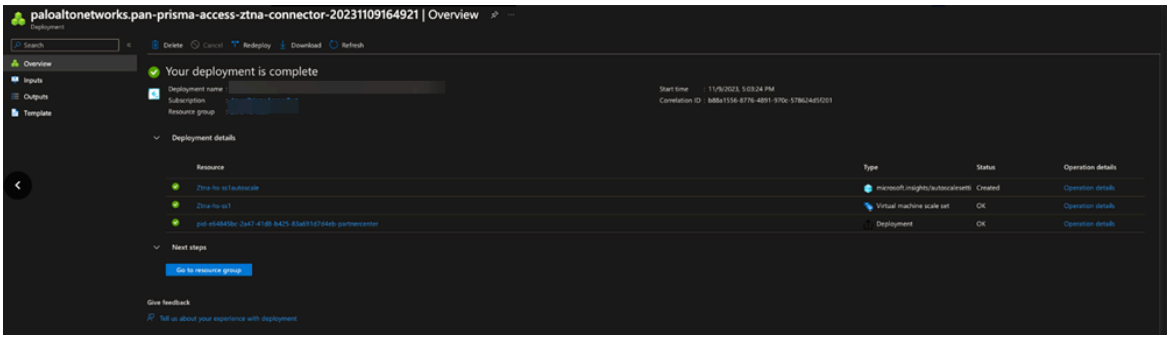

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Bestätigen Sie die angegebenen Details und klicken Sie auf **Erstellen**, um die Bereitstellung der virtuellen Maschine zu starten.




 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** Nach Abschluss der Bereitstellung wählen Sie **Zur Ressourcengruppe wechseln** aus.

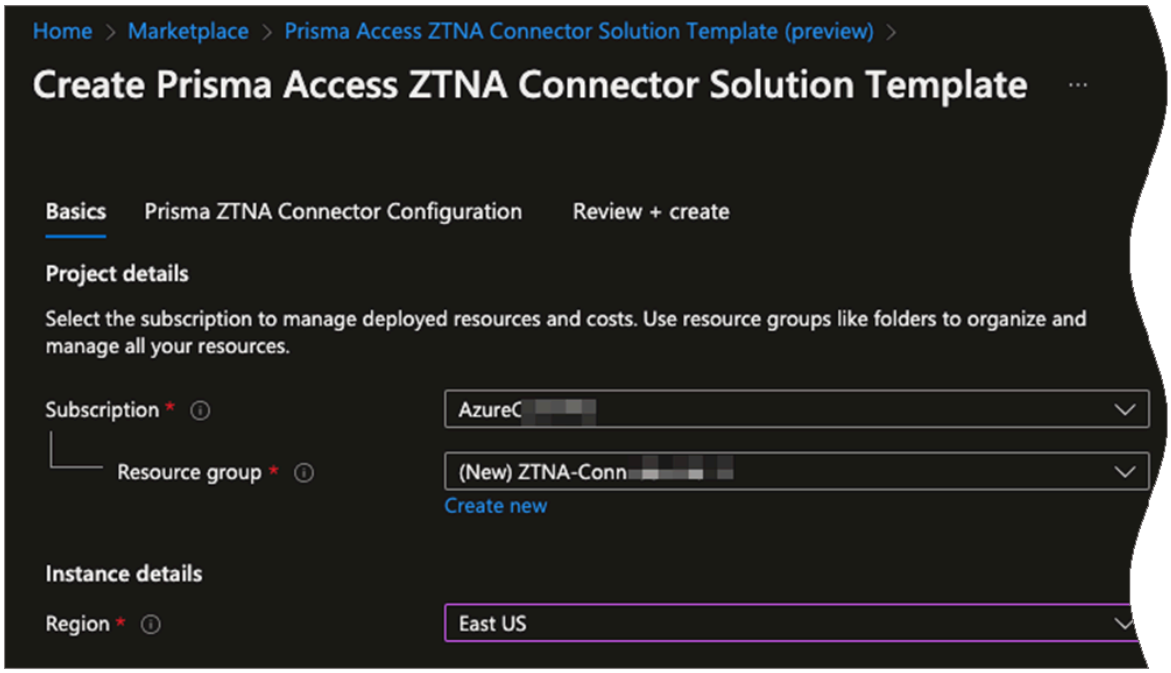



### Zweiarmigen ZTNA Connector in Microsoft Azure bereitstellen

Gehen Sie wie folgt vor, um den zweiarmigen ZTNA-Connector in Microsoft Azure bereitzustellen:

**STEP 1 |** Konfigurieren Sie auf der Registerkarte **Grundlagen** Folgendes:

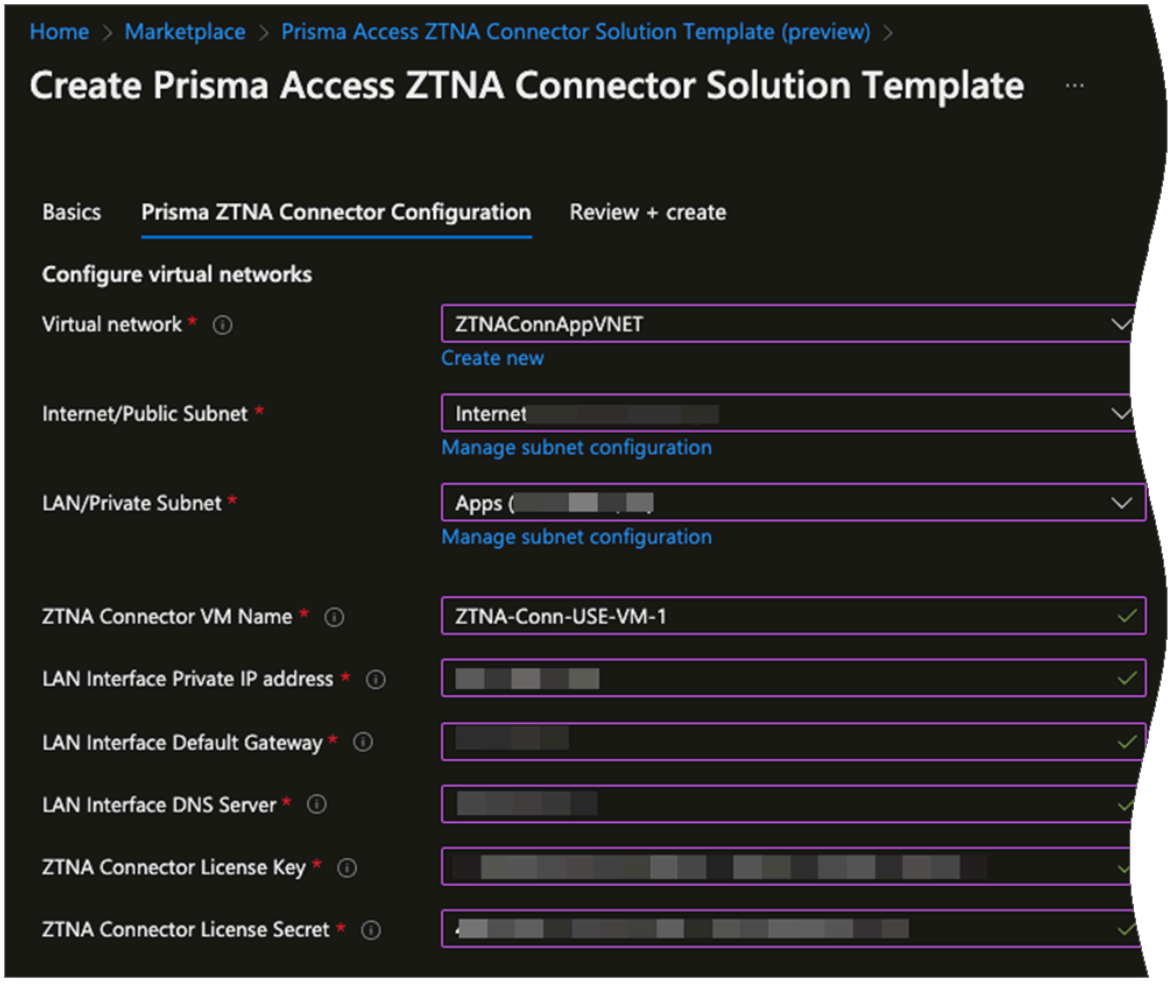
- Wählen Sie Ihr Azure-**Abonnement** aus, um bereitgestellte Ressourcen zu verwalten.
- Wählen Sie eine vorhandene **Ressourcengruppe** oder **Neu erstellen** aus.
- Wählen Sie eine Azure-**Region** aus, die für Ihren Standort relevant ist.
- Klicken Sie auf **Weiter: Prisma ZTNA-Connector-Konfiguration**.




 ©2025 Palo Alto Networks, Inc.

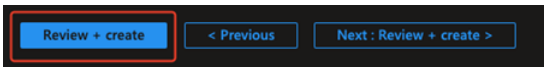
**STEP 2 |** Konfigurieren Sie ein virtuelles Netzwerk auf der Registerkarte **Weiter: Prisma ZTNA-Connector-Konfiguration**:

- Erstellen Sie ein neues **virtuelles Netzwerk** oder verwenden Sie ein vorhandenes **virtuelles Netzwerk**.
- Wählen Sie das **Internet/öffentliche Subnetz** für die WAN-Konnektivität zu IPSec aus. Sie müssen das Subnetz mit einem NAT-Gateway für die Internetkonnektivität verknüpft haben.
- Wählen Sie das **LAN-Subnetz des Rechenzentrums** aus, in dem Sie die Anwendungen bereitgestellt haben, die für diesen Konnektor eingebunden werden sollen.
- Geben Sie den **Namen der VM des Prisma ZTNA-Connectors** ein.
- Geben Sie die **Private IP-Adresse der LAN-Schnittstelle** ein.
- Geben Sie die IP-Adresse des **Standard-Gateways der LAN-Schnittstelle** ein.
- Geben Sie die IP-Adresse des **DNS-Servers der LAN-Schnittstelle** ein.
- Geben Sie den **Lizenzschlüssel** und den **geheimen Lizenzschlüssel** von Prisma Access ZTNA-Connector ein, die Sie aus dem Prisma SASE-Portal abgerufen haben.




- Wählen Sie **Überprüfen + Erstellen** aus, um Ihre verwaltete Prisma ZTNA-Connector-Konfiguration zu überprüfen.

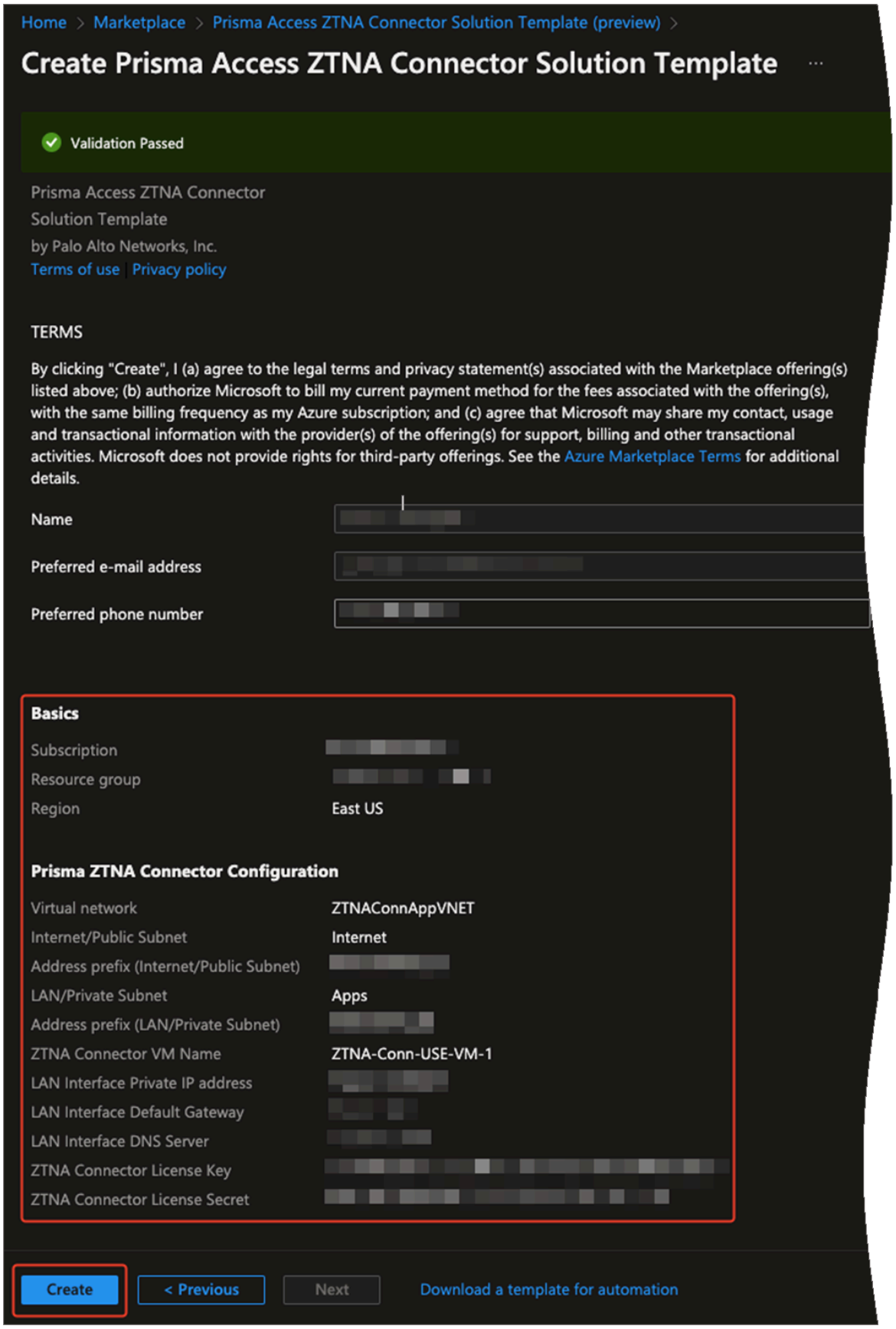
 ©2025 Palo Alto Networks, Inc.




 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Bestätigen Sie die angegebenen Details und klicken Sie auf **Erstellen**, um die Bereitstellung der virtuellen Maschine zu starten.

 ©2025 Palo Alto Networks, Inc.



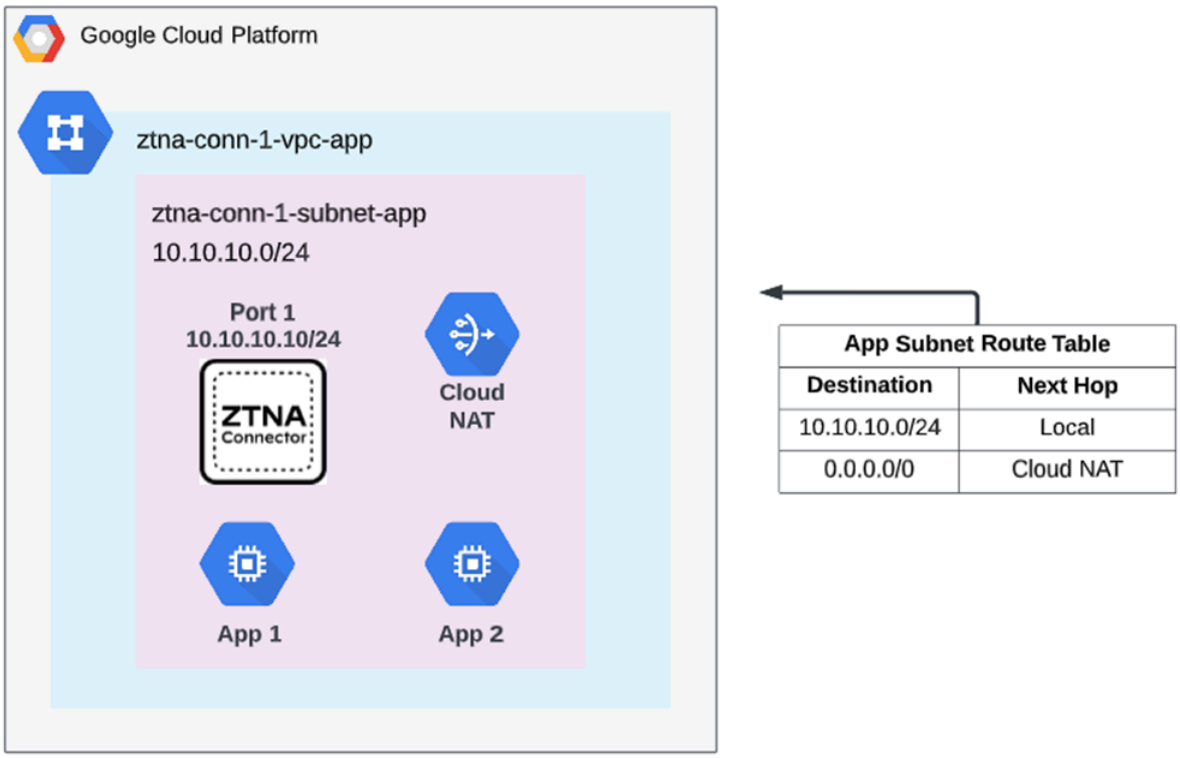

 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** Wählen Sie anschließend **Zur Ressource wechseln** aus.

# Von ZTNA-Connector unterstützte Bereitstellungen der Google Cloud Platform

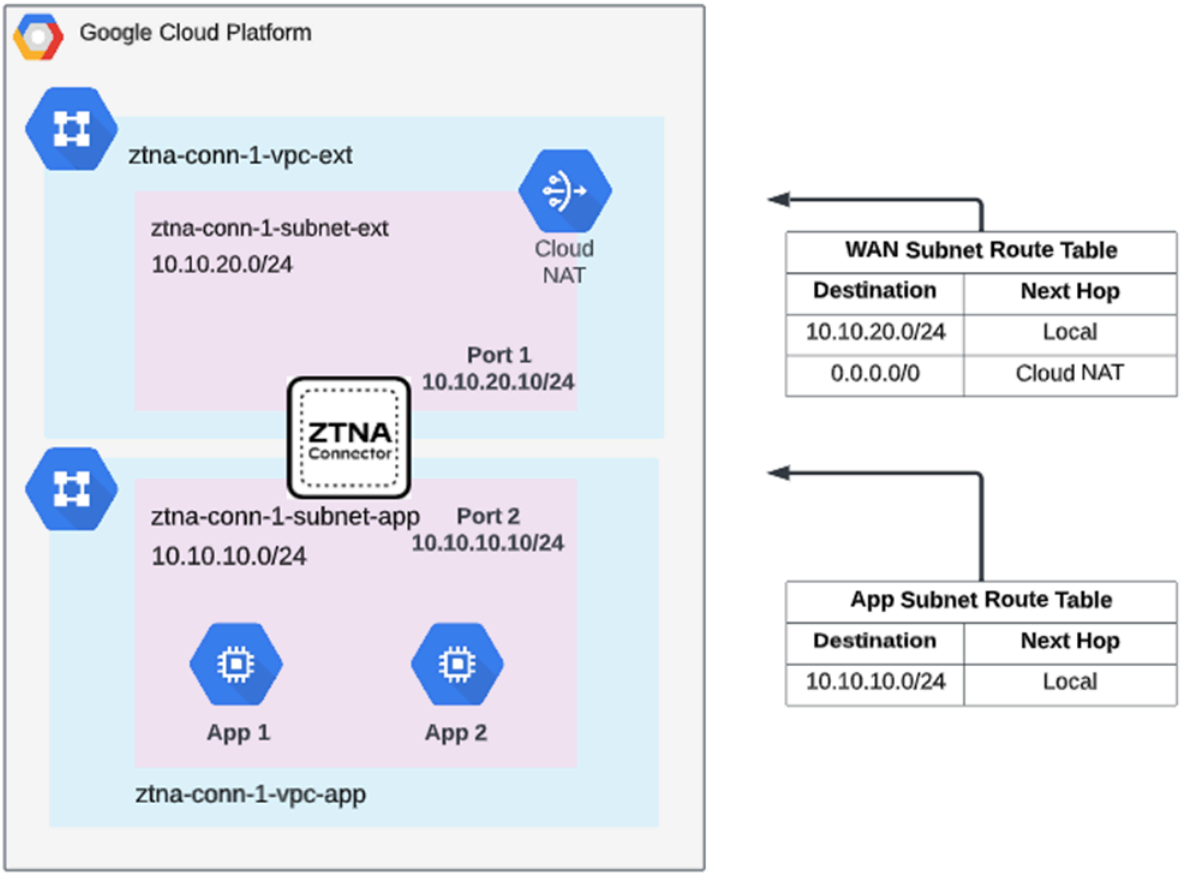
Die Prisma Access ZTNA-Connector-Netzwerkbereitstellung in Google Cloud Platform (GCP) unterstützt zwei Bereitstellungen und eine entsprechende Vorlage für jede Bereitstellung.

Im folgenden Diagramm ist ein Beispiel für eine Prisma Access ZTNA-Connector-Bereitstellung in GCP im einarmigen Modus mit einem NAT-Gateway dargestellt.



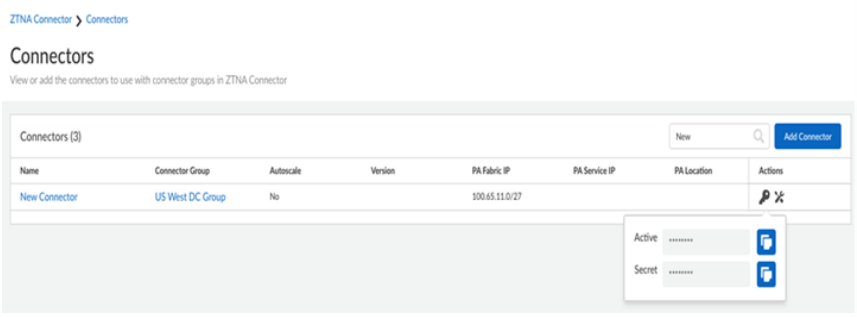

Im folgenden Diagramm ist ein Beispiel für eine Prisma Access ZTNA-Connector-Bereitstellung in GCP im zweiarmigen Modus mit einem NAT-Gateway dargestellt.

 ©2025 Palo Alto Networks, Inc.




## ZTNA-Connector in Google Cloud Platform einbinden

- Überprüfen Sie die Anforderungen und Richtlinien sowie die FQDNs und Ports, die Sie konfigurieren müssen, um Prisma Access ZTNA-Connector in Google Cloud Platform (GCP) zu verwenden.
- Rufen Sie im Prisma SASE-Portal die Werte für den Schlüssel und den geheimen Schlüssel des Konnektors ab und kopieren Sie diese: Wählen Sie **Workflows** > **ZTNA-Connector** > **Konnektoren** aus, suchen Sie nach dem Konnektorobjekt, das Sie in Prisma Access erstellt haben, um es mit dieser VM zu verknüpfen, und wählen Sie **Token kopieren** aus. Kopieren Sie anschließend die Werte für **Schlüssel** und **Geheimer Schlüssel**.




Wenn alle Voraussetzungen erfüllt sind, gehen Sie wie folgt vor, um einen Prisma Access-ZTNA-Connector in GCP einzubinden.

 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** Gehen Sie zum GCP Marketplace und suchen Sie nach **Prisma Access ZTNA Connector**.

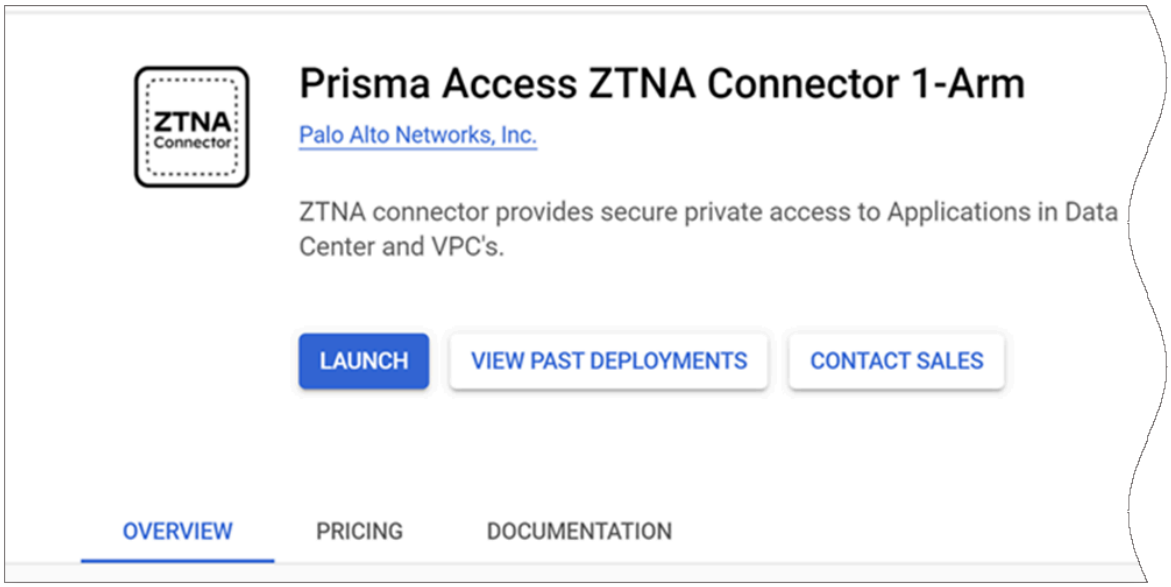
**STEP 2 |** Wählen Sie den Softwareplan aus, der am besten zu Ihren Anforderungen passt.

- Prisma Access ZTNA-Connector – einarmig
- Prisma Access ZTNA-Connector – zweiarmig

### „ZTNA Connector, einarmig“ in GCP bereitstellen

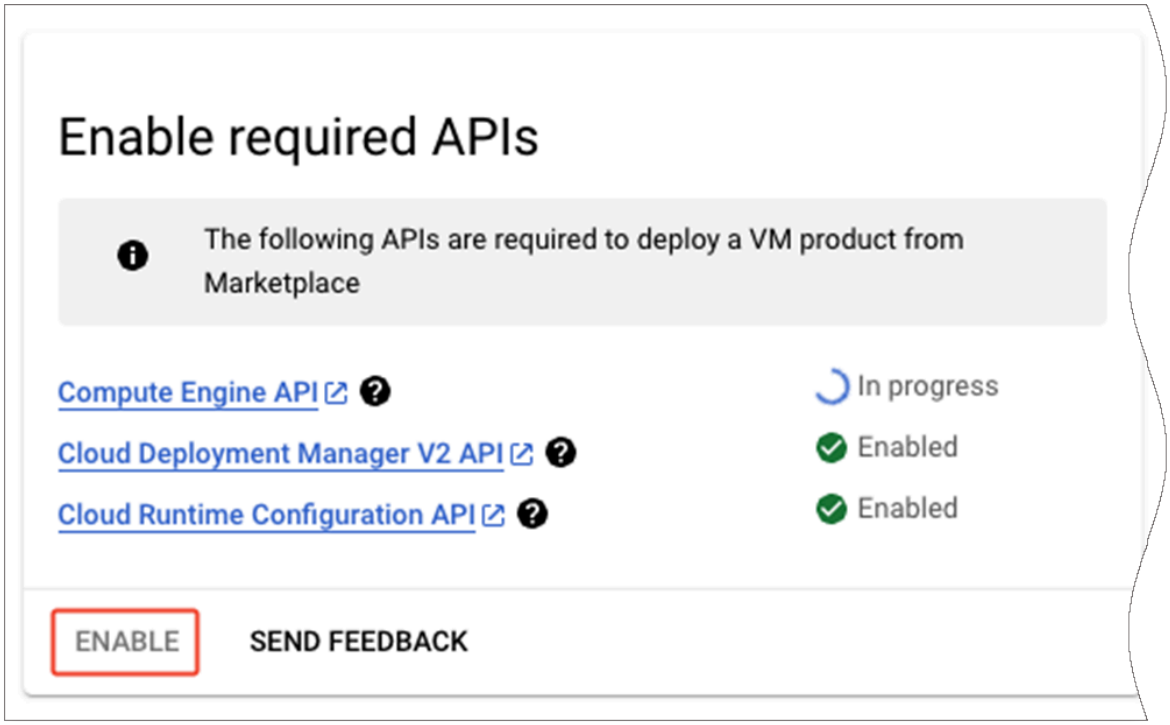
Befolgen Sie diese Schritte, um den einarmigen ZTNA-Connector in GCP bereitzustellen.

**STEP 1 |** Wählen Sie **Starten** aus, um den einarmigen ZTNA-Connector zu konfigurieren.




 ©2025 Palo Alto Networks, Inc.

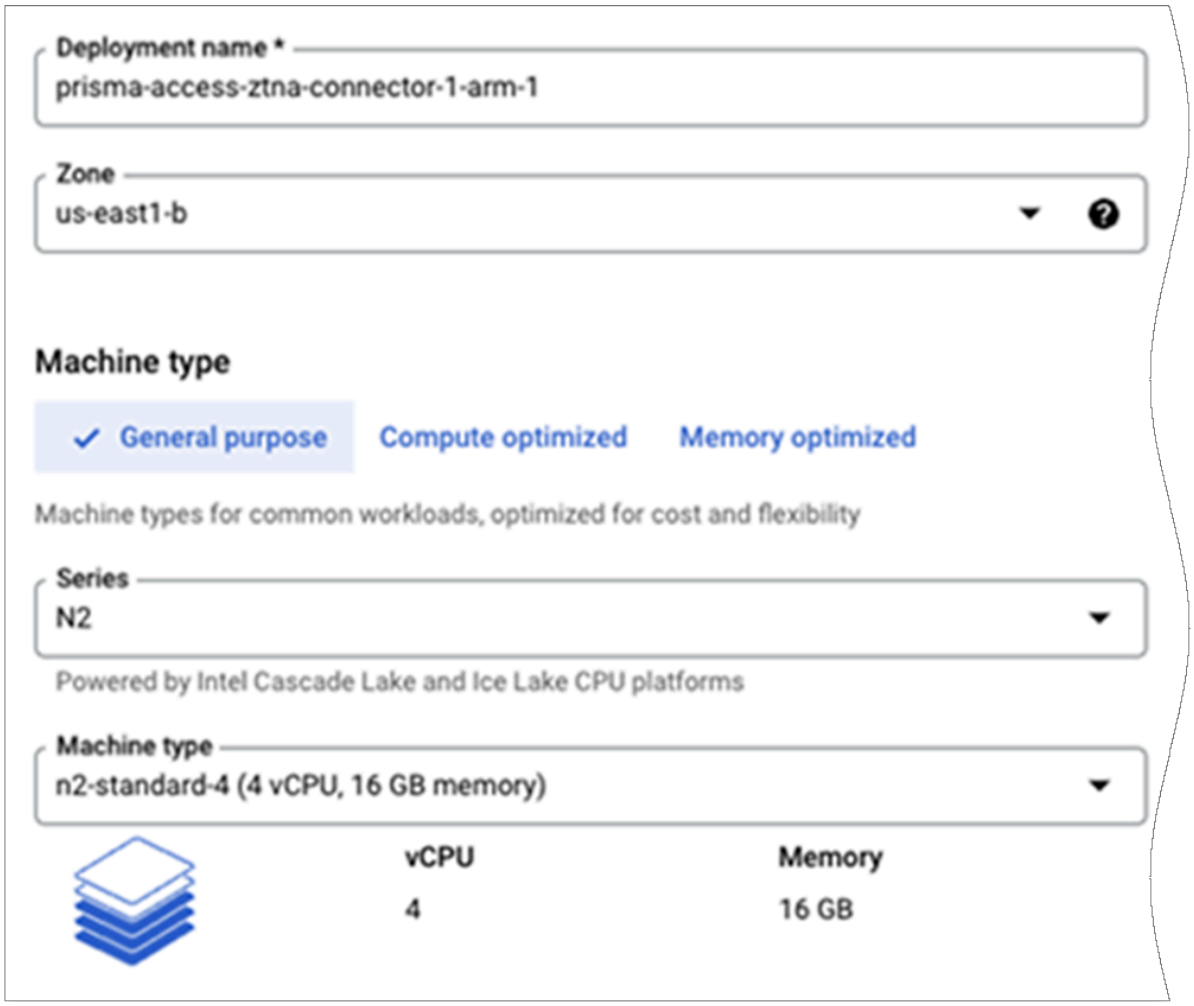
**STEP 2 |** (Optional) **Aktivieren** Sie die GCP-APIs, die für die Bereitstellung einer virtuellen Maschine über den Marketplace erforderlich sind.




 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Konfigurieren Sie Folgendes:

- Geben Sie den **Bereitstellungsnamen** ein, mit dem Sie Ihre virtuelle Maschine identifizieren können.
- Wählen Sie die **Zone** aus, in der sich die Anwendungen für diesen Konnektor befinden.
- Verwenden Sie den Standardwert für den **Maschinentyp** aus. Der qualifizierte Maschinentyp für diesen Konnektor ist **n2-standard-4**.

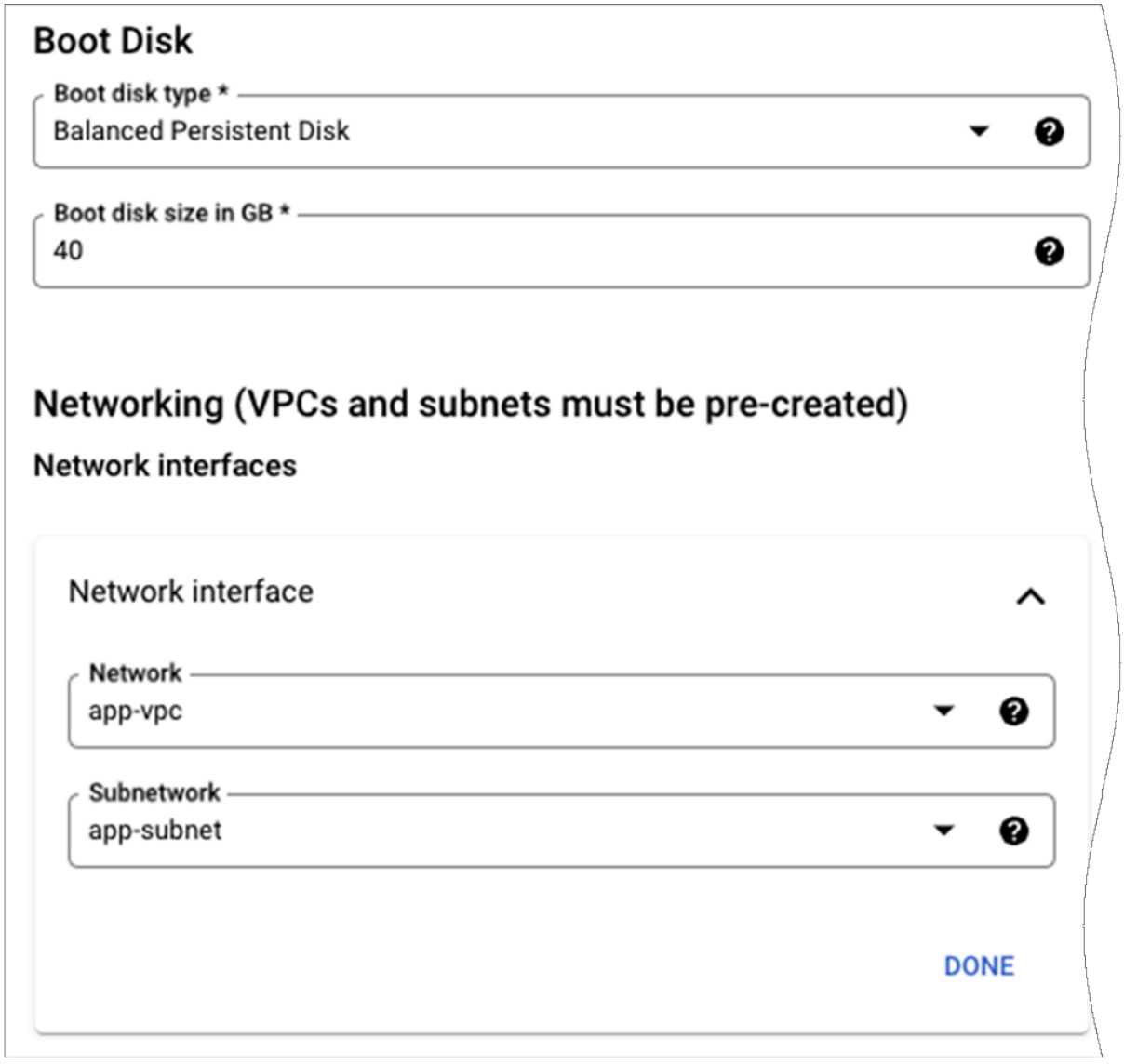



- Geben Sie den **Lizenzschlüssel** und den **geheimen Lizenzschlüssel** von Prisma Access ZTNA-Connector ein, die Sie aus dem Prisma SASE-Portal abgerufen haben.




 ©2025 Palo Alto Networks, Inc.

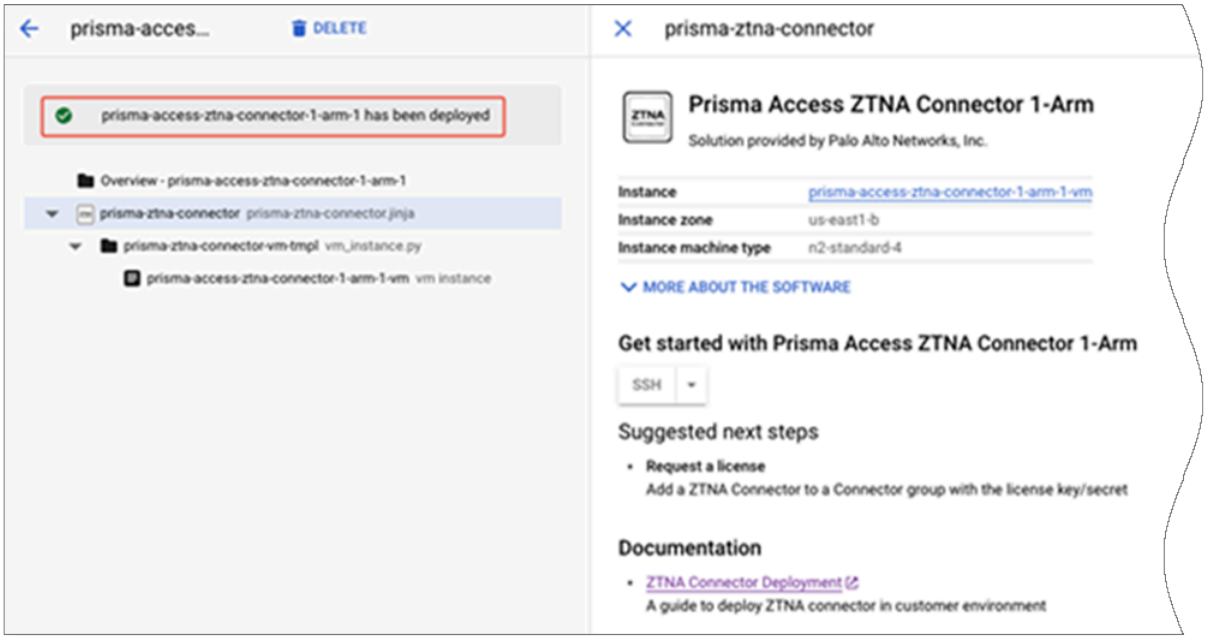
- Konfigurieren Sie Folgendes im Abschnitt **Startdatenträger**:
  - Verwenden Sie den Standard-**Startdatenträger**.
  - Wählen Sie **40 GB** als **Startdatenträgergröße in GB** aus.
- Erweitern Sie den Abschnitt **Netzwerk (VPCs und Subnetze müssen vorab erstellt werden)** und wählen Sie die Details zur **Netzwerkschnittstelle aus**.
  - Wählen Sie das **Netzwerk** aus, das das von Ihnen erstellte Subnetz enthält.
  - Wählen Sie das **Subnetz** für die zu verwendende virtuelle Maschine aus.




**STEP 4 |** Klicken Sie auf **Done (Fertig)**.

 ©2025 Palo Alto Networks, Inc.

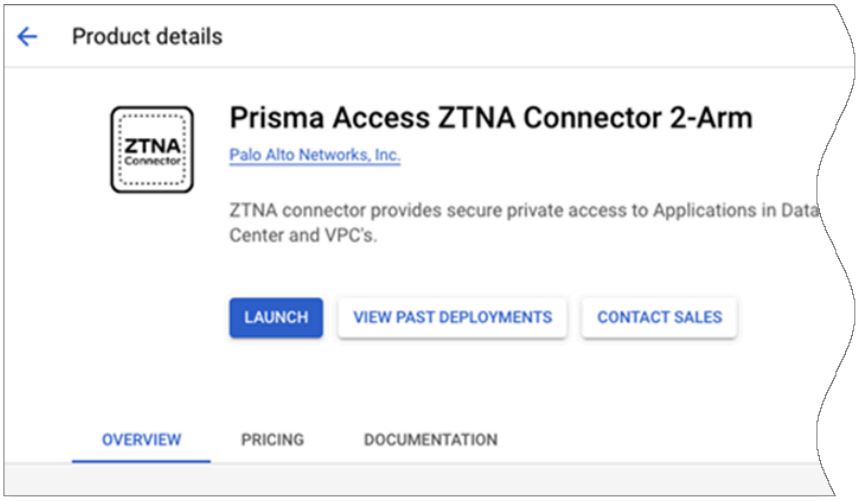
**STEP 5 |** Klicken Sie auf **Bereitstellen**, um den Onboarding-Prozess abzuschließen.




### „ZTNA-Connector – zweiarmig“ in GCP bereitstellen

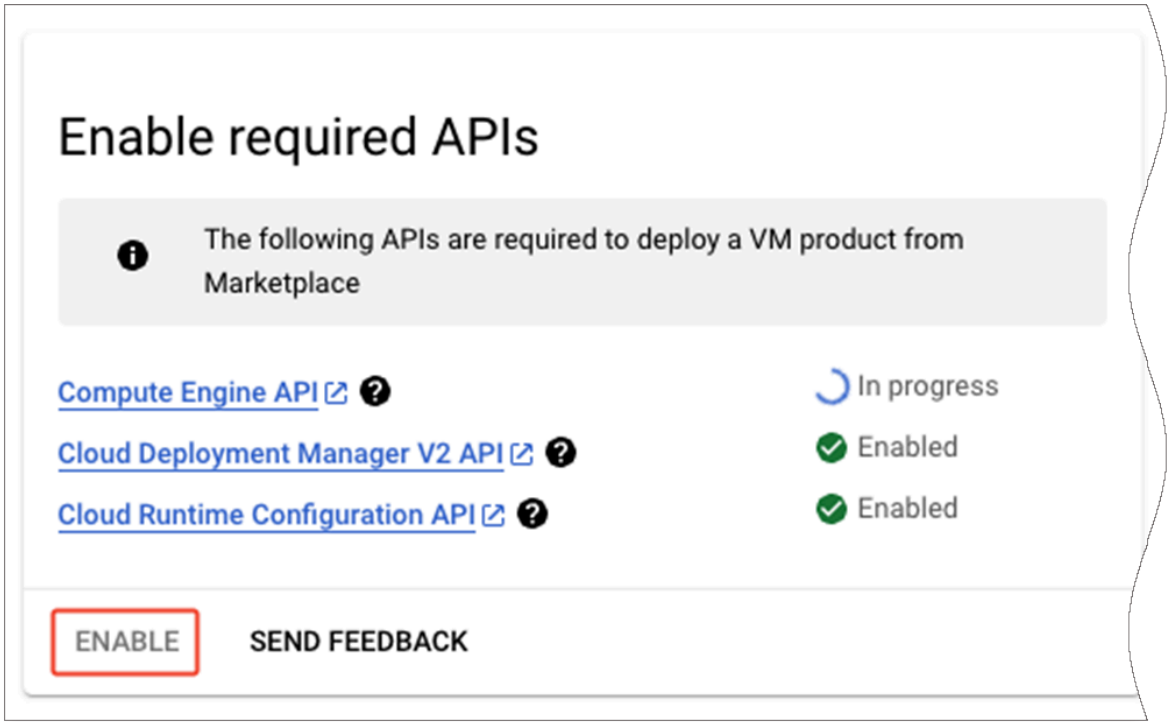
Gehen Sie wie folgt vor, um den ZTNA-Connector in GCP bereitzustellen.

**STEP 1 |** Wählen Sie **Starten** aus, um mit der Konfiguration zu beginnen.




 ©2025 Palo Alto Networks, Inc.

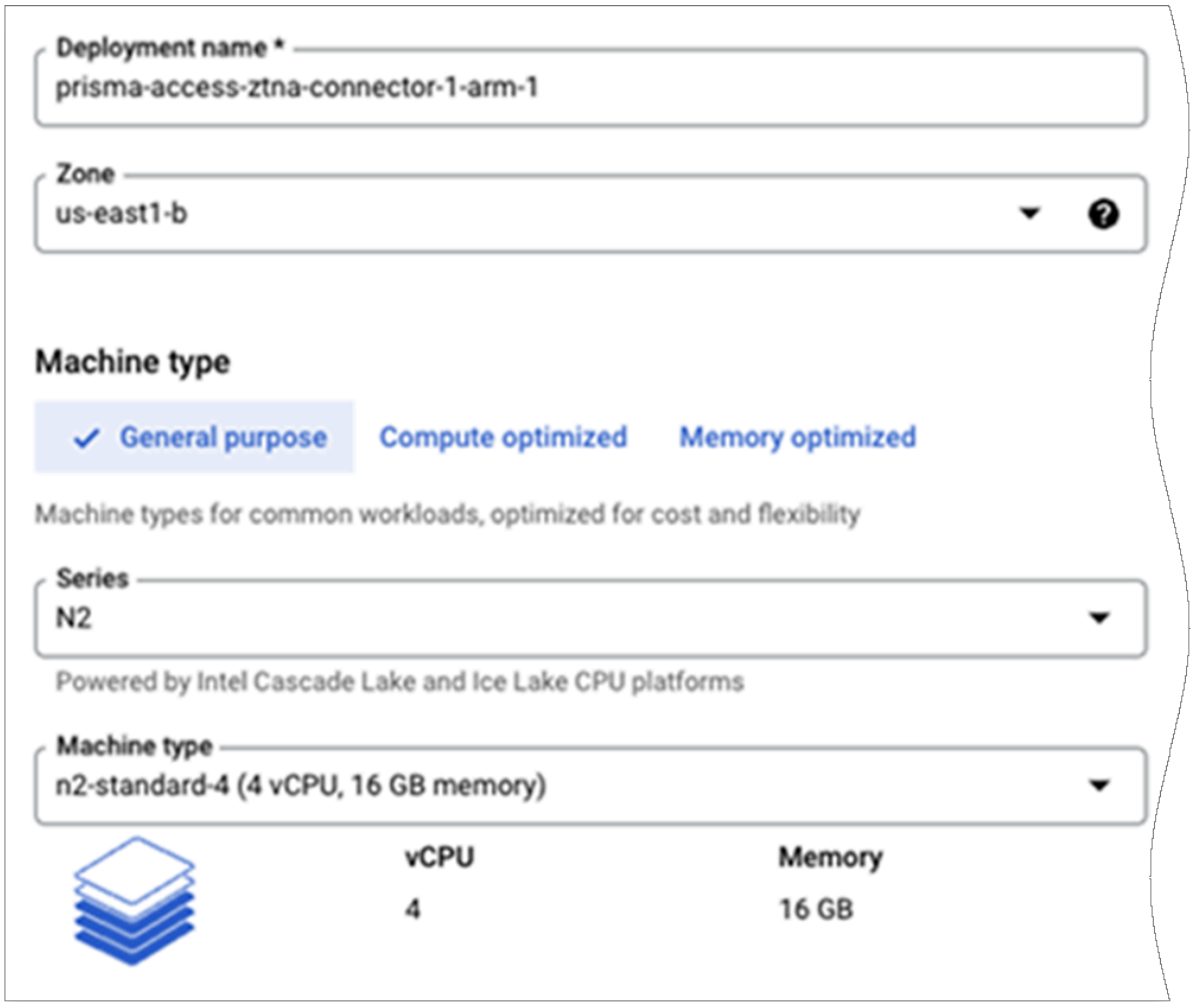
**STEP 2 |** (Optional) **Aktivieren** Sie die APIs, die für die Bereitstellung einer virtuellen Maschine über den Marktplatz erforderlich sind.




 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Konfigurieren Sie Folgendes:

- Geben Sie den **Bereitstellungsnamen** ein, mit dem Sie Ihre virtuelle Maschine identifizieren können.
- Wählen Sie die **Zone** aus, in der sich die Anwendungen für diesen Konnektor befinden.
- Verwenden Sie den Standardwert für den **Maschinentyp** aus. Der qualifizierte Maschinentyp für diesen Konnektor ist **n2-standard-4**.

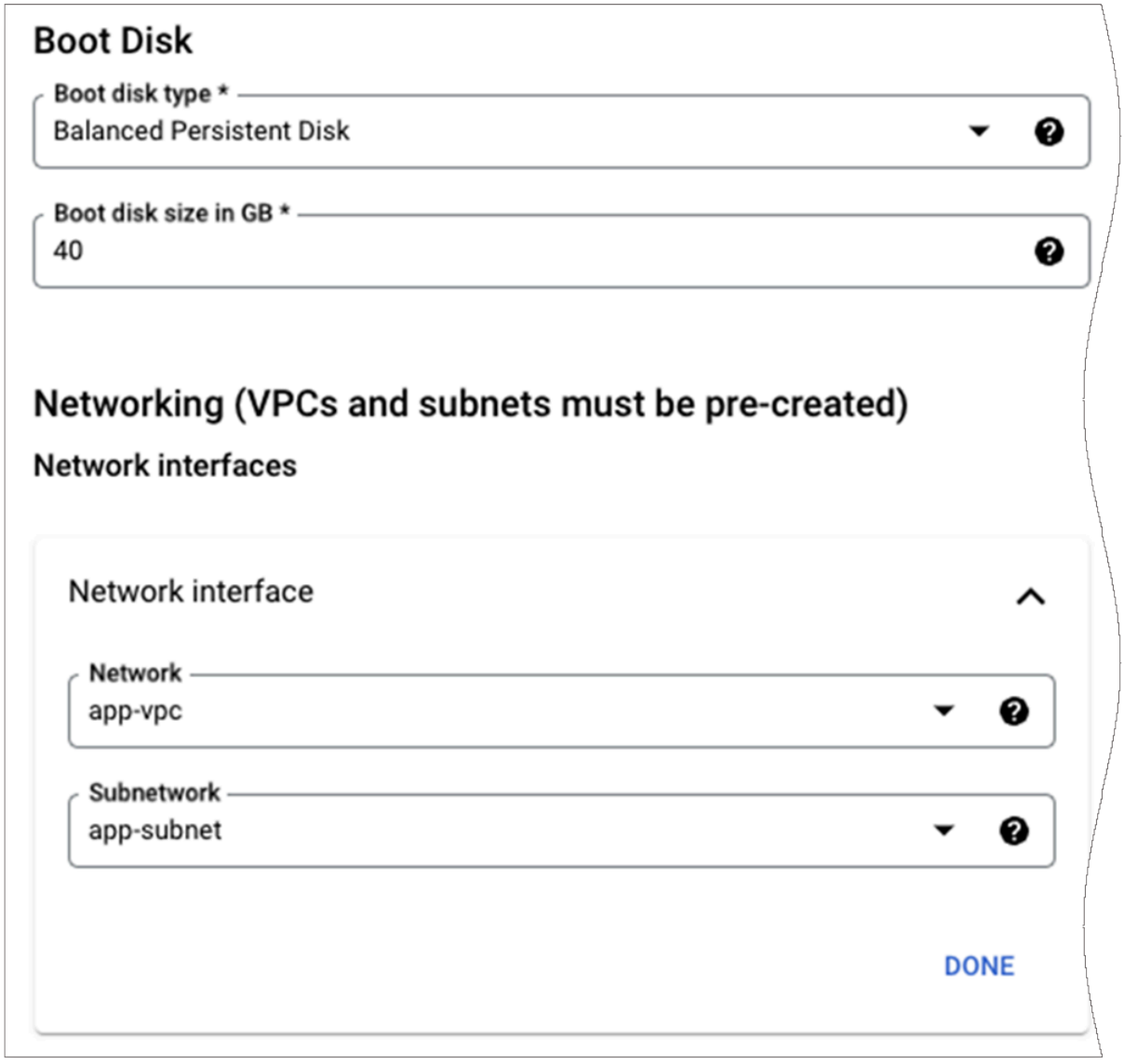



- Geben Sie den **Lizenzschlüssel** und den **geheimen Lizenzschlüssel** von Prisma Access ZTNA-Connector ein, die Sie aus dem Prisma SASE-Portal abgerufen haben.



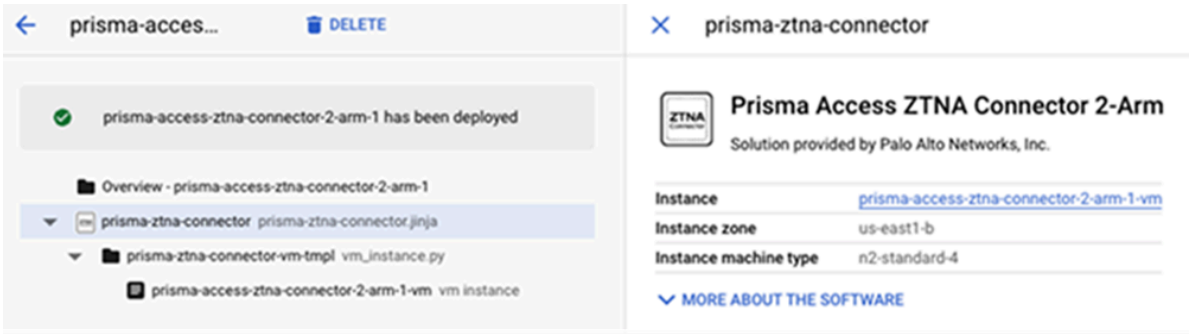

 ©2025 Palo Alto Networks, Inc.

- Gehen Sie im Abschnitt **Startdatenträger** wie folgt vor:
  - Verwenden Sie den Standard-**Startdatenträger**.
  - Wählen Sie **40 GB** als **Startdatenträgergröße in GB** aus.
- Erweitern Sie den Abschnitt **Netzwerk (VPCs und Subnetze müssen vorab erstellt werden)** und wählen Sie die Details zur **Netzwerkschnittstelle aus**.
  - Wählen Sie das **Netzwerk** aus, das das von Ihnen erstellte Subnetz enthält.
  - Wählen Sie das **Subnetz** für die zu verwendende virtuelle Maschine aus.




 ©2025 Palo Alto Networks, Inc.

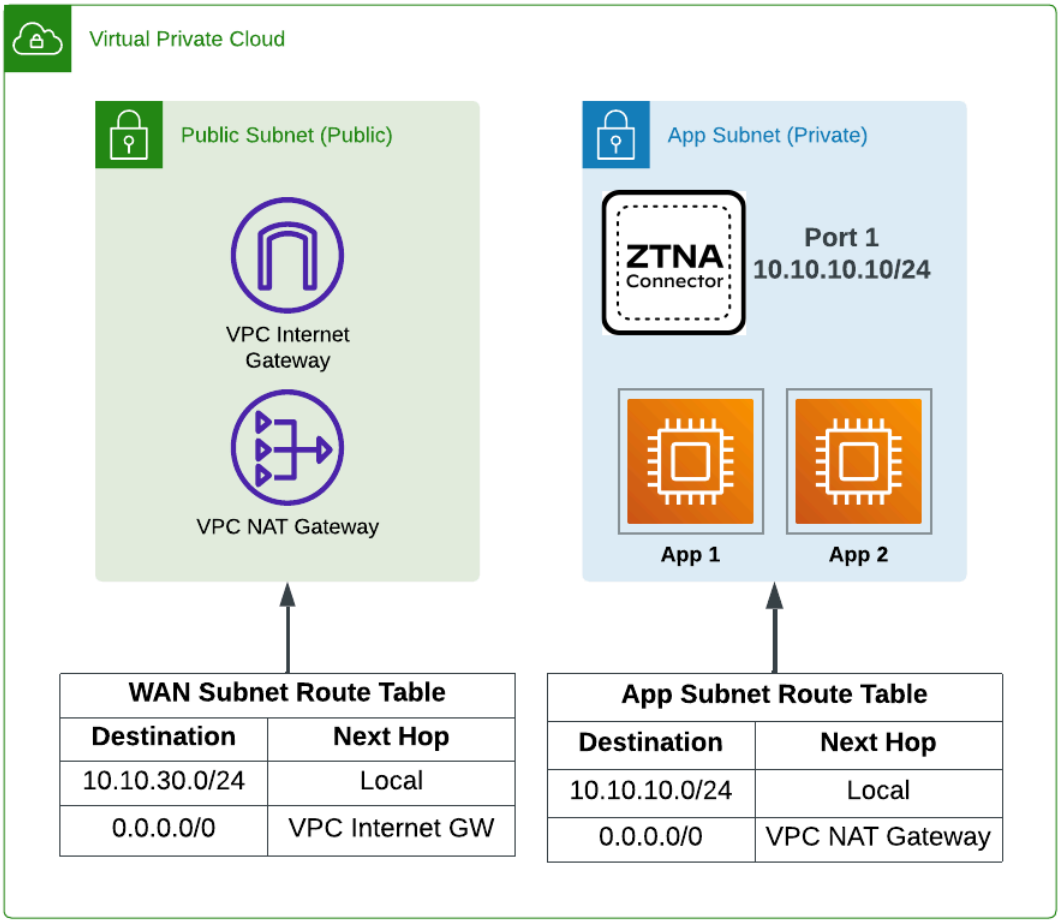
**STEP 4 |** Klicken Sie auf **Bereitstellen**, um den Onboarding-Prozess abzuschließen.




# Von ZTNA-Connector unterstützte Amazon Web Services-Bereitstellungen

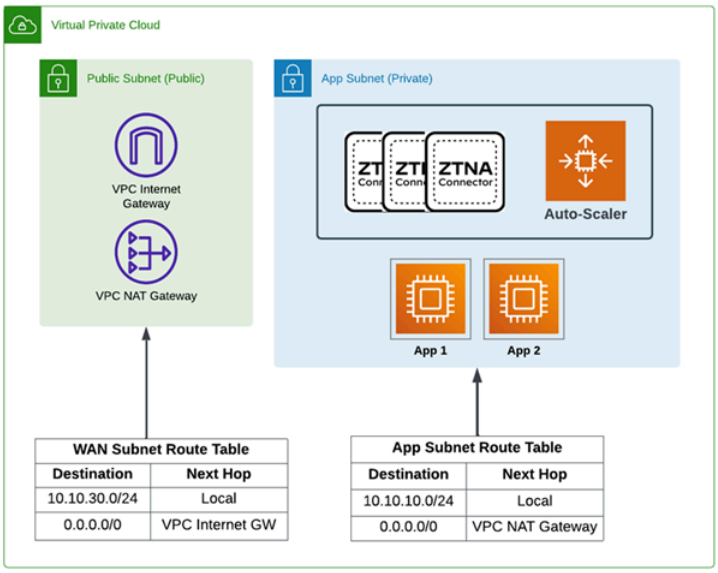
Die Prisma Access- ZTNA-Connector-Netzwerkbereitstellung in Amazon Web Services (AWS) unterstützt drei Bereitstellungstypen und eine entsprechende Vorlage für jede Bereitstellung.

Das folgende Diagramm zeigt ein Beispiel für eine Prisma Access-ZTNA-Connector-Bereitstellung in AWS im Einarmmodus mit einem NAT-Gateway.

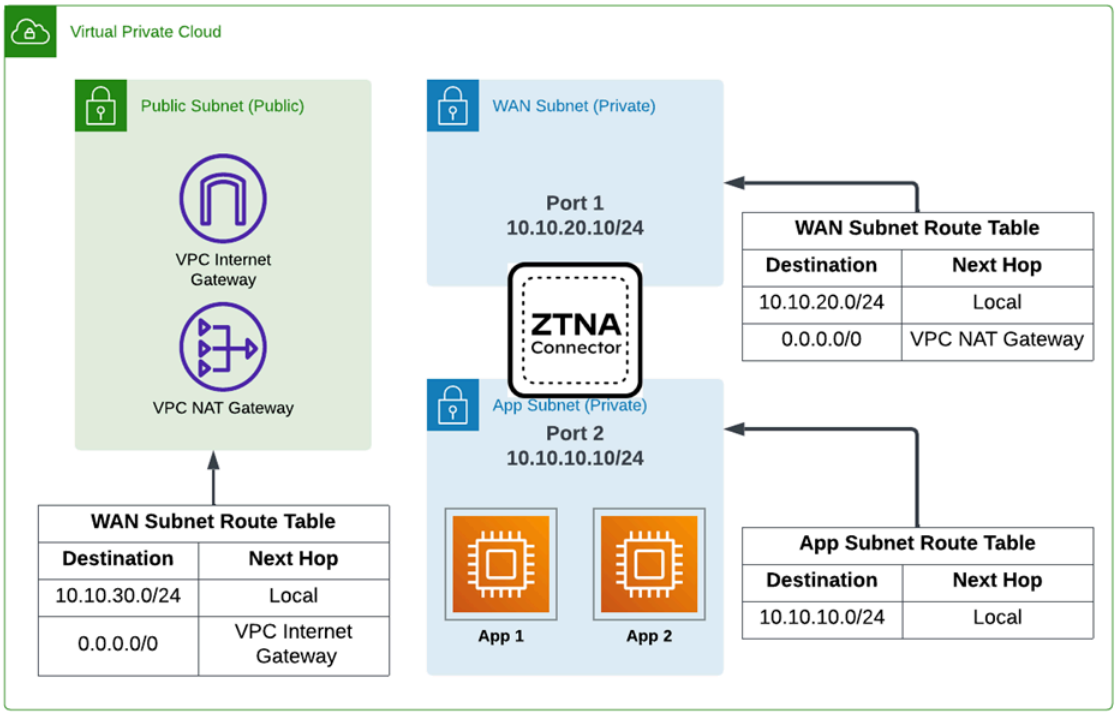



 ©2025 Palo Alto Networks, Inc.

Das folgende Diagramm zeigt eine Beispielbereitstellung für ZTNA-Connector in AWS mit einarmiger Autoskalierung mit einem NAT-Gateway.



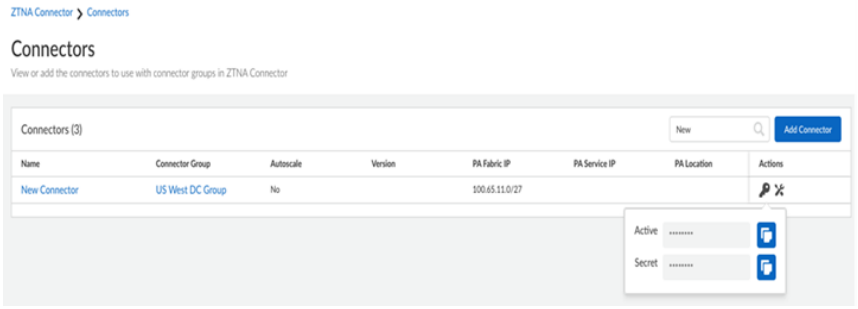

Das folgende Diagramm zeigt ein Beispiel für eine ZTNA-Connector-Bereitstellung in AWS im Zweiarmmodus mit einem NAT-Gateway.



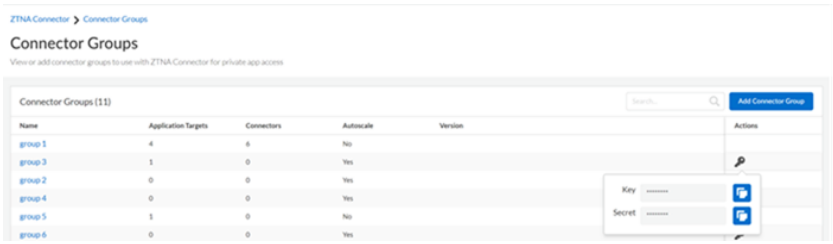

 ©2025 Palo Alto Networks, Inc.

## ZTNA-Connector in Amazon Web Services einbinden

- Überprüfen Sie die Anforderungen und Richtlinien sowie die FQDNs und Ports, die Sie konfigurieren müssen, um ZTNA-Connector in Amazon Web Services (AWS) zu verwenden.
- Rufen Sie auf der Prisma SASE-Plattform die Werte für den Schlüssel und den geheimen Schlüssel des Konnektors ab und kopieren Sie diese: Wählen Sie **Workflows** > **ZTNA-Connector** > **Konnektoren** aus, suchen Sie nach dem Konnektorobjekt, das Sie in Prisma Access erstellt haben, um es mit dieser VM zu verknüpfen, und wählen Sie **Token kopieren** aus. Kopieren Sie anschließend die Werte für **Schlüssel** und **Geheimer Schlüssel**.




- Für die Bereitstellung **Prisma Access ZTNA-Connector – einarmig, Autoskalierung** müssen Sie die Werte für den Schlüssel und den geheimen Schlüssel der Konnektorgruppe abrufen und kopieren: Wählen Sie **Workflows** > **ZTNA-Connector** > **Konnektorgruppen** aus, suchen Sie nach dem Konnektorgruppen-Objekt, das Sie in Prisma Access erstellt haben, um es mit dieser VM zu verknüpfen, und wählen Sie **Token kopieren** aus. Kopieren Sie anschließend den **Schlüssel** und den **geheimen Schlüssel**.




Wenn alle Voraussetzungen erfüllt sind, gehen Sie wie folgt vor, um einen Prisma Access-ZTNA-Connector in AWS einzubinden.

**STEP 1 |** Suchen Sie im AWS Marketplace nach **Prisma Access-ZTNA-Connector**.

**STEP 2 |** Wählen Sie den Softwareplan aus, der am besten zu Ihren Anforderungen passt.

- Prisma Access ZTNA-Connector – einarmig
- Prisma Access ZTNA-Connector – einarmig, Autoskalierung
- Prisma Access ZTNA-Connector – zweiarmig

### „ZTNA-Connector – einarmig“ in AWS bereitstellen

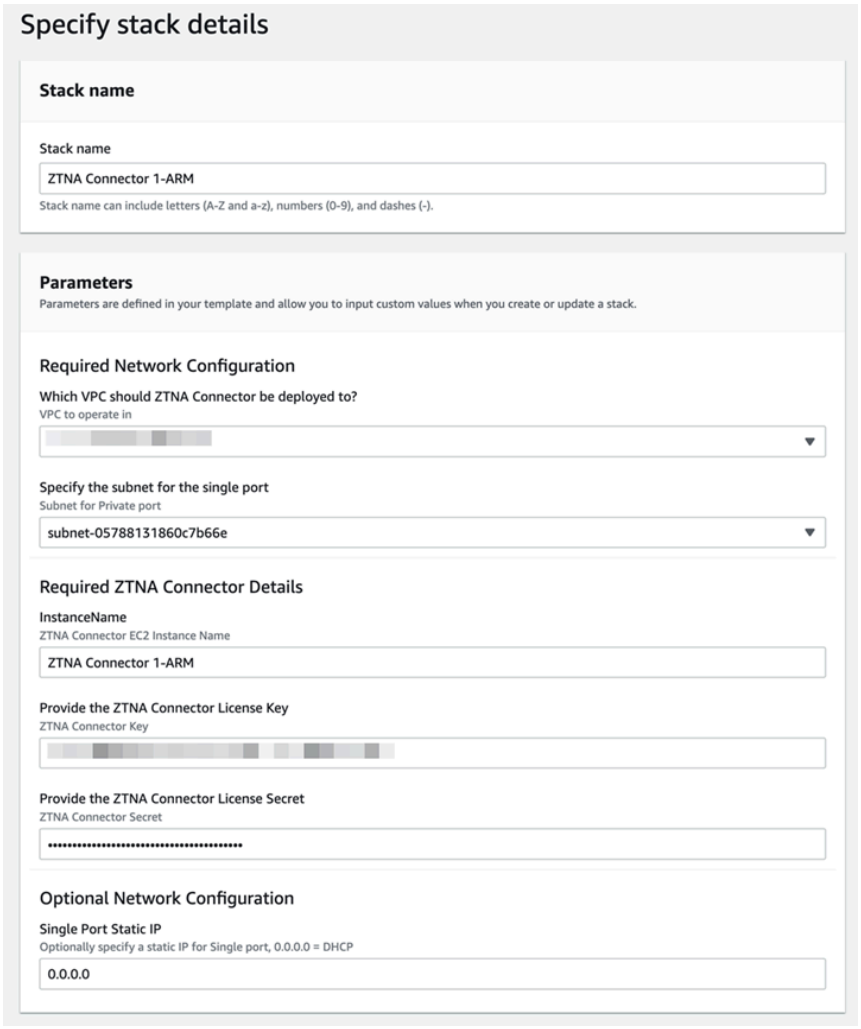
Gehen Sie wie folgt vor, um „ZTNA-Connector – einarmig“ in AWS bereitzustellen.

**STEP 1 |** Wählen Sie die CloudFormation-Vorlage **Prisma Access ZTNA-Connector – einarmig** aus.

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Konfigurieren Sie diese auf der Seite **Stackdetails angeben**:

- Geben Sie den **Stacknamen** ein, um den Stack zu identifizieren.
- Geben Sie im Abschnitt **Parameter** die in der Stackvorlage definierten Parameter an.
  - Wählen **Sie aus, in welcher VPC der ZTNA-Connector bereitgestellt werden soll**.
  - **Geben Sie das Subnetz für den einzelnen Port an**, an dem Sie Anwendungen bereitgestellt haben, um sich mit diesem Connector zu verbinden. Sie müssen von diesem Subnetz über ein NAT-Gateway auf das Internet zugreifen können.
- Geben Sie den **Lizenzschlüssel** und den **geheimen Lizenzschlüssel** von Prisma Access ZTNA-Connector ein, die Sie aus dem Prisma SASE-Portal abgerufen haben.




### Einarmigen ZTNA-Connector mit Autoskalierung in AWS bereitstellen

Gehen Sie wie folgt vor, um den einarmigen ZTNA-Connector mit Autoskalierung in AWS bereitzustellen.

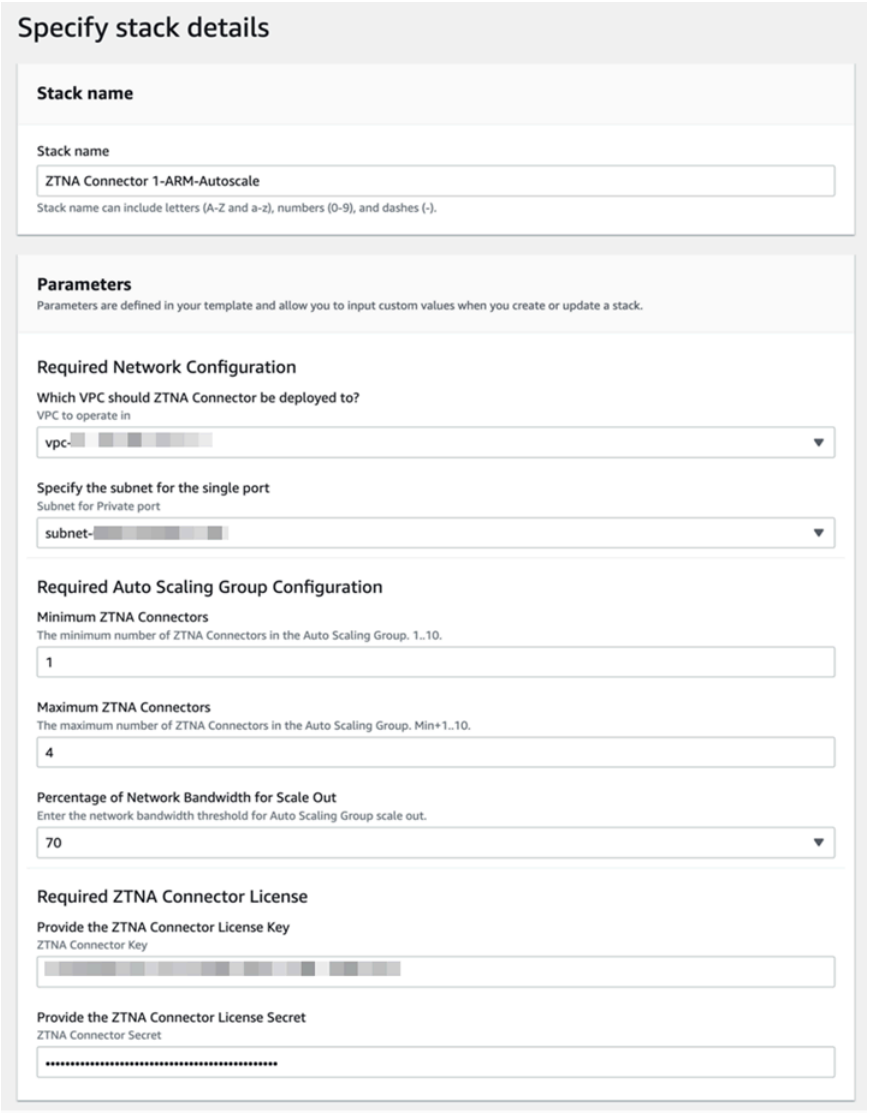
**STEP 1 |** Wählen Sie die CloudFormation-Vorlage „**Prisma Access ZTNA-Connector, einarmig mit Autoskalierung** aus.

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Konfigurieren Sie diese Parameter auf der Seite **Stackdetails angeben**:

- Geben Sie den eindeutigen **Stacknamen** für die Bereitstellung ein.
- Geben Sie in die Stackvorlage die im Abschnitt **Parameter** definierten Parameter an:
  - Wählen **Sie aus, in welcher VPC der ZTNA-Connector bereitgestellt werden soll**.
  - **Geben Sie das Subnetz für den einzelnen Port an**, an dem Sie Anwendungen bereitgestellt haben, um sich mit diesem Connector zu verbinden. Sie müssen von diesem Subnetz über ein NAT-Gateway auf das Internet zugreifen können.
- Gehen Sie in **Erforderliche Konfiguration für die Auto-Skalierungs-Gruppe** wie folgt vor:
  - Geben Sie die erforderliche **Mindestanzahl von ZTNA-Connectors** in die Auto-Skalierungs-Gruppe ein.
  - Geben Sie die erforderliche **Höchstanzahl von ZTNA-Connectors** in die Auto-Skalierungs-Gruppe ein. In der Connector-Gruppe sind maximal 4 ZTNA-Connectors zulässig.
  - Legen Sie den **Prozentsatz der Netzwerkbandbreite für die Skalierung** fest. Standard- und empfohlener Wert ist jeweils 70 %.
- Geben Sie den **Lizenzschlüssel** und den **geheimen Lizenzschlüssel** von Prisma Access ZTNA-Connector ein, die Sie aus dem Prisma SASE-Portal abgerufen haben.

 ©2025 Palo Alto Networks, Inc.




### „ZTNA-Connector – zweiarmig“ in AWS bereitstellen

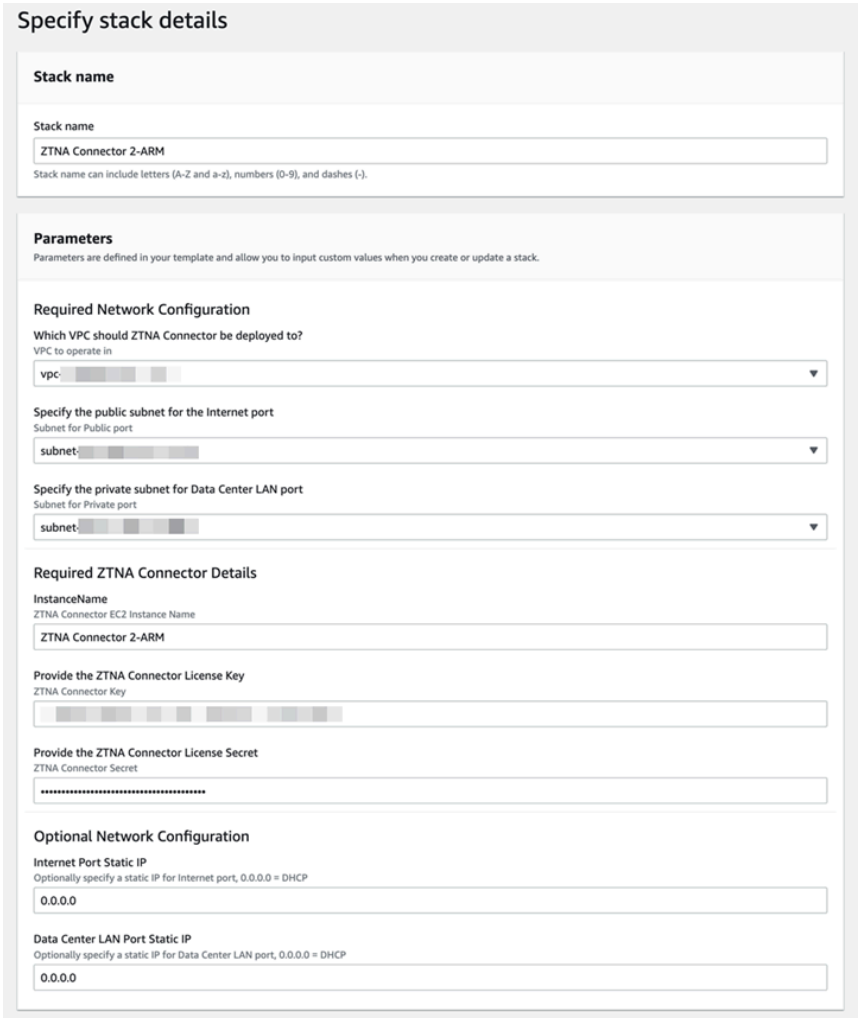
Befolgen Sie diese Schritte, um den zweiarmigen ZTNA-Connector in AWS bereitzustellen.

**STEP 1 |** Wählen Sie die CloudFormation-Vorlage „Prisma Access ZTNA-Connector – einarmig“ aus.

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Gehen Sie auf der Seite **Stackdetails angeben** wie folgt vor:

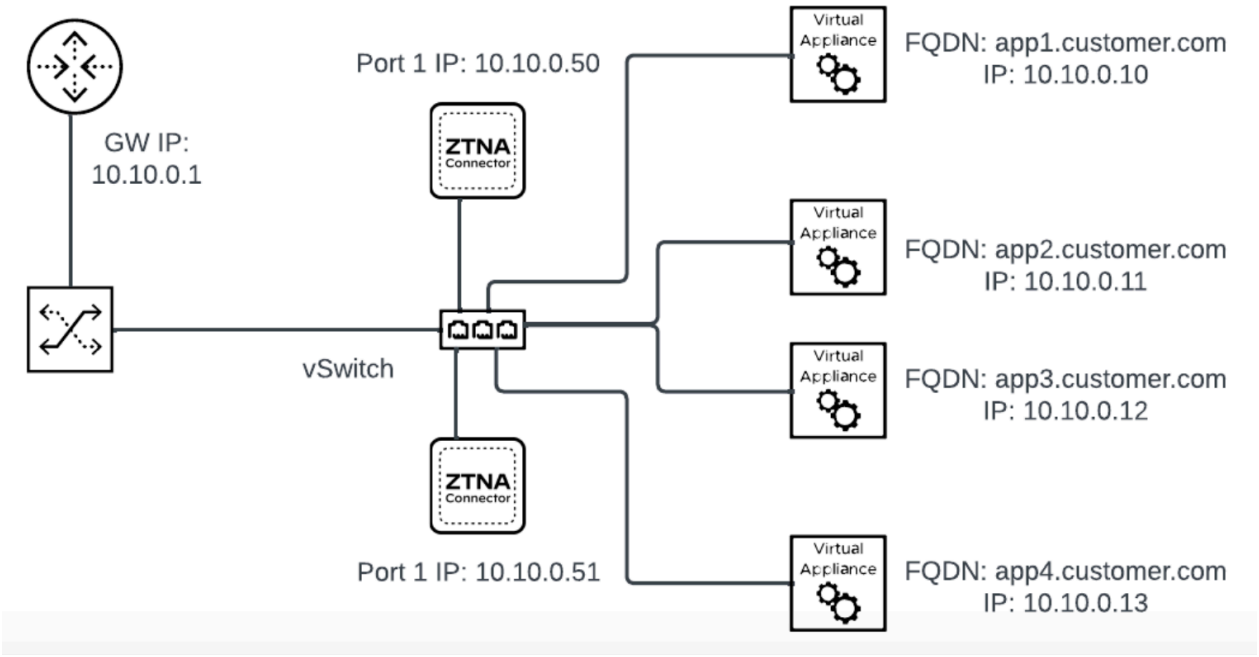
- Geben Sie den **Stacknamen** für die Bereitstellung ein.
- Geben Sie die in Ihrer Stackvorlage definierten Parameter im Abschnitt **Parameter** an.
  - Wählen **Sie aus, in welcher VPC der ZTNA-Connector bereitgestellt werden soll**.
  - **Geben Sie das öffentliche Subnetz für den Internetport** für die WAN-Konnektivität zu IPSec an. Dieses Subnetz muss mit einem NAT-Gateway für die Internetverbindung verbunden werden.
  - **Geben Sie das private Subnetz für den LAN-Port des Rechenzentrums** ein, an dem Sie Anwendungen bereitgestellt haben, die mit diesem Konnektor eingebunden werden sollen.
- Geben Sie den **Instanznamen** ein.
- Geben Sie den **Lizenzschlüssel** und den **geheimen Lizenzschlüssel** von Prisma Access ZTNA-Connector ein, die Sie aus dem Prisma SASE-Portal abgerufen haben.



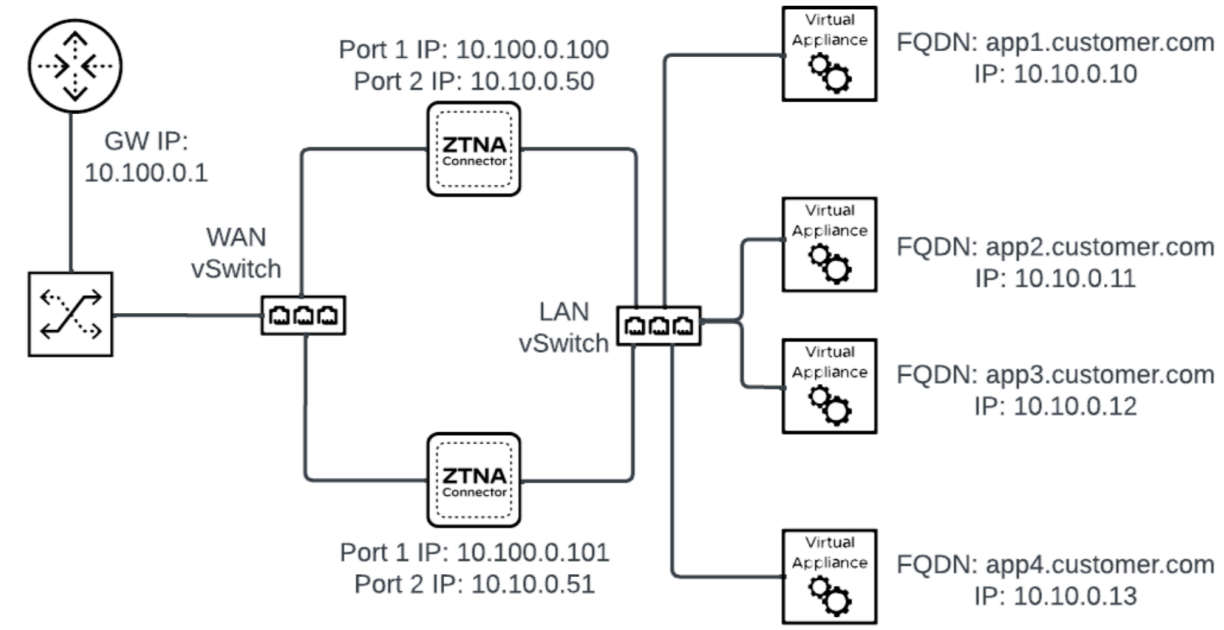

 ©2025 Palo Alto Networks, Inc.

# VMware ESXi-Bereitstellungen, unterstützt von Prisma Access ZTNA-Connector

Im folgenden Diagramm ist ein Beispiel für ein ZTNA-Connector-Netzwerk dargestellt, das VMware ESXi im einarmigen Modus mit einem NAT-Gateway verwendet.




Das folgende Diagramm zeigt das Beispiel einer ZTNA-Connector-Netzwerkbereitstellung mit VMware ESXi im zweiarmigen Modus mit einem NAT-Gateway.




 ©2025 Palo Alto Networks, Inc.

## ZTNA-Connector in VMware ESXi einbinden

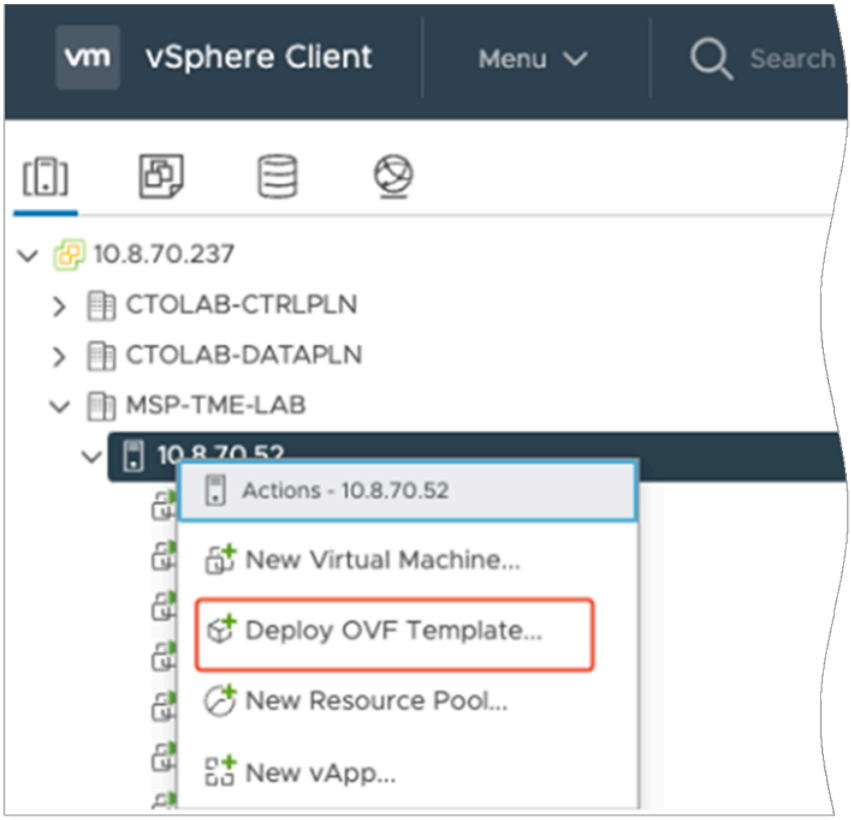
Gehen Sie wie folgt vor, um einen ZTNA-Connector in VMware ESXi einzubinden. Lesen Sie vor Beginn unbedingt die Anforderungen und Richtlinien für ZTNA im Allgemeinen und für VMware ESXi-Bereitstellungen im Besonderen.

Lesen Sie vor Beginn die Anforderungen und Richtlinien sowie die FQDNs und Ports, die Sie konfigurieren müssen, um ZTNA-Connector mit VMware ESXi zu verwenden.

**STEP 1 |** Laden Sie das VMware ESXi-Image für den ZTNA-Connector herunter, das Sie im Kunden-Support-Portal unter **Updates** > **Software-Updates** > **Prisma Access ZTNA-Connector für VMware** finden.

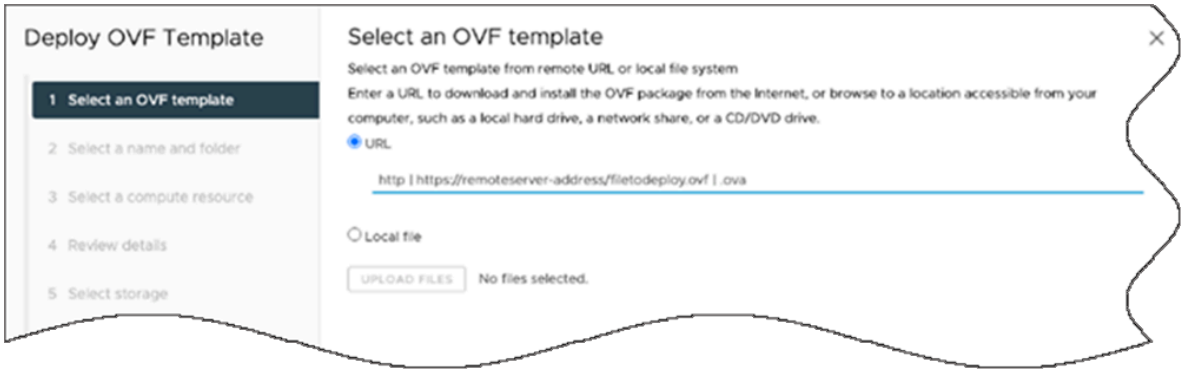
*Laden Sie eine Versionsdatei „1-nic“ für die einarmige Bereitstellung und eine Versionsdatei „2-nic“ für die zweiarmige Bereitstellung herunter.*

**STEP 2 |** Öffnen Sie VMware vCenter, klicken Sie mit der rechten Maustaste auf den Host und wählen Sie **Bereitstellen einer OVF-Vorlage** aus.

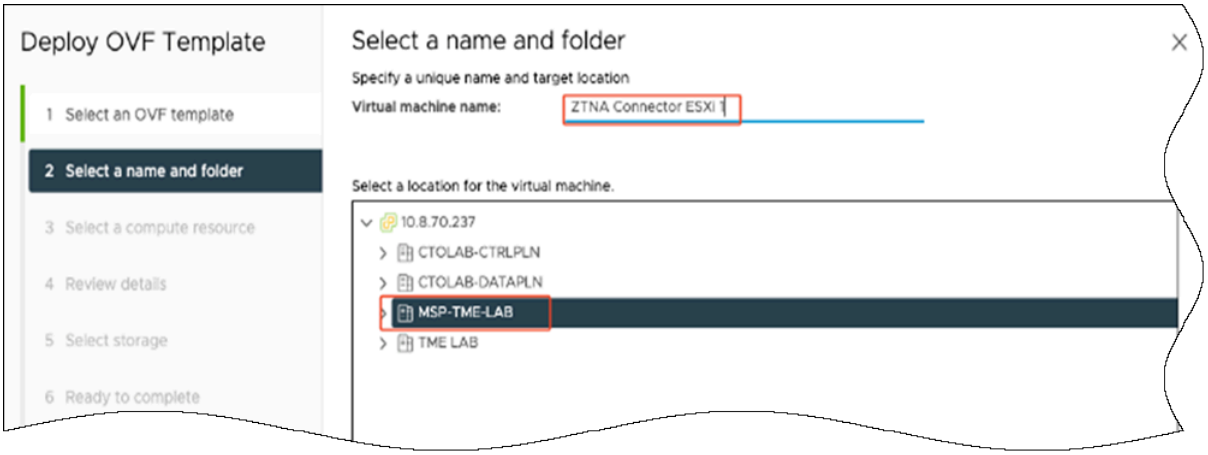



 ©2025 Palo Alto Networks, Inc.

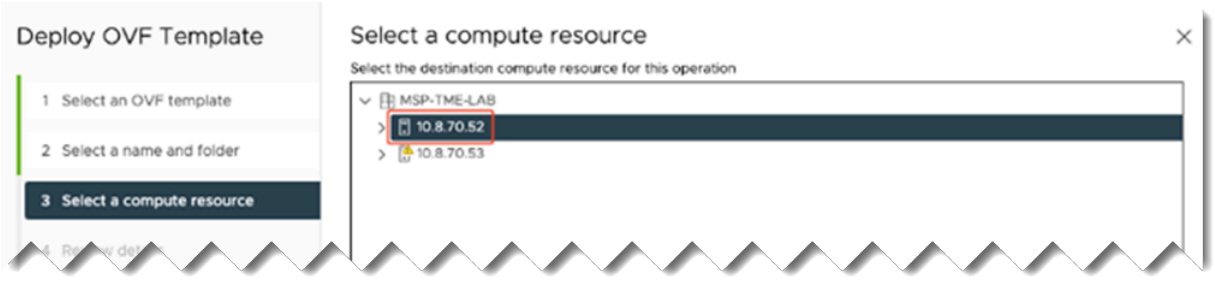
**STEP 3 |** Wählen Sie den Standort aus der Connector-OVA aus (entweder eine URL oder eine lokale Datei), und wählen Sie **Weiter** aus.




**STEP 4 |** Geben Sie den Namen der virtuellen Maschine (VM) und einen Standort für die VM ein.

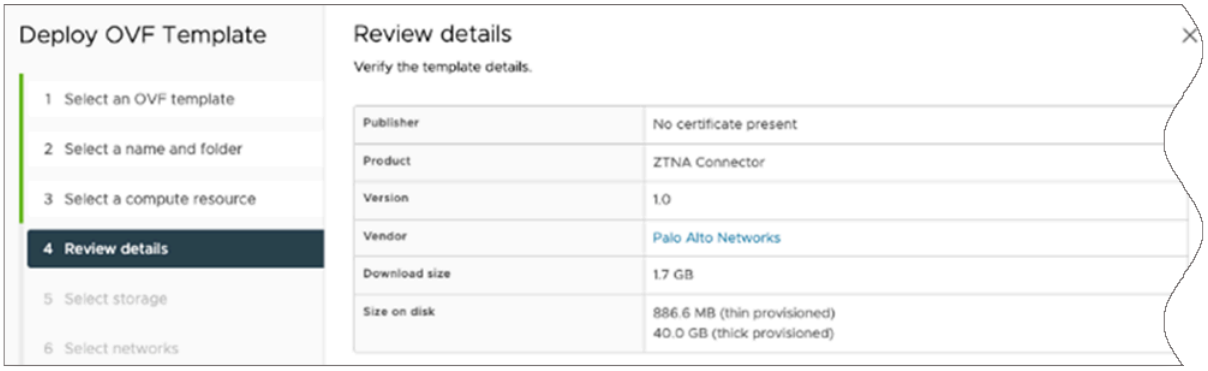



**STEP 5 |** Wählen Sie die Compute-Ressource für die VM aus.

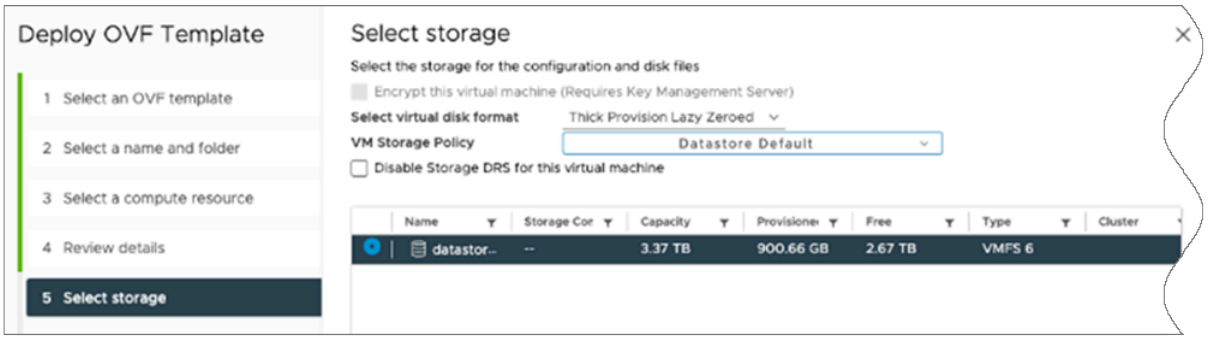



 ©2025 Palo Alto Networks, Inc.

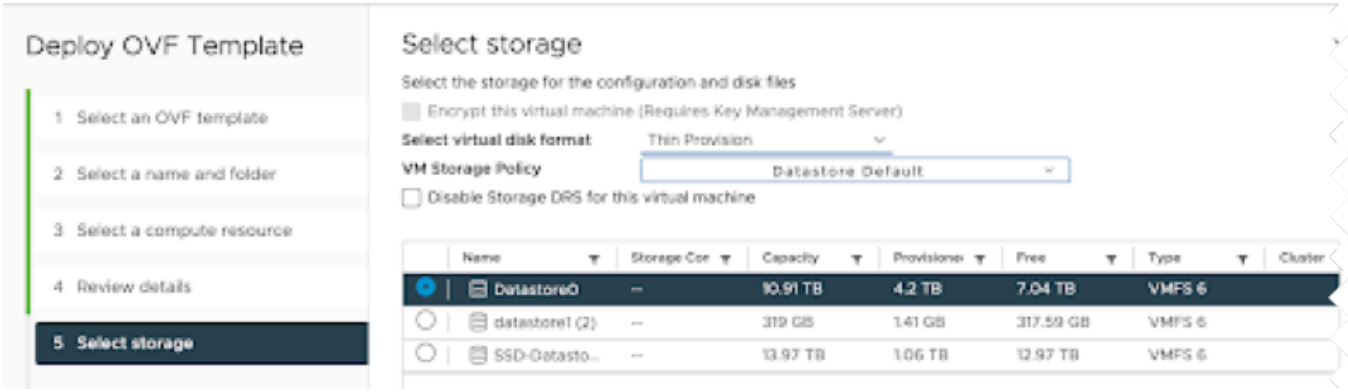
**STEP 6 |** Überprüfen Sie die Details für die Vorlage und wählen Sie **Weiter** aus.




**STEP 7 |** Wählen Sie **Thick Provision Lazy Zeroed** für das Format des virtuellen Datenträgers und den entsprechenden Datenspeicher für die ZTNA Connector-VM aus.



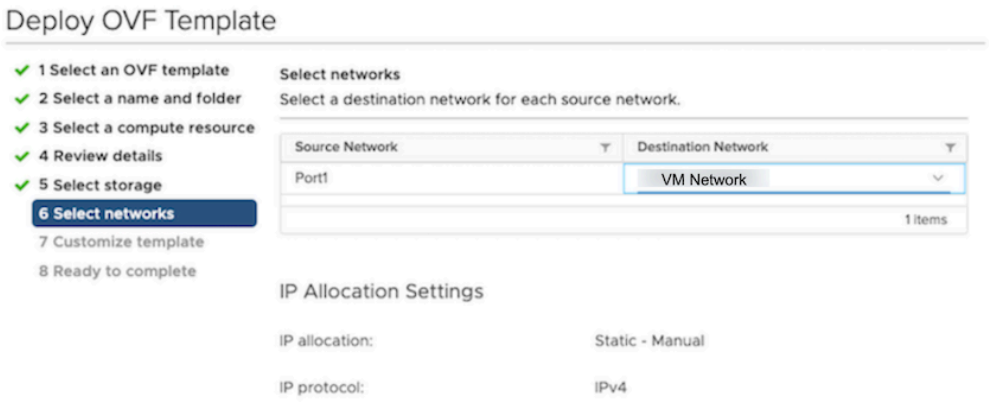

Optional Wählen Sie **Thin Provision** für das Format des virtuellen Datenträgers und den entsprechenden Datenspeicher für die ZTNA-Connector-VM aus, wobei der Server je nach Anforderung nur den Speicherplatz zuweist, den der Host benötigt.



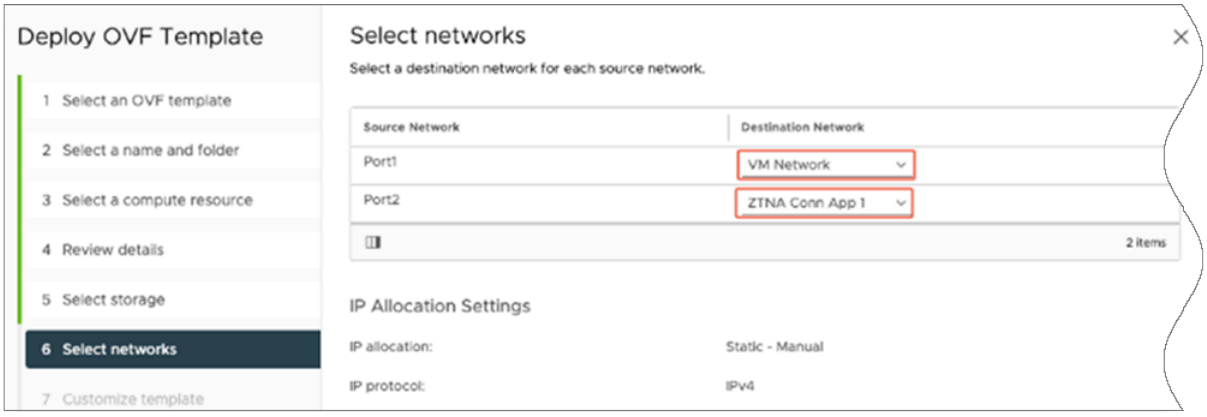

 ©2025 Palo Alto Networks, Inc.

**STEP 8 |** Wählen Sie die Netzwerke (für Port 1 und Port 2) für die Schnittstellen aus, die Sie mit der OVA-Konfigurationsvorlage erstellt haben.

1. Wenn Sie einen einarmigen Steckverbinder bereitstellen, ist **Port 1** das Netzwerk, das WAN- und LAN-App-Server erreichen kann. Wählen Sie das WAN/LAN-Netzwerk für **Port 1** aus.




2. Wenn Sie einen zweiarmigen Konnektor bereitstellen, wählen Sie den Port mit Internetzugriff für **Port 1** und das mit dem App-Server verbundene Netzwerk für **Port 2** aus.
   - Port 1 ist der WAN-Port für die IPSec-Konnektivität Prisma Access.
   - Port 2 ist der Port für die App.




**STEP 9 |** Falls noch nicht geschehen, wählen Sie **Workflows** > **ZTNA-Connector** > **Konnektoren** aus, suchen Sie nach dem Konnektorobjekt, das Sie in Prisma Access erstellt haben, um es mit dieser VM zu verknüpfen, und wählen Sie **Token kopieren** auf der Registerkarte **Aktionen**

 ©2025 Palo Alto Networks, Inc.

(Schlüssel-Symbol) aus. Kopieren Sie anschließend die Werte für **Schlüssel** und **Geheimer Schlüssel**.



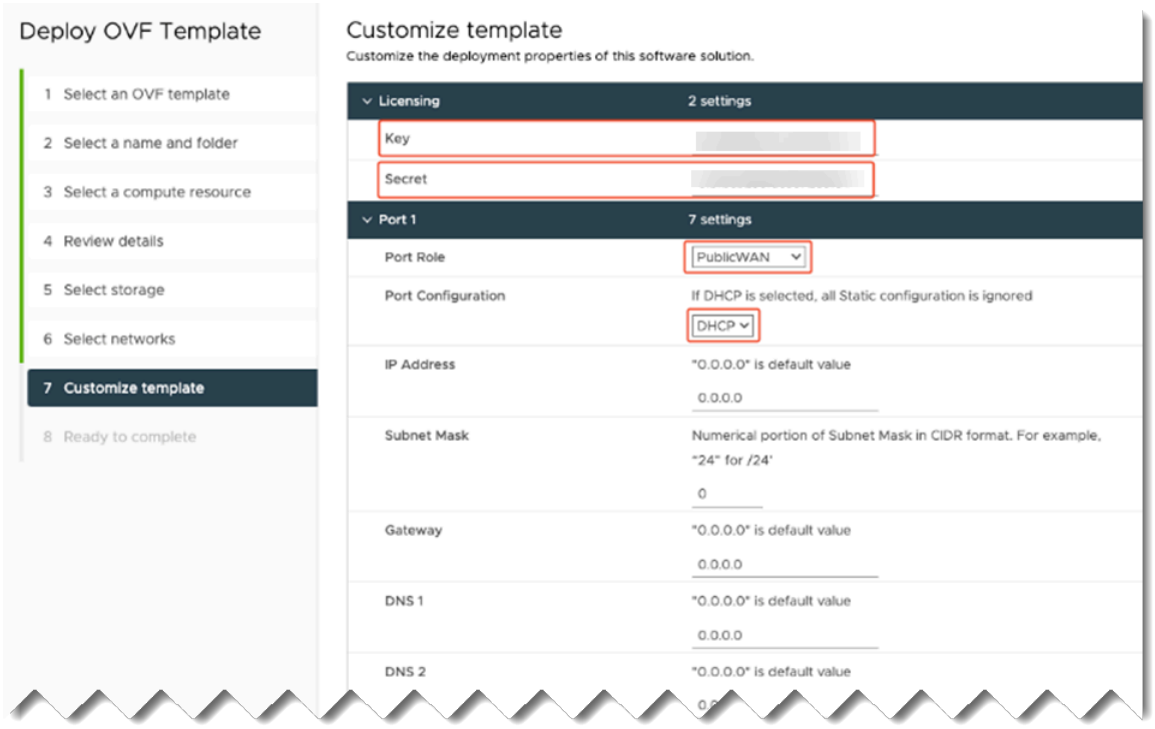

 ©2025 Palo Alto Networks, Inc.

**STEP 10 |** Nehmen Sie im Bildschirm **Vorlage anpassen** die folgenden Konfigurationsänderungen vor:

- **Lizenzierung**: Geben Sie die Werte für **Schlüssel** und **Geheimer Schlüssel** ein, die Sie aus dem Prisma SASE-Portal abgerufen haben.
- **Anschluss 1** (der mit Prisma Access verbundene Port) – Nehmen Sie die folgenden Änderungen vor:
  - **Rolle** – Öffentliches WAN.
  - **Port-Konfiguration** – Entweder **DHCP** oder **Statisch**.

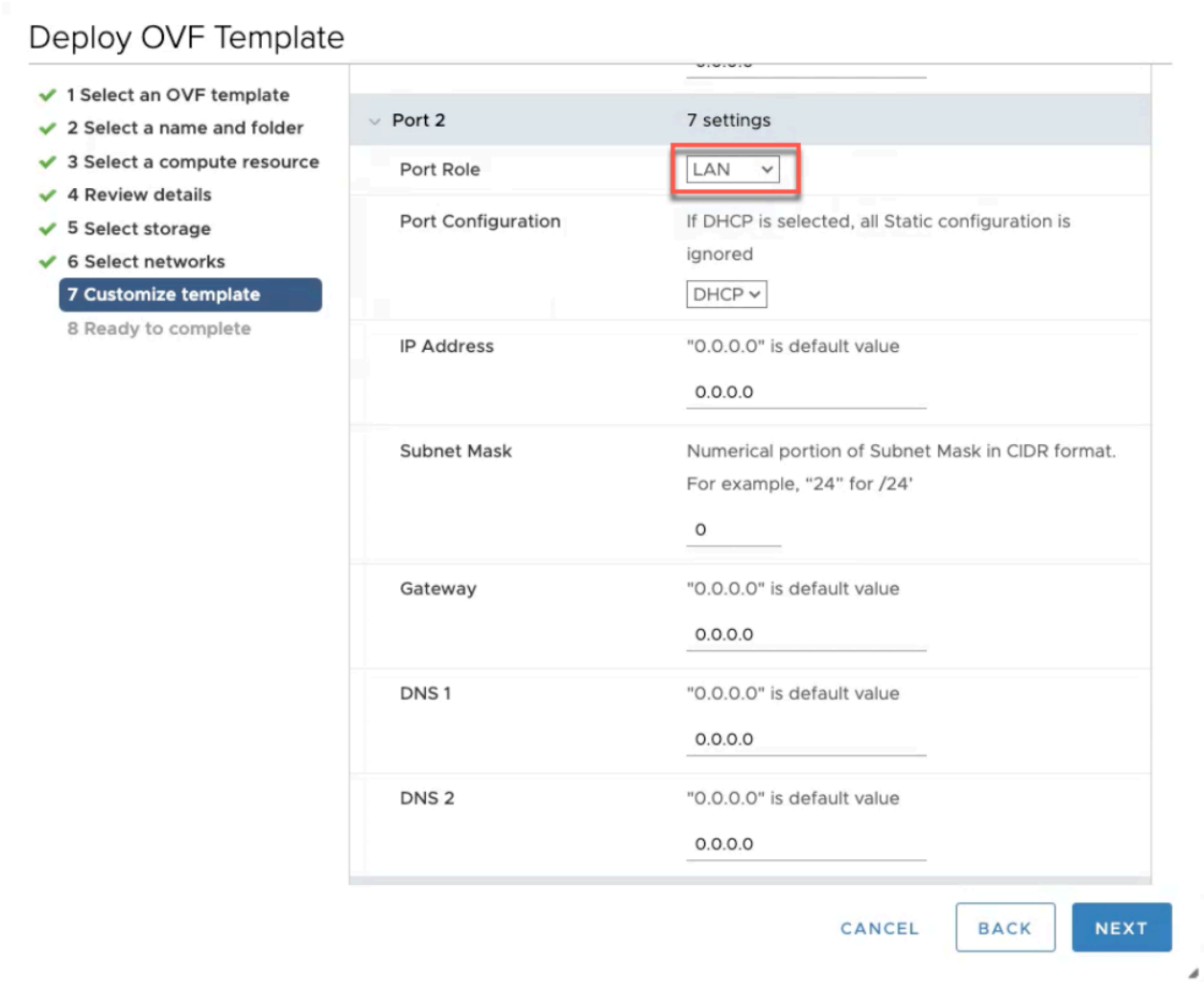
    Wenn Sie **Statisch** auswählen, geben Sie die IP-Adresse, die Subnetzmaske, das Gateway und einen oder zwei DNS-Serverwerte ein.

    Wenn Sie DHCP verwenden, belassen Sie die Standardnullen in den Feldern, wie im folgenden Screenshot dargestellt.



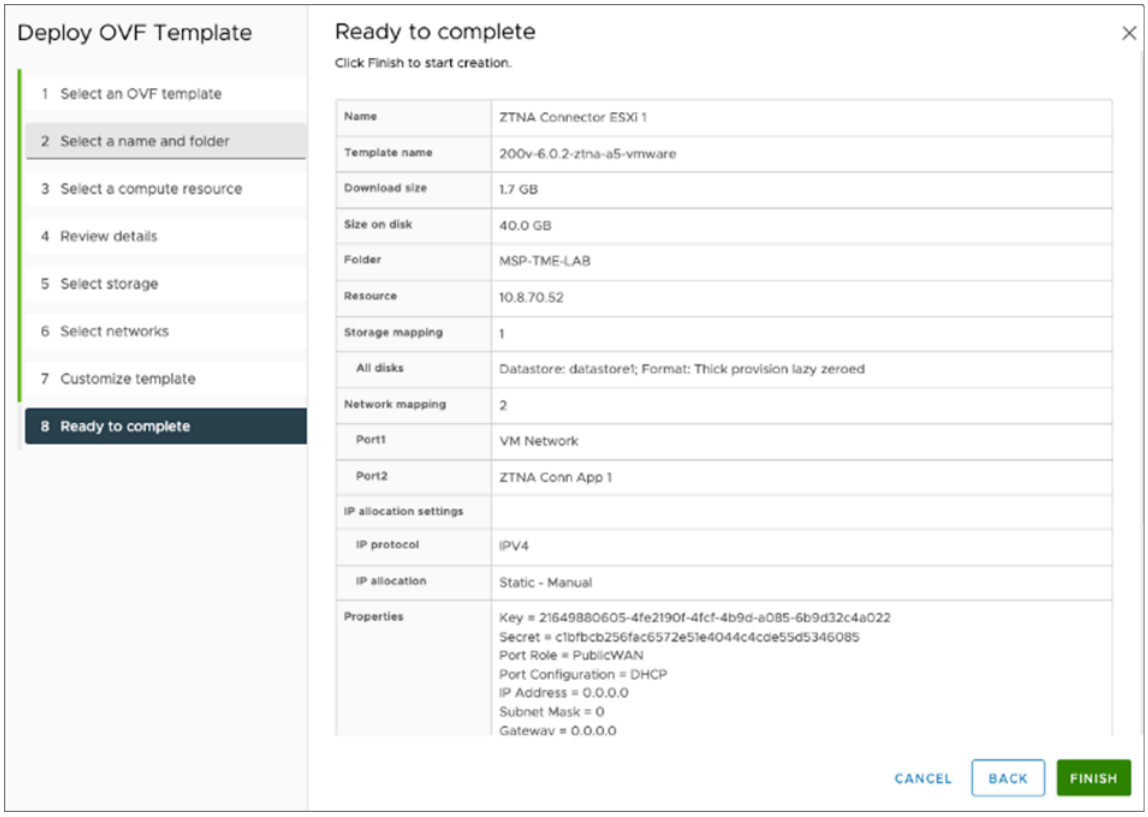

- Nur zweiarmige ESXi-Bereitstellungen Wenn Sie über eine zweiarmige Bereitstellung verfügen, konfigurieren Sie die LAN-IP-Schnittstelle **Port 2** mit den gleichen Regeln, die Sie auch auf **Port 1** in Schritt 10 angewandt haben.

 ©2025 Palo Alto Networks, Inc.




 ©2025 Palo Alto Networks, Inc.

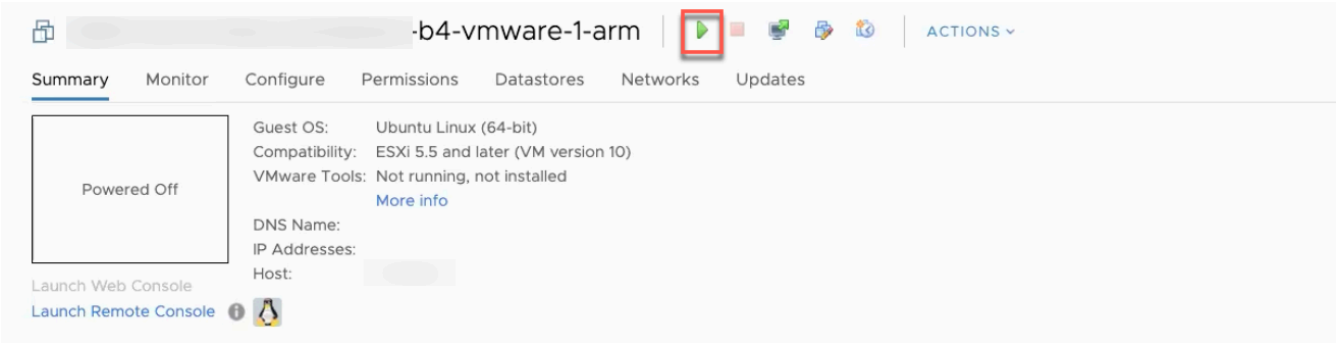
**STEP 11 |** Überprüfen Sie die Zusammenfassung und wählen Sie anschließend **Fertigstellen** aus.




 ©2025 Palo Alto Networks, Inc.

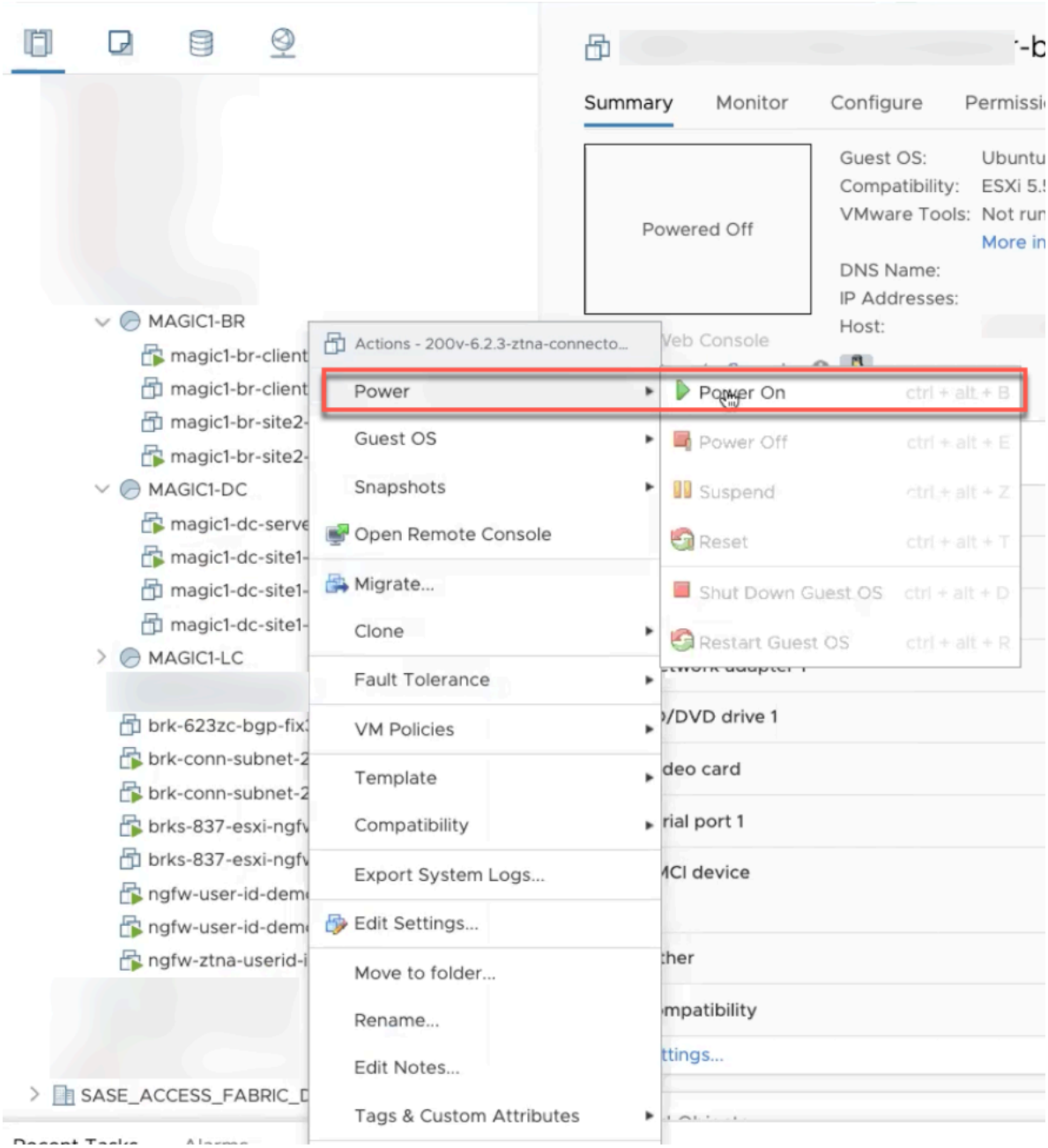
**STEP 12 |** Schalten Sie die VM mit einer der folgenden Methoden ein.

- Wählen Sie **Einschalten** aus, um den virtuellen Server zu starten.




- Klicken Sie mit der rechten Maustaste auf die Schnittstelle und wählen Sie **Einschalten** (**Stromversorgung** > **Einschalten**) aus.

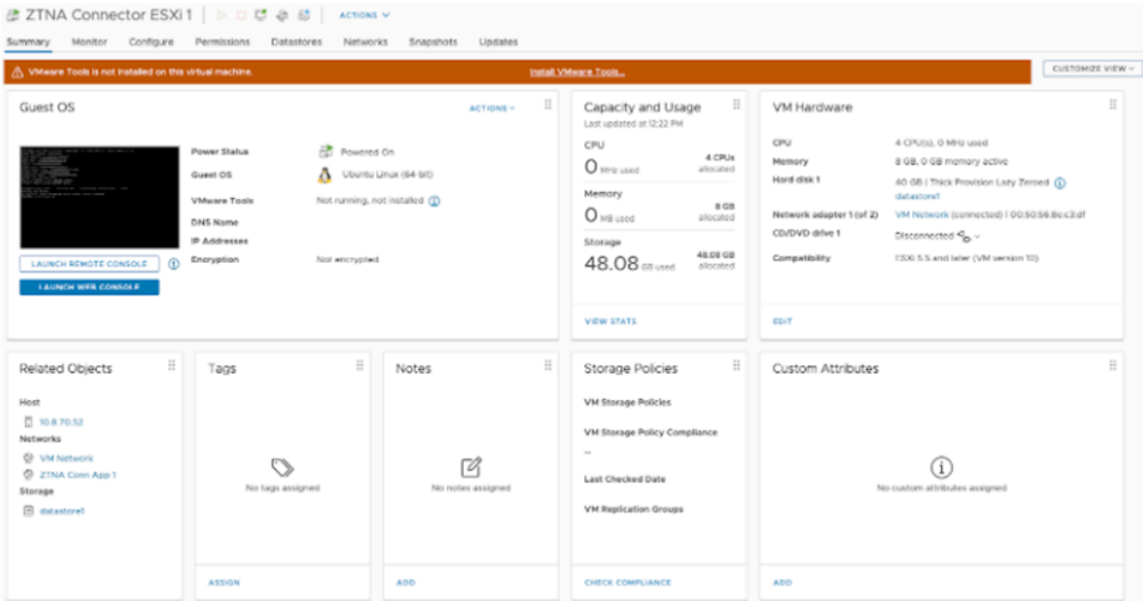

©2025 Palo Alto Networks, Inc.



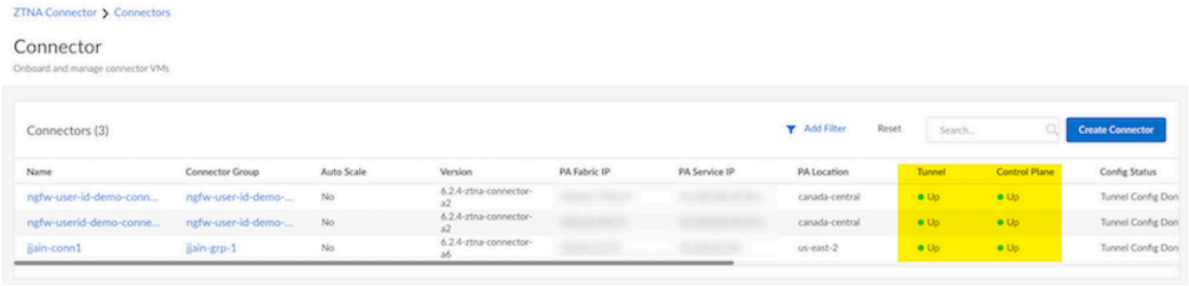

 ©2025 Palo Alto Networks, Inc.

**STEP 13 |** Vergewissern Sie sich nach der Bereitstellung der VM, dass sie hochgefahren wurde.

Nachdem der virtuelle ESXi-Server hochgefahren wurde, schließt Prisma Access die Konfiguration des Geräts ab, das als ZTNA-Connector verwendet werden soll.



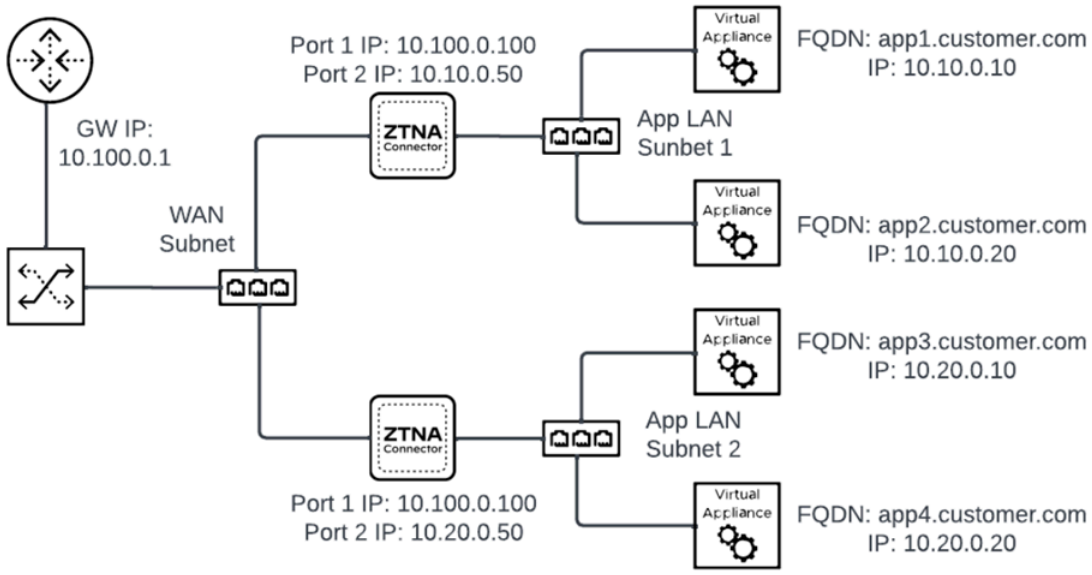

**STEP 14 |** Gehen Sie im Prisma SASE-Portal zu **Workflows** > **ZTNA-Connector** > **Konnektoren**, suchen Sie den Konnektor, den Sie verwenden möchten, und vergewissern Sie sich, dass **Tunnel aktiv** angezeigt wird.




# KVM-Bereitstellungen, die von Prisma Access ZTNA-Connector unterstützt werden

Sie stellen eine Kernel-basierte virtuelle Maschine (KVM) mithilfe einer zweiarmigen Bereitstellung bereit. Im folgenden Diagramm ist ein Beispiel für ein ZTNA-Connector-Netzwerk dargestellt, das eine KVM im zweiarmigen Modus mit einem NAT-Gateway verwendet.

 ©2025 Palo Alto Networks, Inc.




## ZTNA-Connector mithilfe von KVM einbinden

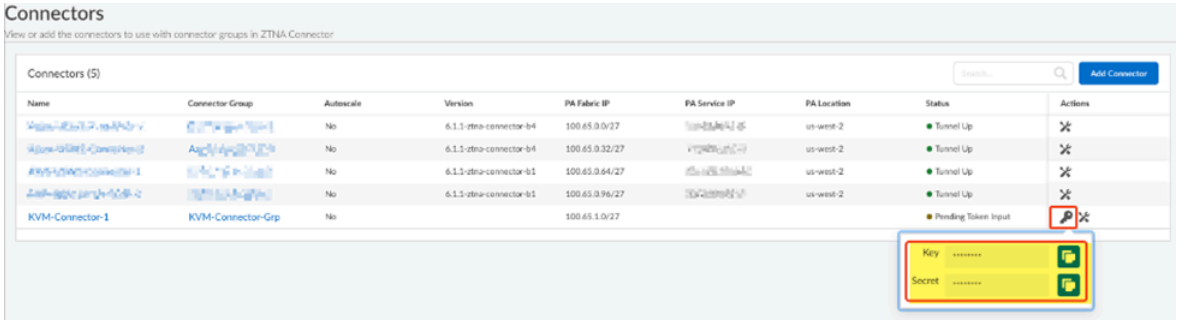
Gehen Sie wie folgt vor, um einen ZTNA-Connector mit Kernel-based Virtual Machine (KVM) einzubinden.

Stellen Sie vor Beginn sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Laden Sie das KVM-Image für den ZTNA-Connector herunter, das Sie im Kunden-Support-Portal unter **Updates** > **Software-Updates** > **Prisma Access ZTNA-Connector für KVM** finden.
- Stellen Sie sicher, dass Sie über einen KVM-Host verfügen, der die Mindestanforderungen an Hosting-Umgebungen für ZTNA-Connector erfüllt.

**STEP 1 |** Erstellen Sie eine Konnektorgruppe für den KVM-Host.

**STEP 2 |** Wählen Sie **Workflows** > **ZTNA-Connector** > **Konnektoren** aus und suchen Sie den Konnektor, den Sie für den KVM-Host erstellt haben, wählen Sie **Token kopieren** im Bereich **Status** aus und kopieren Sie die Werte für **Schlüssel** und **Geheimer Schlüssel**.




**STEP 3 |** Laden Sie das **qcow**-Image, das Sie vom CSP heruntergeladen haben, auf den KVM-Host hoch.

 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** Falls noch nicht geschehen, erstellen und verknüpfen Sie die virtuellen Brückenschnittstellen auf dem KVM-Host und bereiten Sie den Host durch Eingabe der folgenden Befehle vor:

- `brctl addbr virbr0`
- `brctl addbr virbr0`
- `brctl addbr virbr1`
- `brctl addif virbr1 ens192`

**STEP 5 |** Stellen Sie die VM auf dem KVM-Host bereit, indem Sie den Befehl `virt-install` mit den folgenden Optionen ausführen:

- `-name` ist der Name der virtuellen Maschine.
- `-vcpu` ist **4**.
- `-memory` ist **16384** (16 GB).
- `-disk` ist der Speicherort und der Name des **qcow**-Image auf dem KVM-Host.
- `-network` verweist auf die virtuellen Schnittstellen, die an diese VM angehängt werden sollen (Sie müssen Schnittstellen für einen ZTNA-Connector bereitstellen).

Der folgende Beispielbefehl wird zur Bereitstellung des KVM-Hosts verwendet, wobei <kvm-file-name> der Name der qcow-Datei ist, die Sie vom CSP heruntergeladen haben:

```
virt-install --name ztna-conn-1 --vcpus 4 --memory 16384 --disk ./
<kvm-file-name> --import --network bridge=virbr0,model=virtio --
network bridge=virbr1,model=virtio
```

**STEP 6 |** Stellen Sie eine Verbindung mit der VM-Konsole her, indem Sie den folgenden Befehl eingeben:

```
virsh console ztna-conn-1
```

Es wird ein interaktives CLI-Installationsprogramm gestartet.

**STEP 7 |** Konfigurieren Sie das ION-Modell, den Schlüssel und den geheimen Schlüssel.

1. Wählen Sie **1** (das ION-Modell **ion 200v**) aus den angezeigten Optionen aus.

```
root@ubuntu-kvm-vm:/home/ubuntu-kvm/Desktop# virsh console
 ztna-conn-1 Connected to domain ztna-conn-1 Escape character
 is ^] Select an ION model: 1) ion 200v 2) ion 3102v 3) ion
 3104v 4) ion 3108v 5) ion 7108v 6) ion 7116v 7) ion 7132v 8)
 ion 9100v Choose a Number or (Q)uit: 1 CPU: Passed (needed
 4) Memory: Passed (needed 8.0G) Disk: Could not verify
 (needs 40.0G) Network: Passed (needed 1) Select an item to
 modify, or submit config: 1) Model : ion 200v 2) ION Key :
 3) Secret Key : 4) Controller 1 : Controller - DHCP 5) Port
 1 : Disabled/Unused 6) Port 2 : Disabled/Unused 7) Port 3 :
 Disabled/Unused 8) Port 4 : Disabled/Unused 9) Port 5 :
 Disabled/Unused 10) Port 6 : Disabled/Unused 11) Port 7 :
 Disabled/Unused 12) Port 8 : Disabled/Unused 13) Port 9 :
 Disabled/Unused 14) Submit and restart
```

 ©2025 Palo Alto Networks, Inc.

2. Geben Sie den Schlüssel vom Konnektor ein, indem Sie Option **2** auswählen und den Schlüssel eingeben, den Sie in der Benutzeroberfläche von ZTNA-Connector gespeichert haben.

```
Choose a Number or (Q)uit: 2 Enter ION Key[None]: xxxxxxxxxx-
yyyyyyyy-zzz-1234-1234-abcdefghijkl Select an item to modify,
 or submit config: 1) Model : ion 200v 2) ION Key : xxxxxxxxx-
yyyyyyyy-zzz-1234-1234-abcdefghijkl 3) Secret Key : 4)
 Controller 1 : Controller - DHCP 5) Port 1 : Disabled/Unused
 6) Port 2 : Disabled/Unused 7) Port 3 : Disabled/Unused 8)
 Port 4 : Disabled/Unused 9) Port 5 : Disabled/Unused 10) Port
 6 : Disabled/Unused 11) Port 7 : Disabled/Unused 12) Port 8 :
 Disabled/Unused 13) Port 9 : Disabled/Unused 14) Submit and
 restart
```

3. Geben Sie den geheimen Schlüssel für ZTNA-Connector ein, indem Sie Option **3** auswählen und den geheimen Schlüssel eingeben, den Sie in der Benutzeroberfläche von ZTNA-Connector gespeichert haben.

```
Choose a Number or (Q)uit: 3 Enter ION secret[None]: abcde12345
 Select an item to modify, or submit config: 1) Model :
 ion 200v 2) ION Key : xxxxxxxxx-yyyyyyyy-zzz-1234-1234-
abcdefghijkl 3) Secret Key : abcde12345 4) Controller 1 :
 Controller - DHCP 5) Port 1 : Disabled/Unused 6) Port 2 :
 Disabled/Unused 7) Port 3 : Disabled/Unused 8) Port 4 :
 Disabled/Unused 9) Port 5 : Disabled/Unused 10) Port 6 :
 Disabled/Unused 11) Port 7 : Disabled/Unused 12) Port 8 :
 Disabled/Unused 13) Port 9 : Disabled/Unused 14) Submit and
 restart
```

**STEP 8 |** Konfigurieren Sie WAN-Portoptionen.

1. Wählen Sie Option **5** (Port 1) aus.

```
Choose a Number or (Q)uit: 5 Port 1: 1) Role : Disable 2)
 Cancel Port changes 3) Apply and return
```

2. Wählen Sie Option **1** (Öffentlich/WAN) aus.

```
Choose a Number or (Q)uit: 1 Select Port Role: 1) Internet
 facing port (PublicWAN) 2) Private WAN port (PrivateWAN)
 3) Bypass Port Pair 1 (WAN Port) 4) Bypass Port Pair 1 (LAN
 Port) 5) Bypass Port Pair 2 (WAN Port) 6) Bypass Port Pair
 2 (LAN Port) 7) Bypass Port Pair 3 (WAN Port) 8) Bypass Port
 Pair 3 (LAN Port) 9) Bypass Port Pair 4 (WAN Port) 10) Bypass
 Port Pair 4 (LAN Port) 11) Disabled/Unused
```

3. (Optional) Wenn Sie eine statische IP-Adresse festlegen müssen, wählen Sie Option **2** aus und legen Sie die Parameter für IP-Adresse, Gateway und DNS-Server fest. Anderenfalls wählen Sie **1** aus.

```
Choose a Number or (Q)uit: 1 Port 1: 1) Role : PublicWAN 2)
 Config via : DHCP 3) Cancel Port changes 4) Apply and return
```

 ©2025 Palo Alto Networks, Inc.

4. Wählen Sie Option **4** aus, um zum Hauptmenü zurückzukehren.

```
Choose a Number or (Q)uit: 4 Select an item to modify, or
 submit config: 1) Model : ion 200v 2) ION Key : xxxxxxxxx-
yyyyyyyy-zzz-1234-1234-abcdefghijkl 3) Secret Key : abcde12345
 4) Controller 1 : Controller - DHCP 5) Port 1 : PublicWAN
 - DHCP 6) Port 2 : Disabled/Unused 7) Port 3 : Disabled/
Unused 8) Port 4 : Disabled/Unused 9) Port 5 : Disabled/Unused
 10) Port 6 : Disabled/Unused 11) Port 7 : Disabled/Unused
 12) Port 8 : Disabled/Unused 13) Port 9 : Disabled/Unused
 14) Submit and restart Select an item to modify, or submit
 config: 1) Model : ion 200v 2) ION Key : xxxxxxxxx-yyyyyyyy-
zzz-1234-1234-abcdefghijkl 3) Secret Key : abcde12345 4)
 Controller 1 : Controller - DHCP 5) Port 1 : PublicWAN - DHCP
 6) Port 2 : Disabled/Unused 7) Port 3 : Disabled/Unused 8)
 Port 4 : Disabled/Unused 9) Port 5 : Disabled/Unused 10) Port
 6 : Disabled/Unused 11) Port 7 : Disabled/Unused 12) Port 8 :
 Disabled/Unused 13) Port 9 : Disabled/Unused 14) Submit and
 restart
```

**STEP 9 |** Konfigurieren Sie LAN-Port-Optionen.

1. Wählen Sie Option **6** (Port 2) aus.

```
Choose a Number or (Q)uit: 6 Port 2: 1) Role : Disable 2)
 Cancel Port changes 3) Apply and return
```

2. Wählen Sie Option **2** (Privates WAN) aus.

```
Choose a Number or (Q)uit: 2 Select Port Role: 1) Internet
 facing port (PublicWAN) 2) Private WAN port (PrivateWAN)
 3) Bypass Port Pair 1 (WAN Port) 4) Bypass Port Pair 1 (LAN
 Port) 5) Bypass Port Pair 2 (WAN Port) 6) Bypass Port Pair
 2 (LAN Port) 7) Bypass Port Pair 3 (WAN Port) 8) Bypass Port
 Pair 3 (LAN Port) 9) Bypass Port Pair 4 (WAN Port) 10) Bypass
 Port Pair 4 (LAN Port) 11) Disabled/Unused
```

3. (Optional) Wenn Sie eine statische IP-Adresse festlegen müssen, wählen Sie Option **2** aus und legen Sie die Parameter für IP-Adresse, Gateway und DNS-Server fest. Anderenfalls wählen Sie **1** aus.

```
Choose a Number or (Q)uit: 2 Port 2: 1) Role : PrivateWAN 2)
 Config via : DHCP 3) Cancel Port changes 4) Apply and return
```

4. Wählen Sie Option **4** aus, um zum Hauptmenü zurückzukehren.

```
Choose a Number or (Q)uit: 4 Select an item to modify, or
 submit config: 1) Model : ion 200v 2) ION Key : xxxxxxxxx-
yyyyyyyy-zzz-1234-1234-abcdefghijkl 3) Secret Key : abcde12345
 4) Controller 1 : Controller - DHCP 5) Port 1 : PublicWAN
 - DHCP 6) Port 2 : PrivateWAN - DHCP 7) Port 3 : Disabled/
Unused 8) Port 4 : Disabled/Unused 9) Port 5 : Disabled/Unused
 10) Port 6 : Disabled/Unused 11) Port 7 : Disabled/Unused
 12) Port 8 : Disabled/Unused 13) Port 9 : Disabled/Unused 14)
 Submit and restart
```

 ©2025 Palo Alto Networks, Inc.

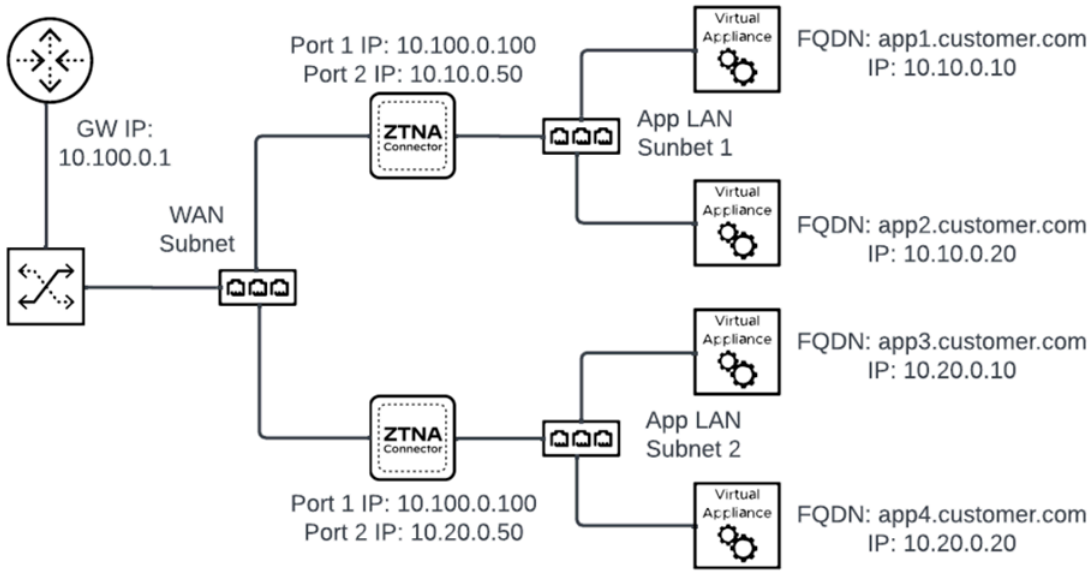
**STEP 10 |** Speichern und starten Sie den Konnektor neu.

```
Choose a Number or (Q)uit: 14 WARNING! After this configuration is
 submitted, all hardware will be signed, logged, and permanently
 tied to the ION Key/Secret Key in the Prisma SDWAN Cloud
 Controller. WHAT THIS MEANS is that hardware cannot be added/
removed (disks, network cards) after this 'SUBMIT' function. If any
 hardware changes are required beyond this 'SUBMIT', the ION will
 need to be re-deployed with a new ION Key and Secret Key. If there
 is a need to add or remove hardware, please answer 'N' below and
 shut down the ION and make the changes now. Submit these changes
 now?[N]: y Building configuration... [VFF:CFG] ZeroTouch Config
 Starting - config file parser [VFF:CFG] Attempting to load/parse
 as Config/INI file. [VFF:CFG] Successfully Loaded config style
 file. [VFF:CFG] Controller 1 successfully set to CONTROLLER/DHCP.
 [VFF:CFG] Port 1 successfully set to PUBLICWAN/DHCP. [VFF:CFG]
 Port 2 successfully set to PRIVATEWAN/DHCP. [VFF:CFG] WARN: Port 3
 had no config section. Defaulting to Disable. [VFF:CFG] WARN: Port
 4 had no config section. Defaulting to Disable. [VFF:CFG] WARN:
 Port 5 had no config section. Defaulting to Disable. [VFF:CFG]
 WARN: Port 6 had no config section. Defaulting to Disable.
 [VFF:CFG] WARN: Port 7 had no config section. Defaulting to
 Disable. [VFF:CFG] WARN: Port 8 had no config section. Defaulting
 to Disable. [VFF:CFG] WARN: Port 9 had no config section.
 Defaulting to Disable. [VFF:CFG] Success with Config/INI file
 parser. [VFF:KVM] Menu config end, continuing normal boot...
 Reboot-reason: manufacture
```

## Hyper-V-Bereitstellungen, die von Prisma Access ZTNA-Connector unterstützt werden

Sie stellen einen Microsoft Hyper-V Hypervisor mithilfe einer zweiarmigen Bereitstellung bereit. Im folgenden Diagramm ist ein Beispiel für ein ZTNA-Connector-Netzwerk dargestellt, das Hyper-V im zweiarmigen Modus mit einem NAT-Gateway verwendet.

 ©2025 Palo Alto Networks, Inc.




## ZTNA-Connector mithilfe von Hyper-V einbinden

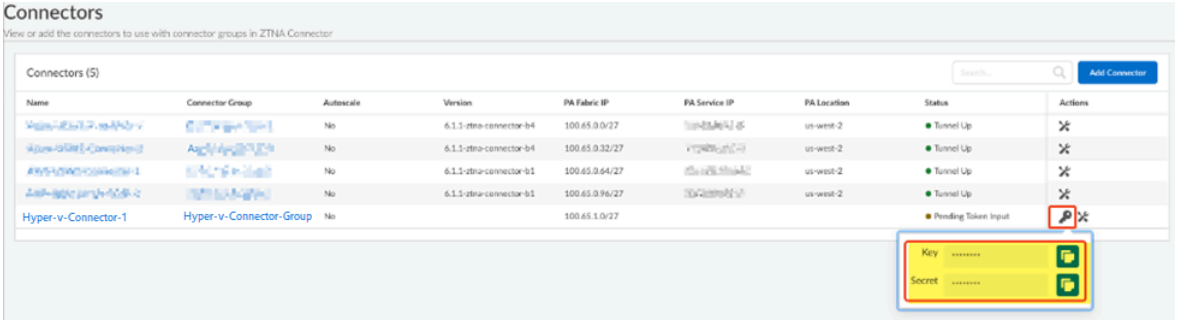
Gehen Sie wie folgt vor, um einen ZTNA-Connector mit einer virtuellen Microsoft Hyper-V-Maschine (Hyper-V-VM) einzubinden.

Stellen Sie vor Beginn sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Laden Sie das Hyper-V-Image für den ZTNA-Connector herunter, das Sie im Kunden-Support-Portal unter **Updates** > **Software-Updates** > **Prisma Access ZTNA-Connector für Hyper-V** finden.
- Stellen Sie sicher, dass Sie über eine Hyper-V-VM verfügen, die die Mindestanforderungen an Hosting-Umgebungen für ZTNA-Connector erfüllt.

**STEP 1 |** Erstellen Sie eine Konnektorgruppe und einen Konnektor für die Hyper-V-VM.

**STEP 2 |** Wählen Sie **Workflows** > **ZTNA-Connector** > **Konnektoren** aus und suchen Sie den Konnektor, den Sie für die Hyper-V-VM erstellt haben, wählen Sie **Token kopieren** im Bereich **Status** aus und kopieren Sie die Werte für **Schlüssel** und **Geheimer Schlüssel**.




**STEP 3 |** Laden Sie das **vhd**-Image, das Sie vom CSP heruntergeladen haben, auf die Hyper-V-VM hoch.

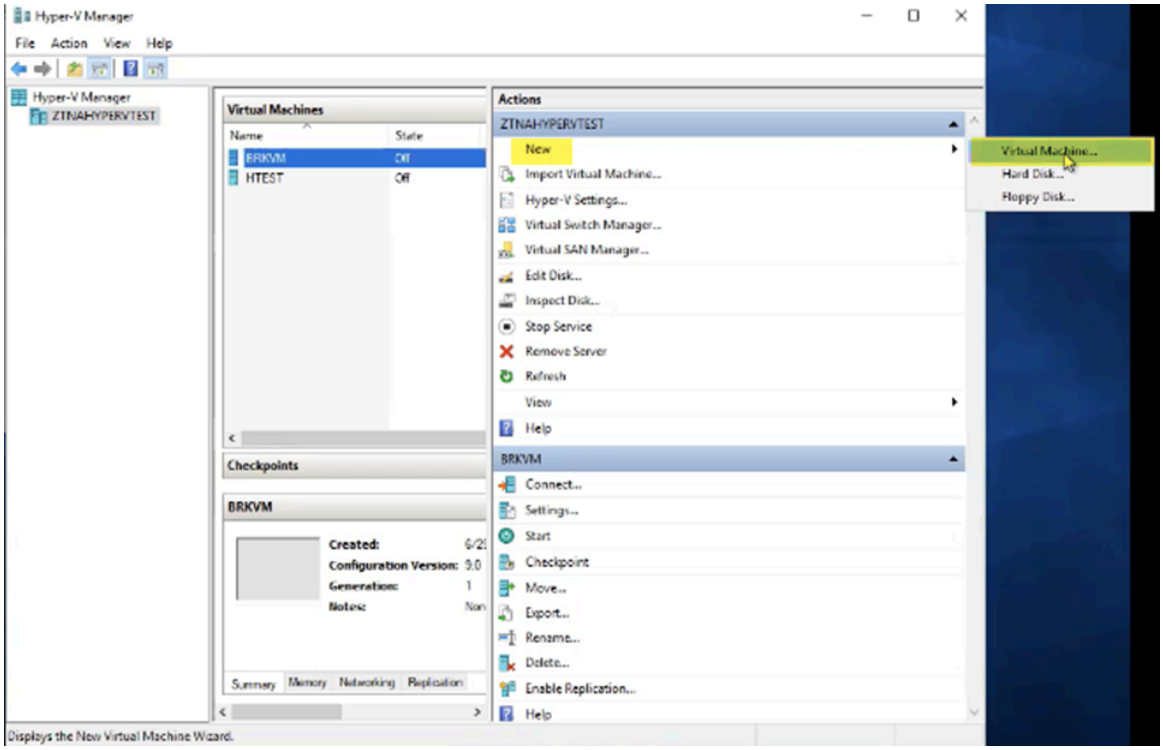
Stellen Sie sicher, dass der von Ihnen gewählte Standort über die Hyper-V-VM erreichbar ist.

Für jede Hyper-V-VM ist eine (vhd-) Datei erforderlich.

 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** Öffnen Sie den Hyper-V Manager und erstellen Sie eine neue virtuelle Maschine, indem Sie **Aktionen** > **Neu** > **Virtuelle Maschine** auswählen.

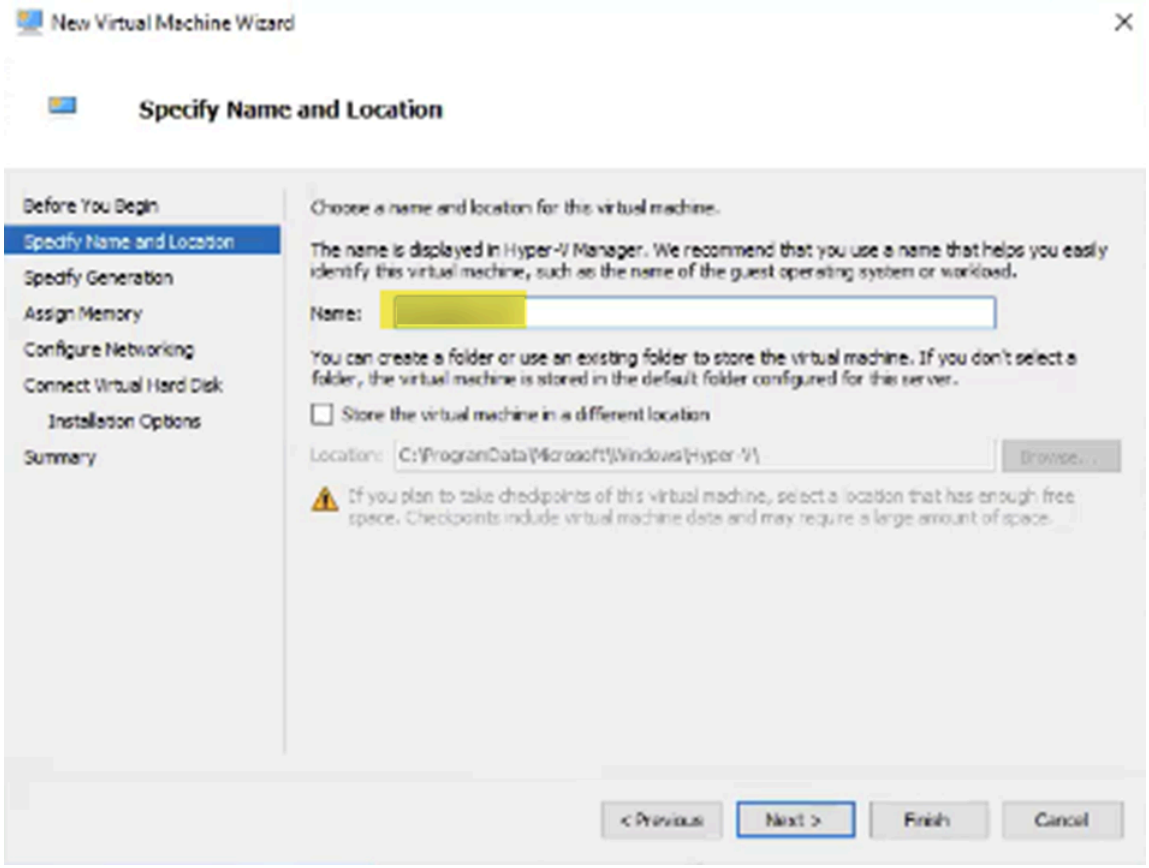
Dieser Workflow zeigt die Schritte, die Sie ausführen, um Hyper-V-VMs in einem Microsoft-Server bereitzustellen. Die Hyper-V-Benutzeroberfläche könnte in Ihrer Umgebung anders aussehen.




**STEP 5 |** Wählen Sie **Weiter** aus, um zum nächsten Bildschirm zu gelangen, und geben Sie einen eindeutigen Namen für die VM ein. Wählen Sie erneut **Weiter** aus, um auf die nächste Seite zu gelangen.

 ©2025 Palo Alto Networks, Inc.

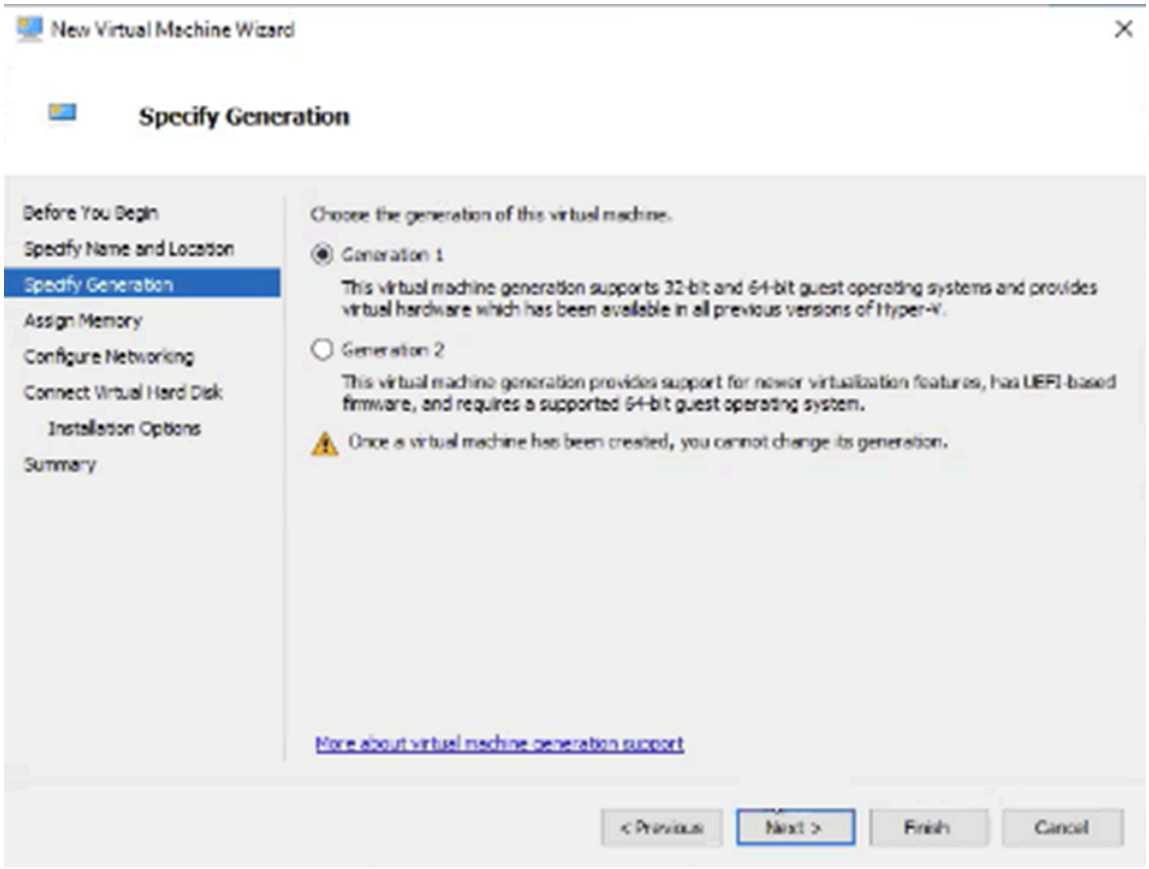
**STEP 6 |** (Optional) Zum Ändern des Standorts der VM **speichern Sie die virtuelle Maschine an einem anderen Standort** und wählen Sie den Standort aus.




 ©2025 Palo Alto Networks, Inc.

**STEP 7 |** Wählen Sie **Generation 1** als VM-Generation aus und wechseln Sie mit **Weiter** zur nächsten Seite.

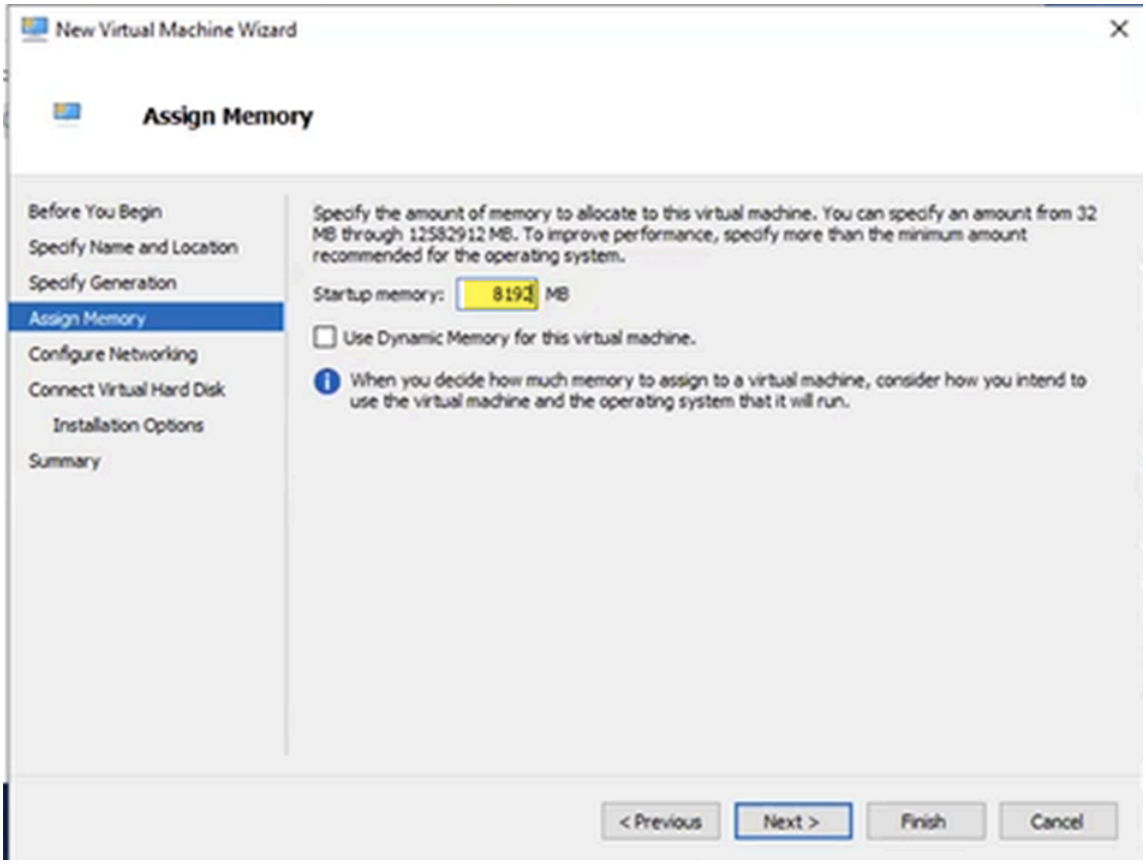
Diese Generation wird von der vhd-Datei von ZTNA-Connector unterstützt.




 ©2025 Palo Alto Networks, Inc.

**STEP 8 |** Weisen Sie der VM Speicher zu.

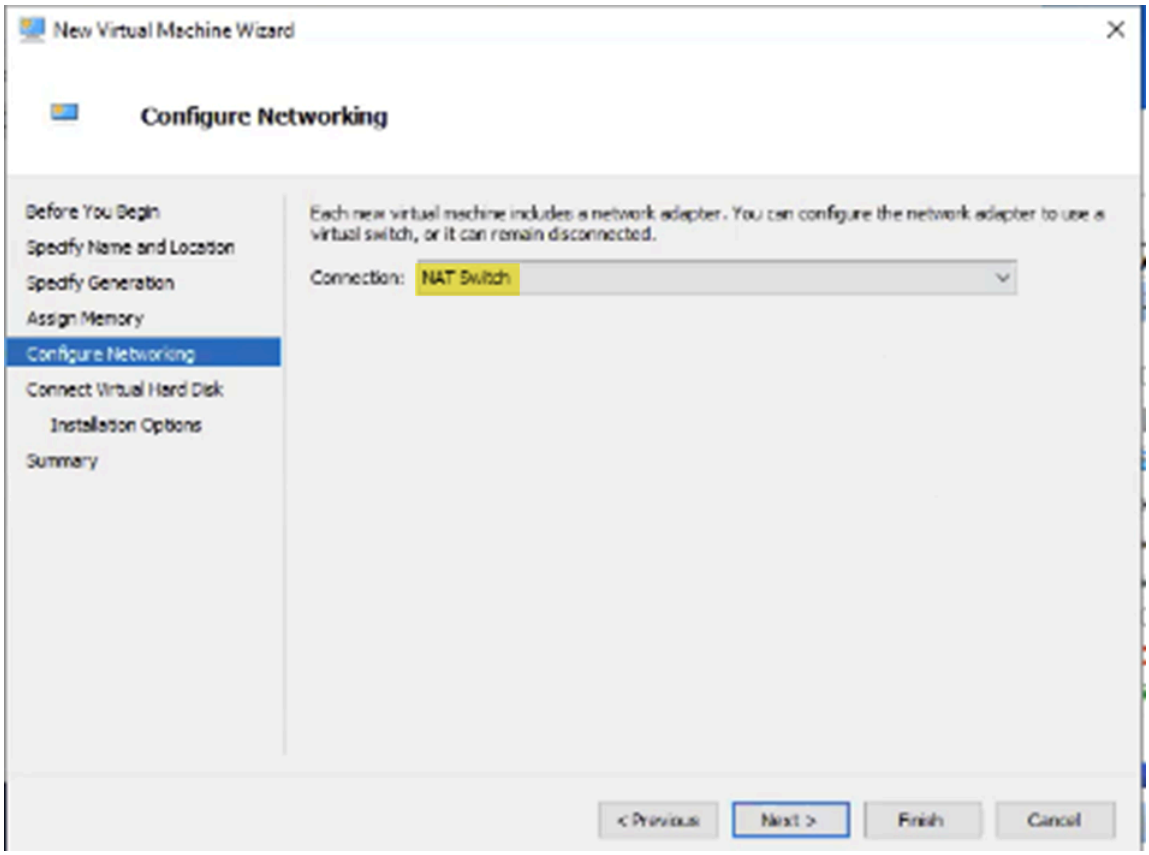
Weisen Sie einen Mindestspeicher von **8192** MB (8 GB) zu, der die Mindestanforderungen für eine Hyper-V-VM erfüllt, und wechseln Sie durch Auswählen von **Weiter** auf die nächste Seite.




 ©2025 Palo Alto Networks, Inc.

**STEP 9 |** Konfigurieren Sie das Netzwerk für Ihre VM und wählen Sie **Weiter** aus, um zur nächsten Seite zu wechseln.

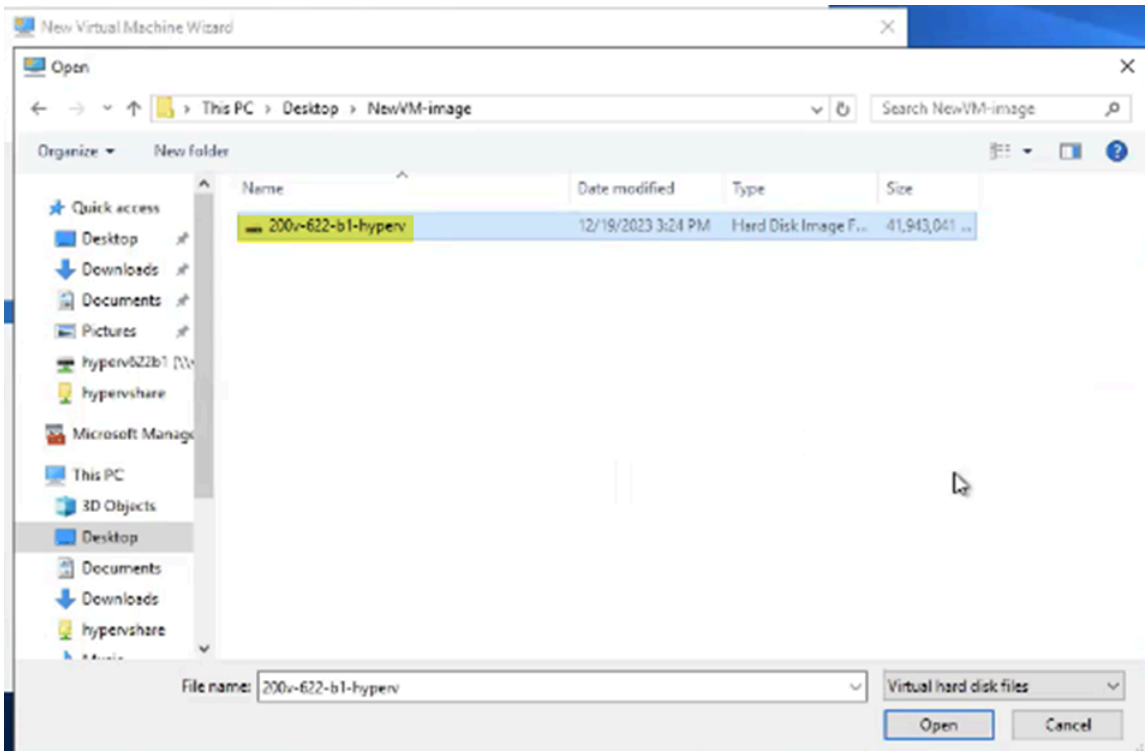
Welches Netzwerk Sie verwenden, hängt von Ihrer Konfiguration ab. In diesem Beispiel wird ein **NAT-Switch** für die Vernetzung verwendet.




 ©2025 Palo Alto Networks, Inc.

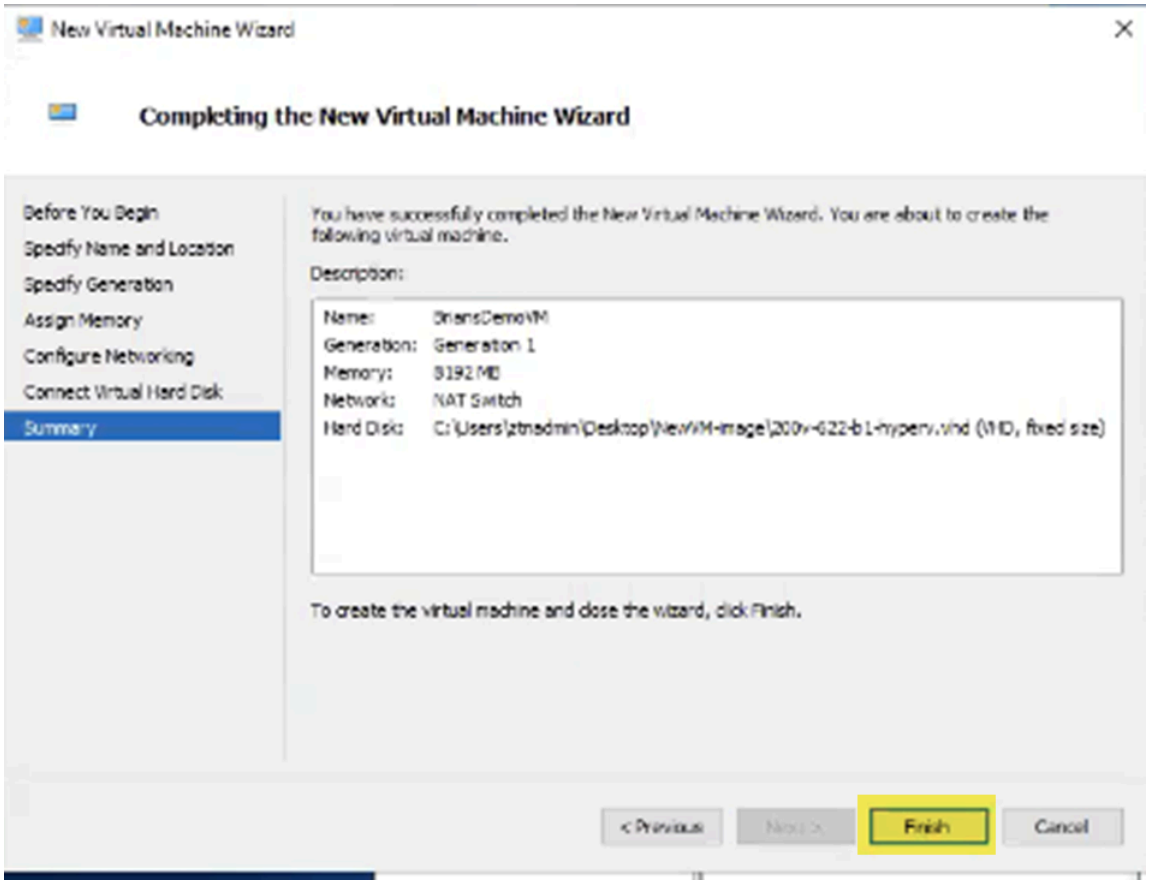
**STEP 10 |** Schließen Sie die virtuelle Festplatte an.

1. Wählen Sie **Bestehende virtuelle Festplatte verwenden** aus und **suchen** Sie nach der heruntergeladenen vhd-Datei.
2. Wählen Sie die heruntergeladene vhd-Datei aus. **Öffnen** Sie die Datei und wählen Sie **Weiter** aus, um zur nächsten Seite zu wechseln.




 ©2025 Palo Alto Networks, Inc.

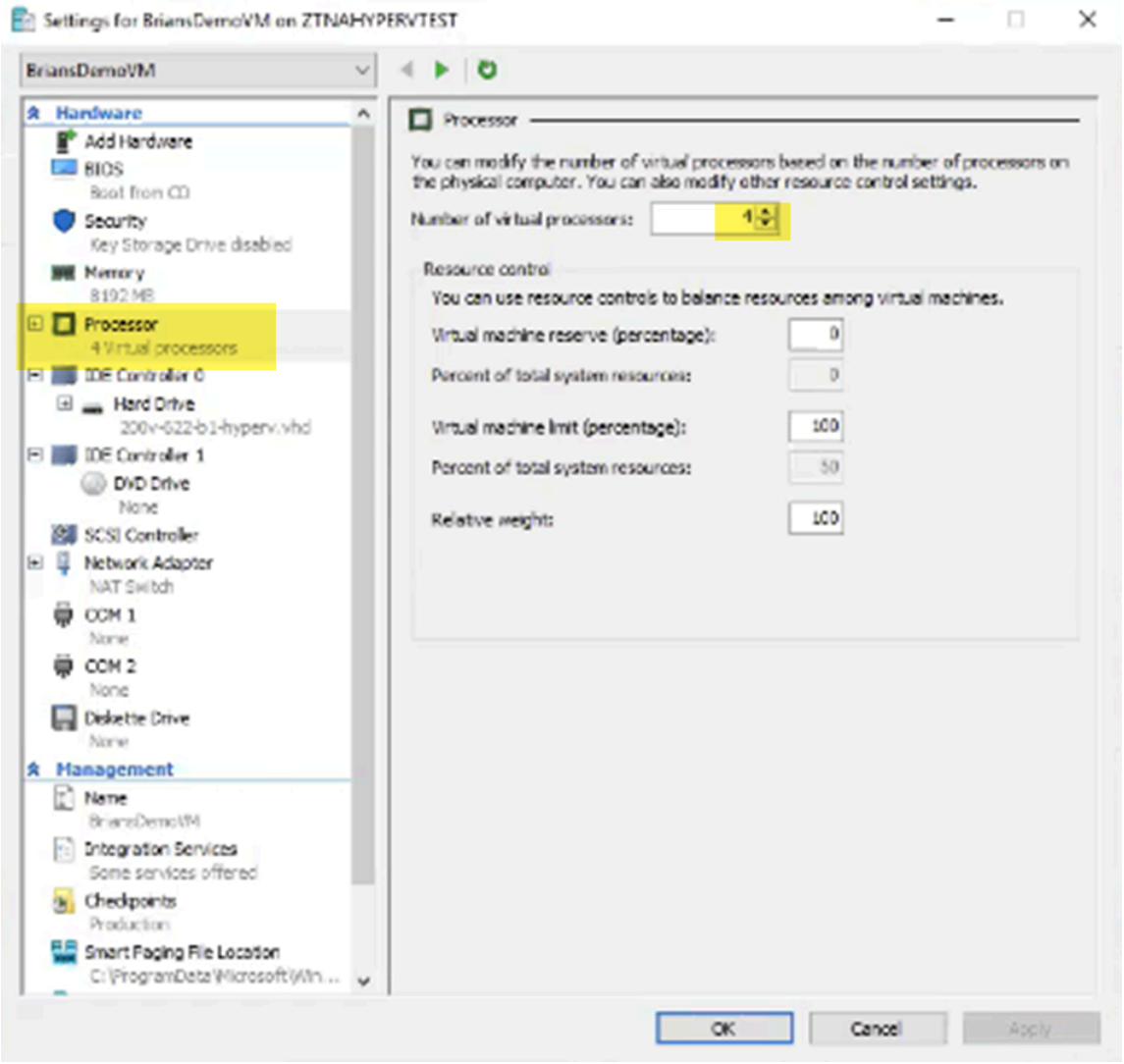
**STEP 11 |** **Beenden** Sie den neuen VM-Assistenten.




Hyper-V erstellt die VM.

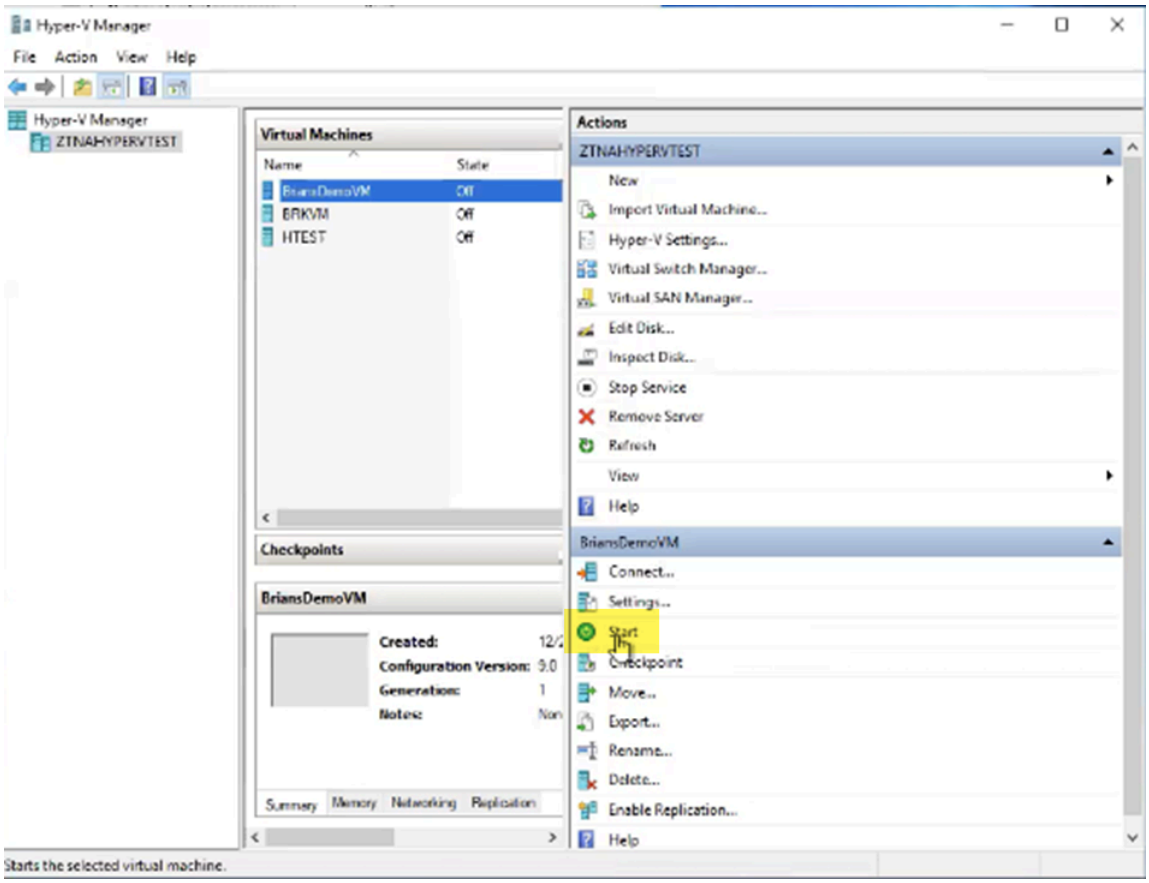
 ©2025 Palo Alto Networks, Inc.

**STEP 12 |** Stellen Sie sicher, dass Ihre VM mindestens vier Prozessoren hat, indem Sie in den Bereich **Prozessor** wechseln und mindestens **4** virtuelle Prozessoren auswählen.

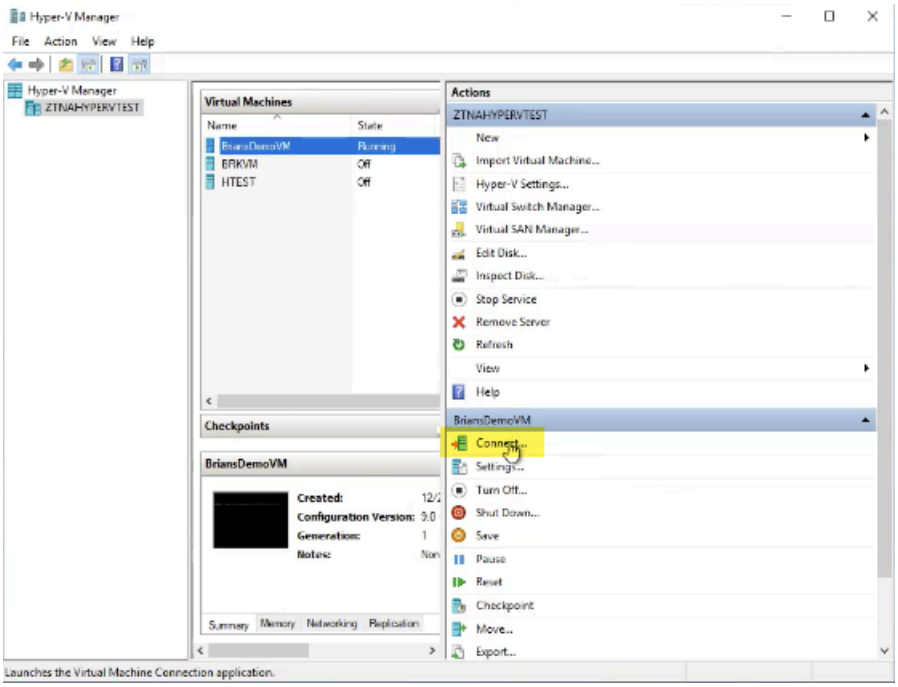



 ©2025 Palo Alto Networks, Inc.

**STEP 13 |** **Starten** Sie die VM.




**STEP 14 |** Wählen Sie **Verbinden** aus, um eine Verbindung mit der seriellen Konsole herzustellen.




 ©2025 Palo Alto Networks, Inc.

**STEP 15 |** Warten Sie, bis das interaktive CLI-Installationsprogramm initialisiert wird, und konfigurieren Sie dann das ION-Modell, den Schlüssel und den geheimen Schlüssel.

1. Wählen Sie **1** (das ION-Modell **ion 200v**) aus den angezeigten Optionen aus.

```
Select an ION model: 1) ion 200v 2) ion 3102v 3) ion 3104v
 4) ion 3108v 5) ion 7108v 6) ion 7116v 7) ion 7132v 8)
 ion 9100v Choose a Number or (Q)uit: 1 CPU: Passed (needed
 4) Memory: Passed (needed 8.0G) Disk: Could not verify
 (needs 40.0G) Network: Passed (needed 1) Select an item to
 modify, or submit config: 1) Model : ion 200v 2) ION Key :
 3) Secret Key : 4) Controller 1 : Controller - DHCP 5) Port
 1 : Disabled/Unused 6) Port 2 : Disabled/Unused 7) Port
 3 : Disabled/Unused 8) Port 4 : Disabled/Unused 9) Port 5 :
 Disabled/Unused 10) Port 6 : Disabled/Unused 11) Port 7 :
 Disabled/Unused 12) Port 8 : Disabled/Unused 13) Port 9 :
 Disabled/Unused 14) Submit and restart
```

2. Geben Sie den Schlüssel vom Konnektor ein, indem Sie Option **2** auswählen und den Schlüssel eingeben, den Sie in der Benutzeroberfläche von ZTNA-Connector gespeichert haben.

```
Choose a Number or (Q)uit: 2 Enter ION Key[None]: xxxxxxxxxx-
yyyyyyyy-zzz-1234-1234-abcdefghijkl Select an item to modify,
 or submit config: 1) Model : ion 200v 2) ION Key : xxxxxxxxx-
yyyyyyyy-zzz-1234-1234-abcdefghijkl 3) Secret Key : 4)
 Controller 1 : Controller - DHCP 5) Port 1 : Disabled/Unused
 6) Port 2 : Disabled/Unused 7) Port 3 : Disabled/Unused 8)
 Port 4 : Disabled/Unused 9) Port 5 : Disabled/Unused 10) Port
 6 : Disabled/Unused 11) Port 7 : Disabled/Unused 12) Port 8 :
 Disabled/Unused 13) Port 9 : Disabled/Unused 14) Submit and
 restart
```

3. Geben Sie den geheimen Schlüssel für ZTNA-Connector ein, indem Sie Option **3** auswählen und den geheimen Schlüssel eingeben, den Sie in der Benutzeroberfläche von ZTNA-Connector gespeichert haben.

```
Choose a Number or (Q)uit: 3 Enter ION secret[None]: abcde12345
 Select an item to modify, or submit config: 1) Model :
 ion 200v 2) ION Key : xxxxxxxxx-yyyyyyyy-zzz-1234-1234-
abcdefghijkl 3) Secret Key : abcde12345 4) Controller 1 :
 Controller - DHCP 5) Port 1 : Disabled/Unused 6) Port 2 :
 Disabled/Unused 7) Port 3 : Disabled/Unused 8) Port 4 :
 Disabled/Unused 9) Port 5 : Disabled/Unused 10) Port 6 :
 Disabled/Unused 11) Port 7 : Disabled/Unused 12) Port 8 :
 Disabled/Unused 13) Port 9 : Disabled/Unused 14) Submit and
 restart
```

 ©2025 Palo Alto Networks, Inc.

**STEP 16 |** Konfigurieren Sie Optionen für den WAN-Port.

1. Wählen Sie Option **5** (Port 1) aus.

```
Choose a Number or (Q)uit: 5 Port 1: 1) Role : Disable 2)
 Cancel Port changes 3) Apply and return
```

2. Wählen Sie Option **1** (Öffentlich/WAN) aus.

```
Choose a Number or (Q)uit: 1 Select Port Role: 1) Internet
 facing port (PublicWAN) 2) Private WAN port (PrivateWAN)
 3) Bypass Port Pair 1 (WAN Port) 4) Bypass Port Pair 1 (LAN
 Port) 5) Bypass Port Pair 2 (WAN Port) 6) Bypass Port Pair
 2 (LAN Port) 7) Bypass Port Pair 3 (WAN Port) 8) Bypass Port
 Pair 3 (LAN Port) 9) Bypass Port Pair 4 (WAN Port) 10) Bypass
 Port Pair 4 (LAN Port) 11) Disabled/Unused
```

3. (Optional) Wenn Sie eine statische IP-Adresse festlegen müssen, wählen Sie Option **2** aus und legen Sie die Parameter für IP-Adresse, Gateway und DNS-Server fest. Anderenfalls wählen Sie **1** aus.

```
Choose a Number or (Q)uit: 1 Port 1: 1) Role : PublicWAN 2)
 Config via : DHCP 3) Cancel Port changes 4) Apply and return
```

4. Wählen Sie Option **4** aus, um zum Hauptmenü zurückzukehren.

```
Choose a Number or (Q)uit: 4 Select an item to modify, or
 submit config: 1) Model : ion 200v 2) ION Key : xxxxxxxxx-
yyyyyyyy-zzz-1234-1234-abcdefghijkl 3) Secret Key : abcde12345
 4) Controller 1 : Controller - DHCP 5) Port 1 : PublicWAN
 - DHCP 6) Port 2 : Disabled/Unused 7) Port 3 : Disabled/
Unused 8) Port 4 : Disabled/Unused 9) Port 5 : Disabled/Unused
 10) Port 6 : Disabled/Unused 11) Port 7 : Disabled/Unused
 12) Port 8 : Disabled/Unused 13) Port 9 : Disabled/Unused
 14) Submit and restart Select an item to modify, or submit
 config: 1) Model : ion 200v 2) ION Key : xxxxxxxxx-yyyyyyyy-
zzz-1234-1234-abcdefghijkl 3) Secret Key : abcde12345 4)
 Controller 1 : Controller - DHCP 5) Port 1 : PublicWAN - DHCP
 6) Port 2 : Disabled/Unused 7) Port 3 : Disabled/Unused 8)
 Port 4 : Disabled/Unused 9) Port 5 : Disabled/Unused 10) Port
 6 : Disabled/Unused 11) Port 7 : Disabled/Unused 12) Port 8 :
 Disabled/Unused 13) Port 9 : Disabled/Unused 14) Submit and
 restart
```

**STEP 17 |** Konfigurieren Sie LAN-Port-Optionen.

1. Wählen Sie Option **6** (Port 2) aus.

```
Choose a Number or (Q)uit: 6 Port 2: 1) Role : Disable 2)
 Cancel Port changes 3) Apply and return
```

2. Wählen Sie Option **2** (Privates WAN) aus.

```
Choose a Number or (Q)uit: 2 Select Port Role: 1) Internet
 facing port (PublicWAN) 2) Private WAN port (PrivateWAN)
 3) Bypass Port Pair 1 (WAN Port) 4) Bypass Port Pair 1 (LAN
```

 ©2025 Palo Alto Networks, Inc.

```
 Port) 5) Bypass Port Pair 2 (WAN Port) 6) Bypass Port Pair
 2 (LAN Port) 7) Bypass Port Pair 3 (WAN Port) 8) Bypass Port
 Pair 3 (LAN Port) 9) Bypass Port Pair 4 (WAN Port) 10) Bypass
 Port Pair 4 (LAN Port) 11) Disabled/Unused
```

3. (Optional) Wenn Sie eine statische IP-Adresse festlegen müssen, wählen Sie Option **2** aus und legen Sie die Parameter für IP-Adresse, Gateway und DNS-Server fest. Anderenfalls wählen Sie **1** aus.

```
Choose a Number or (Q)uit: 2 Port 2: 1) Role : PrivateWAN 2)
 Config via : DHCP 3) Cancel Port changes 4) Apply and return
```

4. Wählen Sie Option **4** aus, um zum Hauptmenü zurückzukehren.

```
Choose a Number or (Q)uit: 4 Select an item to modify, or
 submit config: 1) Model : ion 200v 2) ION Key : xxxxxxxxx-
yyyyyyyy-zzz-1234-1234-abcdefghijkl 3) Secret Key : abcde12345
 4) Controller 1 : Controller - DHCP 5) Port 1 : PublicWAN
 - DHCP 6) Port 2 : PrivateWAN - DHCP 7) Port 3 : Disabled/
Unused 8) Port 4 : Disabled/Unused 9) Port 5 : Disabled/Unused
 10) Port 6 : Disabled/Unused 11) Port 7 : Disabled/Unused
 12) Port 8 : Disabled/Unused 13) Port 9 : Disabled/Unused 14)
 Submit and restart
```

**STEP 18 |** Speichern und starten Sie den Konnektor neu.

```
Choose a Number or (Q)uit: 14 WARNING! After this configuration is
 submitted, all hardware will be signed, logged, and permanently
 tied to the ION Key/Secret Key in the Prisma SDWAN Cloud
 Controller. WHAT THIS MEANS is that hardware cannot be added/
removed (disks, network cards) after this 'SUBMIT' function. If any
 hardware changes are required beyond this 'SUBMIT', the ION will
 need to be re-deployed with a new ION Key and Secret Key. If there
 is a need to add or remove hardware, please answer 'N' below and
 shut down the ION and make the changes now. Submit these changes
 now?[N]: y Building configuration... [VFF:CFG] ZeroTouch Config
 Starting - config file parser [VFF:CFG] Attempting to load/parse
 as Config/INI file. [VFF:CFG] Successfully Loaded config style
 file. [VFF:CFG] Controller 1 successfully set to CONTROLLER/DHCP.
 [VFF:CFG] Port 1 successfully set to PUBLICWAN/DHCP. [VFF:CFG]
 Port 2 successfully set to PRIVATEWAN/DHCP. [VFF:CFG] WARN: Port 3
 had no config section. Defaulting to Disable. [VFF:CFG] WARN: Port
 4 had no config section. Defaulting to Disable. [VFF:CFG] WARN:
 Port 5 had no config section. Defaulting to Disable. [VFF:CFG]
 WARN: Port 6 had no config section. Defaulting to Disable.
 [VFF:CFG] WARN: Port 7 had no config section. Defaulting to
 Disable. [VFF:CFG] WARN: Port 8 had no config section. Defaulting
 to Disable. [VFF:CFG] WARN: Port 9 had no config section.
 Defaulting to Disable. [VFF:CFG] Success with Config/INI file
 parser. [VFF:KVM] Menu config end, continuing normal boot...
 Reboot-reason: manufacture
```

 ©2025 Palo Alto Networks, Inc.

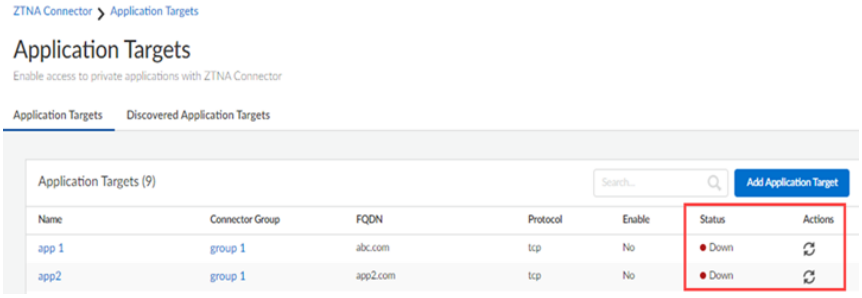
# ZTNA-Connector überwachen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access Version 4.0<br>❑ ZTNA-Connector-Add-on-Lizenz<br>Die Essential-Lizenz mit der Add-on-Lizenz umfasst acht ZTNA-Connectors, 100 FQDNs und vier IP-Subnetzfunktionen.<br>Die Advanced-Lizenz mit der Add-on-Lizenz umfasst 40 ZTNA-Connectors, 300 FQDNs und 1.024 IP-Subnetzfunktionen.<br>Die Premiumlizenz mit der Add-on-Lizenz umfasst 200 ZTNA-Connectors, 4.000 FQDNs und 1.024 IP-Subnetzfunktionen.<br>❑ Wenn Sie die ZTNA-Connector-Add-on-Lizenz nicht erwerben, beinhalten die Prisma Access-Lizenzen vier Konnektoren, 40 FQDNs und vier IP-Subnetze. Diese Funktionalität wird bereitgestellt, um ZTNA-Connectors in Ihrer Umgebung zu testen. |

Alle ZTNA-Connector-Komponenten bieten verständliche Statusinformationen, Protokolle und Diagnosetools, die Sie bei der Behebung auftretender Probleme unterstützen. Verwenden Sie die folgenden Tools, um Ihre ZTNA-Connector-Bereitstellung zu überwachen.


©2025 Palo Alto Networks, Inc.

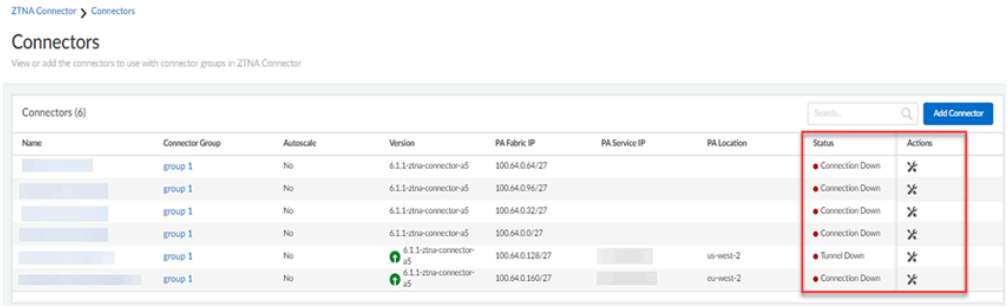
- Zeigen Sie den Status Ihrer Anwendungen und Konnektoren innerhalb der Prisma SASE-Plattform an.
  - Wählen Sie **Workflows** > **ZTNA-Connector** > **Anwendungsziele** aus und stellen Sie sicher, dass der **Status** aller Anwendungsziele **Aktiv** lautet.




Wenn der Status **Ausgefallen** lautet, kann der Connector Ihre Anwendung nicht erreichen. Wenn Sie das Problem mit der Anwendung behoben haben, klicken Sie auf die Aktualisierungs-Schaltfläche in der Spalte **Aktion** und stellen Sie sicher, dass in der Spalte **Status** nun **Aktiv** angezeigt wird (der Status wird automatisch einmal pro Minute aktualisiert).

Der Status lautet auch dann „Aktiv“, wenn die Anwendung über ZTNA-Connector erreichbar ist (dabei wird das Ergebnis der letzten erfolgreichen DNS-Auflösung verwendet), die DNS-Auflösung des Anwendungs-FQDN jedoch über ZTNA-Connector fehlschlägt.

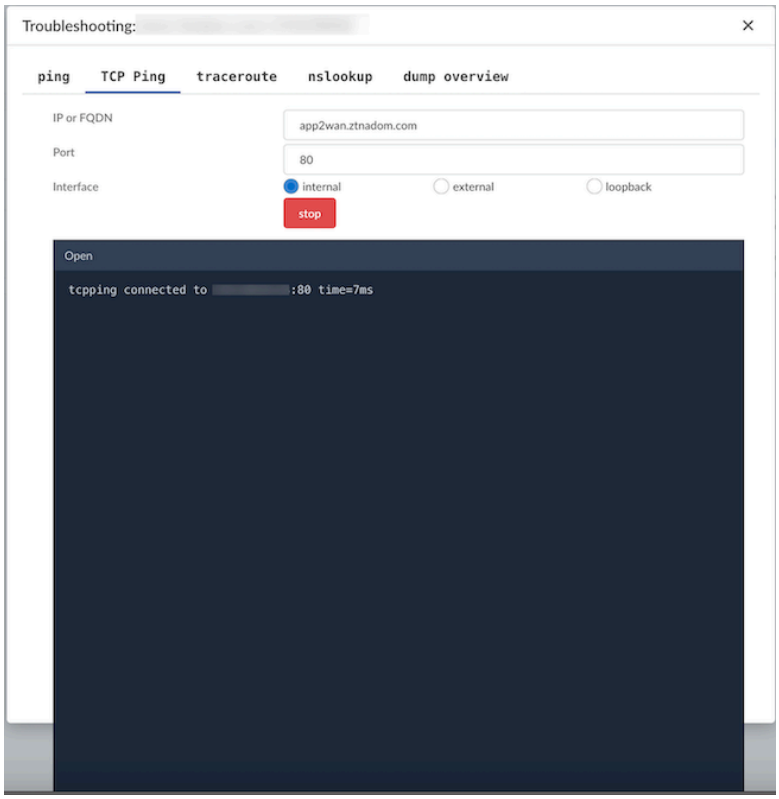
- Wählen Sie **Workflows** > **ZTNA-Connector** > **Konnektoren** aus und stellen Sie sicher, dass der **Status** für alle Konnektoren **Aktiv** lautet.




Wenn der **Status Tunnel inaktiv** angezeigt wird, gibt dies an, dass der IPSec-Tunnel zwischen der Konnektor-VM und Prisma Access inaktiv ist. Wenn für die Option **Status** der Wert **Verbindung ausgefallen** angezeigt wird, ist die Konnektor-VM ausgefallen. Klicken Sie auf das Diagnosesymbol , um eine Remote-Shell-Verbindung zum Konnektor zu starten und das Problem zu beheben. Sie können ein **`Ping`**, **`TCP-Ping`**, **`Traceroute`**, **`NSlookup`**

 ©2025 Palo Alto Networks, Inc.

oder eine **Dump-Übersicht** als Unterstützung bei der Diagnose des Verbindungsproblems ausführen.




 ©2025 Palo Alto Networks, Inc.

# Anzeigen von ZTNA-Connector-Protokollen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access Version 4.0<br>❑ ZTNA-Connector-Add-on-Lizenz<br>Die Essential-Lizenz mit der Add-on-Lizenz umfasst acht ZTNA-Connectors, 100 FQDNs und vier IP-Subnetzfunktionen.<br>Die Advanced-Lizenz mit der Add-on-Lizenz umfasst 40 ZTNA-Connectors, 300 FQDNs und 1.024 IP-Subnetzfunktionen.<br>Die Premiumlizenz mit der Add-on-Lizenz umfasst 200 ZTNA-Connectors, 4.000 FQDNs und 1.024 IP-Subnetzfunktionen.<br>❑ Wenn Sie die ZTNA-Connector-Add-on-Lizenz nicht erwerben, beinhalten die Prisma Access-Lizenzen vier Konnektoren, 40 FQDNs und vier IP-Subnetze. Diese Funktionalität wird bereitgestellt, um ZTNA-Connectors in Ihrer Umgebung zu testen. |

Der gesamte ZTNA-Connector-Datenverkehr wird im Strata Logging Service protokolliert. Um Prisma Access-Protokolle in Strata Logging Service zu speichern, müssen Sie die entsprechende Menge an Protokollspeicher in Strata Logging Service schätzen und kaufen. Es wird empfohlen, den Prozentsatz Ihrer gesamten Strata Logging Service-Speicherkapazität um 10 % zu erhöhen, um ZTNA-Connector-Protokolle speichern zu können.

Vergewissern Sie sich, dass Sie ein Protokollweiterleitungsprofil konfiguriert haben, das die gewünschten Protokolltypen an den Strata Logging Service weiterleitet. Strata Logging Service sendet eine E-Mail-Benachrichtigung, um mehr Speicher zu kaufen, wenn das Protokollspeicherkontingent 90 % erreicht. Wenn Sie keinen weiteren Speicherplatz kaufen, werden die älteren Protokolle gelöscht.

Unabhängig von der Verwaltungsoberfläche, die Sie für Prisma Access (Panorama oder Cloud Management) verwenden, können Sie Ihre Protokolle in Prisma Access (Managed by Strata Cloud Manager) unter **Vorfälle und Benachrichtigungen** > **Protokoll-Viewer** anzeigen.

ZTNA-Connector stellt die folgenden Netzwerkprotokolle zur Verfügung.


©2025 Palo Alto Networks, Inc.

- **Überwachungsprotokolle** – sind über die Prisma SASE-Plattform verfügbar und stellen Aufzeichnungen zu den Konfigurationsänderungen von Administratoren im ZTNA-Connector bereit. Sie können diese Protokolle für Compliance- und Fehlerbehebungszwecke verwenden.

  Sie können die Überwachungsprotokolle nach Zeitbereich, Standort, Gerät und Typ filtern. Die Überwachungsprotokolle enthalten folgende Angaben:

  - Anzahl der versuchten Anmeldungen bei einem Unternehmensportal durch einen bestimmten Benutzer über eine bestimmte IP-Adresse.
  - Informationen dazu, ob eine Anwendung oder ein Anwendungskonnektor eingebunden oder gelöscht wird.
  - Zeitpunkt, zu dem ein Konnektor-Upgrade geplant ist.
  - Ansicht aller Systemänderungen und Zugriffsversuche.

  ZTNA-Connector-Überwachungsprotokolle sind in der Prisma Access-Weboberfläche nicht verfügbar. Um Überwachungsprotokolle anzuzeigen, müssen Sie einen Supportfall beim technischen Support von Palo Alto Networks öffnen.
- **Datenverkehrsprotokolle** – zeigen einen Eintrag für den Beginn und das Ende jeder Sitzung an. Jeder Eintrag enthält Datum und Uhrzeit, Quell- und Zielzone, Adressen und Ports, Anwendungsname, auf den Datenverkehrsfluss angewendeter Name der Sicherheitsregel, Regelaktion (Zulassen, Ablehnen oder Löschen), Eingangs- und Ausgangsschnittstelle, Anzahl der Bytes und Grund für das Sitzungsende.
  - Die Spalte „Typ“ gibt an, ob der Eintrag für den Beginn oder das Ende der Sitzung bestimmt ist.
  - Die Spalte „Aktion“ gibt an, ob die Firewall die Sitzung zugelassen, abgelehnt oder gelöscht hat.
  - Eine Löschung gibt die Sicherheitsregel an, die den Datenverkehr blockiert hat, der eine Anwendung angibt, während eine Ablehnung die Regel angibt, die eine bestimmte Anwendung identifiziert.
  - Wenn die Firewall den Datenverkehr vor der Identifizierung der Anwendung löscht, z. B. wenn eine Regel den gesamten Datenverkehr für einen bestimmten Dienst löscht, wird in der Spalte „Anwendung“ die Information „nicht zutreffend“ angezeigt.
  - Die App-ID für einen ZTNA-Connector ist die benutzerdefinierte App-ID.
  - Wenn der Datenverkehr auf das Gateway für mobile Benutzer trifft, wird in der Spalte **Zieladresse** die IP-Adresse gemäß RFC 6598 angezeigt.
- **Konfigurationsprotokolle** – Zeigen Einträge für Änderungen an der ZTNA-Connector-Konfiguration an. Jeder Eintrag enthält Datum und Uhrzeit, den Benutzernamen des Administrators, die IP-Adresse, über die der Administrator eine Änderung vorgenommen hat, den Typ des Clients, die Art des ausgeführten Befehls, den Befehlsstatus (erfolgreich oder fehlgeschlagen), den Konfigurationspfad und die Werte vor und nach der Änderung.
- Strata Cloud Manager
- Panorama

 ©2025 Palo Alto Networks, Inc.

## Anzeigen von ZTNA-Connector-Protokollen (Panorama)

Verwenden Sie den folgenden Workflow, um ZTNA-Connector-Protokolle in Prisma Access (Managed by Panorama) Access anzuzeigen.

**STEP 1 |** Melden Sie sich bei Prisma Access an.

**STEP 2 |** Wählen Sie **Überwachen** > **Protokolle** aus.

**STEP 3 |** Wählen Sie in der Liste einen Protokolltyp aus: **Überwachungs-**, **Datenverkehrs-**und **Konfig-**Protokolle.

**STEP 4 |** Klicken Sie auf den Pfeil rechts neben einer beliebigen Spaltenüberschrift, und wählen Sie **Spalten** aus.

**STEP 5 |** Wählen Sie die anzuzeigenden Spalten in der Liste aus. Das Protokoll wird automatisch aktualisiert, um Ihrer Auswahl zu entsprechen.

**STEP 6 |** Klicken Sie für einen bestimmten Protokolleintrag auf das Symbol **Fernglas**. Unter **Detaillierte Protokollansicht** finden Sie weitere Informationen zur Quelle und zum Ziel der Sitzung sowie eine Liste der Sitzungen, die sich auf den Protokolleintrag beziehen.

## Anzeigen von ZTNA-Connector-Protokollen (Strata Cloud Manager)

Verwenden Sie den folgenden Workflow, um ZTNA-Connector-Protokolle im Cloud-verwalteten Prisma Access anzuzeigen.

**STEP 1 |** Melden Sie sich bei Prisma Access (Managed by Strata Cloud Manager) an.

**STEP 2 |** Wählen Sie **Vorfälle und Benachrichtigungen** > **Protokoll-Viewer** aus.

**STEP 3 |** Wählen Sie den Protokolltyp aus, den Sie anzeigen möchten: Überwachungs-, Firewall/Datenverkehrs- und Konfigurationsprotokolle.

**STEP 4 |** Wählen Sie einen Zeitraum aus, für den Sie Protokolle anzeigen möchten.

**STEP 5 |** Geben Sie diese Abfragezeichenfolge ein, um die Liste der ZTNA-Connector-Protokolle einzugrenzen. **Subtype = 'netflow' AND Device Name = 'PA_CONN'** .

Die Protokolle enthalten die folgenden Details:

- Timestamp
- Konnektorname
- Ursprüngliche Quell-IP-Adresse des Clients
- Ursprünglicher Quellport des Clients
- Übersetzte IP-Adresse des Konnektors
- Übersetzter Port des Konnektors
- Übersetzte Ziel-IP-Adresse
- Übersetzter Zielport

 ©2025 Palo Alto Networks, Inc.

# Beibehalten der Benutzer-ID-Zuordnung für ZTNA-Connector-Verbindungen mit Quell-NAT

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access Version 5.1.1 |

Sie können ZTNA-Connector in Prisma Access verwenden, um private Anwendungen zu sichern. Um den Zugriff auf die Anwendungen basierend auf der Benutzer-ID einzuschränken, können Sie eine Next-Generation Firewall (NGFW) am Standort des Rechenzentrums oder der Zentrale bereitstellen, an dem sich die privaten Anwendungen befinden. Konfigurieren Sie dann basierend auf der Benutzer-ID-Zuordnung Richtlinienregeln auf der NGFW.

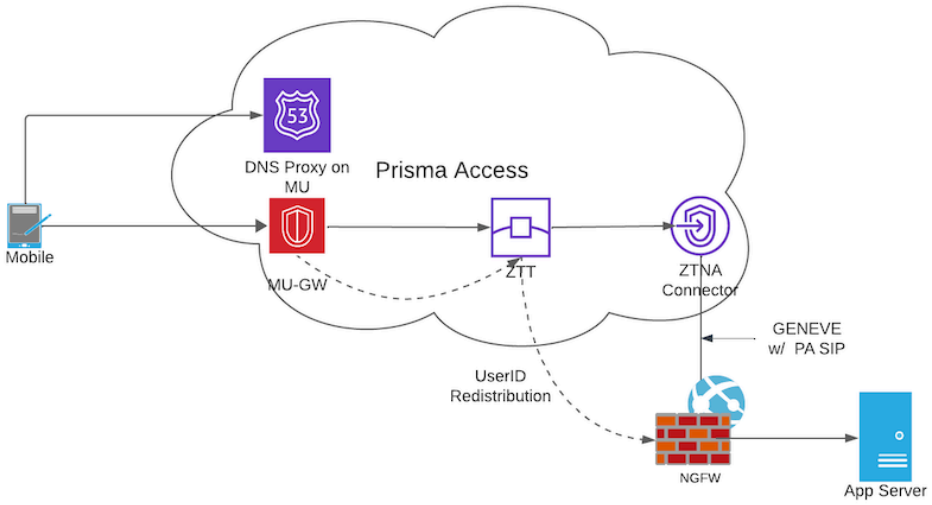
Wenn Ihre Bereitstellung eine Next-Generation Firewall (NGFW) am Standort des Rechenzentrums oder der Zentrale verwendet, an dem sich die privaten Anwendungen befinden, und wenn ZTNA-Connector die Quell-NAT ausführt, kann die NGFW die Benutzer-ID-Zuordnung nicht abrufen. Die Quell-NAT auf ZTNA-Connector verhindert, dass die NGFW die Client-IP-Adresse erhält, die für die Zuordnung unerlässlich ist. Wenn die NGFW diese Client-IP-Adresse nicht abrufen kann, kann sie die zonenbasierten Sicherheitsrichtlinienregeln, die Sie basierend auf der Benutzer-ID-Zuordnung erstellt haben, nicht durchsetzen.

Der ZTNA-Connector hat folgende Verantwortlichkeiten, um die Benutzer-ID innerhalb des NGFW-gesicherten Rechenzentrums zu aktivieren:

1. Stellen Sie eine sichere Verbindung von der NGFW zu den regionalen ZTNA-Connector Tunnel Terminators (ZTTs) bereit, damit sich die NGFW mit dem zugehörigen Umverteilungs-Agent für Benutzer-IDs verbinden kann.
2. Bei FQDN-Anwendungen, bei denen für die Zustandsprüfung die Einstellung „tcpping“ festgelegt wurde, müssen Sie die Anwendungen des Rechenzentrums überprüfen, um festzustellen, ob die Anwendung über diesen spezifischen Konnektor aktiv und erreichbar ist.
3. Verkapseln Sie Benutzer-zu-App-Post-NAT-IP-Pakete im Rechenzentrumsraum innerhalb eines Geneve-Pakets mit der ursprünglichen Quell-IP-Adresse als Option.

Das folgende Diagramm veranschaulicht die Netzwerkelemente, die die Zuordnung zwischen Quell-IP-Adresse und Benutzer-ID für die NGFW bereitstellen und mit Geneve (Generic Network Virtualization Encapsulation) gekapselte Datenpakete einschließlich der ursprünglichen Prisma Access-Quell-IP-Adresse an die NGFW übertragen. Diese Elemente ermöglichen es der NGFW, Sicherheitsrichtlinienregeln auf Basis der Benutzer-ID wirksam durchzusetzen.

 ©2025 Palo Alto Networks, Inc.




**Einschränkungen:**

- Die Benutzer-ID-Unterstützung mit ZTNA-Connector ist nur nach folgenden Versionen verfügbar:
  - Prisma Access Dataplane: Version 10.2.4 und später
  - Saas_agent: Version 5.1.0 und später
  - NGFW-Version: Version 11.2.0 und später
  - Connector-Version: Version 6.2.4-ztna-connector-b3 und später
- Die ICMP-Prüfung wird für FQDN-Ziele nicht unterstützt, die mit Benutzer-ID-basierten Konnektorgruppen verknüpft sind.
- Die NGFW-Dienstroutenkonfiguration für einen UID-Agenten unterstützt nur Schnittstellen mit statischen IP-Adressen. Wenn die NGFW-Schnittstelle in einem dynamischen Modus konfiguriert ist (IP-Adresszuweisung durch DHCP), kann der Benutzer-ID-Kanal von der NGFW zu ZTT keine Unterstützung für die ZTNA-Connector-Benutzer-ID herstellen. Um dieses Problem zu beheben, müssen Sie die Schnittstelle für den UID-Agenten der NGFW mit einer statischen IP-Adresse einrichten.
- Diagnosetools wie „Ping“ und „Traceroute“ werden für Benutzer-ID-basierte Konnektoren nicht unterstützt.

Diese Vorgehensweise setzt voraus, dass Sie über die folgenden Netzwerkkonfigurationen verfügen:

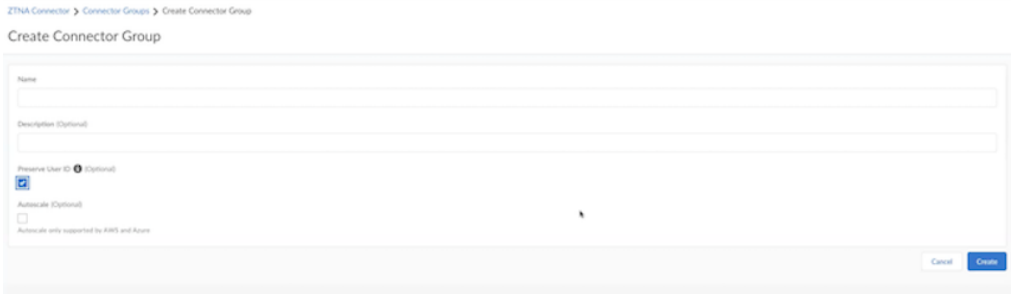
- Sie haben eine NGFW in der Zentrale oder im Rechenzentrum bereitgestellt, in der bzw. dem sich die privaten Apps befinden.
- Sie haben Sicherheitsrichtlinienregeln in der NGFW basierend auf den Zonen (nicht vertrauenswürdige Zone und vertrauenswürdige Zone) angewendet, die Sie in der NGFW erstellt haben. Diese Sicherheitsrichtlinienregeln umfassen die Durchsetzung der Benutzer-ID.

Um sicherzustellen, dass Ihr Netzwerk die Benutzer-ID-Zuordnung an die Zentrale oder das Rechenzentrum verteilt, führen Sie das unten aufgeführte Verfahren aus, das es der NGFW

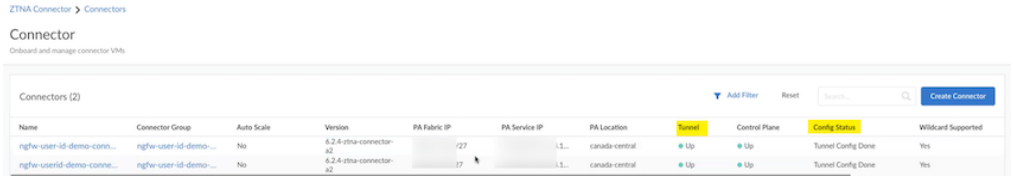
 ©2025 Palo Alto Networks, Inc.

ermöglicht, die Sicherheitsrichtlinienregeln basierend auf der Benutzer-ID-Zuordnung, die sie von GlobalProtect erhält, durchzusetzen.

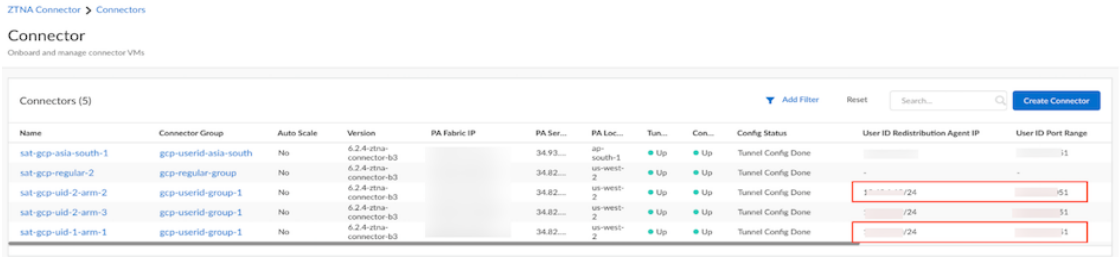
**STEP 1 |** Erstellen Sie eine Konnektorgruppe, aktivieren Sie **Benutzer-ID beibehalten** und fügen Sie die Konnektoren hinzu.



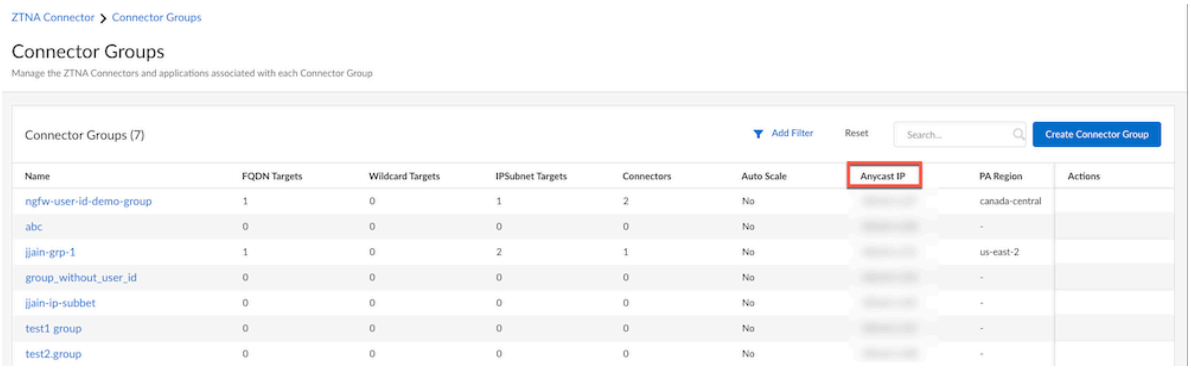

**STEP 2 |** Stellen Sie die Konnektoren in Ihrem Rechenzentrum bereit und binden Sie sie ein. Überprüfen Sie, ob die Tunnel aktiv sind und ordnungsgemäß funktionieren.




**STEP 3 |** Rufen Sie **Konnektor** auf und notieren Sie die **Agent-IP für die Weitergabe der Benutzer-ID** und den **Portbereich der Benutzer-ID** für Ihren Konnektor. Sie benötigen diese IP-Adressen und Portbereiche, um Agents für die Weitergabe von Benutzer-IDs in der NGFW zu konfigurieren.




Wählen Sie außerdem **Konnektorgruppen** aus und notieren Sie die **Anycast-IP**. Diese IP-Adresse ist erforderlich, um NGFW-Sicherheitsrichtlinienregeln zu konfigurieren, damit TCP-Anwendungen über diese Quell-IP-Adresse geprüft werden können.




 ©2025 Palo Alto Networks, Inc.

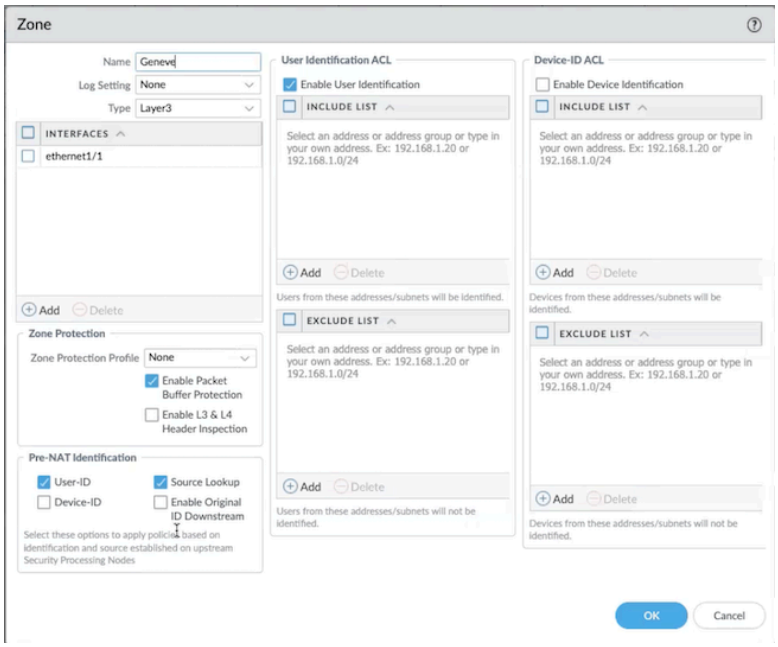
**STEP 4 |** Geben Sie Parameter für die Identifikation vor der Netzwerkadressübersetzung (Pre-NAT-Identifikation) auf der NGFW ein.

1. Melden Sie sich bei der NGFW-Benutzeroberfläche an und rufen Sie dann **Netzwerk** > **Zonen** auf und verwenden Sie **Hinzufügen**, um zwei Zonen (Zone für die

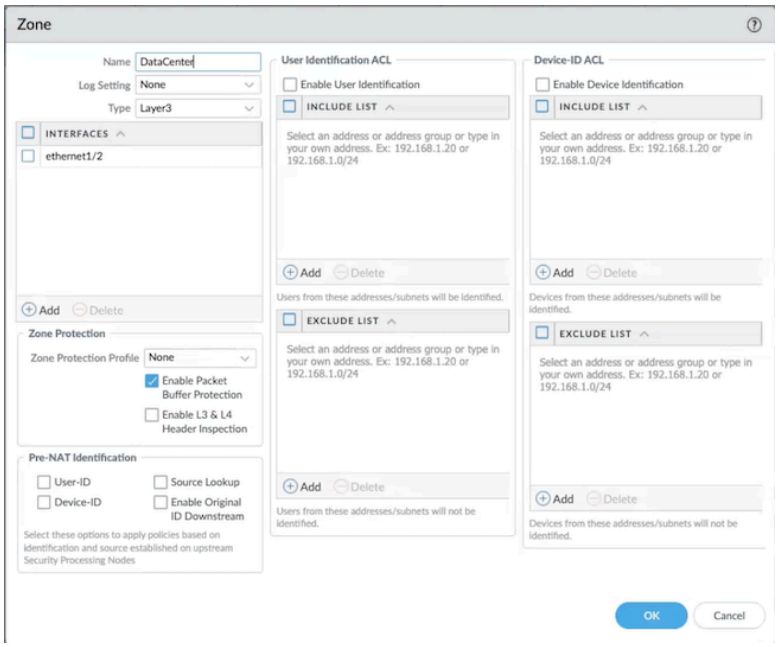
 ©2025 Palo Alto Networks, Inc.

Schnittstellenverbindung zu ZTNA-Connector und Zone für die Schnittstellenverbindung zum Anwendungsserver) hinzuzufügen oder eine bereits vorhandene Zone auszuwählen.

1. Wählen Sie die folgenden Parameter für die **Pre-NAT-Identifikation** für die Zone mit der Schnittstellenverbindung zum ZTNA-Connector aus:
   - **Benutzer-ID** – Erhält die Benutzer-ID-Zuordnung für mobile Benutzer, die vor der NAT der IP-Adressen verwendet wurde. Aktivieren Sie diese Option, wenn Sie die Benutzer-ID in den Sicherheitsrichtlinienregeln verwenden.
   - **Quell-Abfrage** – Ermöglicht es Ihnen, die ursprüngliche Quell-IP-Adresse abzugleichen, die von GlobalProtect empfangen wurde.



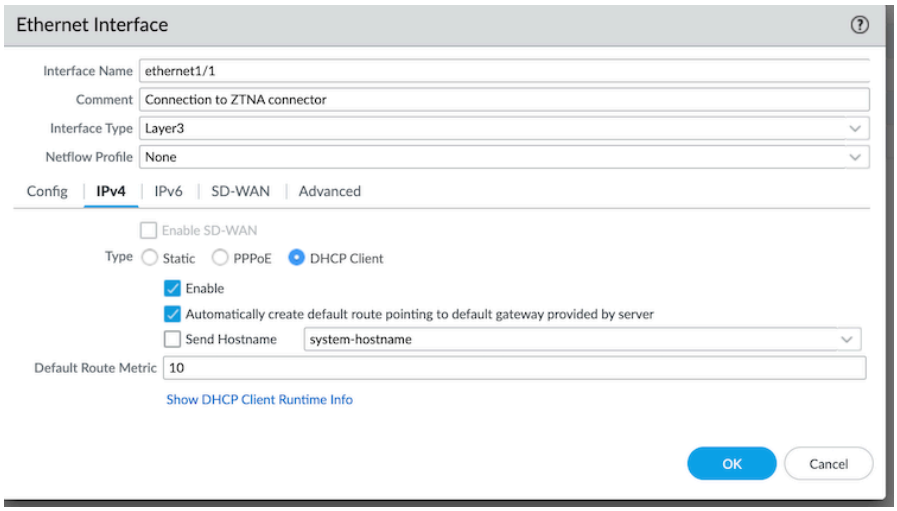

2. Für die Schnittstelle, die mit der Anwendungsserverzone verbunden wird, müssen Sie keine Parameter für die **Pre-NAT-Identifikation** auswählen.



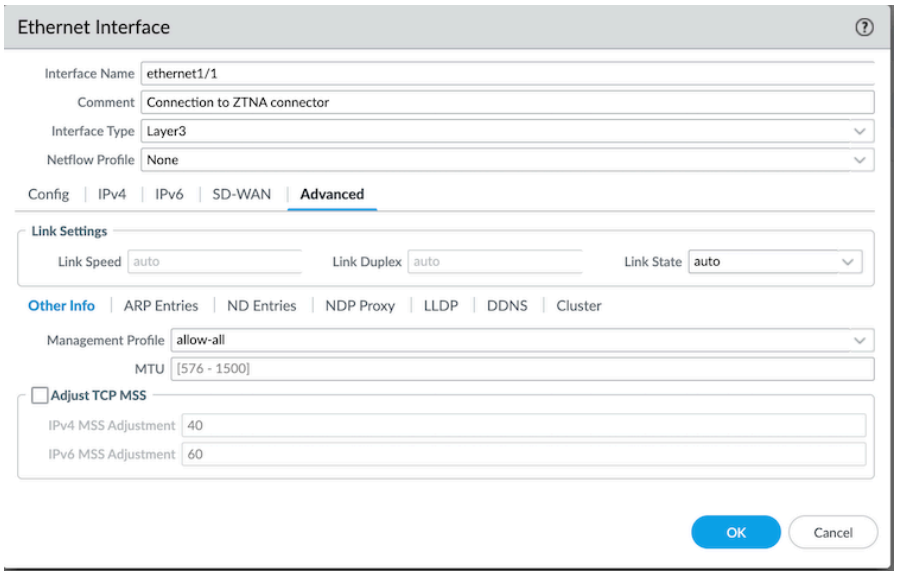

 ©2025 Palo Alto Networks, Inc.

3. Klicken Sie auf **OK** und dann auf **Commit**, um Ihre Änderungen festzuschreiben.

2. Fügen Sie die IP-Adressen zu den Schnittstellen hinzu.
   1. Rufen Sie **Netzwerk** > **Schnittstellen** > **Ethernet** auf.
   2. Wählen Sie die Schnittstelle aus, die eine Verbindung zum ZTNA-Connector und zum Anwendungsserver herstellt, und konfigurieren Sie sie. Fügen Sie den **Schnittstellennamen** und den **Schnittstellentyp** zu **Layer 3** hinzu.




   3. Wählen Sie für die mit dem Anwendungsserver verbundene Ethernet-Schnittstelle das Kontrollkästchen **Automatisches Erstellen einer Standardroute, die auf das vom Server bereitgestellte Standardgateway verweist** ab.




3. Rufen Sie **Schnittstellen** auf und fügen Sie die statischen IP-Adressen zu den Schnittstellen hinzu. Fügen Sie die ZTNA-Connector-Schnittstelle zur ZTNA-Connector-Zone (Geneve) und die Anwendungsserver-Schnittstelle zur Anwendungsserver-Zone (Rechenzentrum) hinzu.

 ©2025 Palo Alto Networks, Inc.

**STEP 5 |** Erstellen Sie eine CLI-Sitzung (Command Line Interface) mit der NGFW und geben Sie im Konfigurationsmodus den folgenden Befehl ein:

```
set deviceconfig setting preserve-prenat-feature yes
```

Wenn Sie diese Funktion in Zukunft deaktivieren müssen, geben Sie den Befehl `set deviceconfig setting preserve-prenat-feature no` ein.

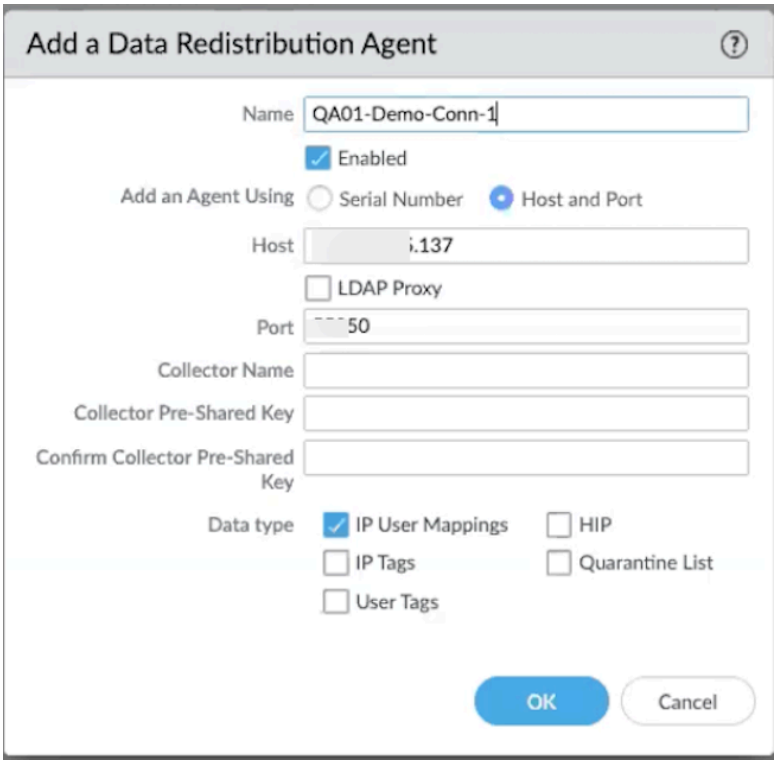
 ©2025 Palo Alto Networks, Inc.

**STEP 6 |** *Beim Einrichten der Benutzer-ID-Umverteilung müssen Sie einen Umverteilungs-Agent-Eintrag für jeden Port innerhalb des angegebenen Bereichs aus Schritt 3* ***Benutzer-ID-Portbereich*** *hinzufügen. Wenn der Bereich beispielsweise 55050-55055 lautet, müssen Sie sechs Einträge konfigurieren, die der Anzahl der von Ihnen bereitgestellten ZTNA-Connector-Regionen entsprechen.*

*Wählen Sie für jeden Port im Bereich für das Feld* ***Host*** *unter* ***Agent-IP für Weitergabe der Benutzer-ID*** *(Schritt 3) eine IP-Adresse aus. Wenn Sie Redundanz auf ZTNA-Connector-Ebene benötigen, können Sie zwei Adressen unter* ***Agent-IP für Weitergabe der Benutzer-ID*** *auswählen und den gesamten Portbereich für beide IP-Adressen anwenden. Alternativ hierzu können alle Ports aller IP-Adressen in* ***Agent-IP für Weitergabe der Benutzer-ID*** *konfiguriert werden.*

Fügen Sie einen Weitergabe-Agent für jeden Port im Bereich **Benutzer-ID-Portbereich** mit mindestens einer der Adressen in **Agent-IP für Weitergabe der Benutzer-ID** hinzu.

1. Gehen Sie in der NGFW-Benutzeroberfläche zu **Gerät** und wählen Sie dann **Datenumverteilung** aus.
2. Klicken Sie auf **Hinzufügen**, fügen Sie den **Namen** hinzu und wählen Sie das Kontrollkästchen **Aktiviert** aus.
3. Wählen Sie **Host und Port** aus, fügen Sie **Agent-IP für Weitergabe der Benutzer-ID** aus Schritt 3 in **Host** hinzu und fügen Sie dann **Portbereich für Benutzer-ID** (kopiert in Schritt 3) hinzu.
4. Aktivieren Sie das Kontrollkästchen **IP-Benutzerzuordnungen** und klicken Sie auf **OK**.

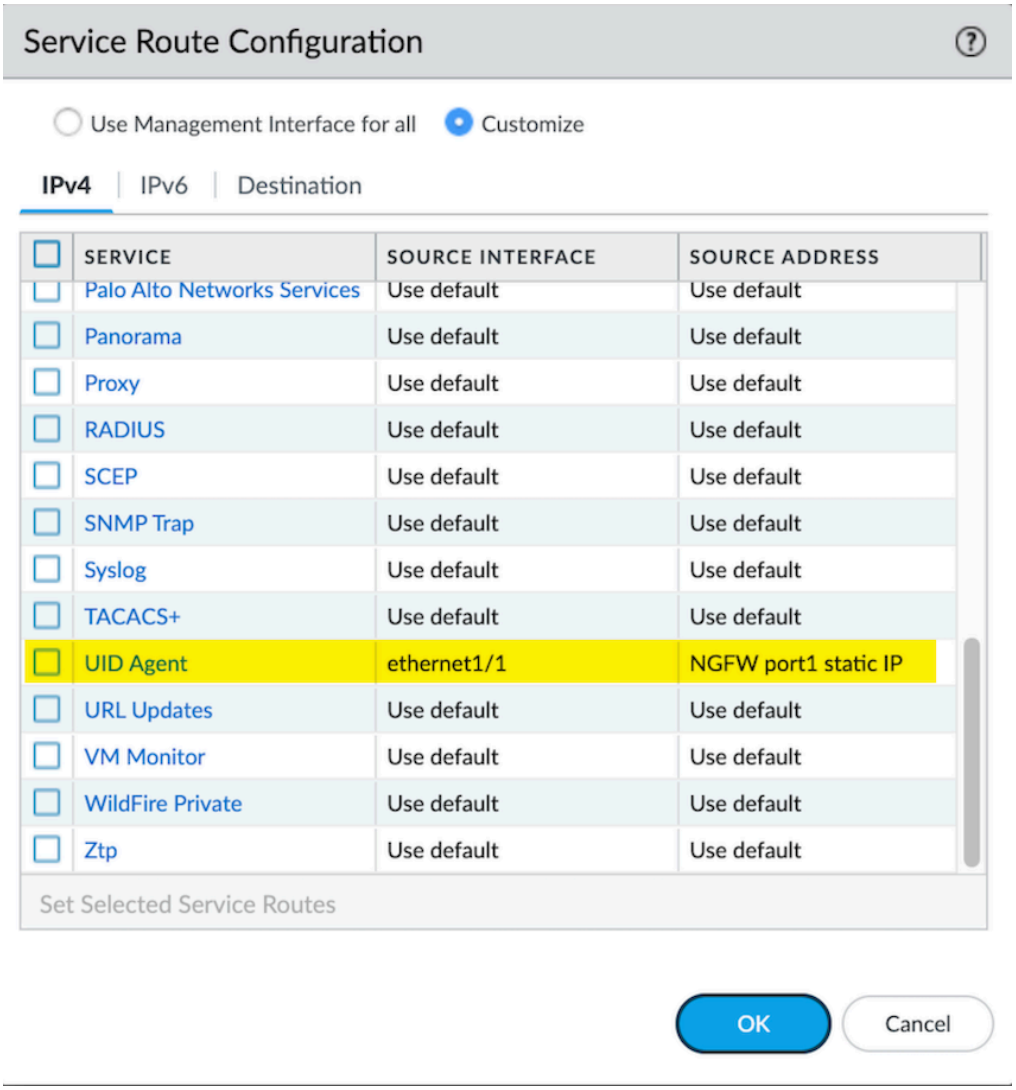



5. Klicken Sie auf **Commit**, um die Konfiguration zu speichern.

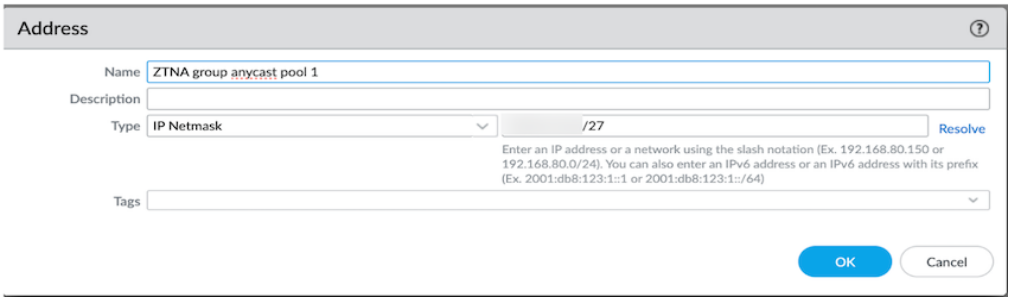
 ©2025 Palo Alto Networks, Inc.

**STEP 7 |** Rufen Sie in der NGFW-Benutzeroberfläche **Gerät** > **Einrichtung** > **Dienste** > **Dienstroutenkonfiguration** > **Anpassen** > **UID-Agent** auf.

1. Wählen Sie unter **IPv4** die **QUELLENSCHNITTSTELLE** als **Ethernet1/1** (Schnittstelle zum ZTNA-Connector) aus und fügen Sie die **QUELLADRESSE** hinzu.



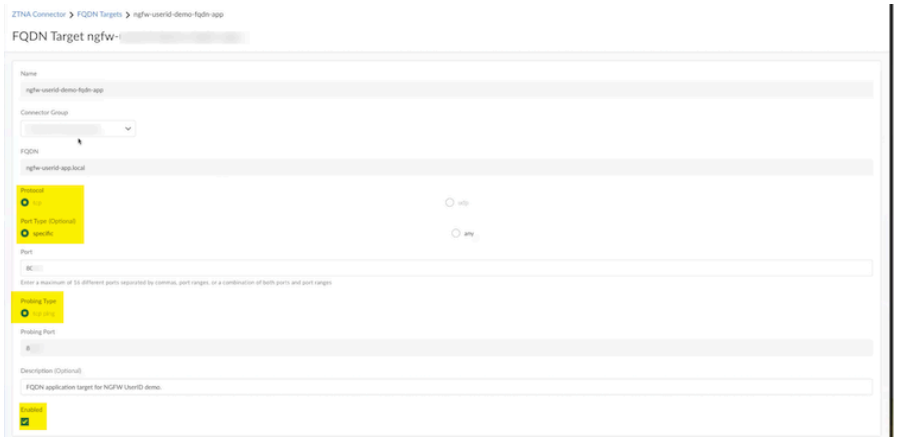

**STEP 8 |** Fügen Sie eine Sicherheitsrichtlinienregel hinzu, um TCP-Pakete mit der Quell-IP-Adresse zuzulassen. Fügen Sie die Quell-IP-Adresse hinzu, bei der es sich um die Anycast-IP-Adresse handelt, die in Schritt 3 kopiert wurde, und klicken Sie dann auf **OK**.



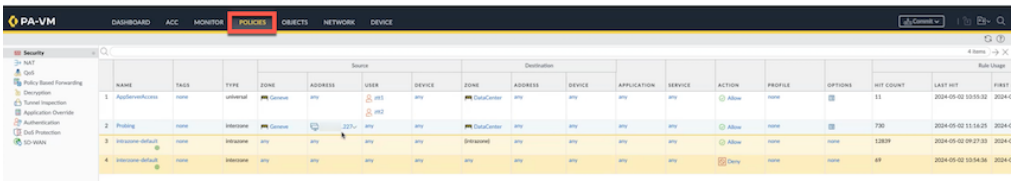

 ©2025 Palo Alto Networks, Inc.

**STEP 9 |** (Optional) Aktivieren Sie die TCP-Prüfung.

1. So erstellen Sie ein FQDN-Ziel:
   1. Rufen Sie **Workflows** > **Anwendungsziele** > **FQDN-Ziele** auf und klicken Sie dann auf **FQDN-Ziel erstellen**.
   2. Fügen Sie einen **Namen** hinzu und wählen Sie die **Konnektorgruppe** aus.
   3. Aktivieren Sie **tcp**, **Spezifisch**, **tcp ping** und **Aktiviert**. Fügen Sie den **Port** hinzu und klicken Sie auf **Erstellen**.



**STEP 10 |** Rufen Sie in der NGFW-Benutzeroberfläche **Richtlinien** auf und definieren Sie die Benutzer-ID-basierten Richtlinien.



 ©2025 Palo Alto Networks, Inc.

 ©2025 Palo Alto Networks, Inc.

# Einstellungen für Zugriff mit dynamischen Rechten konfigurieren

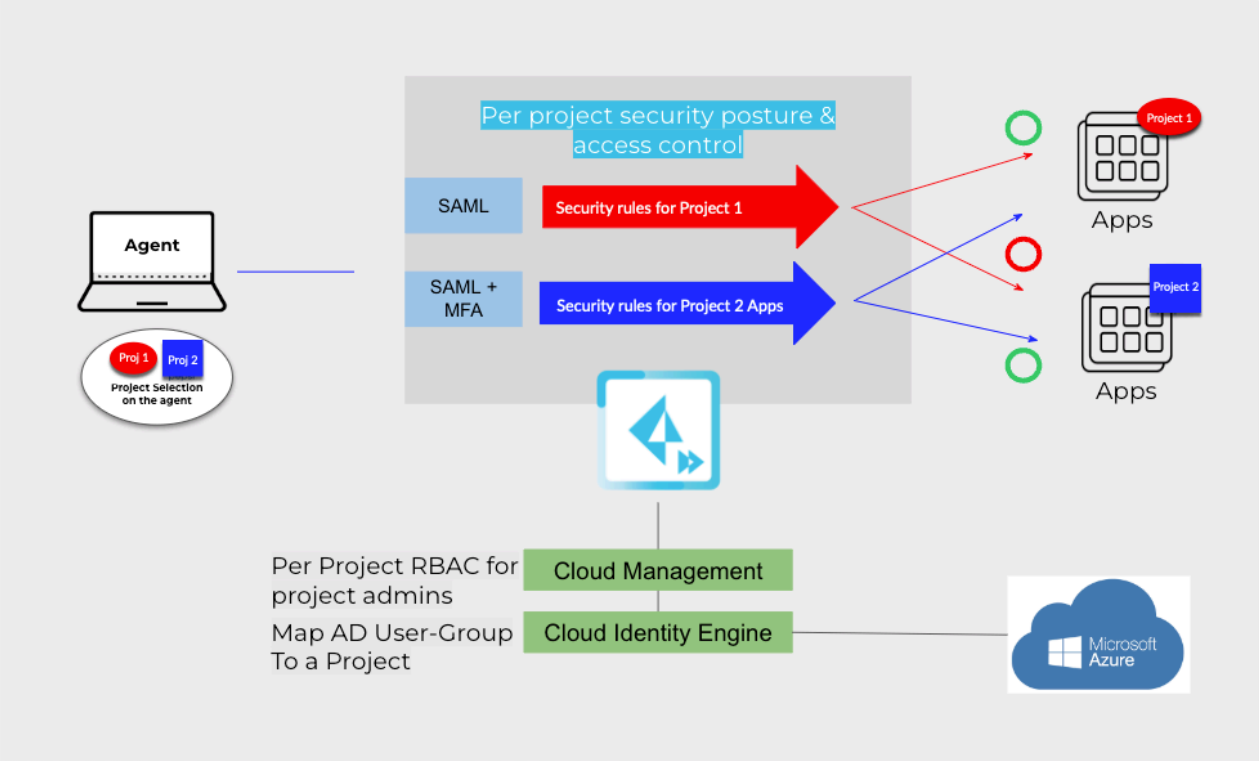
| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access-Lizenz<br>❑ Prisma Access Version 5.1<br>❑ Rolle: Superuser |

Für IT Enterprise-Unternehmen und ITES-Unternehmen (IT Enabled Services), die steuern müssen, welche Benutzer Zugriff auf ihre Kundenprojekte haben, bietet die Funktion für *Zugriff mit dynamischen Rechten* einen nahtlosen, sicheren und abgeschotteten Zugriff für Ihre Benutzer, sodass die Benutzer nur auf die Projekte zugreifen können, denen sie zugewiesen wurden. Diese Unternehmen weisen Mitarbeitern typischerweise mehrere Kundenprojekte zu und bieten isolierten Zugriff auf diese Projekte, sodass ein berechtigter Benutzer immer nur auf ein Kundenprojekt gleichzeitig zugreifen kann.

# Was bedeutet Zugriff mit dynamischen Rechten?

Der Zugriff mit dynamischen Rechten ist eine Funktion in Prisma Access, die dynamische Berechtigungen für Ihre Benutzer basierend auf den Workflows oder Projekten bereitstellt, die Ihre Benutzer in Prisma Access Agent auswählen. Ihre Benutzer können über dynamische Berechtigungen auf Basis der Kombination aus Benutzergruppe und IP-Pool verfügen, die einem Projekt zugewiesen ist. Diese eindeutige Kombination definiert ein Projekt. Mit dem Zugriff mit dynamischen Rechten können Sie Ressourcen in Ihrem Netzwerk isolieren, sodass sie für Ihre Benutzer nur gemäß den Projekten zugänglich sind, denen sie zugewiesen wurden.

Eine neue vordefinierte Rolle namens **Projektadministrator** ist in Prisma Access verfügbar, um Projektadministratoren das Erstellen und Verwalten von Projektdefinitionen zu erlauben. Projektadministratoren können Projekte zuordnen, um Prisma Access-Standortgruppen auszuwählen und IP-Adresszuweisungen mithilfe von DHCP-basierten Methoden für Projekt- und Standortgruppen zu erstellen. Projektadministratoren können nur die Projekte verwalten, denen sie in Strata Cloud Manager zugewiesen sind.




Wenn sich Ihre Endbenutzer auf ihren verwalteten Geräten bei einem Prisma Access Agent anmelden, für den der Zugriff mit dynamischen Rechten aktiviert ist, wird folgender Workflow ausgeführt:

1. Ihr Endbenutzer wählt ein Projekt aus, dem er zugeordnet ist (z. B. Projekt 1).
2. Seine Identität wird in Cloud Identity Engine authentifiziert, wobei die Benutzergruppe des Benutzers dem Projekt zuordnet wird.
3. Nach erfolgreicher Authentifizierung und der Überprüfung der Übereinstimmung der Benutzergruppe mit den vom Projektadministrator festgelegten Projektkriterien verfügt der Benutzer über Zugriff auf Ressourcen im Netzwerk anhand der projektspezifischen

 ©2025 Palo Alto Networks, Inc.

Einstellungen für Projekt 1 und der Sicherheitsregeln, die den Sicherheitsstatus und die Zugriffskontrolle auf Projektbasis zuteilen. Die Sicherheitsinfrastruktur wendet Sicherheitsregeln an, um den Benutzerzugriff auf die zu diesem Projekt gehörenden Ressourcen und Anwendungen zu beschränken. Der Zugriff auf Ressourcen und Anwendungen aus anderen Projekten ist nicht gestattet.

4. Wenn der Benutzer zu einem anderen Projekt wechselt (z. B. Projekt 2), wird er beim vorherigen Projekt (Projekt 1) abgemeldet. Anschließend kann der Benutzer basierend auf den projektspezifischen Einstellungen und Sicherheitsregeln auf die Ressourcen für das zweite Projekt zugreifen.

Sie können Einblick in Ihre Prisma Access Agent-Bereitstellung erhalten, indem Sie Strata Cloud Manager verwenden, um die Projektaktivitäten Ihrer Benutzer zu überwachen und den Dienstverbrauch sowie den Sicherheitsstatus in Ihrem Netzwerk anzuzeigen.

 ©2025 Palo Alto Networks, Inc.

# Zugriff mit dynamischen Rechten für Prisma Access über Common Services aktivieren

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access-Lizenz mit Abonnement für mobile Benutzer<br>❑ Aktivierungslink<br>❑ Strata Logging Service<br>❑ Cloud Identity Engine<br>❑ Prisma Access Agent<br>❑ Rolle: Superuser für mehrere Mandanten oder Superuser mit Zugriff auf das Customer Support Portal |

Mit dem Zugriff mit dynamischen Rechten können IT-Administratoren Endbenutzer mehreren Kundenprojekten zuordnen. Ein berechtigter Benutzer darf jeweils nur auf ein Kundenprojekt zugreifen.

**Zugriff mit dynamischen Rechten** ist eine optionale Funktion während der Aktivierung eines neuen Prisma Access-Mandanten. Nachdem Sie diese Funktion aktiviert haben und der Mandant aktiviert ist, wird DPA für die Lebensdauer des Mandanten eingerichtet und kann nicht deaktiviert werden.

Die Option zur Aktivierung von DPA steht nur einmal während der ersten Aktivierung eines neuen Prisma Access-Mandanten zur Verfügung. Nach der Aktivierung des Mandanten wird die Option für alle folgenden Aktivierungen ausgeblendet, einschließlich Add-ons und Verlängerungen. Die Funktion ist nicht für bestehende Mandanten verfügbar.

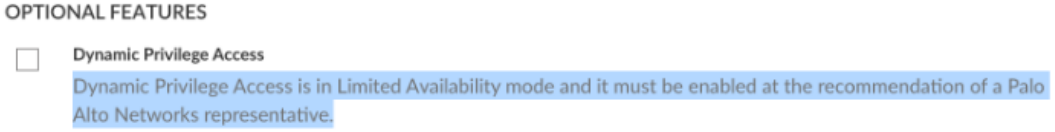
**STEP 1 |** Wenden Sie sich an Ihren Palo Alto Networks-Kontobetreuer, um diese Funktionalität für Ihren Mandanten zu aktivieren.

**STEP 2 |** Aktivieren Sie die Lizenz für Ihre Prisma Access (Managed by Strata Cloud Manager).

**STEP 3 |** Stellen Sie sicher, dass Sie Lizenzen zuweisen, Ihre Dienstverbindungen planen und entsprechend weitere Standorte hinzufügen.

**STEP 4 |** Aktivieren Sie verfügbare Add-ons.

**STEP 5 |** Aktivieren Sie das Kontrollkästchen für **Zugriff mit dynamischen Rechten**.




 ©2025 Palo Alto Networks, Inc.

**STEP 6 |** **Stimmen Sie den allgemeinen Geschäftsbedingungen zu**.

**STEP 7 |** **Jetzt aktivieren**. Die von Ihnen aktivierten Produkte und Add-ons (wie Prisma Access oder Strata Logging Service) werden nun bereitgestellt. Wenn die Abonnements aktiviert sind, wird der Fortschrittsstatus eingeblendet. Wenn der Vorgang abgeschlossen ist, wird der Mandantenstatus als `Aktiv` angezeigt. Sie haben jetzt einen Mandanten, der mit Instanzen der von Ihnen gekauften Produkte ausgestattet ist. Der Mandant hat einen Benutzer – das Konto, das Sie verwendet haben, als Sie diesen Prozess begonnen haben.

**STEP 8 |** Um die restliche Produkteinrichtung abzuschließen, müssen Sie auf die gekauften Produkte zugreifen und alle erforderlichen Konfiguration nach der Installation durchführen. Informationen zu Ihren Produkten finden Sie unter:

- Offene APIs
- Erste Schritte mit Strata Logging Service
- Prisma Access (Managed by Strata Cloud Manager) Administratorhandbuch
- Erste Schritte mit Cloud Identity Engine

**STEP 9 |** Fügen Sie Benutzerzugriff hinzu und weisen Sie Rollen zu.

Ermöglichen Sie Benutzern als **Projektadministrator** Zugriff basierend auf Projekten.

 ©2025 Palo Alto Networks, Inc.

# Autorisieren der Benutzergruppenzuordnung in Cloud Identity Engine für den Zugriff mit dynamischen Rechten

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access-Lizenz<br>❑ Mindestens erforderliche Version von Prisma Access: 5.1<br>❑ Rolle: Superuser |

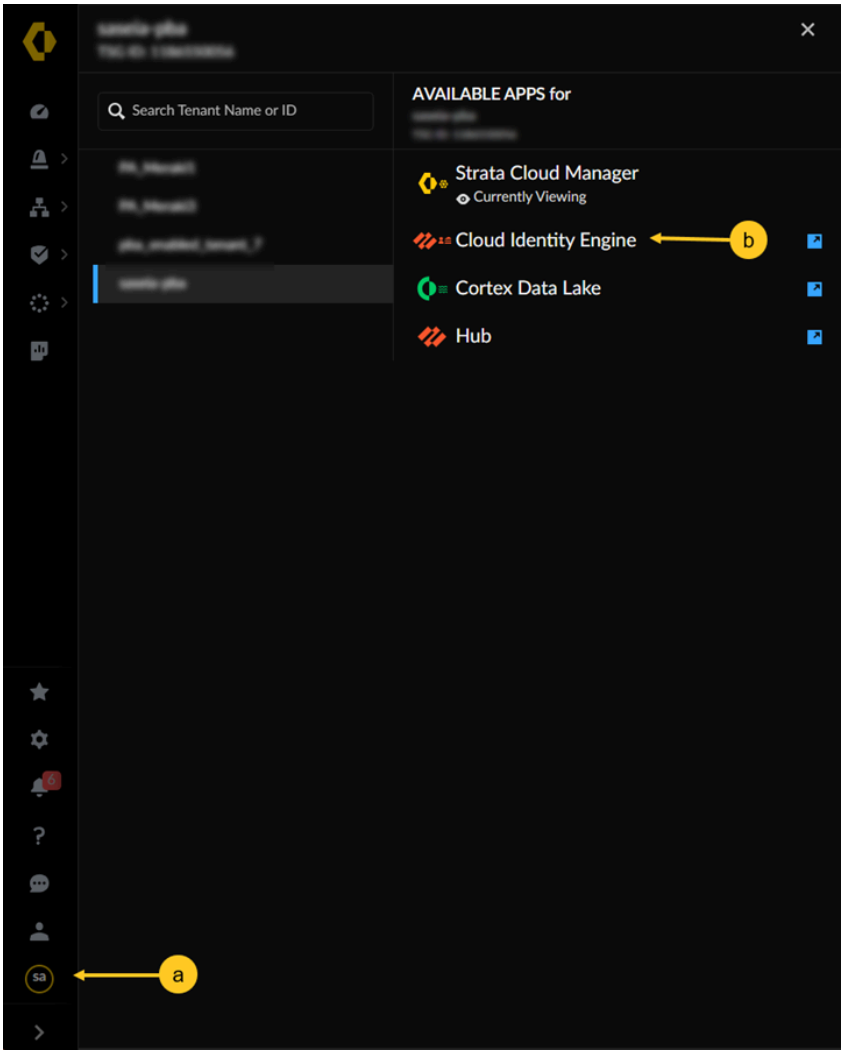
Bevor Sie beginnen, stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Wenden Sie sich an Ihren Ansprechpartner bei Palo Alto Networks, um die Funktionalität für den Zugriff mit dynamischen Rechten zu aktivieren.
- Aktivieren Sie die Cloud Identity Engine und erstellen Sie Ihren ersten Mandanten.
- Richten Sie die Cloud Identity Engine ein.

In diesem Workflow haben wir als Identitätsprovider (IdP) Azure verwendet. Als Identitätsprovider (IdP) können Sie auch Okta verwenden.

 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** Öffnen Sie in Strata Cloud Manager die Cloud Identity Engine-App, die Ihrem Mandanten zugeordnet ist.

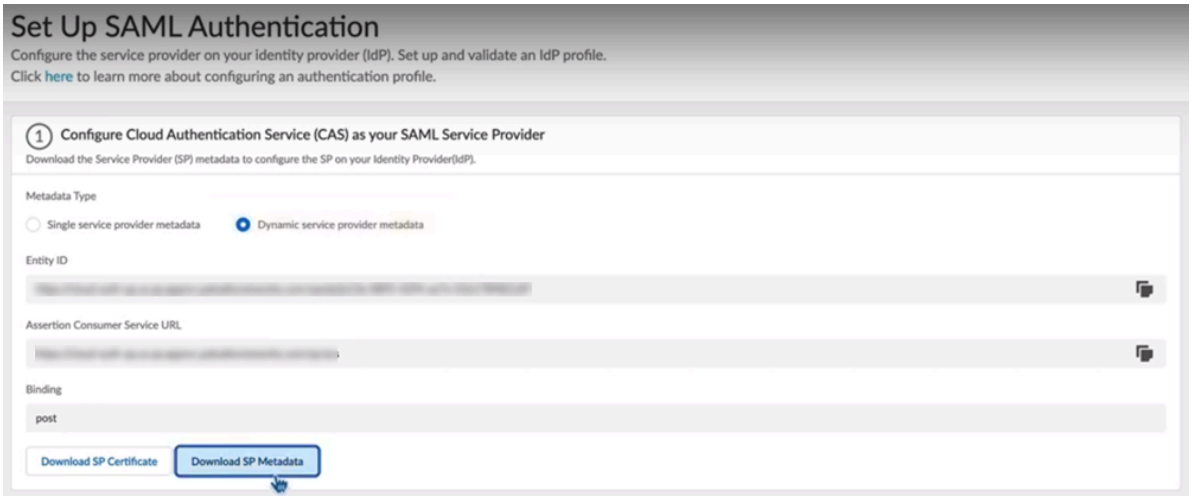



**STEP 2 |** Fügen Sie ein Azure-Verzeichnis oder ein Okta-Verzeichnis als IdP für mobile Benutzer hinzu.

 ©2025 Palo Alto Networks, Inc.

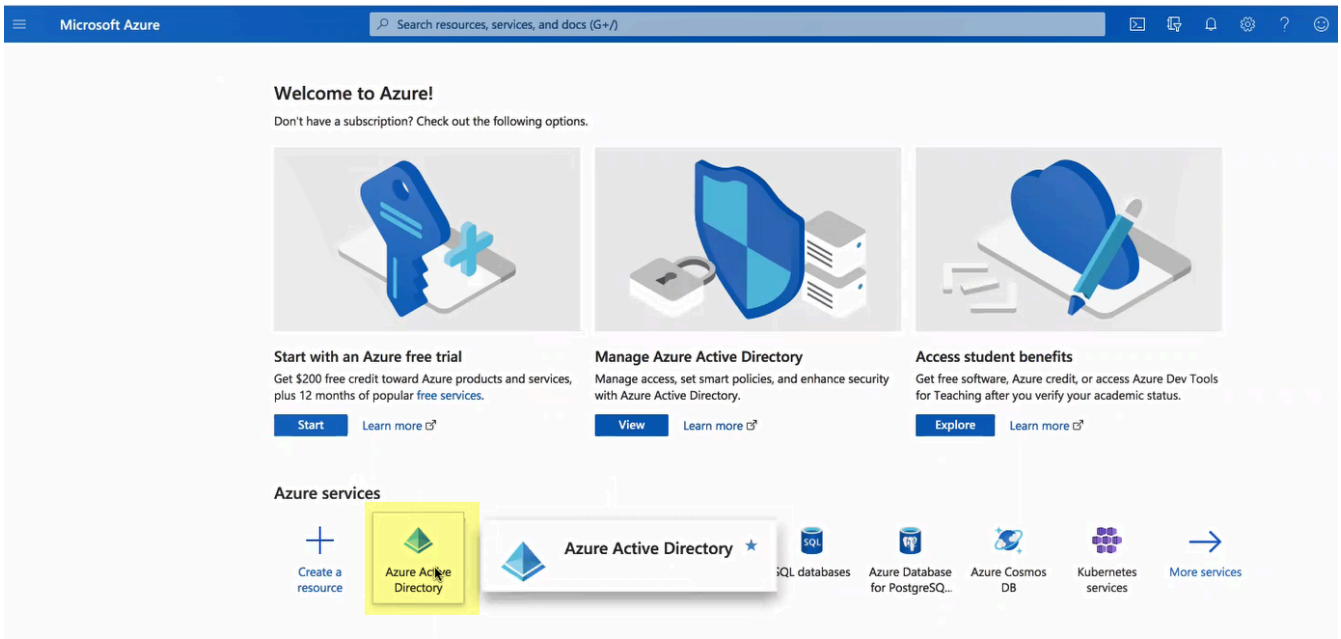
**STEP 3 |** Laden Sie die SP-Metadaten in die Cloud Identity Engine-App herunter.

1. Rufen Sie **Authentifizierung** > **Authentifizierungstypen** > **Neuen Authentifizierungstyp hinzufügen** auf.
2. Verwenden Sie **Einrichten**, um einen SAML-2.0-Authentifizierungstyp einzurichten.
   Wählen Sie **Dynamische Metadaten des Dienstanbieters** aus.
3. **Laden Sie SP-Metadaten** herunter.



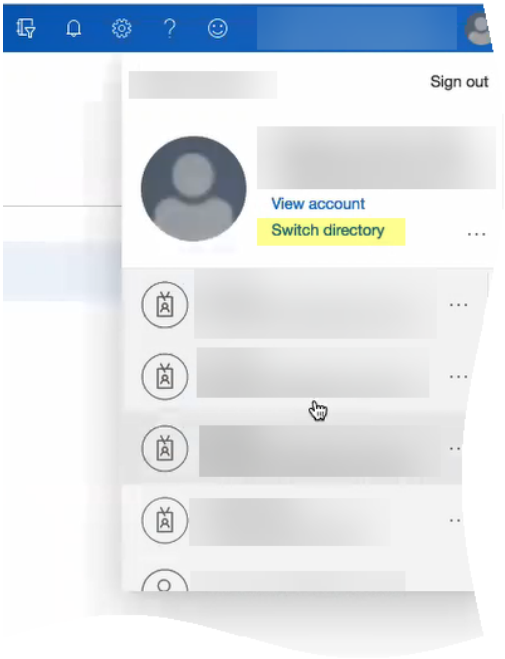

4. Melden Sie sich im Azure Portal an und wählen Sie **Azure Active Directory** aus.

   Vergewissern Sie sich, dass Sie alle notwendigen Schritte im Azure-Portal ausgeführt haben.

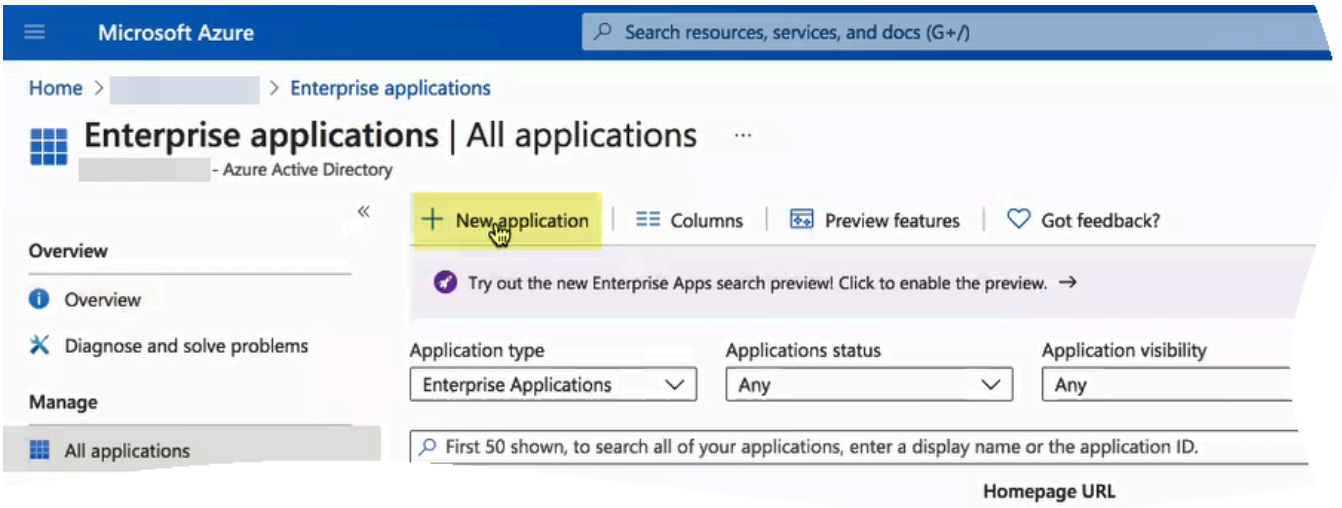



   Wenn Sie über mehrere Verzeichnisse verfügen, verwenden Sie **Verzeichnis wechseln**, um das Verzeichnis auszuwählen, das Sie mit der Cloud Identity Engine verwenden möchten.

 ©2025 Palo Alto Networks, Inc.




5. Wählen Sie **Enterprise-Anwendungen** aus und klicken Sie auf **Neue Anwendung**.




6. Suchen Sie nach **`Palo Alto Networks Cloud Identity Engine – Cloud-Authentifizierungsdienst`** und erstellen Sie die Single Sign-on-Integration für Azure Active Directory (AD).

   Passen Sie den App-Namen bei Bedarf während der Erstellung der Anwendung an.
7. Wählen Sie nach dem Laden der Anwendung **Benutzer und Gruppen** aus und dann **Benutzer/Gruppe hinzufügen**, um sie dieser Anwendung **zuzuweisen**.

   Wählen Sie die Benutzer und Gruppen aus, die den Azure-Identitätsprovider (IdP) in der Cloud Identity Engine für die Authentifizierung verwenden sollen.

 ©2025 Palo Alto Networks, Inc.

> *Vergewissern Sie sich, dass Sie das verwendete Konto zuweisen, damit Sie die Konfiguration nach Abschluss der dazu auszuführenden Arbeiten testen können. Möglicherweise müssen Sie die Seite nach dem Hinzufügen von Konten aktualisieren, um den Test erfolgreich abschließen zu können.*

8. Richten Sie mit **Single Sign-on (SSO) einrichten** die SSO-Funktion ein und wählen Sie dann **SAML** aus.
9. Laden Sie die Metadatendatei hoch, indem Sie **Metadatendatei hochladen** auswählen und dann zu der Metadatendatei navigieren, die Sie in Schritt 3.c von der Cloud Identity Engine-App heruntergeladen haben. Klicken Sie anschließend auf **Hinzufügen**.
10. Geben Sie nach dem Hochladen der Metadaten Ihren regionalen Endpunkt als **Anmelde-URL** im folgenden Format ein: https://<RegionUrl>.paloaltonetworks.com/sp/acs (wobei <RegionUrl> Ihr regionaler Endpunkt ist).

    Alternativ können Sie auch die Antwort-URL als Anmelde-URL kopieren.
11. Wählen Sie zum Speichern Ihrer Konfigurationen **Speichern** aus.

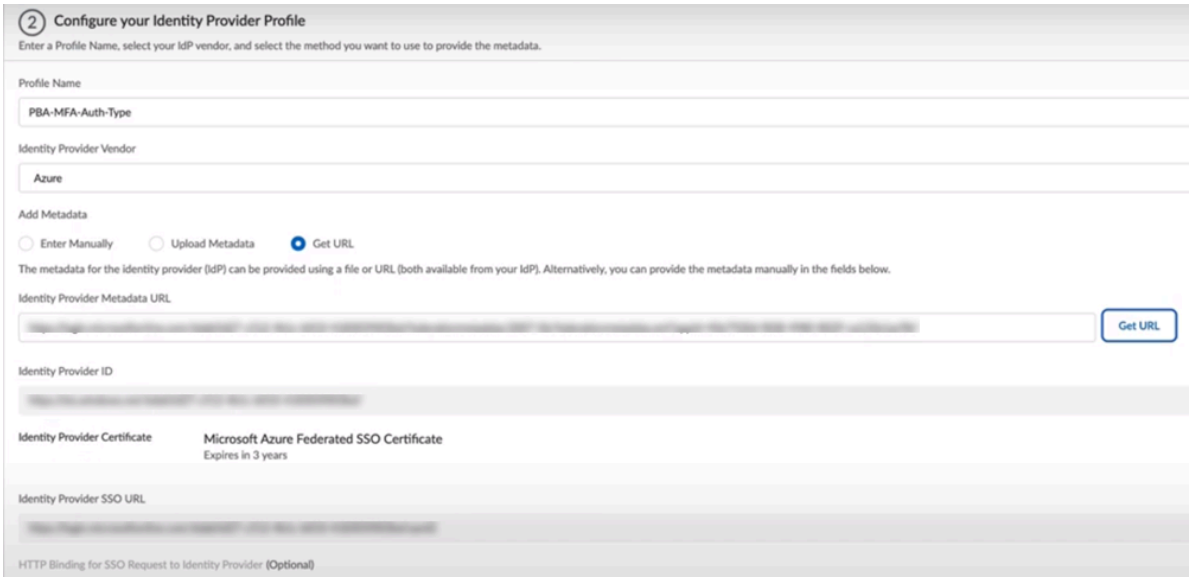
**STEP 4 |** Konfigurieren Sie eine Richtlinie für den bedingten Zugriff, um MFA für ausgewählte Benutzergruppen zu aktivieren.

1. Rufen Sie **Übersicht** > **Bedingter Zugriff** > **Richtlinie erstellen** auf.
2. Fügen Sie durch Auswahl von **Neue Richtlinie** eine neue Richtlinie hinzu.
3. Geben Sie einen Namen für die Richtlinie ein.
4. Wählen Sie im Abschnitt **Benutzer Benutzer und Gruppen auswählen** aus und geben Sie anschließend die entsprechenden Projektgruppen an.
5. Überprüfen Sie die **Zielressourcen**.
6. Wählen Sie die **Bedingungen** aus, die die Richtlinie auslösen.
7. **Erteilen Sie** Zugriff in **Zugriffskontrollen** und verwenden Sie hierzu **Multifaktor-Authentifizierung anfordern**.
8. Aktivieren Sie die Richtlinie, indem Sie den Selektor auf **Ein** umschalten und erstellen Sie mit **Erstellen** den bedingten Zugriff.

 ©2025 Palo Alto Networks, Inc.

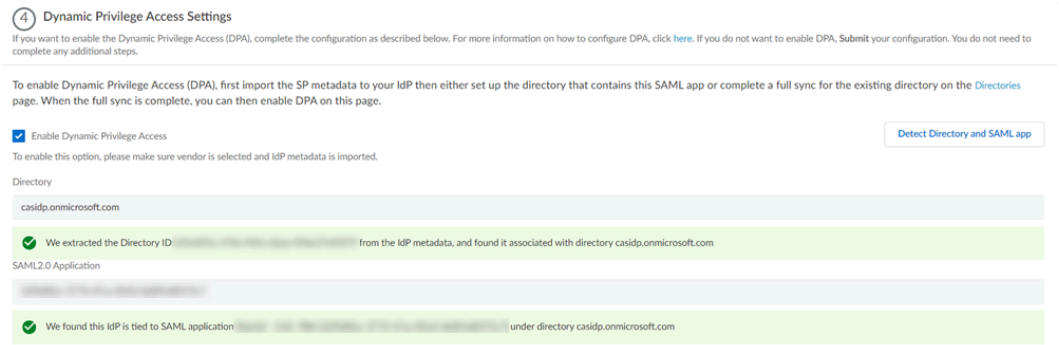
**STEP 5 |** Fügen Sie Ihren IdP-Anbieter als Authentifizierungstyp hinzu.

1. Wählen Sie **Single Sign-on** > **SAML-Zertifikate** und kopieren Sie die **URL für die App-Föderationsmetadaten**.
2. Wählen Sie in der Cloud Identity Engine-App **Authentifizierung** > **Authentifizierungstypen** > **Neuen Authentifizierungstyp hinzufügen** aus.
3. Verwenden Sie **Einrichten**, um einen SAML-2.0-Authentifizierungstyp einzurichten.
4. Geben Sie unter **IdP-Profil konfigurieren** einen Wert für **Profilname** ein.
5. Wählen Sie **Azure** als **IdP-Anbieter** aus.
6. Wählen Sie **URL abrufen** aus, fügen Sie die URL aus Schritt 5.a ein und rufen Sie die Metadaten mithilfe von **URL abrufen** ab.




7. Wählen Sie **Multifaktor-Authentifizierung ist auf Identitätsprovider aktiviert** aus.
8. Mit **SAML-Einrichtung testen** können Sie die Profilkonfiguration überprüfen.
9. Wählen Sie die SAML-Attribute aus, die Prisma Access für die Authentifizierung verwenden soll.
10. Aktivieren Sie **Zugriff mit dynamischen Rechten**.

    Stellen Sie sicher, dass das Verzeichnis, das Sie in Schritt 2 hinzugefügt haben, und die SAML-App synchronisiert werden.




11. **Übermitteln** Sie das IdP-Profil.

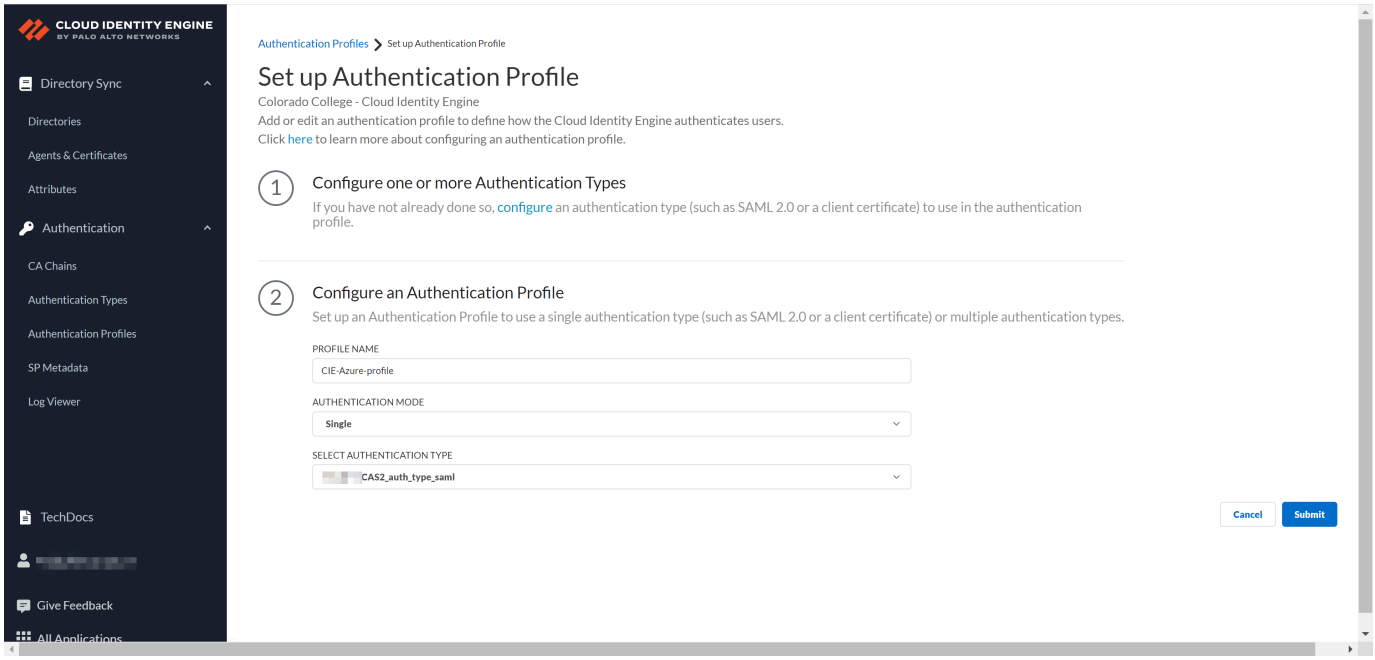
 ©2025 Palo Alto Networks, Inc.

**STEP 6 |** Wiederholen Sie die Schritte von 3 bis 5, um die SAML-App für Benutzergruppen zu konfigurieren, für die keine MFA benötigt wird.

*Aktivieren Sie die MFA in Schritt 5.g nicht für Benutzergruppen, die keine MFA benötigen.*

**STEP 7 |** Fügen Sie ein Authentifizierungsprofil für MFA-Benutzergruppen und Nicht-MFA-Benutzergruppen hinzu.

1. Wählen Sie **Authentifizierung** > **Authentifizierungsprofile** > **Authentifizierungsprofil hinzufügen** aus.
2. Geben Sie einen Wert für **PROFILNAME** ein.
3. Wählen Sie einen **Authentifizierungsmodus** aus.
4. Wählen Sie den **Authentifizierungstyp** aus Schritt 5 oder 6 basierend auf den Benutzergruppen aus, für die eine MFA erforderlich ist. Klicken Sie dann auf **Übermitteln**.

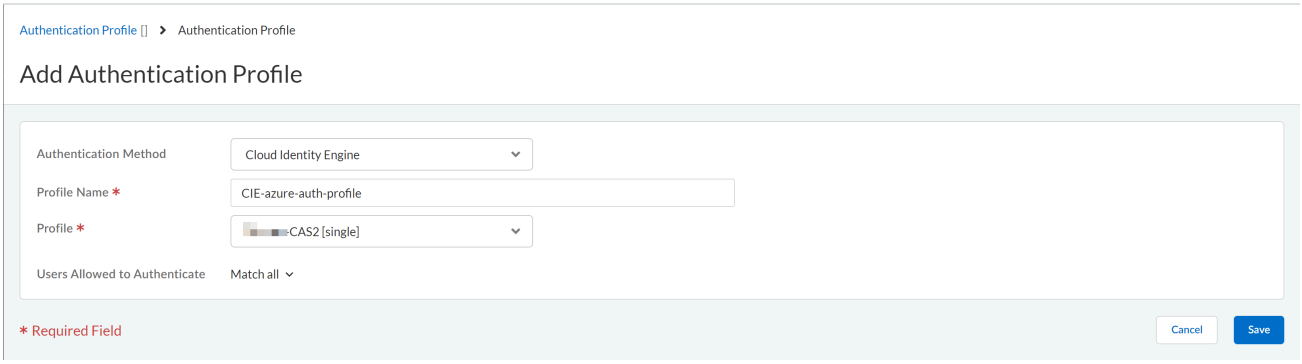



 ©2025 Palo Alto Networks, Inc.

**STEP 8 |** Fügen Sie Prisma Access das Authentifizierungsprofil von Cloud Identity Engine hinzu.

1. Wählen Sie in Strata Cloud Manager **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Identitätsdienste** > **Authentifizierung** > **Authentifizierungsprofile** aus.

   Stellen Sie sicher, dass der Konfigurationsumfang auf den Container für mobile Benutzer **Zugriffsagent** festgelegt wird.
2. **Profil hinzufügen**.
3. Wählen Sie **Cloud Identity Engine** als **Authentifizierungsmethode** aus.
4. Geben Sie einen Wert für **Profilname** ein.
5. Wählen Sie das **Profil** aus, das Sie in Schritt 7 in der Cloud Identity Engine-App hinzugefügt haben.
6. **Speichern** Sie die Änderungen.




**STEP 9 |** Verbinden Sie die Authentifizierung mit den mobilen Benutzern.

1. Starten Sie Prisma Access über den Strata Cloud Manager.
2. Wählen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** aus.
3. Legen Sie als Umfang das von Ihnen erstellte Projekt-Snippet fest und navigieren Sie zu **Sicherheitsdienste** > **Sicherheitsrichtlinie**.
4. Erstellen Sie eine Richtlinie, um Datenverkehr ausschließlich aus dem DHCP-Bereich eines bestimmten Projekts und dieser projektbasierten Benutzergruppe zuzulassen.

 ©2025 Palo Alto Networks, Inc.

# Zugriffsagenten aktivieren

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access 5.1 Innovation<br>❑ Desktop-Geräte mit macOS 12 oder höher oder Desktop-Geräte mit Windows 10 Version 2024 oder höher oder mit Windows 11<br>❑ Prisma Access-Lizenz mit dem Abonnement für mobile Benutzer<br>❑ Rolle: Superuser |

Bevor Sie Ihre Benutzer einbinden können, müssen Sie den **Zugriffsagenten** als Verbindungstyp für mobile Benutzer mit Strata Cloud Manager aktivieren. Nachdem Sie den Verbindungstyp aktiviert haben, können die auf mobilen Benutzergeräten installierten Prisma Access Agents Datenverkehr an Prisma Access senden.

Bevor Sie beginnen, den Prisma Access Agent zu aktivieren, stellen Sie sicher, dass Sie Autorisieren der Benutzergruppenzuordnung in Cloud Identity Engine für den Zugriff mit dynamischen Rechten.

**STEP 1 |** Wählen Sie **Workflows** > **Einrichtung Prisma Access** > **Mobile Benutzer** aus.

**STEP 2 |** **Aktivieren** Sie den Zugriffsagenten.

*„Expliziter Proxy“ wird für den Prisma Access-Agenten nicht unterstützt.*

**STEP 3 |** Klicken Sie auf **Einrichtung Zugriffsagent**, um mit dem Onboarding Ihrer mobilen Benutzer zu beginnen.

Die Seite „Einrichtung Zugriffsagent“ wird angezeigt.


©2025 Palo Alto Networks, Inc.

# Agent-Infrastruktur für den Zugriff mit dynamischen Rechten einrichten

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access 5.1 Innovation<br>❑ Prisma Access-Lizenz mit dem Abonnement für mobile Benutzer<br>❑ Desktop-Geräte mit macOS 12 oder höher oder Desktop-Geräte mit Windows 10 Version 2024 oder höher oder mit Windows 11<br>❑ Rolle: Superuser |

Konfigurieren Sie Infrastruktureinstellungen für den Prisma Access Agenten, damit Prisma Access Ihre mobile Benutzerumgebung bereitstellen kann. Wählen Sie anschließend die Prisma Access-Standorte aus, mit denen sich Ihre Benutzer des Prisma Access Agenten verbinden sollen.

Sie können optional auch die SC-NAT-Unterstützung für Zugriff mit dynamischen Rechten aktivieren, wenn Sie Dienstverbindungen erstellt haben, um auf private Apps in ihrem Rechenzentrum oder ihrer Zentrale zuzugreifen, oder aktivieren Sie die Routenzusammenfassung für Zugriff mit dynamischen Rechten, um die Anzahl der Routen zu reduzieren, die an das Netzwerk gesendet werden.

## Infrastruktureinstellungen konfigurieren

Um Prisma Access für den Internetzugang nur für Benutzer zu aktivieren, stellt Prisma Access einen Standard-IP-Adresspool und einen Cloud-Standard-DNS-Server bereit. Wenn Sie jedoch möchten, dass Ihre mobilen Benutzer auf interne Ressourcen in Ihrer Zentrale, in Rechenzentren oder an Remote-Netzwerkstandorten zugreifen, die Sie in Prisma Access eingebunden haben, müssen Sie Client-IP-Adresspools zuweisen. Prisma Access verwendet die IP-Adresspools, um Ihren mobilen Benutzern IP-Adressen zuzuweisen und die Prisma Access-Dienstinfrastruktur einzurichten.

*Bevor Sie die Infrastruktureinstellungen konfigurieren, stellen Sie sicher, dass Sie mindestens ein Projekt konfigurieren. Andernfalls schlägt der Commit-Vorgang fehl, wenn Sie versuchen, die Infrastruktureinstellungen festzuschreiben und per Push zu übertragen. Weitere Informationen finden Sie unter* Projekt erstellen.

**STEP 1 |** Wählen Sie im Strata Cloud Manager **Workflows** > **Einrichtung Prisma Access** > **Zugriffsagent** > **Infrastruktur** aus.

**STEP 2 |** Wenn Sie die Infrastruktur zum ersten Mal einrichten, klicken Sie auf **Infrastruktureinstellungen einrichten**. Andernfalls bearbeiten Sie die **Infrastruktureinstellungen**.

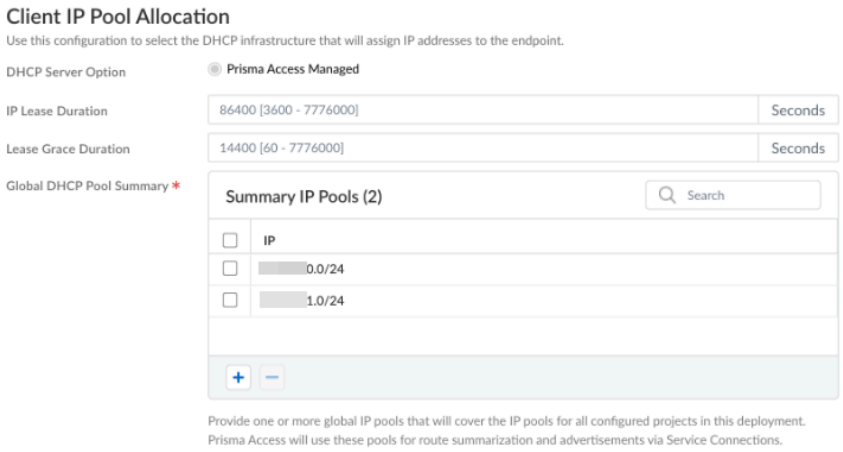
 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Fügen Sie dem **Domänennamen** für den Dienst, mit dem Prisma Access-Agenten eine Verbindung herstellen, einen Hostnamen hinzu.

Standardmäßig können Benutzer, die einen FQDN verwenden, basierend auf Ihrem Hostnamen und der Domäne **`.epm.gpcloudservice.com`** auf den Dienst zugreifen.

**STEP 4 |** In **Zuweisung Client-IP-Pool** stellt Prisma Access einen DHCP-Server bereit, der die Zuweisung von IP-Adressen zu Ihren Endpunkten für Zugriff mit dynamischen Rechten verwaltet.

Der Projektname und die Standortgruppen-ID aus Prisma Access sind Teil der DHCP-Anfrage. Jedem Prisma Access Agenten, der sich mit einem bestimmten Projekt verbindet, wird eine IP-Adresse aus dem IP-Subnetz dieses Projekts zugewiesen. Wenn ein Benutzer zu einem anderen Projekt wechselt, wird dem Prisma Access Agenten eine andere IP-Adresse zugewiesen als dem IP-Subnetz des Projekts.




Sie können folgende Optionen konfigurieren:

- **IP-Lease-Dauer** – Geben Sie die Zeitdauer (in Sekunden) an, für die der DHCP-Server einem Prisma Access Agenten eine Netzwerkadresse zuweist. Die Standard-Lease-Dauer für IP-Adressen beträgt 86.400 Sekunden.
- **Lease-Karenzzeit** – Geben Sie an, wie lange der Prisma Access Agent nach Ablauf der Lease-Zeit sein IP-Adress-Leasing weiter verwenden kann. Die Standard-Lease-Karenzzeit beträgt 14.400 Sekunden.
- **Globaler DHCP-Pool – Zusammenfassung** – Wählen Sie den IP-Pool aus, für den Sie SC-NAT aktivieren möchten. Alternativ dazu können Sie die globalen zusammengefassten IP-Pools für die Routenzusammenfassung konfigurieren und auswählen.

**STEP 5 |** **Speichern** Sie die Infrastruktureinstellungen.

## Prisma Access-Standorte auswählen

Wählen Sie die Prisma Access-Standorte aus, an denen Sie Prisma Access Agent-Benutzer unterstützen möchten. Die Standortgruppen werden für Zugriff mit dynamischen Rechten verwendet.

 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** Wählen Sie im Strata Cloud Manager **Workflows** > **Einrichtung Prisma Access** > **Zugriffsagent** > **Infrastruktur** aus.

**STEP 2 |** Wenn Sie die Infrastruktur zum ersten Mal einrichten, müssen Sie **Standorte hinzufügen**. Andernfalls bearbeiten Sie die **Prisma Access-Standorte**.

**STEP 3 |** Wählen Sie die Prisma Access-Standorte aus, mit denen Ihre mobilen Benutzer eine Verbindung herstellen.

Abhängig von Ihrer Lizenzvereinbarung können Sie entweder lokale oder weltweite Standorte auswählen. Auf der Karte werden die Regionen angezeigt, in denen Sie Prisma Access für Benutzer bereitstellen können. Darüber hinaus bietet Prisma Access mehrere Standorte innerhalb der einzelnen Regionen, um sicherzustellen, dass Ihre Benutzer eine Verbindung zu einem Standort herstellen können, der ein auf den Standort des Benutzers zugeschnittenes Benutzererlebnis bietet. Für eine optimale Leistung wählen Sie **Alles auswählen** aus. Wählen Sie alternativ bestimmte Standorte innerhalb der einzelnen ausgewählten Regionen aus, für die Ihre Benutzer Zugriffsrechte benötigen. Indem Sie Ihre Bereitstellung auf eine einzelne Region beschränken, können Sie die von Ihnen bereitgestellten Regionen genauer steuern und Regionen ausschließen, wenn Ihre Richtlinien oder Branchenvorschriften dies erfordern.

*Für Prisma Access-Agenten können Sie Prisma Access in den folgenden Strata Logging Service-Regionen bereitstellen:*

- *USA*
- *Deutschland*
- *Indien*

*Diese Liste wird aktualisiert, sobald weitere Regionen verfügbar sind.*

Wenn Sie die Anzahl der Standorte begrenzen, wählen Sie für ein optimales Benutzererlebnis die Standorte aus, die Ihren Benutzern am nächsten sind oder sich im selben Land wie Ihre Benutzer befinden. Wenn ein Standort in dem Land, in dem sich Ihre mobilen Benutzer befinden, nicht verfügbar ist, wählen Sie für eine optimale Leistung den Standort aus, der Ihren Benutzern am nächsten ist.

*Die Bilder in diesem Abschnitt dienen nur zur Veranschaulichung.*

1. Wählen Sie auf der Karte eine verfügbare Region aus.

 ©2025 Palo Alto Networks, Inc.

2. Klicken Sie an den Standorten, die Sie hinzufügen möchten, auf das Pluszeichen **+**.

   Sie können zwischen der **Karten-** und **Listenansicht** wechseln. Sie können auch **Alle Standorte auswählen**.

   In der Listenansicht können Sie aus der Liste die verfügbaren Standorte zur Bereitstellung von Prisma Access auswählen. Sie können **alle** Standorte innerhalb einer Region auswählen.

3. **Speichern** Sie Ihre Prisma Access-Standorteinstellungen.

**STEP 4 |** (Optional) Schränken Sie den Zugriff nicht autorisierter Benutzer auf Ihre SaaS-Anwendungen ein.

Sie können die Zulassungslisten mit den Ausgangs-IP-Adressen für vorhandene Bereitstellungen mobiler Benutzer und beim Onboarding neuer Benutzer aktivieren. Wenn Sie Zulassungslisten mit den Ausgangs-IP-Adressen für vorhandene Prisma Access-Bereitstellungen aktivieren, migriert Prisma Access alle Ihren Standorten bereits zugewiesenen Ausgangs-IP-Adressen in die Zulassungslisten mit den Ausgangs-IP-Adressen. Aktivieren Sie für neue Prisma Access-Bereitstellungen die Zulassungsliste für Ausgangs-IP-Adressen beim Onboarding der mobilen Prisma Access-Agent-Benutzer. Jedes Mal, wenn Sie einen Standort hinzufügen oder wenn ein Ereignis mit einem automatischen Skalierungsvorgang auftritt, sollten Sie die neuen von Prisma Access zugewiesenen Ausgangs-IP-Adressen abrufen und sie den Zulassungslisten in Ihren SaaS-Anwendungen hinzufügen. Sie können die Konfiguration dann an Ihre Prisma Access-Bereitstellung übertragen, um die Ihren Standorten zugewiesenen Zulassungslisten für Ausgangs-IP-Adressen zu bestätigen.

1. **Aktivieren Sie die Ausgangs-IP-Zulassungsliste**, um die IP-Adressen für eingebundene Prisma Access-Standorte anzuzeigen.
2. Kopieren Sie die zugewiesenen Adressen und fügen Sie sie den Zulassungslisten Ihrer SaaS-Anwendungen hinzu.
3. Wählen Sie **Migrieren** aus, um die IP-Adressen zu bestätigen, die Sie den eingebundenen Standorten in Prisma Access zugewiesen haben.
4. Rufen Sie die IP-Adressen für neue eingebundene Standorte oder während eines Ereignisses mit automatischer Skalierung ab.
   1. Wählen Sie den **Standort**namen aus, um die dem Standort zugewiesenen neuen Ausgangs-IP-Adressen zu suchen.
   2. Fügen Sie diese IP-Adressen den Zulassungslisten für Ihre SaaS-Anwendungen hinzu, bevor Sie sie in Prisma Access bestätigen.
   3. **Speichern** Sie die zugewiesenen Ausgangs-IP-Adressen.

## SC-NAT-Unterstützung für Zugriff mit dynamischen Rechten aktivieren

Verwenden Sie SC-NAT-Unterstützung für Zugriff mit dynamischen Rechten (Dynamic Privilege Access, DPA), wenn Sie DPA verwenden und Dienstverbindungen erstellt haben, um auf private

 ©2025 Palo Alto Networks, Inc.

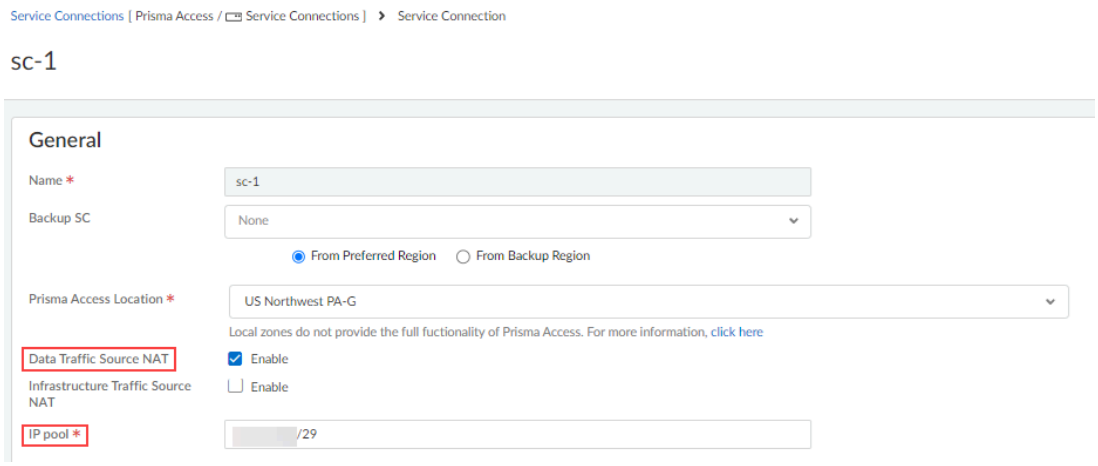
Apps in Ihrem Rechenzentrum oder Ihrer Zentrale zuzugreifen. Bei mehreren Projekten in Ihrer DPA-Umgebung kann es zu einer Erschöpfung der IP-Adressen kommen, wenn sich die IP-Adressen des Infrastruktursubnetzes überschneiden. Um dieses Problem zu beheben, kann Prisma Access Quell-NAT (Source NAT, SNAT) für IP-Adressen implementieren, was Folgendes ermöglicht:

- Prisma Access kann eine einzelne IP-Adresse für einen mobilen Benutzer zuordnen, der über eine Dienstverbindung auf private Apps zugreift
- Einfaches Routing mithilfe von SNAT
- Eliminierung von IP-Pool-Überlappungen
- Vermeidung einer IPv4-Überlastung des IP-Pools zwischen Prisma Access und Ihrem Rechenzentrum oder Hauptsitz

DPA-Kunden können Clientstandorte über Dienstverbindungen in Prisma Access einbinden. Allerdings können mehrere Projekte über große IP-Pools in mehreren Rechenzentren verfügen, was zur potenziellen Erschöpfung privater IP-Pools führt. Zur Lösung dieses Problems bietet Dynamic Privilege Access in Prisma Access Unterstützung für SC-NAT mit definierten Pools. Kunden haben die Möglichkeit, SC-NAT anstelle des Infrastruktursubnetzes zu verwenden, um die IP-Pools aufzuteilen. Wenn Sie SC-NAT für den Dienstverbindungs-Zugriffsknoten eines Unternehmens (Service Connection Corporate Access Node, SC-CAN) aktivieren, wird SC-NAT immer für diese Dienstverbindung unterstützt.

Wenn DPA aktiviert ist, können Sie SC-NAT pro Projekt aktivieren (um SC-NAT zu verwenden ) oder deaktivieren (um das Infrastruktursubnetz zu verwenden).

1. Wählen Sie im Strata Cloud Manager die Optionen **Workflows** > **Einrichtung Prisma Access** > **Dienstverbindungen** aus.
2. Wählen Sie eine Dienstverbindung aus der Tabelle **Dienstverbindungen** aus.
3. Aktivieren Sie das Kontrollkästchen für **Quell-NAT des Datenverkehrs**.
4. Nachdem Sie das Kontrollkästchen **Quell-NAT des Datenverkehrs** angeklickt haben, wird das obligatorische Feld **IP-Pool** angezeigt. Geben Sie die Subnetze ein, für die Sie SC-NAT aktivieren möchten.
5. **Speichern** Sie Ihre Änderungen.




 ©2025 Palo Alto Networks, Inc.

# Routenzusammenfassung für Zugriff mit dynamischen Rechten aktivieren

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access 5.2 Innovation<br>❑ Mindestens Dataplane-Version Prisma Access 11.2.3<br>❑ Prisma Access-Lizenz mit dem Abonnement für mobile Benutzer<br>❑ Rolle: Superuser |

Für Unternehmen, die über lokale Hardware mit begrenzter Kapazität verfügen, wie einfache Cloud-Router, die nur wenige hundert Routen aufnehmen können, kann Prisma Access Routen für mobile Benutzer zusammenfassen, wenn die Routen im lokalen Netzwerk angekündigt werden. Die Routenzusammenfassung minimiert die Anforderungen an diese Geräte, indem sie innerhalb der Routenkapazität des Rechenzentrums bleibt.

Zum Aktivieren der Routenzusammenfassung konfigurieren Sie globale Zusammenfassungspools, also Listen großer IP-Pools, die in mehreren Projekten verwendet werden können. Wenn ein Benutzer mit dem Prisma Access-Agent eine Verbindung zu einem Projekt herstellt und dem Agenten eine IP-Adresse im Bereich eines globalen Zusammenfassungspools zugewiesen wird, kündigt die Prisma Access-Dienstverbindung anstelle der kleineren aggregierten Route den globalen Zusammenfassungspool an.

Im folgenden Szenario ist die Routenzusammenfassung für Projekte veranschaulicht:

- Sie konfigurieren einen globalen Zusammenfassungspool von 10.10.0.0/16 und aktivieren die Option zur Routenzusammenfassung auf der Dienstverbindung **SC-A**.
- **Benutzer-A** stellt eine Verbindung mit **Projekt-A** her, dem der IP-Projektpool 10.10.10.0/24 zugewiesen ist. Wenn die Verbindung hergestellt ist, erhält der Prisma Access-Agent die IP-Adresse 10.10.10.10/32.
- **Benutzer-B** stellt eine Verbindung mit **Projekt-B** her, dem der IP-Projektpool 10.10.11.0/24 zugewiesen ist. Wenn die Verbindung hergestellt ist, erhält der Prisma Access Agent die IP-Adresse 10.10.11.10/32.
- In diesem Fall kündigt die Dienstverbindung nur ein Subnetz (den globalen Zusammenfassungspool von 10.10.0.0/16) anstelle der aggregierten /24-Routen zum lokalen Netzwerk über eBGP an.



- *Prisma Access fasst keine IP-Pools zusammen, die nicht Teil eines Projekts sind.*
- *Projekt-IP-Pools innerhalb eines Projekts können sich ebenso überlappen wie globale zusammengefasste IP-Pools.*
- *Die globalen Zusammenfassungspools sollten große IP-Pools sein, die die Projekt-IP-Pools enthalten, die mehreren Projekten zugeordnet sind.*

So aktivieren Sie die Routenzusammenfassung für Projekte in Strata Cloud Manager:

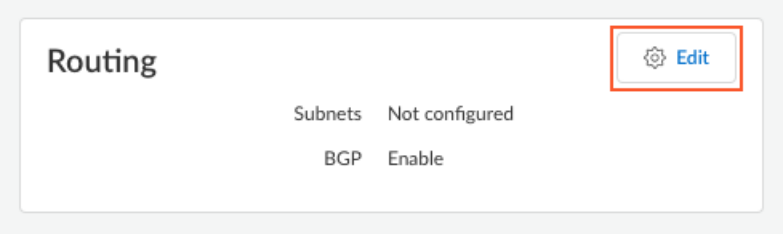
 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** Konfigurieren Sie die Projekt-IP-Pools in den Projekteinstellungen unter **Verwalten** > **NGFW und Prisma Access** > **<Snippet>** > **Objekte** > **Zugriff mit dynamischen Rechten** > **Projekte**.

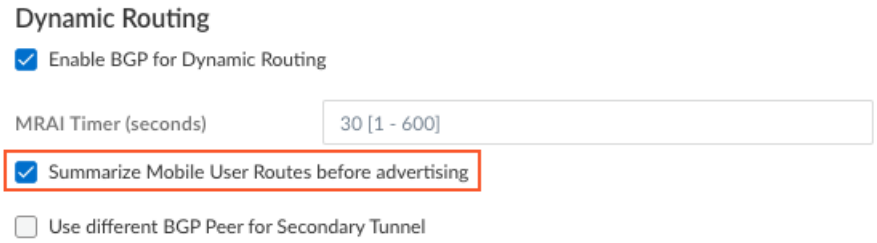
**STEP 2 |** Konfigurieren Sie die globalen zusammengefassten IP-Pools in **Workflows** > **Einrichtung Prisma Access** > **Zugriffsagent** > **Infrastruktureinstellungen**.

**STEP 3 |** Aktivieren Sie die Routenzusammenfassung in der Dienstverbindung.

1. Gehen Sie zu **Workflows** > **Einrichtung Prisma Access** > **Dienstverbindungen**.
2. Wählen Sie eine Dienstverbindung aus der Tabelle **Dienstverbindungen** aus.
3. **Bearbeiten** Sie die Routing-Einstellungen.




4. Wählen Sie **Mobile Benutzerrouten vor dem Mitteilen zusammenfassen** aus.




**STEP 4 |** **Speichern** Sie die Routingeinstellungen.

**STEP 5 |** **Speichern** Sie die Dienstverbindungseinstellungen.

**STEP 6 |** Führen Sie eine Push-Konfiguration für Prisma Access durch.

 ©2025 Palo Alto Networks, Inc.

# Erstellen eines Snippets

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access 5.1 Innovation<br>❑ Prisma Access-Lizenz mit dem Abonnement für mobile Benutzer<br>❑ Rolle: Superuser |

Sie können ein Snippet erstellen, um die Konfigurationen von Prisma Access Agents zu gruppieren, die Sie schnell per Push an Ihre Bereitstellungen übertragen können. Snippets werden verwendet, um eine gemeinsame Basiskonfiguration für einen Satz projektbasierter Bereitstellungen zu standardisieren. So können Sie neue Geräte mit einer bekanntermaßen funktionsfähigen Konfiguration schnell integrieren und die Zeit für das Onboarding neuer Geräte reduzieren.

Nachdem Sie das Snippet erstellt haben, ordnen Sie es einem Bereich zu, weisen dem Bereich einen Benutzer zu und erteilen dem Benutzer die Rolle eines Projektadministrators. Der Benutzer kann sich dann als Projektadministrator anmelden und mithilfe des Snippets die Projekteinstellungen für den Prisma Access Agent verwalten. Der Projektadministrator kann nur die Einstellungen des Prisma Access Agent für die Snippets ändern, denen sie zugewiesen sind.

Führen Sie die folgenden Schritte aus, um ein Snippet zu erstellen.

**STEP 1 |** Melden Sie sich bei Strata Cloud Manager als Superuser an.

**STEP 2 |** Wählen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** aus.

**STEP 3 |** Wählen Sie **Übersicht** aus und erweitern Sie den Konfigurationsbereich, um die **Snippets** anzuzeigen.

 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** Fügen Sie über **Snippet hinzufügen** ein Snippet hinzu und geben Sie die folgenden Details ein:

1. Geben Sie einen **Namen** für das Snippet ein.
2. (Optional) Geben Sie eine **Beschreibung** für das Snippet ein.
3. (Optional) Weisen Sie ein oder mehrere **Beschriftungen** zu.

   Sie können eine vorhandene Beschriftung auswählen oder eine neue Beschriftung erstellen, indem Sie die Beschriftung eingeben, die Sie erstellen möchten.
4. Um sicherzustellen, dass Objektnamen in einem Snippet eindeutig sind, ist standardmäßig **Präfix zu Objektnamen hinzufügen** aktiviert.

   Wählen Sie aus, ob Sie ein Zufallspräfix **automatisch** generieren möchten, oder wählen Sie **Manuell** aus und fügen Sie Ihren eigenen **Präfixwert** hinzu. Der Präfixwert kann alphanumerisch sein und darf maximal sechs Zeichen umfassen.

   Das Präfix hat das Format **xxxxxx-**. Wenn Sie ein Objekt hinzufügen, wird Strata Cloud Manager den Objektnamen mit dem Präfix vorab ausfüllen.
5. **Erstellen** Sie das Snippet.

   Nachdem Sie das Snippet erstellt haben, befinden Sie sich im Konfigurationsumfang für das Snippet. Alle Konfigurationen, die Sie im Snippet-Umfang erstellen, gelten nur für das Snippet.

**STEP 5 |** Verknüpfen Sie das Snippet mit dem Ordner **Access Agent** (Zugriffsagent).

1. Wählen Sie auf der Übersichtsseite Ihres Snippets die Einstellungen für **Snippet-Zuordnungen** aus.
2. Wählen Sie den Ordner **Access Agent** (Zugriffsagent) aus der **Konfigurationsstruktur** aus.
3. Klicken Sie auf das **X**, um das Fenster „Snippet-Zuordnungen“ zu schließen.

   **Access Agent** wird in der Liste der Snippet-Zuordnungen angezeigt.

 ©2025 Palo Alto Networks, Inc.

**STEP 6 |** Falls noch nicht geschehen, erstellen Sie eine Identität für den Benutzer, der Projekte verwalten wird, und weisen Sie dem Benutzer die Rolle eines Projektadministrators für Push-Übertragungen (Projekt-Admin Push) zu.

1. Wählen Sie im Strata Cloud Manager **Einstellungen** > **Identität und Zugriff** aus.
2. Wählen Sie **Identität hinzufügen** aus.
3. Geben Sie die **Identitätsadresse** für den Benutzer ein, der als Projektadministrator vorgesehen ist, und klicken Sie auf **Weiter**.
4. Wählen Sie **Zugriff hinzufügen** > **Prisma Access- & NGFW-Konfiguration** und die Rolle **Projekt-Admin Push** für den Benutzer aus.
5. Klicken Sie auf **Submit (Senden)**.

**STEP 7 |** Erstellen Sie einen Verwaltungsumfang für das Snippet und weisen Sie diesem Umfang einen Benutzer zu.

1. Wählen Sie **Verwalten** > **Zugriffssteuerung** > **Verwaltung des Umfangs** aus.
2. Wählen Sie **Neuen Umfang erstellen**.
3. Geben Sie einen **Namen** für den Umfang ein und sehen Sie sich die **Snippets** an.
4. Ordnen Sie das Snippet dem Umfang zu. Wählen Sie das erstellte Snippet aus und **fügen Sie es hinzu**.
5. Wählen Sie in den Umfangsobjekten die Option **Benutzer zuweisen** aus, um dem Umfang, den Sie für Ihr Snippet erstellt haben, Benutzer zuzuweisen.
6. Weisen Sie dem Umfang einen Benutzer zu, indem Sie einen Benutzer aus der Liste auswählen und dem Benutzer die Rolle **Projektadministrator** zuweisen.
7. **Schließen** Sie das Fenster.
8. Übertragen Sie die Konfiguration per Push.
   1. Wählen Sie **Verwalten** > **Vorgänge** > **Konfiguration übertragen** aus.
   2. Wählen Sie den Administratorbereich **Alle Admins** aus und wählen Sie **Konfiguration übertragen** > **Push** aus.

   Nachdem die Übertragung der Konfiguration per Push abgeschlossen ist, wird das Snippet erstellt und die Rollen werden dem Snippet zugeordnet.

   Der zugewiesene Benutzer (Projektadministrator) kann sich nun mit dem von Ihnen erstellten Snippet bei Strata Cloud Manager anmelden und projektspezifische Einstellungen des Prisma Access Agent konfigurieren. Der Benutzer kann andere Umfänge anzeigen, denen er nicht zugeordnet ist, aber er kann nicht mit ihnen interagieren, z. B. keine Konfigurationen ändern.

 ©2025 Palo Alto Networks, Inc.

# Konfigurieren projektspezifischer Prisma Access Agent-Einstellungen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access 5.1 Innovation<br>❑ Prisma Access-Lizenz mit dem Abonnement für mobile Benutzer<br>❑ Desktop-Geräte mit macOS 12 oder höher oder Desktop-Geräte mit Windows 10 Version 2024 oder höher oder mit Windows 11<br>❑ Rolle: Projektadministrator |

Nachdem der Superuser-Administrator die Infrastruktur eingerichtet hat, ein Snippet erstellt und Ihnen das Snippet zugewiesen hat, können Sie sich als Projektadministrator anmelden, um projektspezifische Prisma Access Agents-Einstellungen wie private IP, Split-Tunnel und DNS-Informationen einzurichten, die Endpunkten zugewiesen werden, wenn sich diese mit dem Prisma Access Agent bei einem Projekt anmelden.

Sie können projektspezifische Einstellungen für einzelne oder mehrere Prisma Access Agents erstellen oder die Standard-Agent-Einstellungen verwenden. Sie können für jedes von Ihnen verwaltete Projekt einen anderen Agent verwenden oder einen Agent für mehrere Projekte gemeinsam nutzen.

# Konfigurieren von Weiterleitungsprofilen zum Verwalten des Agent-Datenverkehrs für Agenten für den Zugriff mit dynamischen Rechten

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access 5.1 Innovation<br>❑ Prisma Access-Lizenz mit dem Abonnement für mobile Benutzer<br>❑ Desktop-Geräte mit macOS 12 oder höher oder Desktop-Geräte mit Windows 10 Version 2024 oder höher oder mit Windows 11<br>❑ Rolle: Projektadministrator |

Unter **Weiterleitungsprofile** finden Sie ein zentrales Fenster zur Konfiguration und Verwaltung von Regeln für die Weiterleitung von Datenverkehr. Hier können Sie beispielsweise Split-

 ©2025 Palo Alto Networks, Inc.

Tunnel-Einstellungen festlegen und Datenverkehr außerhalb der Tunnelverbindung verwalten. „Weiterleitungsprofile“ verbessert nicht nur die unzusammenhängende Konfiguration von Datenverkehrsrichtlinien, wie sie bei anderen Agenten für den mobilen Zugriff auftritt, sondern erweitert zudem die Anzahl der Regeln und Einträge, die Sie konfigurieren können, beträchtlich. Durch die Vereinfachung der zugehörigen Konfigurationen und die Verbesserung der Übersichtlichkeit können Sie sich darauf konzentrieren, wie der Endpunktverkehr geleitet und durchgesetzt werden soll.

Das Weiterleitungsprofil ist ein Profiltyp, der mehrere logische und geordnete Abschnitte enthält. Diese Abschnitte veranschaulichen die verschiedenen Phasen, die eine Verbindung durchläuft, bevor der Agent festlegt, wie die Verbindung geleitet werden soll. Dank dieser Organisationsstruktur können Sie besser verstehen, warum Datenverkehr auf eine bestimmte Weise geleitet wird, indem sie die geordneten Einträge in jedem Abschnitt darstellen. Innerhalb der einzelnen Abschnitte können Sie Einträge hinzufügen, bearbeiten, entfernen oder neu anordnen.

Sobald Sie die Weiterleitungsprofile eingerichtet haben, können Sie sie auf der Seite „Agent-Einstellungen“ Benutzern oder Benutzergruppen zuweisen.

Regeln für die Weiterleitung von Datenverkehr werden im Weiterleitungsprofil von oben nach unten angewendet. Konfigurieren Sie daher das Weiterleitungsprofil von oben nach unten, z. B. zuerst die spezifischsten Regeln und zuletzt die am wenigsten spezifischen Regeln.

**Weiterleitungsregeln**

Ein Weiterleitungsprofil besteht aus verschiedenen Regeln zur Weiterleitung von Datenverkehr, die angeben, welcher Quellanwendungs- oder Zieldomänen- und Ziel-IP-Adressverkehr durch den Tunnel oder außerhalb des Tunnels geleitet wird, ob DNS-Verkehr gesplittet werden soll und welche Datenverkehrsdurchsetzung wirksam ist. Datenverkehr, der einer Regel entspricht, wird gemäß den Spezifikationen für die Weiterleitung von Datenverkehr an Prisma Access weitergeleitet. Die Spezifikationen in einer Weiterleitungsregel sind in folgende Abschnitte gegliedert:

- **Quellanwendungen** – Gibt die privaten oder SaaS-Apps an, für die die Regel gilt. Wenn der Datenverkehr von einem Endpunkt mit der Quell-App übereinstimmt, wird der Datenverkehr gemäß der Weiterleitungsregel geleitet.
- **Ziele** – Gibt die Domänen und IP-Adressen an, für die die Regel gilt. Wenn der Datenverkehr mit den Zielen übereinstimmt (angegeben als FQDNs oder IP-Adressen), wird der Datenverkehr gemäß der Weiterleitungsregel geleitet.

**Datenverkehrsüberwachung**

Jedes Weiterleitungsprofil enthält außerdem Einstellungen für die Datenverkehrsüberwachung, die Ihnen Folgendes ermöglichen:

- Blockieren des gesamten ausgehenden Datenverkehrs, der keinen Weiterleitungsregeln entspricht
- Blockieren des ausgehenden LAN-Zugriffs
- Blockieren des eingehenden Zugriffs, wenn der Agent mit dem Tunnel verbunden ist

Führen Sie zum Konfigurieren eines Weiterleitungsprofils die folgenden Schritte aus:

**STEP 1 |** Melden Sie sich bei Strata Cloud Manager als Projektadministrator an.

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Wählen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Übersicht** aus und erweitern Sie den Konfigurationsumfang, um die **Snippets** anzuzeigen.

**STEP 3 |** Wählen Sie das Snippet aus, das Ihnen der Superuser-Administrator zugewiesen hat.

Sie können auch die Snippets anzeigen, die Ihnen nicht zugewiesen wurden, aber Sie können nicht mit ihnen interagieren, um beispielsweise die Konfiguration zu ändern.

**STEP 4 |** Wählen Sie **Objekte** > **Zugriff mit dynamischen Rechten** aus, um die Einstellungen für den Zugriff mit dynamischen Rechten zu öffnen.

**STEP 5 |** Wählen Sie **Weiterleitungsprofile** aus und bearbeiten Sie die **Einrichtung für Weiterleitungsprofile**.

**STEP 6 |** Richten Sie **Quellanwendungen** ein, wenn Sie Split-Tunnel basierend auf dem SaaS-Anwendungsnamen oder dem Anwendungsnamen der öffentlichen Cloud erstellen möchten.

1. Wählen Sie auf der Seite „Einrichtung von Weiterleitungsprofilen“ die Optionen **Quellanwendungen** > **Quellanwendung hinzufügen** aus.
2. Geben Sie einen aussagekräftigen **Namen** für die Anwendung ein, die Sie hinzufügen möchten.
3. Klicken Sie in der Tabelle **Anwendungen** auf **+** und geben Sie den vollständigen Pfad der Anwendung ein. Sie können eine oder mehrere Anwendungen hinzufügen, um zu verwalten, ob der Anwendungsdatenverkehr vom Tunnel ausgeschlossen oder in den Tunnel eingeschlossen werden soll.

   Wenn Sie den Anwendungsverkehr ausschließen möchten (indem Sie in der Weiterleitungsregel die Konnektivität **Direkt** auswählen), wird der Datenverkehr von diesen Anwendungen über den physischen Adapter an den Endpunkten und nicht über den Tunnel (den virtuellen Adapter) gesendet.

   Wenn Sie Anwendungsdatenverkehr einschließen möchten (indem Sie in der Weiterleitungsregel die Konnektivität **Tunnel** auswählen), wird der Datenverkehr dieser Anwendungen an Prisma Access weitergeleitet, selbst wenn er die Ausschlusskriterien für den Datenverkehr erfüllt.

   Fügen Sie beispielsweise die folgenden vollständigen Pfade hinzu, um den Datenverkehr aus der Zoom-Anwendung heraus zu verwalten:

   - Windows-Endpunkte: **`%AppData%\Roaming\Zoom\bin\Zoom.exe`**
   - macOS-Endpunkte: **`/Applications/zoom.us.app/Contents/MacOS/zoom.us`**

   Wenn Ihnen eine Liste von Anwendungen in einer Textdatei als kommagetrennte Werte (`.csv`) vorliegt, können Sie **CSV-Datei hochladen** auswählen.
4. **Speichern** Sie die Quellanwendung.
5. Wiederholen Sie diese Schritte, um weitere Quellanwendungen hinzuzufügen.

 ©2025 Palo Alto Networks, Inc.

**STEP 7 |** Richten Sie **Ziele** ein, wenn Sie Split-Tunnel basierend auf der Zieldomäne oder den Zugangsrouten erstellen möchten.

1. Wählen Sie auf der Seite „Einrichtung von Weiterleitungsprofilen“ die Optionen **Ziele** > **Ziel hinzufügen** aus.
2. Geben Sie einen aussagekräftigen **Namen** für das Ziel ein, das Sie hinzufügen möchten.
3. Fügen Sie ein Ziel hinzu, indem Sie den Domainnamen, die Zugangsroute oder beides angeben.

   - Um eine Zieldomäne hinzuzufügen, klicken Sie in der Tabelle **FQDNs** auf **+** und geben Sie den FQDN für die Zieldomäne ein. Sie können optional einen Port hinzufügen. Wenn Sie keinen Port angeben, unterliegen alle Ports für die angegebene Domäne der Weiterleitungsregel. Sie können eine oder mehrere Domänen für die Datenverkehrsverwaltung hinzufügen.

     Wenn Sie den Datenverkehr basierend auf dem Domänennamen ausschließen möchten (wählen Sie dazu in der Weiterleitungsregel die Konnektivität **Direkt** aus), wird der Datenverkehr von der Domäne über den physischen Adapter an den Endpunkten und nicht über den Tunnel (den virtuellen Adapter) gesendet.

     Wenn Sie Datenverkehr basierend auf dem Domänennamen einschließen möchten (indem Sie in der Weiterleitungsregel die Konnektivität **Tunnel** auswählen), wird der Datenverkehr von der Domäne an Prisma Access auch dann weitergeleitet, wenn dieser die Ausschlusskriterien für den Datenverkehr erfüllt.

   - Um eine Zugangsroute hinzuzufügen, klicken Sie in der Tabelle **IP-Adressen** auf **+** und geben Sie ein Zielsubnetz ein. Sie können eine oder mehrere Zugangsrouten zur Datenverkehrsverwaltung hinzufügen.

     *Fügen Sie keine Platzhalterzeichen in die IP-Adresse ein. Platzhalter in IP-Adressen werden in Weiterleitungsprofilen nicht unterstützt.*

     Wenn Sie Routen oder Anwendungen nicht einschließen oder ausschließen, wird jede Anfrage durch den Tunnel geleitet (ohne Split-Tunnel). Außerdem wird der gesamte Datenverkehr überprüft und auf die Einhaltung der Richtlinien kontrolliert, wenn Benutzer eine Verbindung zu Prisma Access herstellen.

     Wenn Sie Split-Tunnel-Datenverkehr definieren, um Zugriffsrouten auszuschließen (indem Sie in der Weiterleitungsregel die Konnektivität **Direkt** auswählen), werden diese Routen nicht über den virtuellen Adapter (den Tunnel) durch den Tunnel gesendet, sondern über den physischen Adapter am Endpunkt. Durch den Ausschluss von Split-Tunnel-Datenverkehr nach Zugriffsrouten können Sie latenzanfälligen Datenverkehr oder Datenverkehr mit hoher Bandbreite außerhalb des Tunnels senden, während der gesamte andere Datenverkehr vom Prisma Access-Gateway zur Inspektion und Richtliniendurchsetzung durch den Tunnel geleitet wird.

     Wenn Sie Split-Tunnel-Datenverkehr definieren, um Zugriffsrouten einzubeziehen (indem Sie in der Weiterleitungsregel die Konnektivität **Tunnel** auswählen), überträgt das Prisma Access-Gateway diese Routen per Push an die Endpunkte der Remote-

 ©2025 Palo Alto Networks, Inc.

Benutzer, um festzulegen, welchen Datenverkehr diese Endpunkte durch den Tunnel senden können.

Geben Sie ausgeschlossene Routen an, die spezifischer sind als eingeschlossene Routen. Andernfalls könnten Sie mehr Datenverkehr als beabsichtigt ausschließen.

Wenn Ihnen eine Liste von IP-Adressen in einer Textdatei als kommagetrennte Werte (`.csv`) vorliegt, können Sie **CSV-Datei hochladen** auswählen.

4. **Speichern** Sie die Ziele.
5. Wiederholen Sie diese Schritte, um weitere Ziele hinzuzufügen.

**STEP 8 |** Erstellen Sie ein Weiterleitungsprofil, das basierend auf den von Ihnen konfigurierten Quellanwendungen oder Zielen Datenverkehr zulässt oder ausschließt.

1. Um ein Weiterleitungsprofil hinzuzufügen, wählen Sie **Weiterleitungsprofile** > **Weiterleitungsprofil hinzufügen** > **Prisma Access Agent** aus.

   Um ein Weiterleitungsprofil zu bearbeiten, wählen Sie den Namen des Profils in der Tabelle „Weiterleitungsprofile“ aus.
2. Geben Sie einen aussagekräftigen **Namen** für das Weiterleitungsprofil ein.
3. Wählen Sie **Hinzufügen** aus, um eine Weiterleitungsregel hinzuzufügen.

   In der Tabelle „Weiterleitungsregeln“ werden die Regeln angezeigt, aus denen das Weiterleitungsprofil besteht. Alle Weiterleitungsprofile enthalten die **Standard**weiterleitungsregel, die den gesamten DNS- und Netzwerkverkehr durch den Tunnel sendet. Alle neuen Regeln, die Sie hinzufügen, werden über der Standardregel eingefügt. Sie können die Standardweiterleitungsregel nicht löschen oder verschieben, aber Sie können für sie die Einstellung **Konnektivität** ändern.
4. Geben Sie die Spezifikationen für die Weiterleitungsregel ein.

   1. **Aktivieren** Sie die Regel.
   2. Geben Sie einen **Namen** für die Regel ein.
   3. Wählen Sie die zuvor definierte **Quellanwendung** aus. Wenn Sie **Beliebige** auswählen, gilt die Weiterleitungsregel für den Datenverkehr von beliebigen Quellanwendungen.

      Die Regel stimmt nur überein, wenn die Verbindung von der angegebenen Quellanwendung hergestellt wird.
   4. Wählen Sie einen **Benutzerstandort** aus. Wenn Sie keinen Benutzerstandort eingerichtet haben oder zulassen, dass die Regel mit einem beliebigen

 ©2025 Palo Alto Networks, Inc.

Benutzerstandort übereinstimmt, wählen Sie **Beliebige** aus. (Gilt nicht für Agenten, für die der Zugriff mit dynamischen Rechten aktiviert wurde.)

Die Regel stimmt nur überein, wenn ein Endpunkt mit dem von Ihnen angegebenen Benutzerstandort verbunden ist.

5. Wählen Sie ein zuvor definiertes **Ziel** aus. Wenn Sie **Beliebig** auswählen, gilt die Weiterleitungsregel für den Datenverkehr von einer beliebigen Zieldomäne oder IP-Adresse.

   Die Regel wird nur übereinstimmen, wenn das Verbindungsziel mit der angegebenen Zieldomäne oder IP-Adresse übereinstimmt.

6. Wählen Sie die **Konnektivität** aus:

   - **Direkt** – Sendet den Datenverkehr außerhalb des Tunnels. Der gesamte Datenverkehr für die ausgewählte Anwendung oder das ausgewählte Ziel wird ohne Überprüfung direkt an den physischen Adapter am Endpunkt gesendet.
   - **Tunnel** – Sendet den Datenverkehr durch den Tunnel. Der gesamte Datenverkehr zur ausgewählten Anwendung oder zum ausgewählten Ziel wird zur Überprüfung und Durchsetzung der Richtlinien durch den Tunnel an Prisma Access gesendet.

7. Wählen Sie den **Datenverkehrstyp** aus:

   Geben Sie an, ob Split-DNS verwendet werden soll, damit Benutzer ihre DNS-Abfragen für Anwendungen und Ressourcen zusätzlich zum Netzwerkverkehr über den Tunnel oder außerhalb des Tunnels leiten können.

   - **Netzwerkverkehr + DNS** – Stellt sicher, dass der Split-Tunnel basierend auf der Zieldomäne, die Sie für Ein- oder Ausschlüsse angegeben haben, auf den DNS-Verkehr und den zugehörigen Anwendungsdatenverkehr im Netzwerk für diese Domäne angewendet wird.
   - **Netzwerkverkehr** – Schließt Regeln ein oder aus, die nur auf Netzwerkanwendungsverkehr und nicht auf DNS-Verkehr angewendet werden. Der gesamte DNS-Verkehr geht durch den Tunnel unabhängig vom Split-Tunnel basierend auf der Zieldomäne, die Sie für Ein- oder Ausschlüsse angegeben haben.

   > *Für Windows-Agenten wird die Split-Tunnel-Option **Netzwerkverkehr + DNS** für anwendungsbasierte Split-Tunnel-Regeln nicht unterstützt. Wenn Sie Split-Tunneling so einrichten, dass Datenverkehr basierend auf Anwendungsnamen aus dem Tunnel eingeschlossen oder ausgeschlossen wird, und Sie **Netzwerkverkehr + DNS** auswählen, werden DNS-Abfragepakete für ausgeschlossene und eingeschlossene Apps die Split-Tunnel-Regel nicht einhalten.*

5. Wählen Sie **Hinzufügen** aus, um die Weiterleitungsregel hinzuzufügen.

   Die Regel wird der Tabelle „Weiterleitungsregeln“ hinzugefügt. Sie können dem Weiterleitungsprofil mehrere Regeln hinzufügen.

 ©2025 Palo Alto Networks, Inc.

**STEP 9 |** Konfigurieren Sie die Optionen für die **Datenverkehrsüberwachung**, um festzulegen, wie Datenverkehr durchgesetzt werden soll.

*Vergewissern Sie sich, dass Sie die Option **Alle abwählen** ausgewählt haben, da diese Optionen für den Zugriff mit dynamischen Rechten nicht empfohlen werden.*

- **Blockieren Sie alle anderen nicht übereinstimmenden ausgehenden Verbindungen** – Sofern aktiviert, werden alle Verbindungen blockiert, die keiner der Weiterleitungsregeln entsprechen. Der Verkehr wird nicht durch den Tunnel geleitet.
- **Blockieren Sie den ausgehenden LAN-Zugriff, wenn eine Verbindung zum Tunnel besteht** – Sofern aktiviert, wird der direkte Zugriff auf das lokale Netzwerk blockiert, wenn der Agent mit dem Tunnel verbunden ist. Durch das

  Blockieren des Zugriffs auf Ihr lokales Netzwerk wird der gesamte Datenverkehr an den lokalen Adapter gesendet. Darüber hinaus können Ihre Benutzer nicht auf Ressourcen im lokalen Subnetz, z. B. Drucker, zugreifen. Split-Tunnel-Datenverkehr, der auf Zugangsroute, Zieldomain und Anwendung basiert, funktioniert noch immer wie erwartet.

  Wenn Sie diese Option deaktivieren, können Ihre Endbenutzer auf lokale Ressourcen zugreifen, ohne dass sie zuvor eine Verbindung mit Prisma Access über den Prisma Access-Agenten herstellen müssen.
- **Blockieren Sie den eingehenden Zugriff, wenn eine Verbindung zum Tunnel besteht** – Sofern aktiviert, werden alle eingehenden Verbindungen aus dem Tunnel blockiert.

**STEP 10 |** **Speichern** Sie Ihr Weiterleitungsprofil.

**STEP 11 |** Übertragen Sie die Konfiguration per Push, indem Sie **Konfiguration übertragen** > **Push** auswählen. Mit dieser Aktion wird Ihr Weiterleitungsprofil auf der Seite „Agent-Einstellungen“ zur Auswahl bereitgestellt.

## Überprüfen und Beheben von Problemen mit Weiterleitungsprofilkonfigurationen für Dynamic Privilege Access Agents

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (verwaltet von Strata Cloud Manager) | ☐ Prisma Access 5.1 Preferred oder Innovation<br>☐ Prisma Access-Lizenz mit dem Abonnement für mobile Benutzer<br>☐ Desktop-Geräte mit macOS 12 oder höher oder Desktop-Geräte mit Windows 10 Version 2024 oder höher oder mit Windows 11<br>☐ Rolle: Superuser |

Nachdem Sie ein Weiterleitungsprofil konfiguriert haben, können Sie überprüfen, ob der Datenverkehr wie vorgesehen geleitet wird, indem Sie die Protokolldateien zum Datenverkehr

 ©2025 Palo Alto Networks, Inc.

anzeigen. Sie können die Verkehrs-Protokolle im Protokoll-Viewer von Strata Cloud Manager oder über das Prisma Access-Befehlszeilentool (PACli) auf einem Endpunkt anzeigen.

- So zeigen Sie die Verkehrs-Protokolldateien im Protokoll-Viewer von Strata Cloud Manager an:
  1. Wählen Sie **Vorfälle und Benachrichtigungen** > **Protokoll-Viewer** aus.
  2. Weitere Informationen finden Sie in den Protokollen unter **Firewall/Datenverkehr**.

- So zeigen Sie die Protokolldateien zum Datenverkehr auf einem Endpunkt an:
  1. Starten Sie die Remote-Shell unter **Verwalten** > **Prisma Access-Agent** oder öffnen Sie eine Windows-Eingabeaufforderung oder ein macOS-Terminalfenster auf dem Gerät eines Endbenutzers.
  2. Zum Anzeigen von Weiterleitungsregeln in einem Weiterleitungsprofil geben Sie den folgenden Befehl ein:
     - Unter Windows:

       ```
       "C:\Program Files\Palo Alto Networks\Prisma Access Agent
       \pacli" traffic show
       ```

     - Unter macOS:

       ```
       /Applications/Prisma\ Access\ Agent.app/Contents/Helpers/
       pacli traffic show
       ```

     *Wenn Sie eine Umgebungsvariable für das PACli-Tool (`pacli`) einrichten, können Sie einfach **`pacli traffic show`** eingeben.*

     Das Beispiel für die PACli-Befehlszeilenausgabe zeigt eine Tabelle mit den Weiterleitungsregeln, die im Weiterleitungsprofil wirksam sind, einschließlich der Prioritäten der Weiterleitungsregeln. Auch die Optionen zur Datenverkehrsüberwachung für das Weiterleitungsprofil werden angezeigt. Diese Tabelle entspricht den Weiterleitungsregeln, die Sie in Ihrem Weiterleitungsprofil eingerichtet haben.
  3. Zum Anzeigen der Details einer Weiterleitungsregel geben Sie den folgenden Befehl ein:

     ```
     pacli traffic show <number>
     ```

     Dabei ist **<number>** die Zahl in der Spalte `Priorität`, beispielsweise:

  4. Um Split-Tunnel-Probleme zu beheben, müssen Sie möglicherweise überprüfen, welcher Agentenverkehr sich innerhalb oder außerhalb des Tunnels befindet. Zeigen Sie hierfür

 ©2025 Palo Alto Networks, Inc.

das Verbindungsprotokoll des Prisma Access-Agenten an. Geben Sie den folgenden Befehl ein:

```
pacli traffic log
```

Zum Anzeigen eines einzelnen Protokolleintrags geben Sie den folgenden Befehl ein:

```
pacli traffic log <index>
```

Dabei entspricht **<index>** der Indexzahl für den Eintrag. Beispiel:

Sie können das Verbindungsprotokoll auch zur weiteren Analyse in eine Datei exportieren, indem Sie folgenden Befehl eingeben:

```
pacli traffic log export <filename>
```

# Konfigurieren der Einstellungen der Prisma Access Agent-App für den Zugriff mit dynamischen Rechten

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | ☐ Prisma Access 5.1 Innovation<br>☐ Prisma Access-Lizenz mit dem Abonnement für mobile Benutzer<br>☐ Desktop-Geräte mit macOS 12 oder höher oder Desktop-Geräte mit Windows 10 Version 2024 oder höher oder mit Windows 11<br>☐ Rolle: Projektadministrator |

Strata Cloud Manager bietet die standardmäßigen App-Konfigurationen für Prisma Access Agent, die für alle Benutzergruppen in allen Projekten gelten. Sie können eine App-Konfiguration hinzufügen, um die Art der Interaktion Ihrer Endbenutzer in einem Projekt mit dem Prisma Access Agent anzupassen.

**STEP 1 |** Melden Sie sich bei Strata Cloud Manager als Projektadministrator an.

**STEP 2 |** Wählen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Übersicht** aus und erweitern Sie den Konfigurationsumfang, um die **Snippets** anzuzeigen.

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Wählen Sie das Snippet aus, das Ihnen der Superuser-Administrator zugewiesen hat.

Sie können auch die Snippets anzeigen, die Ihnen nicht zugewiesen wurden, aber Sie können nicht mit ihnen interagieren, um beispielsweise die Konfiguration zu ändern.

**STEP 4 |** Wählen Sie **Objekte** > **Zugriff mit dynamischen Rechten** aus, um die Einstellungen für den Zugriff mit dynamischen Rechten zu öffnen.

**STEP 5 |** Wählen Sie die Registerkarte **Agent-Einstellungen** aus.

**STEP 6 |** Strata Cloud Manager stellt Ihnen die Standardeinstellungen des Agenten zur Verfügung. Wenn Sie die Standardeinstellungen nicht verwenden möchten. Wählen Sie **Agent-Einstellungen hinzufügen** aus.

Um die Einstellungen für einen Agenten zu bearbeiten, wählen Sie einen Agentennamen in der Tabelle aus.

**STEP 7 |** Erstellen Sie eine App-Konfigurationsregel. Die Konfigurationsregel verknüpft eine oder mehrere Projekte mit bestimmten Einstellungen, die speziell für diese Projekte gelten.

1. Geben Sie einen **Namen** für die Regel ein.
2. Geben Sie die **Übereinstimmungskriterien** an, indem Sie **Projekte** hinzufügen. Benutzer und Gruppen, die den Kriterien für das **Projekt** entsprechen, erhalten die App-Einstellungen, wenn sie sich mit dem Prisma Access Agent am Projekt anmelden.
   - Um die Konfiguration für alle Benutzer bereitzustellen, geben Sie für **Projekte** die Option **Beliebig** an.
   - Um die Konfiguration für Benutzer bereitzustellen, die sich bei bestimmten Projekten anmelden, legen Sie für **Projekte** die Option **Projekte hinzufügen** fest und treffen Sie dann in der Liste der Projekte Ihre Auswahl.

 ©2025 Palo Alto Networks, Inc.

**STEP 8 |** Konfigurieren Sie die App-Einstellungen für den Prisma Access-Agenten.

- **Verbinden** – Geben Sie an, wie der Prisma Access-Agent eine Verbindung zu Prisma Access herstellt. Diese Einstellung ist erforderlich.
  - Wählen Sie **Immer eingeschaltet** aus, um immer dann, wenn sich der Benutzer bei einem Endpunkt anmeldet, automatisch eine Verbindung zum Prisma Access-Agenten herzustellen.
  - Wählen Sie **On-Demand** aus, um nur dann eine Verbindung zum Prisma Access-Agenten herzustellen, wenn sich der Benutzer durch Klicken auf die Sperrschaltfläche beim Prisma Access-Agenten anmeldet.
- **Support-Seite** – Geben Sie die Website ein, auf die Benutzer zugreifen können, wenn sie im Prisma Access-Agenten auf **Support-Ressourcen** klicken.

  Die Standard-Supportseite ist die Website für die Dokumentation zum Prisma Access-Agenten.
- **Access Experience (ADEM, App-Beschleunigung, Endbenutzer-Coaching) (nur Windows und MAC)** – Geben Sie an, ob der Autonomous DEM-(ADEM-)Endpunkt-Agent während der Installation der Prisma Access-Agent-App installiert werden soll, und erlauben Sie Endbenutzern, Benutzererfahrungstests aus der App zu aktivieren oder zu deaktivieren.
  - **Agent installieren**
  - **Agent deinstallieren**
  - **Keine Aktion (der Agent-Status bleibt unverändert)** (Dies ist der Standardwert)

  Einzelheiten zu den ersten Schritten mit ADEM auf von der Cloud verwaltetem Prisma Access finden Sie unter Erste Schritte mit Autonomous DEM.
- **ADEM-Aktualisierungsbenachrichtigungen anzeigen** – **Aktivieren** Sie diese Einstellung, um Benachrichtigungen von ADEM anzuzeigen, wenn am dem Endpunkt ein Update verfügbar ist.
- **Sitzungs-Timeout** – Prisma Access-Agent-Benutzersitzungen werden erstellt, wenn ein Benutzer eine Verbindung zum Prisma Access-Gateway (Standort) herstellt und sich erfolgreich authentifiziert. Die Sitzung wird dann einem bestimmten Gateway zugewiesen, das basierend auf den definierten Split-Tunnel-Regeln bestimmt, welcher Datenverkehr getunnelt wird. Die minimale Dataplane-Version für Prisma Access muss 11.2 sein.

  Geben Sie die Zeitspanne an, die vergehen muss, bevor die Sitzung wegen Inaktivität abläuft. Diese Einstellung ist erforderlich.

  *Wenn Sie die Nebula-Dataplane (10.2) in Prisma Access verwenden, ist der Wert für **Sitzungs-Timeout** nicht konfigurierbar und beträgt standardmäßig 7 Tage.*
- **Lokale Suchdomänen an Tunnel-DNS-Suffixe anhängen (nur Mac)** – **Aktivieren** Sie diese Einstellung, um Tunnel-DNS-Suchdomänen an lokale DNS-Suchdomänen auf macOS-Endpunkten anzuhängen. Durch das Anhängen von Tunnelsuchdomänen an die lokalen DNS-Suchdomänen eines Endpunkts können Benutzer schnell auf lokale und

 ©2025 Palo Alto Networks, Inc.

Remote-Unternehmenswebsites und -server zugreifen, die sie häufig besuchen, ohne die vollständige Adresse eingeben zu müssen.

- **Proxy für jede Verbindung erkennen (nur Windows)** – **Aktivieren** Sie diese Einstellung, um den Proxy bei jeder Verbindung automatisch zu erkennen. Deaktivieren Sie diese Einstellung, wenn der Proxy für die Gateway-Verbindung automatisch erkannt und dieser Proxy für nachfolgende Verbindungen zu Prisma Access verwendet werden soll.
- **Tunnel über Proxy einrichten (nur Windows und Mac)** – **Aktivieren** Sie diese Einstellung, um das Netzwerkverkehrsverhalten basierend auf der Proxy-Nutzung des Prisma Access-Agenten zu konfigurieren. Wählen Sie **Aktivieren** aus, um den Prisma Access-Agenten zur Verwendung von Proxys zu verpflichten. Deaktivieren Sie diese Einstellung, wenn der Prisma Access-Agent Proxys umgehen soll. Abhängig von der Proxy-Nutzung des Prisma Access-Agenten, dem Endpunkt-Betriebssystem und dem Tunneltyp verhält sich der Netzwerkverkehr unterschiedlich.

  Wenn Sie diese Option deaktivieren, umgeht der Prisma Access-Agent die Proxys. Der gesamte HTTP- oder HTTPS-Verkehr, der den Proxy- oder PAC-Dateiregeln entspricht, muss den Prisma Access-Agent-Tunnel durchlaufen, bevor er das vorgesehene Ziel erreicht. Durch das Umgehen von Proxys können Sie verhindern, dass Benutzer einen persönlichen Proxy einrichten, um auf Webressourcen zuzugreifen, ohne zur Überprüfung und Richtliniendurchsetzung den Tunnel durchlaufen zu müssen.

- **Optimierte MTU** – Die maximale Übertragungseinheit (Maximum Transmission Unit, MTU) ist die größte Paketgröße, die während einer Übertragung in einem Paket gesendet werden kann. **Aktivieren** Sie diese Option, um automatisch die beste MTU für Paketübertragungen zu bestimmen.

  Prisma Access-Agent-Verbindungen können mehrere ISPs und Netzwerk-Hops mit MTU-Werten unter den standardmäßig konfigurierten 1.500 Bytes durchlaufen. Wenn der statische MTU-Wert des Agenten niedriger ist als der vom ISP angebotene Wert, kommt es zu übermäßiger Fragmentierung und zusätzlichem Overhead, was zu einem geringeren Durchsatz führt. Verloren gegangene Pakete im Netzwerkpfad des ISP lösen außerdem erneute Übertragungen aus, die zu einer suboptimalen Leistung beitragen.

  Wenn Sie **Optimierte MTU** aktivieren, müssen Sie den optimalen MTU-Wert nicht mühsam ermitteln und konfigurieren und können zudem verhindern, dass Benutzer Leistungseinbußen hinnehmen müssen, die sich auf ihre Produktivität auswirken.

  **Optimierte MTU** ist standardmäßig aktiviert. Wenn Sie die Option deaktivieren, können Sie die MTU manuell konfigurieren. Der Bereich für **Konfigurierbare MTU (Bytes)** beträgt 256 bis 1.420 Bytes. Der Standardwert ist 1.400.
- **Eingehende Authentifizierungsaufforderungen von MFA-Gateways** – Um die Multi-Faktor-Authentifizierung (MFA) zu unterstützen, muss ein Prisma Access-Agent-Endpunkt UDP-Aufforderungen empfangen, die vom Gateway eingehen. **Aktivieren** Sie diese Einstellung, um einem Prisma Access-Agent-Endpunkt das Empfangen und Bestätigen der UDP-Eingabeaufforderungen zu ermöglichen. Diese Einstellung ist standardmäßig aktiviert. Deaktivieren Sie diese Einstellung, um UDP-Eingabeaufforderungen vom Gateway zu blockieren.
- **Netzwerkport für eingehende Authentifizierungsaufforderungen (UDP)** – Gibt die Portnummer an, die ein Prisma Access-Agent-Endpunkt verwendet, um eingehende

 ©2025 Palo Alto Networks, Inc.

Authentifizierungsaufforderungen von MFA-Gateways zu empfangen. Der Standardport ist 4501. Um den Port zu ändern, geben Sie eine Zahl zwischen 1 und 65.535 an.

- **Liste vertrauenswürdiger Hosts für MFA** – Wählen Sie **Hinzufügen** aus, um die Hosts für Firewalls oder Authentifizierungs-Gateways hinzuzufügen, denen ein Prisma Access-Agent-Endpunkt bei der Multi-Faktor-Authentifizierung vertrauen kann. Wenn ein Endpunkt eine UDP-Nachricht auf dem angegebenen Netzwerkport empfängt, zeigt der Prisma Access-Agent nur dann eine Authentifizierungsnachricht an, wenn die UDP-Eingabeaufforderung von einem vertrauenswürdigen Gateway stammt.
- **Eingehende Authentifizierungsnachricht** – Passen Sie eine Benachrichtigungsmeldung so an, dass sie angezeigt wird, wenn Benutzer versuchen, auf eine Ressource zuzugreifen, die eine zusätzliche Authentifizierung erfordert.

  Wenn Benutzer versuchen, auf eine Ressource zuzugreifen, die eine zusätzliche Authentifizierung erfordert, empfängt der Prisma Access-Agent ein UDP-Paket mit der eingehenden Authentifizierungsaufforderung und zeigt diese Meldung an. Das UDP-Paket enthält auch die URL für die Seite „Authentifizierungsportal“, die Sie bei der Konfiguration der Multi-Faktor-Authentifizierung angegeben haben. Der Prisma Access-Agent hängt die URL automatisch an die Nachricht an.

  Beispiel:

  ```
  Sie haben versucht, auf eine geschützte Ressource zuzugreifen,
   die eine zusätzliche Authentifizierung erfordert. Fahren Sie mit
   der Authentifizierung fort unter
  ```

  Die Nachricht kann bis zu 255 Zeichen lang sein.
- **Mehrere eingehende MFA-Aufforderungen unterdrücken (Sek.)** – Geben Sie an, wie viele Sekunden gewartet werden soll, bevor der Prisma Access-Agent mehrere eingehende UDP-Eingabeaufforderungen unterdrücken kann. Der Standardwert ist 180 Sekunden.
- **Zulassen, dass sich Benutzer abmeldet** – **Aktivieren** Sie diese Einstellung, um Ihren Benutzern die Abmeldung vom Prisma Access-Agenten zu erlauben. Diese Einstellung ist standardmäßig deaktiviert.

**STEP 9 |** Wählen Sie ein **Weiterleitungsprofil** aus, das Sie zuvor konfiguriert haben, um den Datenverkehrsfluss zwischen dem Agenten und Prisma Access zu verwalten.

**STEP 10 |** Konfigurieren Sie DNS-Einstellungen für den Zugriff mit dynamischen Rechten.

**STEP 11 |** Konfigurieren Sie die Einstellungen der Profile für Hostinformationen

**STEP 12 |** Wenn Sie die Einrichtung der Prisma Access Agent-Einstellungen abgeschlossen haben, klicken Sie auf **Speichern**.

 ©2025 Palo Alto Networks, Inc.

# Konfigurieren von DNS-Einstellungen für den Zugriff mit dynamischen Rechten

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | ☐ Prisma Access 5.1 Innovation<br>☐ Prisma Access-Lizenz mit dem Abonnement für mobile Benutzer<br>☐ Desktop-Geräte mit macOS 12 oder höher oder Desktop-Geräte mit Windows 10 Version 2024 oder höher oder mit Windows 11<br>☐ Rolle: Projektadministrator |

Sie können DNS-Server so konfigurieren, dass Prisma Access Ihre internen Domänen auflösen kann.

**STEP 1 |** Wählen Sie in Strata Cloud Manager die Optionen **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Übersicht** aus und erweitern Sie den Konfigurationsumfang, um die **Snippets** anzuzeigen.

**STEP 2 |** Wählen Sie das Snippet aus, das Ihnen der Superuser-Administrator zugewiesen hat.

**STEP 3 |** Wählen Sie **Objekte** > **Zugriff mit dynamischen Rechten** aus, um die Einstellungen für den Zugriff mit dynamischen Rechten zu öffnen.

**STEP 4 |** Wählen Sie die Registerkarte **Agent-Einstellungen** aus.

**STEP 5 |** Wählen Sie **Agent-Einstellungen hinzufügen** oder eine vorhandene Einstellung in der Tabelle der Agent-Einstellungen aus.

**STEP 6 |** Geben Sie den **primären DNS**-Server und den **sekundären DNS**-Server ein, die Prisma Access zur Auflösung interner Domänennamen verwenden soll.

**STEP 7 |** Sie können eine **Suffixliste für Client-DNS** hinzufügen, um das Suffix anzugeben, das der Client lokal verwenden soll, wenn ein nicht qualifizierter Hostname eingegeben wird, den er nicht auflösen kann, z. B. **`acme.local`**.

Geben Sie vor dem Domänensuffix (z. B. acme.com) kein Platzhalterzeichen (*) ein. Sie können mehrere Suffixe hinzufügen.

 ©2025 Palo Alto Networks, Inc.

# Konfigurieren der Einstellungen für HIP-Datenerfassung für den Zugriff mit dynamischen Rechten

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access 5.1 Innovation<br>❑ Desktop-Geräte mit macOS 12 oder höher oder Desktop-Geräte mit Windows 10 Version 2024 oder höher oder mit Windows 11<br>❑ Prisma Access-Lizenz mit dem Abonnement für mobile Benutzer<br>❑ Rolle: Projektadministrator |

Der Prisma Access-Agent sammelt Informationen über den Host, auf dem er ausgeführt wird, und übermittelt diese Hostinformationen nach dem erfolgreichen Herstellen einer Verbindung an den Prisma Access-Standort (Gateway). Das Gateway gleicht diese vom Prisma Access-Agenten übermittelten Rohdaten vom Host mit allen von Ihnen definierten Host Information Profile-(HIP-)Objekten und HIP-Profilen ab. Findet es eine Übereinstimmung, wird ein Eintrag im HIP-Übereinstimmungsprotokoll generiert. Findet es darüber hinaus eine HIP-Profilübereinstimmung in einer Richtlinienregel, setzt es die entsprechende Sicherheitsrichtlinie durch.

Auf der Registerkarte **HIP-Benachrichtigungen** der Seite „Bearbeiten der globalen Agent-Einstellungen“ können Sie HIP-Benachrichtigungen erstellen, HIP-Objekte erstellen und verwalten sowie HIP-Profile erstellen und verwalten, die für den Prisma Access-Agenten auf allen Endpunkten gelten.

Hier können Sie benutzerdefinierte HIP-Daten definieren, die der Prisma Access-Agent erfassen oder ausschließen soll. Wenn diese Option aktiviert ist, sammelt der Prisma Access-Agent Daten von Geräten, auf denen macOS- oder Windows-Betriebssysteme ausgeführt werden.

Mithilfe einer benutzerdefinierten Prüfung können Sie beispielsweise feststellen, ob eine bestimmte Anwendung auf einem Endpunkt installiert ist oder ausgeführt wird. Die Daten, die Sie für die Erfassung in einer benutzerdefinierten Prüfung definieren, sind in den Rohdaten der Hostinformationen enthalten, die der Prisma Access-Agent erfasst und dann an Prisma Access übermittelt, wenn der Prisma Access-Agent eine Verbindung herstellt.

**STEP 1 |** Wählen Sie in Strata Cloud Manager die Optionen **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Übersicht** aus und erweitern Sie den Konfigurationsumfang, um die **Snippets** anzuzeigen.

**STEP 2 |** Wählen Sie das Snippet aus, das Ihnen der Superuser-Administrator zugewiesen hat.

**STEP 3 |** Wählen Sie **Objekte** > **Zugriff mit dynamischen Rechten** aus, um die Einstellungen für den Zugriff mit dynamischen Rechten zu öffnen.

**STEP 4 |** Wählen Sie die Registerkarte **Agent-Einstellungen** aus.

 ©2025 Palo Alto Networks, Inc.

**STEP 5 |** Wählen Sie **Agent-Einstellungen hinzufügen** oder eine vorhandene Konfiguration in der Tabelle der Agent-Einstellungen aus.

**STEP 6 |** Wählen Sie im Abschnitt „Host Information Profile (HIP)“ die Option **HIP-Daten erfassen** aus, um die HIP-Datenerfassung an den Endpunkten zu aktivieren, die sich mit einem Projekt angemeldet haben.

**STEP 7 |** Wählen Sie **Erweiterte Optionen anzeigen** aus.

**STEP 8 |** Geben Sie die **maximale Wartezeit** (in Sekunden) an, während der der Prisma Access-Agent nach HIP-Daten suchen soll, bevor er die verfügbaren Daten übermittelt. Der Bereich liegt zwischen 10 und 60 Sekunden; der Standardwert ist 20 Sekunden.

**STEP 9 |** **Bearbeiten** Sie Ausschlusskategorien, um bestimmte Kategorien oder Anbieter, Anwendungen oder Versionen innerhalb einer Kategorie von der HIP-Datenerfassung auszuschließen.

Wählen Sie eine **Kategorie** aus (z. B. Data Loss Prevention), die von der HIP-Datenerfassung ausgeschlossen werden soll. Nachdem Sie eine Kategorie ausgewählt haben, können Sie einen bestimmten **Anbieter hinzufügen** und dann ein bestimmtes **Produkt** dieses Anbieters **hinzufügen**, um den Ausschluss nach Bedarf weiter zu verfeinern. Sie können der Ausschlussliste mehrere Anbieter und Produkte hinzufügen. **Speichern** Sie Ihre Einstellungen in jedem Dialog.

Wenn Sie nicht einen ganzen Anbieter ausschließen möchten, können Sie bestimmte Patches eines Anbieters ausschließen. Nachdem Sie den Anbieter hinzugefügt haben, können Sie den Patchnamen oder die Patchnummer und optional ein Datum angeben, bis zu dem Sie die Patchaktualisierungen aus dem HIP-Bericht ausschließen möchten. Verwenden Sie hierfür das folgende Format:

```
Exclude: [kb-article-id1: MM/TT/JJJJ], [kb-article-id2: MM/TT/JJJJ]
```

Dabei ist **<kb-article-id>** der Name oder die Nummer im Attribut (zum Beispiel **<kb-article-id>2267602</kb-article-id>**) und **MM/TT/JJJJ** gibt das Datum an, bis zu dem der Patch vom HIP-Bericht ausgeschlossen ist. Wenn Sie kein Datum festlegen, wird der Patch auf unbestimmte Zeit vom HIP-Bericht ausgeschlossen. Wenn Sie ein Datum festlegen, wird der Patch bis zum angegebenen Datum ausgeschlossen.

**STEP 10 |** **Bearbeiten** Sie benutzerdefinierte Überprüfungen, um alle benutzerdefinierten Daten zu definieren, die Sie von den Hosts erfassen möchten, auf denen diese Konfiguration ausgeführt wird.

Wenn Sie beispielsweise über erforderliche Anwendungen verfügen, die nicht in den Anbieter- oder Produktlisten zum Erstellen von HIP-Objekten enthalten sind, können Sie eine benutzerdefinierte Prüfung erstellen, um zu ermitteln, ob die Anwendung installiert ist (sie

 ©2025 Palo Alto Networks, Inc.

verfügt über einen entsprechenden Windows-Registrierungs- oder Mac-Plist-Schlüssel) oder derzeit ausgeführt wird (es läuft ein entsprechender Prozess):

- **Windows** – Sie können eine Prüfung für einen bestimmten Registrierungsschlüssel oder Registrierungswert **hinzufügen**. Um die Datenerfassung auf einen bestimmten Registrierungswert zu beschränken, wählen Sie **Hinzufügen** aus, um diesen hinzuzufügen und anschließend die spezifischen Registrierungswerte zu definieren.
- **Mac** – Wählen Sie **Hinzufügen** aus, um eine Prüfung für einen bestimmten **Plist**-Schlüssel oder **Schlüssel**wert hinzuzufügen. Um die Datenerfassung auf bestimmte Schlüsselwerte zu beschränken, wählen Sie **Hinzufügen** aus, um die Schlüsselwerte hinzuzufügen. Klicken Sie auf „OK“, um die Einstellungen zu speichern.
- **Prozessliste** – Wählen Sie **Hinzufügen** aus, um die Prozesse hinzuzufügen, die Sie auf Benutzerendpunkten überprüfen möchten, um festzustellen, ob sie ausgeführt werden. Um beispielsweise zu bestimmen, ob eine Softwareanwendung ausgeführt wird, fügen Sie der Prozessliste den Namen der ausführbaren Datei hinzu. Sie können einen Prozess zur Registerkarte **Windows** und/oder zur Registerkarte **Mac** hinzufügen.

**Speichern** Sie abschließend die benutzerdefinierten Prüfeinstellungen.

**STEP 11 |** Wenn Sie die Konfiguration der projektspezifischen Prisma Access Agent-Einstellungen abgeschlossen haben, wählen Sie **Speichern** aus, um die Konfiguration zu speichern.

 ©2025 Palo Alto Networks, Inc.

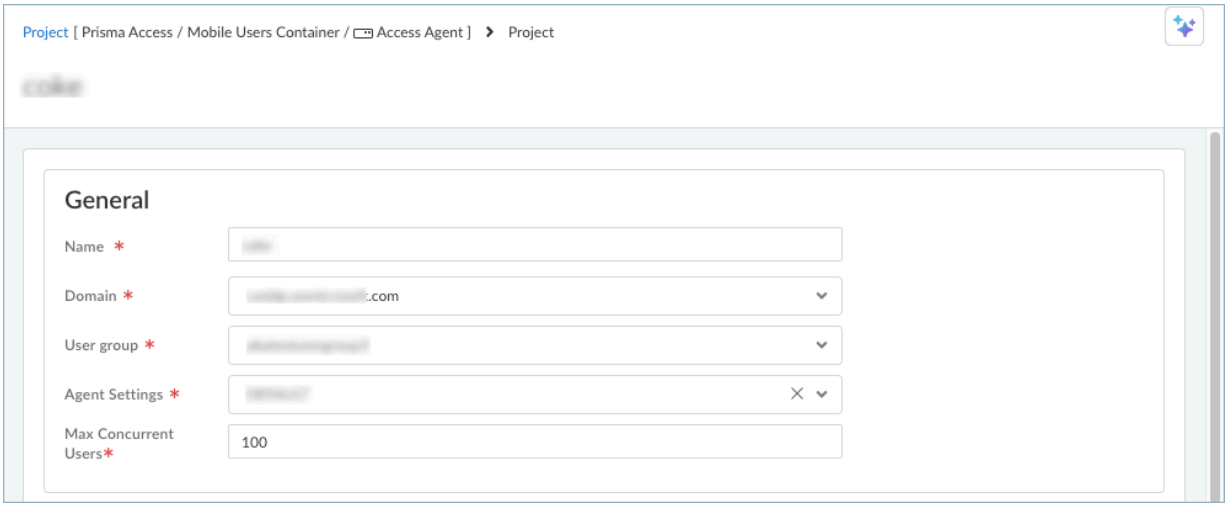
# Projekt erstellen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | ☐ Prisma Access-Lizenz<br>☐ Mindestens erforderliche Version von Prisma Access: 5.1<br>☐ Rolle: Superuser |

Fügen Sie Projekte hinzu, auf die Benutzer mit dem Prisma Access Agent zugreifen sollen. Nur ein Projektadministrator kann Projektdefinitionen erstellen und verwalten.

**STEP 1 |** Wählen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** aus.

**STEP 2 |** Legen Sie als Geltungsbereich das von Ihnen erstellte Projekt-Snippet fest und navigieren Sie zu **Objekte** > **Zugriff mit dynamischen Rechten** > **Projekte** > **Projekt hinzufügen**.

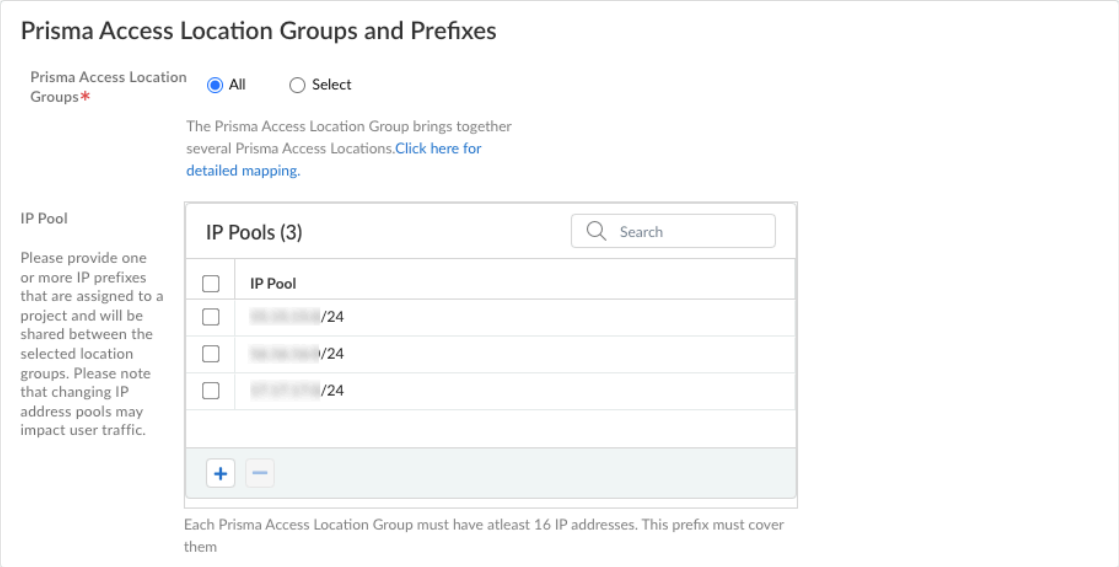



1. Geben Sie für das Projekt unter **Name** einen Projektnamen ein.
2. Wählen Sie die **Domäne** aus, die Sie in der Cloud Identity Engine hinzugefügt haben, und außerdem unter **Benutzergruppe** die Benutzergruppe, die dem Verzeichnis zugeordnet ist.
3. Wählen Sie die zuvor hinzugefügten **Agent-Einstellungen** und unter **Max. gleichzeitige Benutzer** die maximal zulässige Anzahl gleichzeitig aktiver Benutzer für das Projekt aus.
4. Wählen Sie die **Gruppen für den Prisma Access-Standort** aus. Die Liste der Standortgruppen wird auf Basis der Standorte ausgefüllt, an denen Sie die GlobalProtect-Gateways hinzufügen.

   Das Projekt, das Sie erstellen, ist bestimmten IP-Pools und Standortgruppen zugeordnet. Die Benutzer erhalten die IP-Adressen abhängig von dem Projekt und des Prisma Access-Compute-Standorts, zu denen mithilfe des Prisma Access Agent eine Verbindung hergestellt wird. Ein Projekt kann nur zu dem Standort innerhalb der Standortgruppe eine Verbindung herstellen, der dem Projekt zugeordnet ist. Sie können **Klicken Sie hier**

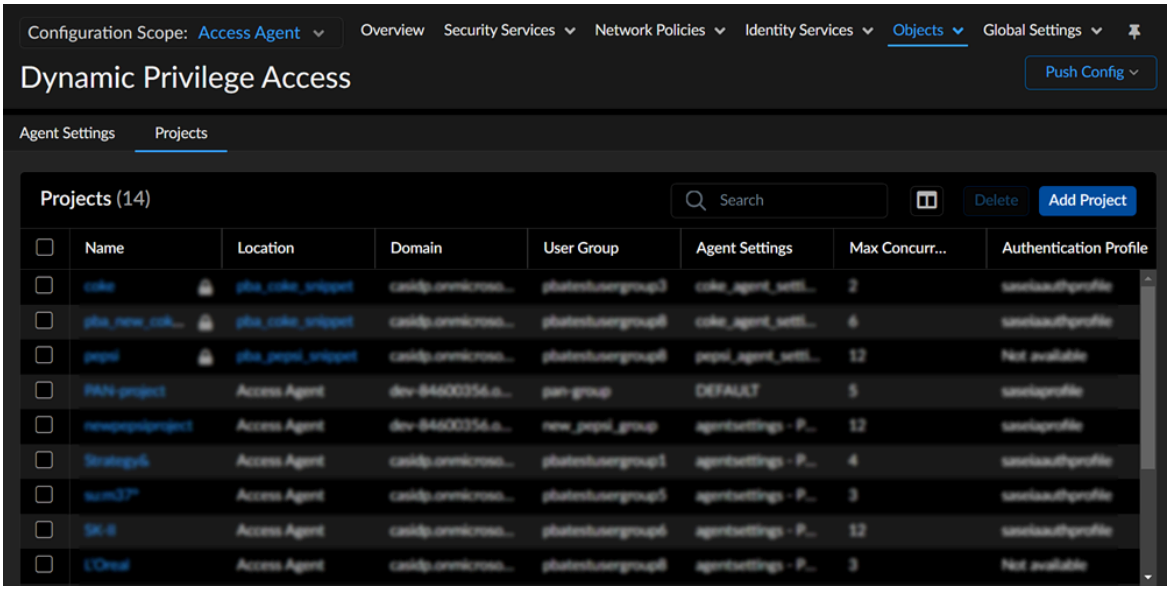
 ©2025 Palo Alto Networks, Inc.

**für eine detaillierte Zuordnung** auswählen, um die Zuordnung zwischen den Prisma Access-Standortgruppen und den Prisma Access-Compute-Standorten anzuzeigen.




5. Fügen Sie die **IP-Pools** für Ihr Projekt hinzu oder wählen Sie die IP-Pools aus. Die IP-Präfixe werden Ihrem Projekt zugeordnet und von den von Ihnen ausgewählten Prisma Access-Standortgruppen gemeinsam verwendet.

   Diese Projekt-IP-Pools können zusammengefasst werden, um die Anzahl der Routen zu reduzieren, die an das Netzwerk gesendet werden.
6. **Speichern** Sie die Projekteinstellungen.




 ©2025 Palo Alto Networks, Inc.

- *Wenn Sie ein Projekt-Snippet in Ihrem Konfigurationsumfang auswählen, können Sie lediglich auf die Einstellungen und Details zugreifen, die diesem speziellen Projekt zugeordnet sind.*
- *Wenn Sie sich als Projektadministrator oder Projekt-Push-Administrator bei Strata Cloud Manager anmelden, können Sie nur die Projektdetails anzeigen, auf die Sie Zugriff haben. Wenn Sie den Konfigurationsumfang eines anderen Projekt-Snippets auswählen, können Sie nicht auf die Einstellungen und Details eines anderen Projekts zugreifen.*
- *Um zwischen Projekten zu wechseln, müssen Sie sich bei Strata Cloud Manager mit den Anmeldeinformationen des anderen Projekts als Projektadministrator oder Projekt-Push-Administrator anmelden.*

**STEP 3 |** Übertragen Sie Ihre Änderungen mit der Aktion **Push**.

Nachdem Sie ein Projekt in Prisma Access erstellt haben, kann es bis zu 15 Minuten dauern, bis sich der Benutzer mit dem Prisma Access Agent bei diesem Projekt authentifizieren kann.

 ©2025 Palo Alto Networks, Inc.

# Datenverkehrslenkung für den Zugriff mit dynamischen Rechten

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access-Lizenz<br>❑ Minimal erforderliche Prisma Access-Version: 5.1<br>❑ Rolle: Projektadministrator |

Verwenden Sie die Datenverkehrslenkung, um den Datenverkehr eines Projekts an eine Dienstverbindung und projektspezifische Routen weiterzuleiten.

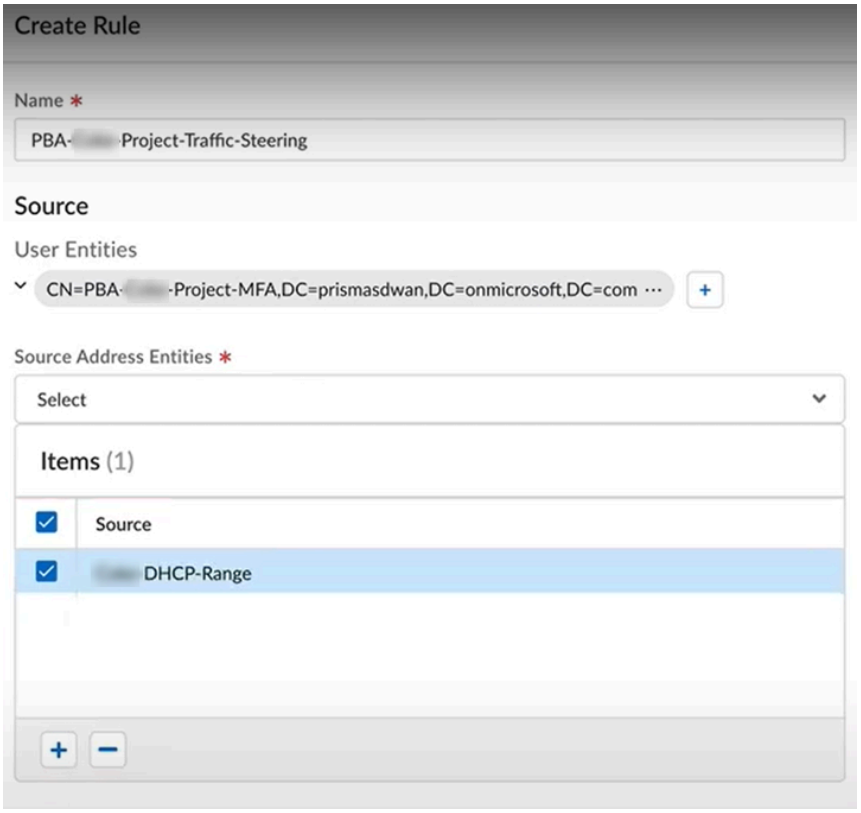
**STEP 1 |** Wählen Sie **Workflows** > **Einrichtung Prisma Access** > **Dienstverbindungen** aus.

**STEP 2 |** Fügen Sie eine Dienstverbindung hinzu.

**STEP 3 |** Bearbeiten Sie die **erweiterten Einstellungen**, um den Datenverkehr weiterzuleiten.

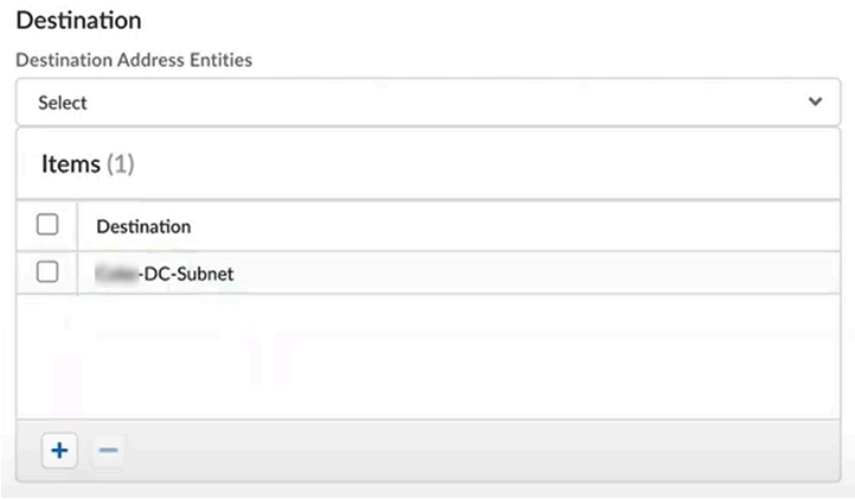
**STEP 4 |** **Fügen Sie eine Regel** unter **Datenverkehrslenkung** für Ihre Projekte hinzu.

**STEP 5 |** Stimmen Sie die **Quelle** mit Benutzern ab und fügen Sie den Projekt-DHCP-Bereich als **Quell-Adressentitäten** hinzu.

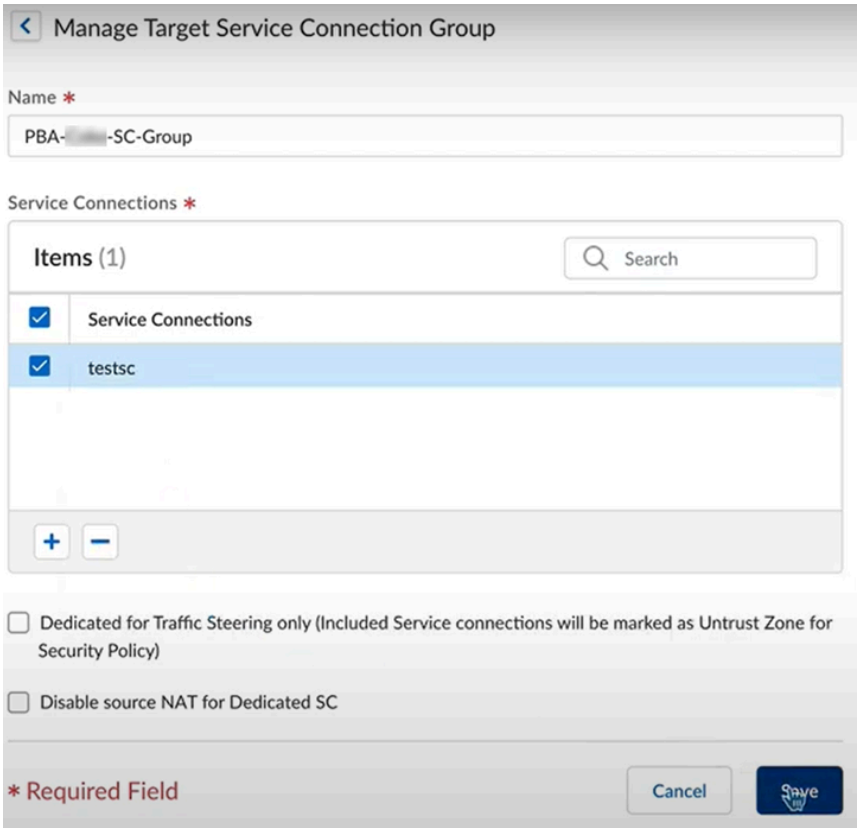



 ©2025 Palo Alto Networks, Inc.

**STEP 6 |** Stimmen Sie die **Ziel-Adressentitäten** ab.




**STEP 7 |** Wählen Sie die Dienste und Aktionen aus.




**STEP 8 |** Speichern Sie die Änderungen und übertragen Sie sie per Push.


©2025 Palo Alto Networks, Inc.

# Prisma Access Agent für Zugriff mit dynamischen Rechten einrichten

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access 5.1 Innovation<br>❑ Prisma Access-Lizenz mit dem Abonnement für mobile Benutzer<br>❑ Desktop-Geräte mit macOS 12 oder höher oder Desktop-Geräte mit Windows 10 Version 2024 oder höher oder mit Windows 11<br>❑ Rolle: Superuser |

Ihre Endbenutzer verwenden den Prisma Access Agenten, um basierend auf den Kundenprojekten, denen Ihre Benutzer zugewiesen sind, auf das Netzwerk Ihrer Organisation zuzugreifen.

Nachdem Sie die projektspezifischen Agent-Einstellungen eingerichtet und die Projekte erstellt haben, können Sie andere Prisma Access Agent-Einstellungen wie z. B. mehrstufige Rollouts und globale Agent-Einstellungen konfigurieren.

Sie können die folgenden Einstellungen des Prisma Access Agenten konfigurieren:

- Konfigurieren mehrstufiger Rollouts für den Prisma Access-Agenten
- Konfigurieren allgemeiner globaler Einstellungen für den Prisma Access-Agenten
- Konfigurieren von HIP-Benachrichtigungen für den Prisma Access-Agenten

## Konfigurieren mehrstufiger Rollouts für den Prisma Access Agent

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (verwaltet von Strata Cloud Manager) | ❑ Prisma Access 5.1 Preferred oder Innovation<br>❑ Prisma Access-Lizenz mit dem Abonnement für mobile Benutzer<br>❑ Desktop-Geräte mit macOS 12 oder höher oder Desktop-Geräte mit Windows 10 Version 2024 oder höher oder mit Windows 11<br>❑ Rolle: Superuser |

Mit der Rollout-Funktion für Upgrades des Prisma Access-Agenten können Administratoren Gerätegruppen in einer bestimmten Reihenfolge aktualisieren. Mit Upgrade-Rollouts sind

 ©2025 Palo Alto Networks, Inc.

Sie bei Upgrades von Prisma Access-Agenten nicht mehr auf Mobile Device Management-(MDM-)Software wie Jamf Pro und Microsoft Intune angewiesen.

*Mehrstufige Upgrade-Rollouts können erst nach der ersten Bereitstellung oder Installation des Prisma Access-Agenten auf den Geräten Ihrer Endbenutzer durchgeführt werden.*

Für ein mehrstufiges Rollout des Prisma Access-Agenten können Sie Upgrade-Ringe mit Übereinstimmungskriterien basierend auf Benutzern, Gruppen und Betriebssystemen konfigurieren. Geräte, die die Kriterien erfüllen, werden in der Reihenfolge der Upgrade-Ringe (Ring0 bis Ring4, Standardring) aktualisiert.

Sie können optional Upgrade-Ringe definieren, wenn Sie mobile Benutzer über die Seite „Einrichtung Zugriffsagent“ für den Prisma Access-Agenten einbinden. Wenn Sie bei der anfänglichen Agent-Konfiguration keine Upgrade-Ringe definieren, werden alle Geräte in den Standard-Ring eingefügt. Sie können später zur Seite „Einrichtung Zugriffsagent“ zurückkehren, um die Upgrade-Ringe zu definieren und die Konfiguration an Prisma Access zu übertragen. Diese Änderungen werden während des nächsten mehrstufigen Rollouts wirksam oder nachdem Sie ein mehrstufiges Rollout gestoppt und erneut gestartet haben.

So konfigurieren Sie einen Upgrade-Ring:

**STEP 1 |** Wählen Sie im Strata Cloud Manager **Workflows** > **Einrichtung Prisma Access** > **Zugriffsagent** > **Prisma Access-Agent** aus.

**STEP 2 |** Klicken Sie im Abschnitt **Mehrstufiges Rollout** auf **Ring hinzufügen**.

**STEP 3 |** Wählen Sie einen vordefinierten **Namen** für den Ring aus. Sie können Werte von **Ring0** bis **Ring4**auswählen. Der erste Ring, den Sie hinzufügen, ist **Ring0**.

**STEP 4 |** Geben Sie eine aussagekräftige **Beschreibung** für den Ring ein.

**STEP 5 |** Geben Sie die Kriterien für den Ring basierend auf den Attributen **Benutzer**, **Gruppen** oder **Gerätebetriebssystem** an.

1. Wählen Sie **Hinzufügen** aus, um ein Kriterium hinzuzufügen.

2. Wählen Sie für jedes Kriterium ein **Attribut**, einen **Operator** und einen **Wert** aus und klicken Sie dann auf **Hinzufügen**.

   Sie können pro Kriterium nur ein Attribut und einen Operator auswählen. Der Wert hängt davon ab, was Sie für das Attribut und den Operator ausgewählt haben:

   - Für das Attribut **Benutzername**:
     - Wenn Sie für **Operator** > **Enthält** ausgewählt haben, wählen Sie aus der Liste unter dem Feld **Wert** einen Benutzernamen aus oder suchen Sie nach einem bestimmten Benutzernamen. Um eine Suche zu starten, beginnen Sie mit der Eingabe des Benutzernamens. Sie können einen oder mehrere Benutzernamen aus der Liste auswählen.

 ©2025 Palo Alto Networks, Inc.

- Wenn Sie für **Operator** > **Gleich** ausgewählt haben, wählen Sie aus der Liste unter dem Feld **Wert** einen Benutzernamen aus oder suchen Sie nach einem bestimmten Benutzernamen. Um eine Suche zu starten, beginnen Sie mit der Eingabe des Benutzernamens. Sie können einen Benutzernamen aus der Liste auswählen.

- Für das Attribut **Gruppen**:
  - Wenn Sie für **Operator** > **Enthält** ausgewählt haben, wählen Sie aus der Liste unter dem Feld **Wert** eine Gruppe aus oder suchen Sie nach einer bestimmten Gruppe. Um eine Suche zu starten, beginnen Sie mit der Eingabe des Gruppennamens. Sie können eine oder mehrere Gruppen aus der Liste auswählen.
  - Wenn Sie für **Operator** > **Gleich** auswählen, wählen Sie aus der Liste unter dem Feld **Wert** eine Gruppe aus oder suchen Sie nach einer bestimmten Gruppe. Um eine Suche zu starten, beginnen Sie mit der Eingabe des Gruppennamens. Sie können eine Gruppe aus der Liste auswählen.

- Wählen Sie für das Attribut **Betriebssystem** einen Betriebssystemtyp (**Windows** oder **macOS**) aus. Anschließend:
  - Wenn Sie **Operator** > **Enthält** ausgewählt haben, suchen Sie in der Liste unter dem Feld **Wert** nach einer oder mehreren Betriebssystemversionen bzw. wählen Sie diese aus. Um eine Suche zu starten, beginnen Sie mit der Eingabe des Betriebssystems und der Version. Sie können eine oder mehrere Betriebssystemversionen aus der Liste auswählen.
  - Wenn Sie für den Operator den Wert **Größer als** oder **Kleiner als** auswählen, suchen Sie in der Liste **Wert** nach einer Betriebssystemversion oder wählen Sie eine aus. Um eine Suche zu starten, beginnen Sie mit der Eingabe des Betriebssystems und der Version. Sie können eine Betriebssystemversion aus der Liste auswählen.

3. Bei Bedarf können Sie weitere Kriterien **hinzufügen**. Sie können pro Ring bis zu drei Kriterien angeben.

   Sie können ein Attribut nur einmal pro Ring verwenden. Nachdem Sie mithilfe eines Attributs ein Kriterium hinzugefügt haben, wird dieses Attribut nicht mehr in der Dropdown-Liste **Attribut** angezeigt.

   Nachdem Sie die Kriterien hinzugefügt haben, werden diese in der Tabelle **Kriterium** auf der Seite mit den Ringkriterien angezeigt. Wenn Prisma Access die Kriterien auswertet, werden die in derselben Zelle aufgelisteten Werte mit dem logischen ODER-Operator

 ©2025 Palo Alto Networks, Inc.

ausgewertet, während die Attribute und Werte zwischen den Zeilen mit dem logischen UND-Operator ausgewertet werden.

Beispielsweise stimmen die Kriterien in der folgenden Abbildung mit den Geräten überein, die zur Gruppe **`gp-auto-saml-group`** oder **`Okta Administrators`** gehören und auf denen das Betriebssystem Windows 11 ausgeführt wird.

4. **Speichern** Sie die Ringkriterien.

**STEP 6 |** Um weitere Ringe zu erstellen, wiederholen Sie die Schritte 2 bis 5. Sie können insgesamt fünf Ringe erstellen (Ring0 bis Ring4).

**STEP 7 |** Übertragen Sie die Konfiguration per Push auf Prisma Access.

1. Wählen Sie **Konfiguration übertragen** > **Push** aus.
2. Geben Sie eine **Beschreibung** für den Job ein.
3. Wählen Sie den Container **Global** > **Prisma Access** > **Mobile Benutzer** > **Zugriffsagent** aus und klicken Sie auf **Push**.
4. Warten Sie, bis der Job abgeschlossen ist, und **schließen** Sie das Dialogfeld „Jobs“.

**STEP 8 |** Sie können das mehrstufige Rollout unter **Verwalten** > **Prisma Access-Agent** in Strata Cloud Manager verwalten.

## Konfigurieren allgemeiner globaler Einstellungen für Prisma Access Agents

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | ☐ Prisma Access 5.1 Innovation<br>☐ Prisma Access-Lizenz mit dem Abonnement für mobile Benutzer<br>☐ Desktop-Geräte mit macOS 12 oder höher oder Desktop-Geräte mit Windows 10 Version 2024 oder höher oder mit Windows 11<br>☐ Rolle: Superuser |

Sie können die globalen Agent-Einstellungen anpassen, die für Prisma Access-Agenten auf allen Endpunkten gelten.

Zu den allgemeinen globalen Agent-Einstellungen gehört die Anti-Tamper-Funktion, die Benutzer daran hindert, den Prisma Access-Agenten zu manipulieren, z. B. ihn vom Gerät eines Endbenutzers zu deinstallieren. Darüber hinaus können Sie die Einstellungen zur Authentifizierungsüberschreibung sowie die Einstellung für das Inaktivitäts-Timeout konfigurieren und die Anmeldung von Geräten in Quarantäne blockieren.

 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** Wählen Sie im Strata Cloud Manager **Workflows** > **Einrichtung Prisma Access** > **Zugriffsagent** > **Prisma Access-Agent** aus.

**STEP 2 |** Bearbeiten Sie die **globalen Agent-Einstellungen**.

**STEP 3 |** Wählen Sie **Allgemein** aus.

**STEP 4 |** Konfigurieren Sie ein Passwort zum Freischalten der Anti-Tamper-Funktion.

Sie können den Prisma Access-Agenten schützen, indem Sie die Anti-Tamper-Funktion aktivieren, die verhindert, dass unbefugte Benutzer den Prisma Access-Agenten manipulieren. Die Anti-Tamper-Funktion kann die folgenden Prisma Access-Agent-Ressourcen auf Ihren Endpunkten schützen:

- Prisma Access-Agent-Ordner und -Dateien – Nicht autorisierte Benutzer können keine mit dem Prisma Access-Agenten verbundenen Dateien und Ordner löschen oder umbenennen.
- Prisma Access-Agent-Dienste und Host Information Profile-(HIP-)Prozesse – Nicht autorisierte Benutzer können keine mit dem Prisma Access-Agenten verbundenen Dienste und HIP-Prozesse stoppen. Die HIP-Prozesse sammeln Informationen über den Host, auf dem der Prisma Access-Agent ausgeführt wird, und übermitteln die Hostinformationen zur Überprüfung an Prisma Access. Wenn ein Benutzer versucht, einen Prozess zu stoppen, muss er das Passwort zum Freischalten der Anti-Tamper-Funktion eingeben.
- Prisma Access-Agent-Registrierungsschlüssel (unter Windows) oder `.plist--`Datei (unter macOS) – Nicht autorisierte Benutzer können die Windows-Registrierungsschlüssel oder die `.plist-`Datei für den Prisma Access-Agenten nicht löschen oder aktualisieren.
- Die PACli-Befehlszeilenschnittstelle – Nicht autorisierte Benutzer können den Prisma Access-Agenten oder die Anti-Tamper-Funktion nicht über die PACli-Befehlszeilenschnittstelle deaktivieren. Administratoren und autorisierte Benutzer, die bestimmte Aktionen zur Fehlerbehebung in der Befehlszeile ausführen müssen, müssen bei entsprechender Aufforderung das Passwort zum Freischalten der Anti-Tamper-Funktion (Supervisor-Passwort) eingeben.

Um die Anti-Tamper-Funktion zur Fehlerbehebung des Prisma Access-Agenten freizuschalten, müssen Sie ein Passwort zum Freischalten der Anti-Tamper-Funktion (auch Supervisor-Passwort genannt) einrichten.

1. **Aktivieren** Sie das Anti-Tamper-Passwort.

   Wenn Sie das Anti-Tamper-Passwort nicht aktivieren, wird kein Passwort zugewiesen und ein Benutzer kann ein beliebiges Passwort (einschließlich eines leeren Passworts) eingeben, wenn er in der Befehlszeile des Prisma Access-Agenten dazu aufgefordert wird.

   Wenn Sie das Anti-Tamper-Passwort nach der Aktivierung deaktivieren, können Benutzer bestimmte PACli-Befehle auf dem Agenten ausführen, z. B. die Befehle **`pacli disable`**, **`pacli hip status`**, **`pacli protect disable`** und **`pacli switchto GlobalProtect`**, ohne das Supervisor-Passwort anzugeben. Sie müssen lediglich die **Eingabetaste** drücken, wenn Sie zur Eingabe des Passworts aufgefordert werden.

 ©2025 Palo Alto Networks, Inc.

2. Geben Sie das **Passwort** ein und **bestätigen Sie das Passwort**, indem Sie es erneut eingeben. Das Passwort muss mindestens acht alphanumerische Zeichen enthalten.

   Wenn Sie kein Passwort angeben, wird das Standardpasswort verwendet. Standardmäßig besteht das Anti-Tamper-Passwort aus den ersten drei Zeichen des Prisma Access-Mandantennamens in Großbuchstaben, der Prisma Access-**Datenregion** in Kleinbuchstaben und den letzten fünf Ziffern der Prisma Access-**Instanz-ID**, zum Beispiel: **PANamericas56789**.

   Sie können die Prisma Access-**Instanz-ID** und die **Datenregion** abrufen, indem Sie **Einstellungen** > **Mandanten** > **<your_tenant>** und die QuickInfo **Supportinformationen anzeigen** neben der Seriennummer für Prisma Access auswählen.

   *Um Ihren Agenten ein höheres Maß an Sicherheit zu bieten, richten Sie ein neues Passwort zum Freischalten der Anti-Tamper-Funktion ein, um das Standardpasswort zu überschreiben, da es möglicherweise nicht das sicherste Passwort ist.*

**STEP 5 |** Konfigurieren Sie die Einstellungen für **Authentifizierungsüberschreibung**, damit Prisma Access sichere, verschlüsselte Cookies zur Benutzerauthentifizierung generieren und akzeptieren kann. Durch die Authentifizierungsüberschreibung muss der Benutzer während der angegebenen **Cookie-Lebensdauer** nur einmal seine Anmeldeinformationen angeben.

- **Cookie zur Authentifizierungsüberschreibung generieren** – Ermöglicht Prisma Access, verschlüsselte endpunktspezifische Cookies zu generieren und Authentifizierungscookies an den Endpunkt auszugeben.
- **Cookie zur Authentifizierungsüberschreibung akzeptieren** – Ermöglicht Prisma Access, Benutzer mit einem gültigen, verschlüsselten Cookie zu authentifizieren. Wenn die App ein gültiges Cookie vorlegt, überprüft Prisma Access, ob das Cookie ursprünglich von Prisma Access verschlüsselt wurde, entschlüsselt das Cookie und authentifiziert dann den Benutzer.
- **Zertifikat zum Ver-/Entschlüsseln von Cookies** – Wählen Sie ein RSA-Zertifikat zum Verschlüsseln und Entschlüsseln von Cookies aus.
- **Cookie-Lebensdauer** – Gibt die Stunden, Tage oder Wochen an, für die das Cookie gültig ist (Standard sind 24 Stunden). Der Bereich für Stunden liegt zwischen 1 und 72, der Bereich für Wochen zwischen 1 und 52 und der Bereich für Tage zwischen 1 und 365. Nach Ablauf des Cookies muss der Benutzer seine Anmeldeinformationen erneut eingeben. Prisma Access verschlüsselt dann ein neues Cookie, um es an den Agenten zu senden. Dieser Wert kann mit der von Ihnen konfigurierten Cookie-Lebensdauer identisch sein oder sich davon unterscheiden.

**STEP 6 |** Geben Sie die Anzahl der Minuten für die **Inaktivitätsabmeldung** ein, um die Zeitspanne festzulegen, nach der inaktive Benutzer vom Prisma Access-Agenten abgemeldet werden.

Sie können die Frist für die Inaktivitätsabmeldung nutzen, um eine Sicherheitsrichtlinie durchzusetzen, den Datenverkehr von Endpunkten zu überwachen, während Sie mit Prisma Access verbunden sind, und um inaktive Prisma Access-Agent-Sitzungen schnell abzumelden.

 ©2025 Palo Alto Networks, Inc.

Sie können eine kürzere Frist für die Inaktivitätsabmeldung erzwingen. Benutzer werden abgemeldet, wenn der Prisma Access-Agent den Datenverkehr nicht durch den Tunnel geleitet hat oder wenn das Gateway innerhalb des konfigurierten Zeitraums keine HIP-Prüfung vom Endpunkt erhält.

**STEP 7 |** **Anmeldung für Geräte in Quarantäne blockieren** soll verhindern, dass sich Prisma Access-Agent-Benutzer von Geräten in Quarantäne aus anmelden.

Wenn diese Einstellung aktiviert ist und ein Benutzer versucht, sich von einem Gerät in Quarantäne aus anzumelden, benachrichtigt der Prisma Access-Agent den Benutzer, dass das Gerät in Quarantäne ist und sich der Benutzer von diesem Gerät aus nicht anmelden kann. Wenn diese Einstellung nicht aktiviert ist, erhält der Benutzer die Benachrichtigung, kann sich aber von diesem Gerät aus anmelden.

**STEP 8 |** **Speichern** Sie Ihre Einstellungen.

## Konfigurieren von HIP-Benachrichtigungen für den Zugriff mit dynamischen Rechten in Prisma Access Agent

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | ☐ Prisma Access 5.1 Innovation<br>☐ Prisma Access-Lizenz mit dem Abonnement für mobile Benutzer<br>☐ Desktop-Geräte mit macOS 12 oder höher oder Desktop-Geräte mit Windows 10 Version 2024 oder höher oder mit Windows 11<br>☐ Rolle: Superuser |

Auf der Registerkarte **HIP-Benachrichtigungen** der Seite „Bearbeiten der globalen Agent-Einstellungen“ können Sie Host Information Profile-(HIP-)Benachrichtigungen erstellen, HIP-Objekte erstellen und verwalten und HIP-Profile erstellen und verwalten, die für den Prisma Access-Agenten auf allen Endpunkten gelten.

Der Prisma Access-Agent sammelt Informationen über den Host, auf dem er ausgeführt wird, und übermittelt diese Hostinformationen nach dem erfolgreichen Herstellen einer Verbindung an den Prisma Access-Standort (Gateway). Das Gateway gleicht diese vom Prisma Access-Agenten übermittelten Rohdaten der Hostinformationen mit allen von Ihnen definierten HIP-Objekten und HIP-Profilen ab. Findet es eine Übereinstimmung, wird ein Eintrag im HIP-Übereinstimmungsprotokoll generiert. Findet es darüber hinaus eine HIP-Profilübereinstimmung in einer Richtlinienregel, setzt es die entsprechende Sicherheitsrichtlinie durch.

HIP-Prüfungen werden durchgeführt, wenn die App eine Verbindung zum Gateway herstellt. Nachfolgende Prüfungen werden stündlich durchgeführt, während der Prisma Access-Agent verbunden ist. Der Prisma Access-Agent kann einen aktualisierten HIP-Bericht anfordern, wenn sich die vorherige HIP-Prüfung geändert hat. Pro Endpunkt wird jeweils nur der neueste HIP-Bericht auf dem Gateway gespeichert.

 ©2025 Palo Alto Networks, Inc.

Die Verwendung von HIP-Profilen zur Richtliniendurchsetzung ermöglicht granulare Sicherheit, die gewährleistet, dass die Remote-Hosts, die auf Ihre kritischen Ressourcen zugreifen, ordnungsgemäß verwaltet werden und Ihre Sicherheitsstandards einhalten, bevor ihnen der Zugriff auf Ihre Netzwerkressourcen gestattet wird. Bevor Sie beispielsweise den Zugriff auf Ihre sensibelsten Datensysteme zulassen, möchten Sie möglicherweise sicherstellen, dass auf den Festplatten der Hosts, die auf die Daten zugreifen, die Verschlüsselung aktiviert ist. Sie können diese Richtlinie durchsetzen, indem Sie eine Sicherheitsregel erstellen, die den Zugriff auf die Anwendung nur dann zulässt, wenn auf dem Endpunktsystem die Verschlüsselung aktiviert ist.

Darüber hinaus können Sie für Endpunkte, die diese Regel nicht einhalten, eine Benachrichtigungsmeldung erstellen, die den Benutzern mitteilt, warum ihnen der Zugriff verweigert wurde. Sie können außerdem einen Link zu dem Speicherort angeben, an dem das Installationsprogramm für die fehlende Verschlüsselungssoftware verfügbar ist. Um dem Benutzer den Zugriff auf diese Dateifreigabe zu gewähren, müssen Sie eine entsprechende Sicherheitsregel erstellen, die den Zugriff auf die jeweilige Freigabe für Hosts mit dieser spezifischen HIP-Profilübereinstimmung erlaubt.

Sie können die folgenden Aufgaben ausführen:

- HIP-Benachrichtigung für den Prisma Access Agent mit Zugriff mit dynamischen Rechten erstellen
- Erstellen und Verwalten von HIP-Objekten für den Prisma Access Agent mit Zugriff mit dynamischen Rechten
- Erstellen und Verwalten von HIP-Profilen für den Prisma Access Agent mit Zugriff mit dynamischen Rechten

## HIP-Benachrichtigung für den Prisma Access Agent mit Zugriff mit dynamischen Rechten erstellen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access 5.1 Innovation<br>❑ Prisma Access-Lizenz mit dem Abonnement für mobile Benutzer<br>❑ Desktop-Geräte mit macOS 12 oder höher oder Desktop-Geräte mit Windows 10 Version 2024 oder höher oder mit Windows 11<br>❑ Rolle: Superuser |

Sie können die Benachrichtigungsmeldungen definieren, die Endbenutzer sehen, wenn eine Sicherheitsregel mit einem HIP-Profil durchgesetzt wird.

Die Entscheidung, ob eine Benachrichtigungsmeldung angezeigt werden soll, wenn die Konfiguration des Benutzers mit einem HIP-Profil in der Richtlinie übereinstimmt oder nicht, hängt weitgehend von Ihrer Richtlinie sowie davon ab, was eine HIP-Übereinstimmung (oder Nichtübereinstimmung) für den Benutzer bedeutet. Bedeutet eine Übereinstimmung also, dass den Benutzern uneingeschränkter Zugriff auf Ihre Netzwerkressourcen gewährt wird, oder

 ©2025 Palo Alto Networks, Inc.

bedeutet sie, dass die Benutzer aufgrund eines Konformitätsproblems nur eingeschränkten Zugriff haben?

Angenommen, Sie erstellen ein HIP-Profil, das den Anforderungen entspricht, wenn die erforderlichen Antiviren- und Antispyware-Softwarepakete des Unternehmens nicht installiert sind. Sie könnten eine HIP-Benachrichtigungsmeldung für Benutzer erstellen, die dem HIP-Profil entsprechen, um sie darüber zu informieren, dass sie die Software installieren müssen. Wenn Ihr HIP-Profil mit der Installation derselben Anwendungen übereinstimmt, möchten Sie möglicherweise auch die Nachricht für Benutzer erstellen, die nicht dem Profil entsprechen.

**STEP 1 |** Wählen Sie im Strata Cloud Manager **Workflows** > **Einrichtung Prisma Access** > **Zugriffsagent** > **Prisma Access-Agent** aus.

**STEP 2 |** **Bearbeiten** Sie die **globalen Agent-Einstellungen**.

**STEP 3 |** Wählen Sie **HIP-Benachrichtigungen** aus und klicken Sie auf **Hinzufügen**.

**STEP 4 |** Wählen Sie in der Dropdown-Liste **Hostinformationen** das HIP-Profil aus, auf das sich diese Meldung bezieht.

Wenn es keine HIP-Profile gibt, müssen Sie ein HIP-Profil erstellen.

**STEP 5 |** Je nachdem, ob Sie die Meldung anzeigen möchten, wenn das entsprechende HIP-Profil übereinstimmt oder nicht, wählen Sie **Match-Nachricht** oder **Keine Match-Nachricht** aus. In einigen Fällen möchten Sie möglicherweise Nachrichten sowohl für eine Übereinstimmung als auch für eine Nichtübereinstimmung erstellen, je nachdem, welche Objekte Sie abgleichen und welche Ziele Sie mit der Richtlinie verfolgen.

**STEP 6 |** Wählen Sie **Nachricht aktivieren** aus und wählen Sie dann aus, ob die Nachricht als **Sprechblase in der Taskleiste** oder als **Pop-up-Nachricht** angezeigt werden soll.

**STEP 7 |** Geben Sie Ihren **Nachrichten**text ein und klicken Sie dann auf **Hinzufügen**.

**STEP 8 |** Wiederholen Sie diesen Vorgang für jede Nachricht, die Sie definieren möchten.

## Erstellen und Verwalten von HIP-Objekten für den Prisma Access Agent mit Zugriff mit dynamischen Rechten

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | ☐ Prisma Access 5.1 Innovation<br>☐ Prisma Access-Lizenz mit dem Abonnement für mobile Benutzer<br>☐ Desktop-Geräte mit macOS 12 oder höher oder Desktop-Geräte mit Windows 10 Version 2024 oder höher oder mit Windows 11 |

 ©2025 Palo Alto Networks, Inc.

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| | ❑ Rolle: Superuser |

Sie können definieren, welche Hostattribute Sie überwachen oder zur Richtliniendurchsetzung verwenden möchten, indem Sie HIP-Objekte und HIP-Profile auf dem Prisma Access-Gateway erstellen.

HIP-Objekte bestehen aus den Übereinstimmungskriterien, die zum Herausfiltern der Hostinformationen verwendet werden, die Sie zum Durchsetzen der Richtlinie aus den vom Prisma Access-Agenten gemeldeten Rohdaten verwenden möchten. So können beispielsweise die Rohdaten des Hosts Informationen zu mehreren auf dem Endpunkt installierten Antivirenpaketen enthalten, während Sie vielleicht nur an einer bestimmten Anwendung interessiert sind. In diesem Fall würden Sie ein HIP-Objekt erstellen, das der spezifischen Anwendung entspricht, die Sie erzwingen möchten.

Um zu ermitteln, welche HIP-Objekte Sie benötigen, können Sie am besten festlegen, wie Sie die erfassten Hostinformationen zur Durchsetzung der Richtlinie verwenden. Bedenken Sie, dass die HIP-Objekte selbst lediglich Bausteine sind, mit denen Sie die HIP-Profile erstellen können, die in Ihren Sicherheitsrichtlinien verwendet werden. Versuchen Sie daher, Ihre Objekte einfach zu halten, indem Sie sie anhand eines Elements abgleichen, beispielsweise dem Vorhandensein eines bestimmten Typs der erforderlichen Software, der Mitgliedschaft in einer bestimmten Domäne oder einem bestimmten Betriebssystem. Auf diese Weise erhalten Sie die Flexibilität, eine differenzierte, HIP-erweiterte Richtlinie zu erstellen.

**STEP 1 |** Wählen Sie im Strata Cloud Manager **Workflows** > **Einrichtung Prisma Access** > **Zugriffsagent** > **Prisma Access-Agent** aus.

**STEP 2 |** **Bearbeiten** Sie die **globalen Agent-Einstellungen**.

**STEP 3 |** Wählen Sie **HIP-Benachrichtigungen** aus und klicken Sie auf **Hinzufügen**.

**STEP 4 |** Klicken Sie auf **HIP-Objekt erstellen**.

**STEP 5 |** Geben Sie einen **Namen** und eine **Beschreibung** für das Objekt ein.

**STEP 6 |** Wählen Sie die Registerkarte aus, die der Kategorie der Hostinformationen entspricht, mit denen Sie einen Abgleich durchführen möchten, und aktivieren Sie anschließend das Kontrollkästchen, um den Abgleich des Objekts mit der Kategorie zu ermöglichen.

Um beispielsweise ein Objekt zu erstellen, das nach Informationen zu Antiviren- oder Antispyware-Software sucht, wählen Sie die Registerkarte **Anti-Malware** aus und aktivieren Sie anschließend das Kontrollkästchen **Anti-Malware**, um die entsprechenden Felder zu aktivieren. Füllen Sie die Felder aus, um die gewünschten Übereinstimmungskriterien zu definieren.

Die folgende Abbildung zeigt beispielsweise, wie ein HIP-Objekt erstellt wird, das übereinstimmt, wenn auf dem Endpunkt die Softwareanwendung AVAST Free Antivirus

 ©2025 Palo Alto Networks, Inc.

installiert ist, der **Echtzeitschutz** aktiviert ist und die Malware-Definitionen innerhalb der letzten 5 Tage aktualisiert wurden.

Wiederholen Sie diesen Schritt für jede Kategorie, die Sie in diesem Objekt abgleichen möchten. Weitere Informationen finden Sie unter Tabelle: Datenerfassungskategorien.

**STEP 7 |** Sie können Ihr HIP-Objekt jetzt **speichern** und **hinzufügen**.

**STEP 8 |** Um Ihre HIP-Objekte zu verwalten, können Sie ein vorhandenes Objekt aus der Tabelle „HIP-Benachrichtigungen“ auswählen oder auf der Seite „Bearbeiten der globalen Agent-Einstellungen“ auf **Hinzufügen** klicken, um das Fenster „HIP-Benachrichtigungen“ zu öffnen.

Klicken Sie dort auf **HIP-Objekt verwalten**, um die Liste der von Ihnen konfigurierten HIP-Objekte anzuzeigen. Sie können ein HIP-Objekt auswählen und es **löschen**, **klonen** oder **verschieben**.

## Erstellen und Verwalten von HIP-Profilen für den Prisma Access Agent mit Zugriff mit dynamischen Rechten

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | ☐ Prisma Access 5.1 Innovation<br>☐ Prisma Access-Lizenz mit dem Abonnement für mobile Benutzer<br>☐ Desktop-Geräte mit macOS 12 oder höher oder Desktop-Geräte mit Windows 10 Version 2024 oder höher oder mit Windows 11<br>☐ Rolle: Superuser |

Ein HIP-Profil ist eine Sammlung von HIP-Objekten, die zusammen ausgewertet werden, entweder zur Überwachung oder zur Durchsetzung von Sicherheitsrichtlinien. Wenn Sie Ihre HIP-Profile erstellen, können Sie die HIP-Objekte und HIP-Profile, die Sie zuvor mithilfe der booleschen Logik erstellt haben, kombinieren, sodass ein Datenverkehrsfluss, der anhand des resultierenden HIP-Profils ausgewertet wird, entweder übereinstimmt oder nicht. Wenn es eine Übereinstimmung gibt, wird die entsprechende Richtlinienregel durchgesetzt. Wenn es keine Übereinstimmung gibt, wird der Datenfluss anhand der nächsten Regel bewertet, wie bei allen anderen Richtlinienausgleichskriterien.

**STEP 1 |** Wählen Sie im Strata Cloud Manager **Workflows** > **Einrichtung Prisma Access** > **Zugriffsagent** > **Prisma Access-Agent** aus.

**STEP 2 |** **Bearbeiten** Sie die **globalen Agent-Einstellungen**.

**STEP 3 |** Wählen Sie **HIP-Benachrichtigungen** aus und klicken Sie auf **Hinzufügen**.

 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** Klicken Sie auf **HIP-Profil erstellen**.

**STEP 5 |** Geben Sie einen **Namen** und eine **Beschreibung** für die Identifizierung des Profils ein.

**STEP 6 |** Klicken Sie in das Feld **Abgleichen**, um den HIP Profile Builder zu öffnen.

1. Wählen Sie das HIP-Objekt oder -Profil, das Sie als Übereinstimmungskriterium verwenden möchten, aus der Liste aus.
2. Wählen Sie einen booleschen Operator (**Und**, **Oder**) aus. Wenn das HIP-Profil das Objekt nur dann als Übereinstimmung bewerten soll, wenn die Kriterien im Objekt für einen Flow nicht zutreffen, aktivieren Sie das Kontrollkästchen **Nicht**, bevor Sie das Objekt hinzufügen.
3. Wählen Sie ein anderes HIP-Objekt oder -Profil aus, um es anhand des ersten HIP-Objekts zu bewerten.

**STEP 7 |** Fügen Sie weitere Übereinstimmungskriterien für das Profil hinzu, das Sie erstellen, und achten Sie darauf, zwischen den einzelnen Hinzufügungen das entsprechende Optionsfeld für den booleschen Operator (**Und** oder **Oder**) auszuwählen, und verwenden Sie gegebenenfalls das Kontrollkästchen **Nicht**. Das HIP-Profil kann bis zu 2.048 Zeichen lang sein.

**STEP 8 |** Wenn Sie einen komplexen booleschen Ausdruck erstellen, müssen Sie die Klammern manuell an den richtigen Stellen im Textfeld **Abgleichen** hinzufügen, um sicherzustellen, dass das HIP-Profil mit der von Ihnen beabsichtigten Logik ausgewertet wird.

**STEP 9 |** **Speichern** Sie Ihr HIP-Profil und wählen Sie **Hinzufügen** aus.

**STEP 10 |** Um Ihre HIP-Profile zu verwalten, können Sie ein vorhandenes Profil aus der Tabelle „HIP-Benachrichtigungen“ auswählen oder auf der Seite „Bearbeiten der globalen Agent-Einstellungen“ auf **Hinzufügen** klicken, um das Fenster „HIP-Benachrichtigungen“ zu öffnen.

Klicken Sie in diesem Fenster auf **HIP-Profil verwalten**, um die Liste der von Ihnen konfigurierten HIP-Profile anzuzeigen. Sie können ein HIP-Profil auswählen und es **löschen**, **klonen** oder **verschieben**. Sie können von hier aus auch ein HIP-Profil **hinzufügen**.

 ©2025 Palo Alto Networks, Inc.

# Prisma Access Agent-Konfiguration per Push übertragen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | ☐ Prisma Access 5.1 Innovation<br>☐ Prisma Access-Lizenz mit dem Abonnement für mobile Benutzer<br>☐ Desktop-Geräte mit macOS 12 oder höher oder Desktop-Geräte mit Windows 10 Version 2024 oder höher oder mit Windows 11<br>☐ Rolle: Superuser |

Nachdem Sie die Prisma Access Agent-Konfiguration abgeschlossen oder die Konfiguration aktualisiert haben, müssen Sie die Konfiguration per Push an Prisma Access übertragen.

*Erstellen Sie mindestens ein Projekt, bevor Sie den Commit ausführen können. Ansonsten schlägt der Commit fehl.*

**STEP 1 |** Wählen Sie **Workflows** > **Einrichtung Prisma Access** > **Zugriffsagent**.

**STEP 2 |** Wählen Sie **Konfiguration übertragen** > **Push** aus.

**STEP 3 |** Geben Sie eine **Beschreibung** für den Job ein.

**STEP 4 |** Wählen Sie den Container **Global** > **Prisma Access** > **Mobile Benutzer** > **Zugriffsagent** aus und klicken Sie auf **Push**.

**STEP 5 |** Warten Sie, bis der Job abgeschlossen ist, und **schließen** Sie das Dialogfeld „Jobs“.

 ©2025 Palo Alto Networks, Inc.

# Prisma Access Agent-Paket mit aktiviertem Zugriff mit dynamischen Rechten herunterladen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access 5.1 Innovation<br>❑ Prisma Access-Lizenz mit dem Abonnement für mobile Benutzer<br>❑ Rolle: Superuser |

Nachdem Sie die Prisma Access Agent- und projektspezifischen Prisma Access Agent-Einstellungen konfiguriert haben, können Sie das Prisma Access Agent-Paket herunterladen, um es Ihren Endbenutzern zum Download und zur Installation zur Verfügung zu stellen.

Stellen Sie außerdem sicher, dass Sie die Konfigurationsdatei herunterladen. Ihre Agent- und projektspezifischen Agent-Konfigurationen sowie die Prisma Access-Mandanten-ID und die Serverdomäne werden in der Prisma Access Agent-Konfigurationsdatei gespeichert. Die Konfigurationsdatei wird bei der Installation und Registrierung vom Prisma Access Agent verwendet.

**STEP 1 |** Laden Sie das Prisma Access Agent-Paket und die Konfigurationsdatei herunter.

1. Wählen Sie **Verwalten** > **Prisma Access Agent** > **Inventar** aus.
2. Klicken Sie auf **Agent herunterladen**.
3. Klicken Sie auf den jeweiligen Abwärtspfeil bei den Elementen, die Sie herunterladen möchten.

   Stellen Sie sicher, dass Sie die **Konfigurationsdatei** herunterladen, da sie während der Installation und Registrierung vom Prisma Access Agent verwendet wird.
4. Speichern Sie das Paket an einem Speicherort auf Ihrem System und **schließen** Sie das Dialogfenster „Agent herunterladen“.

**STEP 2 |** Laden Sie das Paket an einen zentralen Speicherort im Netzwerk Ihrer Organisation hoch oder verteilen Sie das Paket, damit Ihre Endbenutzer den Prisma Access Agent herunterladen und installieren können.

 ©2025 Palo Alto Networks, Inc.

# Mit dem Prisma Access Agent auf Ihre Projekte zugreifen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access Agent | ❑ Desktop-Geräte mit macOS 12 oder höher oder Desktop-Geräte mit Windows 10 Version 2024 oder höher oder mit Windows 11<br>❑ Internetzugang |

Für IT-Unternehmen und ITES-Unternehmen (IT Enabled Services), die steuern müssen, welche Benutzer Zugriff auf ihre Kundenprojekte haben, bietet die Funktion für Zugriff mit dynamischen Rechten einen nahtlosen, sicheren und abgeschotteten Zugriff, sodass Sie nur auf die Projekte zugreifen können, die Ihnen zugewiesen wurden.

Wenn Ihr Administrator Prisma Access und den Prisma Access Agent für einen Zugriff mit dynamischen Rechten eingerichtet hat, können Sie mit dem Prisma Access Agent auf die Ihnen zugewiesenen Projekte zugreifen und daran arbeiten.

Nachdem Sie sich bei Ihrem Projekt angemeldet haben, können Sie auf das Netzwerk Ihres Unternehmens, auf Ressourcen im Netzwerk oder projektspezifische Software-as-a-Service-Anwendungen zugreifen. Erfahren Sie mehr über folgende Aktionen:

- Beim Prisma Access-Agent mit aktiviertem Zugriff mit dynamischen Rechten anmelden
- Status Ihrer Verbindung anzeigen
- Einstellungen für den Prisma Access-Agent mit aktiviertem Zugriff mit dynamischen Rechten ändern
- Verbindung zu einem anderen Prisma Access-Standort herstellen
- App-Benachrichtigungen anzeigen

Darüber hinaus können Sie zu einem anderen Projekt wechseln oder den Prisma Access-Agent mit einem anderen Server verbinden, wenn Ihnen verschiedene Arbeitsprojekte zugewiesen wurden.

## Prisma Access Agent installieren

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access Agent | ❑ Desktop-Geräte mit macOS 12 oder höher bzw. Desktop-Geräte mit Windows 10 Version 2024 oder höher oder mit Windows 11 und Administratorberechtigungen<br>❑ Internetzugang |

 ©2025 Palo Alto Networks, Inc.

Wenn Ihr Administrator den Prisma Access Agent nicht per Push auf Ihr Gerät übertragen hat, können Sie den Prisma Access Agent auf Ihrem macOS- oder Windows-Gerät manuell installieren.

*Der Prisma Access Agent und die GlobalProtect-App können zwar auf demselben Gerät koexistieren, es kann aber nur entweder der Agent oder die App eine Verbindung mit Prisma Access herstellen. Wenn die GlobalProtect-App auch auf Ihrem Gerät installiert und aktiviert ist, wird die Installation des Prisma Access Agent die GlobalProtect-App automatisch deaktivieren. Um die GlobalProtect-App nach der Installation des Prisma Access Agent zu verwenden, müssen Sie* zur GlobalProtect-App wechseln.

- macOS
- Windows

## Prisma Access Agent (macOS) installieren

So installieren Sie den Prisma Access-Agenten manuell auf Ihrem macOS-Gerät:

**STEP 1 |** Rufen Sie das Prisma Access-Agent-Paket ab, das Sie von Ihrem Administrator erhalten haben. Der Paketname hat das folgende Format:

`PrismaAccessAgentInstaller_<version>.pkg`

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Öffnen Sie das Installationspaket in Ihrem Download-Ordner (oder wo auch immer Sie das Installationspaket abgelegt haben) und befolgen Sie die Anweisungen zur Installation des Prisma Access-Agenten.

1. Klicken Sie im Installationsprogramm auf **Weiter**.
2. Wählen Sie den Ordner für die Installation des Prisma Access-Agenten aus und klicken Sie auf **Weiter**.
3. Überprüfen Sie die Informationen auf der Seite „Installationstyp“ und klicken Sie auf **Installieren**.
4. Geben Sie nach Aufforderung Ihren **Benutzernamen** und Ihr **Passwort** ein und klicken Sie dann auf **Software installieren**, um mit der Installation zu beginnen.

   Alternativ können Sie „Touch ID“ (sofern aktiviert) verwenden, um diesen Schritt abzuschließen.
5. Wenn Sie aufgefordert werden, dem Installationsprogramm den Zugriff auf Dateien in dem Ordner zu erlauben, in den Sie das Installationspaket heruntergeladen haben, klicken Sie auf **OK**.
6. Standardmäßig blockiert macOS die Prisma Access-Agent-Systemerweiterungen. Die System- oder Netzwerkerweiterungen werden angezeigt, wenn Ihr Administrator den Prisma Access-Agenten mit Verkehrsweiterleitungsregeln für Folgendes konfiguriert hat:
   - Split-Tunneling – Leitet den Netzwerkverkehr über die Prisma Access-Verbindung oder außerhalb der Prisma Access-Verbindung.
   - Split-DNS – Leitet zusätzlich zum Netzwerkverkehr DNS-Abfragen für Anwendungen und Ressourcen über Prisma Access oder außerhalb von Prisma Access.

   Damit der Prisma Access-Agent funktioniert, müssen Sie die Systemerweiterungen aktivieren:

   1. Klicken Sie auf **Systemeinstellungen öffnen**.
   2. Klicken Sie im Fenster „Datenschutz und Sicherheit“ auf **Details** für **Eine Systemsoftware erfordert Ihre Aufmerksamkeit, bevor sie verwendet werden kann**.
   3. Aktivieren Sie beide **PASrv.app**-Apps und klicken Sie auf **OK**.
7. Wenn Ihr Administrator die Funktion zum Erzwingen von Prisma Access-Verbindungen für den Netzwerkzugriff aktiviert hat, werden Sie aufgefordert, eine Konfiguration zum Filtern von Netzwerkinhalten hinzuzufügen. Klicken Sie zum Fortfahren auf **Zulassen**.

   Wenn Sie dies tun, werden Ihre Netzwerkverbindungen aus Sicherheitsgründen gefiltert und überwacht.
8. Wenn die Installation abgeschlossen ist, **schließen** Sie das Installationsprogramm.

 ©2025 Palo Alto Networks, Inc.

9. Wenn Ihr Administrator den Agenten so konfiguriert hat, dass der Autonomous DEM-Agent zusammen mit dem Prisma Access-Agenten installiert wird, klicken Sie auf **OK**, damit Sie nicht erneut dazu aufgefordert werden.
10. Klicken Sie auf das Pop-up „Prisma Access-Agent-Benachrichtigungen“, um das Fenster mit den Benachrichtigungseinstellungen zu öffnen.

**STEP 3 |** Aktivieren Sie nach Aufforderung die Prisma Access-Agent-Benachrichtigungen.

Wenn das Pop-up „Prisma Access-Agent-Benachrichtigungen“ auf Ihrem Desktop angezeigt wird, bewegen Sie den Cursor über das Pop-up und wählen Sie **Optionen** > **Zulassen** aus.

**STEP 4 |** Damit der Prisma Access-Agent auf Daten im Safari-Browser zugreifen kann, müssen Sie der Sicherheitserweiterung und dem Prisma Access-Agenten uneingeschränkten Zugriff auf die Festplatte gewähren.

1. Wählen Sie unter macOS **Systemeinstellungen** > **Datenschutz und Sicherheit** > **Vollständiger Festplattenzugriff** aus. Aktivieren Sie in der Liste der Apps **Prisma Access-Agent** und **securityExtension**.
2. Nach Aufforderung müssen Sie den Prisma Access-Agenten **beenden und erneut öffnen**, damit die Änderungen wirksam werden.

## Prisma Access Agent (Windows) installieren

So installieren Sie den Prisma Access-Agenten manuell auf Ihrem Windows-Gerät:

**STEP 1 |** Rufen Sie das Prisma Access-Agent-Paket ab, das Sie von Ihrem Administrator erhalten haben. Der Paketname hat das folgende Format:

`PrismaAccessAgent_x64_<version>.msi`

**STEP 2 |** Doppelklicken Sie in Ihrem Download-Ordner (oder wo auch immer Sie das Installationspaket abgelegt haben) auf das Symbol für das Installationspaket und befolgen Sie die Anweisungen zur Installation des Prisma Access-Agenten.

1. Wenn der Einrichtungsassistent angezeigt wird, klicken Sie auf **Weiter**, um fortzufahren.
2. Prüfen Sie die Endbenutzer-Lizenzvereinbarung, wählen Sie **Ich akzeptiere die Bedingungen der Lizenzvereinbarung** aus und klicken Sie auf **Weiter**.
3. Klicken Sie auf **Install (Installieren)**, um mit der Installation zu beginnen.
4. Wenn Sie aufgefordert werden, **zuzulassen, dass diese App Änderungen an Ihrem Gerät vornehmen darf**, klicken Sie auf **Ja**.
5. Wenn die Installation abgeschlossen ist, klicken Sie auf **Fertigstellen**.
6. Wenn Ihr Administrator den Agenten so konfiguriert hat, dass der Autonomous DEM-Agent zusammen mit dem Prisma Access-Agenten installiert wird, klicken Sie auf **OK**, damit Sie nicht erneut dazu aufgefordert werden.

 ©2025 Palo Alto Networks, Inc.

# Anmeldung beim Prisma Access Agent, für den der Zugriff mit dynamischen Rechten aktiviert ist

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access Agent | ❑ Desktop-Geräte mit macOS 12 oder höher oder Desktop-Geräte mit Windows 10 Version 2024 oder höher oder mit Windows 11<br>❑ Internetzugang |

Für den Zugriff auf das Netzwerk, die Ressourcen, die SaaS-Anwendungen Ihrer Organisation oder auf das Internet melden Sie sich mit Ihren Anmeldeinformationen beim Prisma Access-Agenten an.

Nachdem Sie sich beim Prisma Access-Agenten angemeldet haben, werden Sie automatisch über den besten Prisma Access-Standort (manchmal auch Gateway genannt) mit Ihrem Netzwerk verbunden. Der beste Standort wird automatisch ausgewählt, um Ihnen die optimale Leistung zu bieten und ein besseres Erlebnis zu ermöglichen, z. B. das Anzeigen von Websites in Ihrer Landessprache. Wenn sich Ihr Gerät außerhalb des Netzwerks Ihrer Organisation befindet, ermittelt der Agent den besten Standort, um Ihnen beim Herstellen der Verbindung mit dem Netzwerk die beste Leistung zu bieten.

Bevor Sie beginnen, muss der Prisma Access-Agent auf Ihrem Gerät installiert werden. Normalerweise stellt Ihr Administrator den Prisma Access-Agenten auf dem Gerät bereit, das Sie für den Zugriff auf das Netzwerk, die Ressourcen und die Anwendungen Ihrer Organisation verwenden. Der Agent ist gemäß den von Ihrem Administrator definierten Richtlinienregeln konfiguriert und steht auf Ihrem Gerät zur Verfügung. Wenn Ihr Administrator den Prisma Access-Agenten jedoch nicht auf Ihrem Gerät bereitgestellt hat, müssen Sie den Prisma Access-Agenten manuell installieren.

Je nachdem, wie Prisma Access in Ihrer Organisation eingerichtet ist, sollte Ihr Administrator Ihnen die folgenden Anmeldeinformationen zur Verfügung stellen:

- Name des Prisma Access-Servers, der den Dienst zur Verwaltung Ihres Prisma Access Agent hostet. Je nach Einrichtung von Prisma Access können mehrere Server vorhanden sein.
- Name der Projekte, an denen Sie arbeiten, wenn Ihre Organisation *Zugriff mit dynamischen Rechten* verwendet. Der Zugriff mit dynamischen Rechten ermöglicht es Ihnen, auf das Netzwerk und die Ressourcen Ihrer Organisation basierend auf den Ihnen zugewiesenen Projekten zuzugreifen, damit Sie nicht versehentlich auf die Ressourcen eines anderen Projekts zugreifen. Wenn Sie mit der Arbeit an mehreren Projekten beauftragt sind, können Sie problemlos zwischen Projekten wechseln.

*Abhängig von den Einstellungen für Ihr Betriebssystem können die App-Symbole und die App-Oberfläche im Dunkel- oder Hellmodus angezeigt werden.*

Melden Sie sich beim Prisma Access-Agenten an, indem Sie die folgenden Schritte ausführen:

**STEP 1 |** Starten Sie Prisma Access Agent, indem Sie auf das Prisma Access Agent-Symbol in der Menüleiste (macOS) oder der Taskleiste (Windows) klicken.

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Geben Sie nach Aufforderung den **Servernamen** für den Prisma Access-Server ein, den Sie von Ihrem Administrator erhalten haben, oder wählen Sie ihn aus. Klicken Sie dann auf **Weiter**.

Der Servername hat das Format **<example.domain.com>** (ohne das Protokoll **https://**). Der Servername kann maximal 256 Zeichen lang sein.

**STEP 3 |** Geben Sie den Projektnamen ein, den Sie von Ihrem Administrator erhalten haben, und wählen Sie **Weiter** aus.

Die maximale Länge für den Projektnamen beträgt 32 Zeichen.

**STEP 4 |** Melden Sie sich auf der Anmeldeseite, die in Ihrem Standard-Webbrowser angezeigt wird, bei der Single Sign-On-(SSO-)App Ihrer Organisation an, beispielsweise Okta oder Azure Active Directory (AD), indem Sie Ihre Anmeldeinformationen für Ihre Organisation eingeben.

Wenn Ihr Administrator die Multi-Faktor-Authentifizierung (MFA) aktiviert hat, ist bei der Anmeldung eine zusätzliche Verifizierung im Browser erforderlich.

**STEP 5 |** Klicken Sie nach Aufforderung durch Ihren Webbrowser auf **Öffnen**.

Wenn Sie bei der nächsten Anmeldung keine Aufforderung durch Ihren Webbrowser mehr wünschen, wählen Sie **<site> immer erlauben, diese Art von Links in der zugehörigen App zu öffnen** aus. Klicken Sie anschließend auf **Öffnen** (sofern dies von Ihrem Standard-Webbrowser unterstützt wird).

**STEP 6 |** Warten Sie, während der Prisma Access-Agent eine Verbindung zu Prisma Access herstellt.

**STEP 7 |** Nach erfolgreicher Anmeldung werden Sie automatisch mit dem besten verfügbaren Prisma Access-Standort verbunden. Wenn Sie sich mithilfe eines Projekts angemeldet haben, werden Sie mit dem besten verfügbaren Standort für Ihr Projekt verbunden.

Sie können jetzt auf die Ressourcen und SaaS-Apps Ihrer Organisation zugreifen und erhalten sicheren Zugriff auf das Internet.

*Wenn Ihr Administrator den Modus **Immer eingeschaltet** für den Prisma Access Agent aktiviert hat, können Sie die Verbindung zu Prisma Access aufgrund der Richtlinie Ihrer Organisation nicht trennen. Sie können jedoch weiterhin die Prisma Access-Standorte ändern.*

*Wenn Ihr Administrator den Modus **On-Demand** für den Prisma Access Agent aktiviert hat, klicken Sie auf das Sperrsymbol, um eine Verbindung zum neu ausgewählten Standort herzustellen.Prisma Access*

 ©2025 Palo Alto Networks, Inc.

# Ändern der Vorgaben für den aktivierten Zugriff mit dynamischen Rechten Prisma Access Agent

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access Agent | ❑ Desktop-Geräte mit macOS 12 oder höher oder Desktop-Geräte mit Windows 10 Version 2024 oder höher oder mit Windows 11<br>❑ Internetzugang |

Verwenden Sie das Prisma Access Agent-Einstellungsfenster, um Informationen zu Ihrem Gerät anzuzeigen und Optionen für Ihren Agenten zu ändern, wie z. B. das Aktivieren von Desktop-Benachrichtigungen .

**STEP 1 |** Starten Sie Prisma Access Agent, indem Sie in der macOS-Menüleiste oder Windows-Taskleiste auf das Prisma Access Agent-Symbol  klicken.

**STEP 2 |** Klicken Sie auf das Hamburger-Menü, um das Einstellungsfenster zu öffnen.

**STEP 3 |** Im Einstellungsfenster können Sie die folgenden Informationen anzeigen:

| Symbol | Beschreibung |
|---|---|
| | Ihre Benutzer-ID. |
| | Den Prisma Access-Standort, mit dem Ihr Gerät verbunden ist. |
| | Die IP-Adresse des Prisma Access-Standorts. |
| | Den Hostnamen oder die IP-Adresse für die administrative Schnittstelle (Server), mit der Sie verbunden sind. Sie können auf das Pluszeichen (+) klicken, um eine Verbindung zu einem anderen Server herzustellen. |
| | Das Projekt, bei dem Sie angemeldet sind. |

**STEP 4 |** Um Prisma Access Agent-Benachrichtigungen in der Menüleiste (unter macOS) oder in der Taskleiste (unter Windows) zu empfangen, müssen Sie **Desktop-Benachrichtigungen zulassen**. Diese Einstellung ist standardmäßig aktiviert.

Die Desktop-Benachrichtigungen richten sich nach allen „Bitte nicht stören“-Einstellungen, die Sie zum Zeitpunkt der Installation festgelegt haben. Das Betriebssystem fordert Sie während der Installation auf, Benachrichtigungen von Prisma Access Agent zuzulassen.

 ©2025 Palo Alto Networks, Inc.

**STEP 5 |** Welche Daten Prisma Access Agent erfasst und wie die Informationen verwendet werden, erfahren Sie in unserer **Datenschutzrichtlinie**.

**STEP 6 |** Um Unterstützung bei Problemen zu erhalten, die beim Arbeiten mit Prisma Access Agent möglicherweise auftreten, klicken Sie auf **Unterstützungsressourcen**.

**STEP 7 |** Wenn Ihr Administrator dies zulässt, können Sie eine **Abmeldung** von Prisma Access Agent durchführen.

**STEP 8 |** Wenn Ihr Administrator die Funktion aktiviert hat, können Sie Prisma Access Agent **Deaktivieren**, damit Sie zur GlobalProtect-App wechseln können (wenn sie auf Ihrem Gerät installiert ist).

**STEP 9 |** Zeigen Sie die Version Ihres Prisma Access Agent an.

**STEP 10 |** Um das Fenster zu schließen, klicken Sie auf das **X**.

## Verbindung von Prisma Access Agent mit aktiviertem Zugriff mit dynamischen Rechten zu einem anderen Standort herstellen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access Agent | ☐ Desktop-Geräte mit macOS 12 oder höher oder Desktop-Geräte mit Windows 10 Version 2024 oder höher oder mit Windows 11<br>☐ Internetzugang |

Nachdem Sie sich bei Prisma Access Agent angemeldet haben, werden Sie automatisch mit dem besten verfügbaren Prisma Access-Standort verbunden. Wenn Sie Standorte ändern möchten, verwenden Sie dazu das Dropdown-Menü **Standort**.

**STEP 1 |** Starten Sie Prisma Access Agent, indem Sie auf das Prisma Access Agent-Symbol in der Menüleiste (macOS) oder der Taskleiste (Windows) klicken.

**STEP 2 |** Wählen Sie einen anderen **Standort** aus. Sie können nach einem Standort **suchen** oder einen Standort aus der Liste auswählen.

Die Liste der verfügbaren Standorte wird nach der besten Erfahrung hinsichtlich Reaktionszeit, Verfügbarkeit und anderen Faktoren sortiert. Der Standort, der das beste Erlebnis bietet, wird als **Bester Standort** angezeigt.

**STEP 3 |** Wenn Ihr Administrator den Modus **On-Demand** für den Prisma Access Agent aktiviert hat, klicken Sie auf das Sperrsymbol, um eine Verbindung zum neu ausgewählten Standort herzustellen. Anderenfalls fährt der Prisma Access Agent mit wechselnden Standorten fort.

 ©2025 Palo Alto Networks, Inc.

# Zu einem anderen Projekt wechseln

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access Agent | ❑ Desktop-Geräte mit macOS 12 oder höher oder Desktop-Geräte mit Windows 10 Version 2024 oder höher oder mit Windows 11<br>❑ Internetzugang |

Wenn Sie mehreren Projekten in Ihrer Organisation zugewiesen sind, können Sie zu einem anderen Projekt wechseln, um auf das Netzwerk und die Ressourcen zuzugreifen, die diesem Projekt zugeordnet sind.

*Wenn das Projekt, zu dem Sie wechseln möchten, von einem anderen Server aus zugänglich ist, müssen Sie zunächst* zu diesem Server wechseln.

**STEP 1 |** Starten Sie den Prisma Access Agenten, indem Sie in der macOS-Menüleiste oder in der Windows-Taskleiste auf das Prisma Access Agent-Symbol  klicken.

**STEP 2 |** Wählen Sie ein anderes **Projekt** aus. Sie können nach einem Standort **suchen** oder einen Standort aus der Liste auswählen.

Sie müssen dem Projekt zugewiesen sein, zu dem Sie wechseln.

**STEP 3 |** Wenn Ihr Administrator den Modus **On-Demand** für den Prisma Access Agenten aktiviert hat, klicken Sie auf das Sperrsymbol, um zwischen den Projekten zu wechseln. Anderenfalls fährt der Prisma Access Agent mit dem Wechseln von Projekten fort.

**STEP 4 |** Jedes Mal, wenn Sie zwischen Projekten wechseln, trennt der Prisma Access Agent die Verbindung zum aktuellen Projekt und stellt eine Verbindung mit dem neu ausgewählten Projekt her. Möglicherweise werden Sie aufgefordert, den Prisma Access Agenten erneut zu **öffnen**.

# Verbindung von Prisma Access Agent mit aktiviertem Zugriff mit dynamischen Rechten zu einem anderen Server herstellen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access Agent | ❑ Desktop-Geräte mit macOS 12 oder höher oder Desktop-Geräte mit Windows 10 Version 2024 oder höher oder mit Windows 11<br>❑ Internetzugang |

 ©2025 Palo Alto Networks, Inc.

Eine Instanz des Prisma Access-Servers wird auch als *Mandant* bezeichnet. Wenn Ihre Administratoren mehrere Prisma Access-Server einrichten, können Sie sich mit einem anderen Server verbinden, um über diesen auf das Netzwerk oder die Ressourcen zuzugreifen.

Wenn Sie beispielsweise an einem anderen Projekt arbeiten müssen, dieses Projekt jedoch nur auf einem anderen Server zugänglich ist. Sie müssen eine Verbindung mit diesem Server herstellen, bevor Sie zu diesem Projekt wechseln können.

**STEP 1 |** Starten Sie Prisma Access Agent, indem Sie auf das Prisma Access Agent-Symbol in der Menüleiste (macOS) oder der Taskleiste (Windows) klicken.

**STEP 2 |** Bearbeiten Sie die Servereinstellungen, indem Sie das Serververwaltungssymbol auswählen.

**STEP 3 |** Das Serverinformationsfenster zeigt den Server an, mit dem Sie verbunden sind. Wenn andere Server aufgeführt sind, wählen Sie einen Server aus und klicken Sie auf **Verbinden**, um die Verbindung herzustellen.

**STEP 4 |** Wenn Sie einen Server hinzufügen müssen, führen Sie die folgenden Schritte aus:

1. Klicken Sie auf das Pluszeichen **+**.
2. Geben Sie den neuen Servernamen ein (der von Ihrem Administrator bereitgestellt wird) und wählen Sie **Hinzufügen** aus.

   Der Servername hat das Format **`<example.domain.com>`** (ohne **`https://`**). Der Servername kann maximal 256 Zeichen lang sein. Auf dieser Seite sind maximal 20 Server zulässig.

3. Nachdem Sie den Server hinzugefügt haben, wählen Sie ihn aus und klicken Sie auf **Verbinden**.

**STEP 5 |** Wenn das Bestätigungsfenster angezeigt wird, klicken Sie auf **Ja**, um die Verbindung zum aktuellen Server zu trennen und eine Verbindung zum anderen Server herzustellen. Sie müssen Ihre Anmeldeinformationen erneut angeben.

**STEP 6 |** Wenn Sie dazu aufgefordert werden, melden Sie sich am neuen Server an, indem Sie den Projektnamen angeben (falls zutreffend).

## Zwischen dem Prisma Access Agenten und der GlobalProtect-App wechseln

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access Agent | ☐ Desktop-Geräte mit macOS 12 oder höher oder Desktop-Geräte mit Windows 10 Version 2024 oder höher oder mit Windows 11<br>☐ Internetzugang |

 ©2025 Palo Alto Networks, Inc.

In einigen Organisationen ist der Prisma Access Agent auf Benutzergeräten installiert, auf denen bereits die GlobalProtect-App installiert ist. Nach der Installation des Prisma Access Agenten können Sie bei Bedarf zwischen dem Prisma Access Agenten und der GlobalProtect-App wechseln.

Nach dem Wechsel zur GlobalProtect-App befindet sich der Prisma Access-Agent im deaktivierten Zustand. Deaktiviert:

- Der gesamte Datenverkehr zu den Standorten von Prisma Access ist deaktiviert und die Multi-Faktor-Authentifizierung (MFA) ist deaktiviert.

  Der Prisma Access-Agent und GlobalProtect verwenden denselben GlobalProtect-Port, um MFA-Anfragen zu empfangen (für eine zusätzliche Authentifizierung für bestimmte Anwendungen), aber es kann jeweils nur ein Agent den Port verwenden. Wenn Sie den Prisma Access-Agenten deaktivieren, wird der Port für die Verwendung durch GlobalProtect freigegeben.
- Die Kommunikation mit dem Server bleibt bestehen, sodass der Agent weiterhin gestaffelte Rollout-Upgrades, ADEM-Benachrichtigungen und Remote-Shell-Anfragen vom Administrator empfangen und HIP-Prüfungen durchführen kann.
- Wenn die Anti-Tamper-Funktion vom Administrator konfiguriert wurde, schützt sie den Agenten weiterhin vor unbefugten Manipulationen.
- Auf macOS-Geräten sind die System- und Netzwerkerweiterungen für den Prisma Access-Agenten weiterhin aktiv, und auch der Inhaltsfilter bleibt aktiv.
- Wenn Sie zu einem anderen Server wechseln, wird der Prisma Access-Agent automatisch wieder aktiviert. Wenn Sie versuchen, eine Verbindung zu einem Prisma Access-Standort herzustellen, während der Agent deaktiviert ist, verbindet sich der Agent mit dem besten Standort.

Sie können entweder die Prisma Access-Agent-App oder das Prisma Access-Befehlszeilentool (PACli) verwenden, um zwischen den beiden Apps zu wechseln.

- Prisma Access-Agent-App
- Prisma Access-Befehlszeile (PACli)

## Zwischen dem Prisma Access Agenten und der GlobalProtect-App wechseln (mit der Prisma Access-Agent-App)

## Zwischen dem Prisma Access Agenten und der GlobalProtect-App wechseln (mit dem PACli-Tool)

 ©2025 Palo Alto Networks, Inc.

# Anzeigen und Überwachen von Benutzern mit Zugriff mit dynamischen Rechten

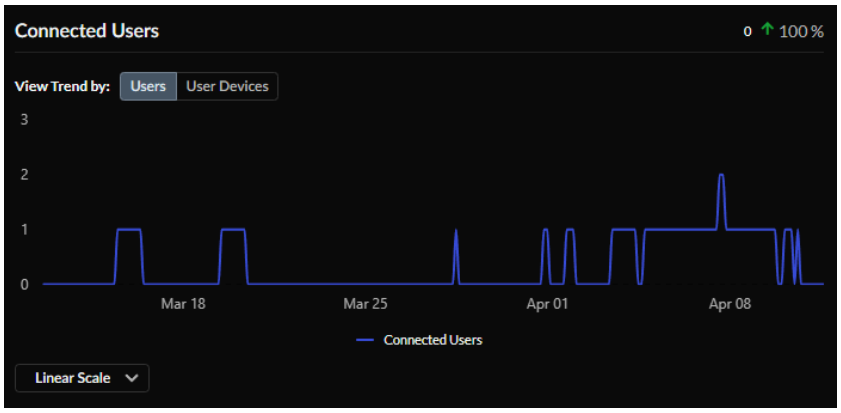
| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access-Lizenz |

Mit dem Zugriff mit dynamischen Rechten (Dynamic Privilege Access) kann Prisma Access je nach Projekt, an dem Ihre Benutzer arbeiten, unterschiedliche Netzwerk- und Sicherheitsrichtlinienregeln auf mobile Benutzerflüsse anwenden. Navigieren Sie im Strata Cloud Manager Command Center zu **Insights** > **Benutzer**, um benutzerbasierte Zugriffsinformationen in Ihrer Umgebung anzuzeigen.

## Verbundene Benutzer

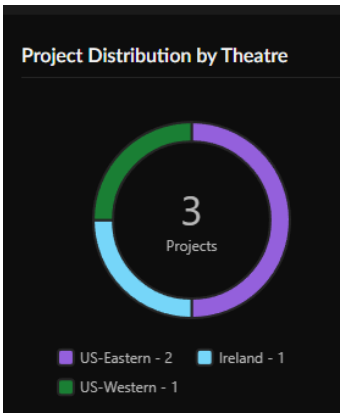
Unter **Verbundene Benutzer** können Sie sich aktuell verbundene Benutzer oder verbundene Benutzergeräte ansehen. Der Aufwärts- oder Abwärtspfeil vergleicht diesen Zeitbereich mit einem vorherigen Zeitbereich, um die prozentuale Differenz der Anzahl verbundener Benutzer oder Geräte anzugeben.

Wählen Sie **Trend nach Benutzern anzeigen** aus, um die Anzahl der derzeit mit Prisma Access Agent verbundenen Benutzer anzuzeigen. Klicken Sie auf **Trend nach Benutzergeräten anzeigen**, um die Anzahl der derzeit mit Prisma Access Agent verbundenen Benutzergeräte anzuzeigen.

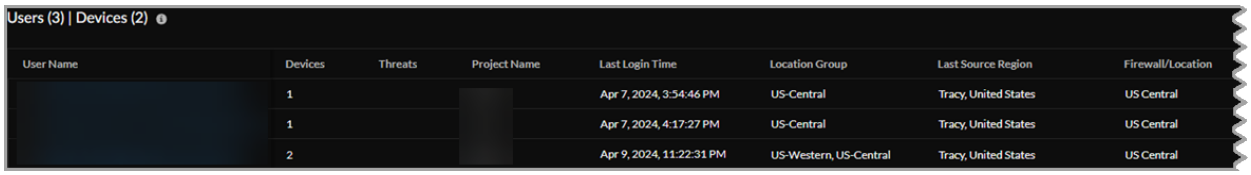



Unter **Projektverteilung nach Theatern** sehen Sie die Anzahl der Projekte nach Standort oder Theatern.


©2025 Palo Alto Networks, Inc.




Die Tabelle **Benutzer | Geräte** zeigt den **Namen des Projekts** an, der jedem Benutzer und Gerät zugeordnet ist. Sie können auch sehen, wie viele Geräte nach Benutzer, letztem Anmeldezeitpunkt, letztem Quellstandort, zuletzt verbundenem Prisma Access-Standort, dem Quell-Internetprotokoll und der Betriebssystemfamilie und -version verbunden sind.

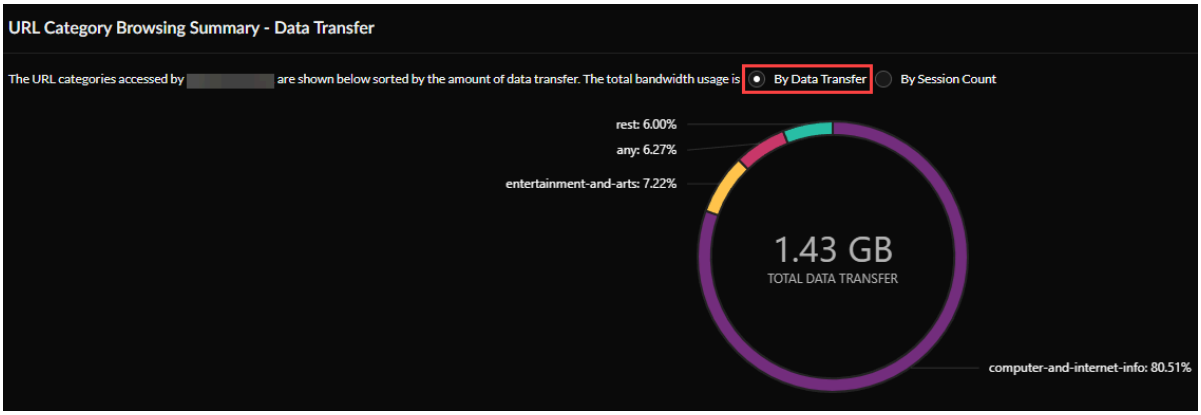



Wählen Sie einen beliebigen **Namen des Projekts** aus, um zur Seite **Projekte** zu gelangen.

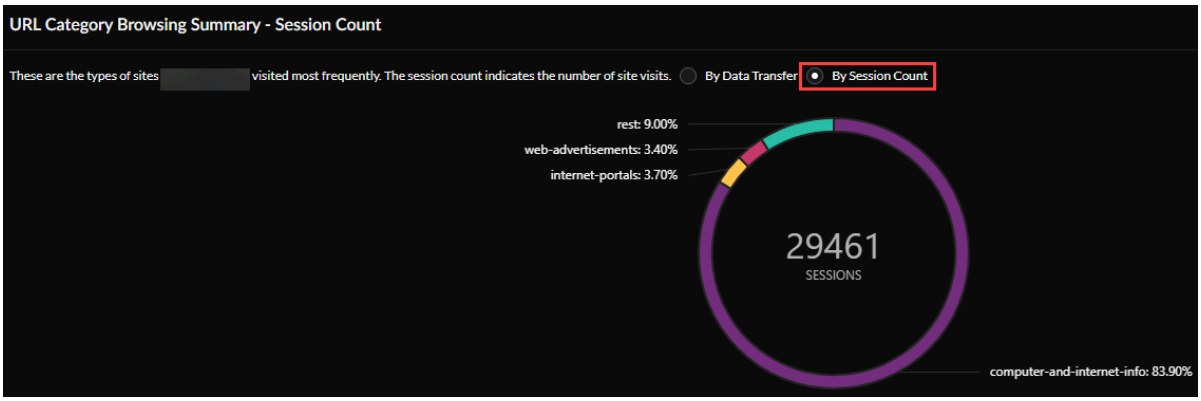
Wählen Sie einen beliebigen **Benutzernamen** aus, um Benutzerdetails wie **Aktivität** und **Konnektivität** anzuzeigen.

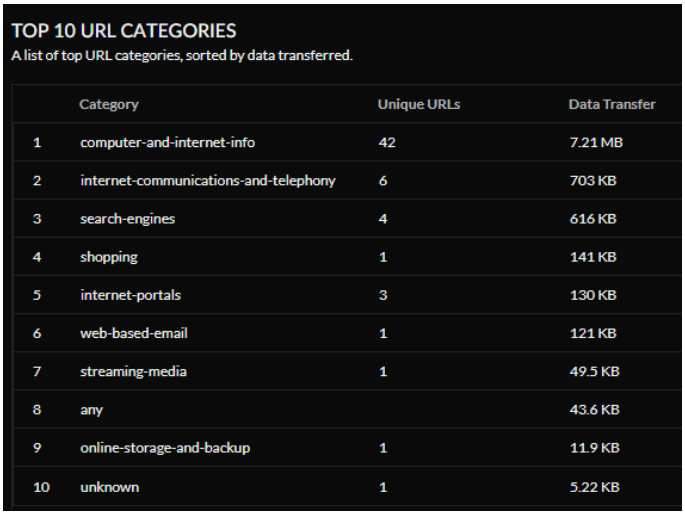
## Aktivität

**Übersicht URL-Browsingkategorie – Datenübertragung**: Zeigen Sie die Übersicht der Datenübertragungen Ihrer Browsingkategorie **nach Datenübertragung** oder **nach Sitzungsanzahl** an. Sie können auch eine Liste der **Top 10 der URL-Kategorien** anzeigen, sortiert nach übertragenen Daten.




 ©2025 Palo Alto Networks, Inc.



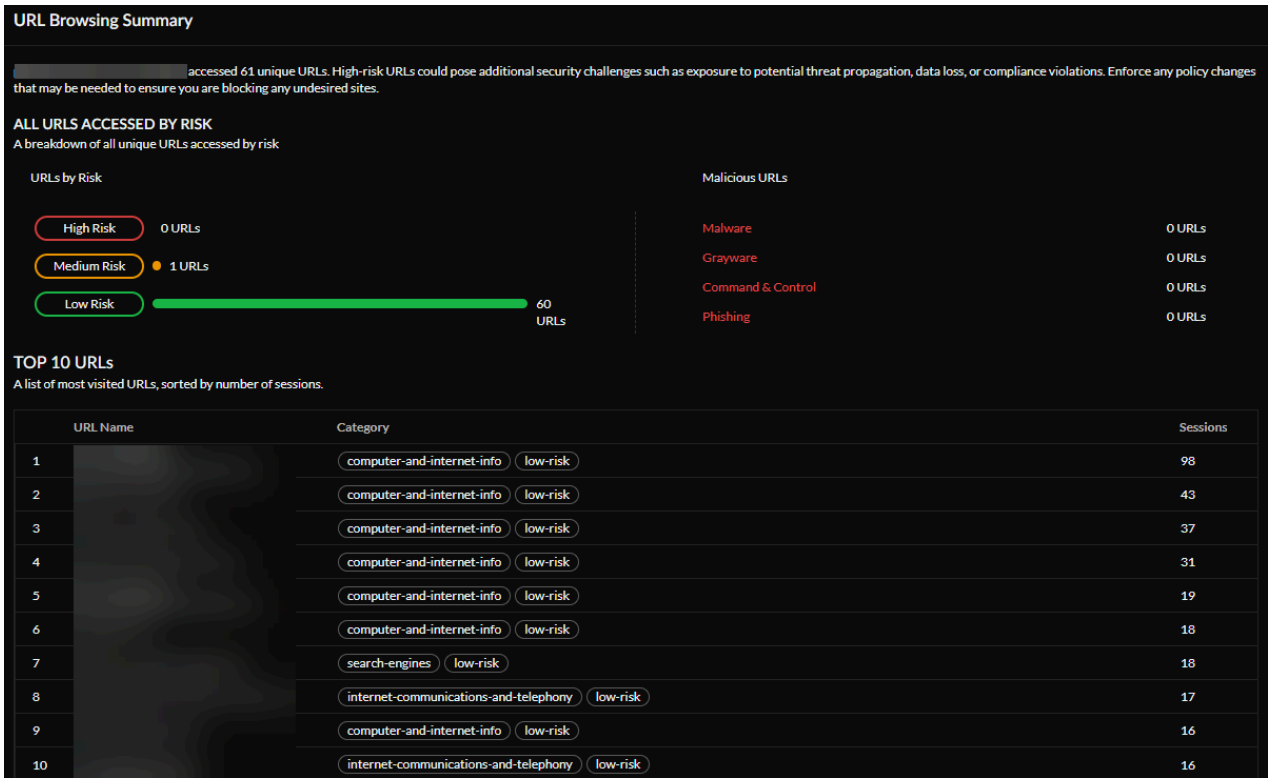
TOP 10 URL CATEGORIES

A list of top URL categories, sorted by data transferred.

| | Category | Unique URLs | Data Transfer |
|---|---|---|---|
| 1 | computer-and-internet-info | 42 | 7.21 MB |
| 2 | internet-communications-and-telephony | 6 | 703 KB |
| 3 | search-engines | 4 | 616 KB |
| 4 | shopping | 1 | 141 KB |
| 5 | internet-portals | 3 | 130 KB |
| 6 | web-based-email | 1 | 121 KB |
| 7 | streaming-media | 1 | 49.5 KB |
| 8 | any | | 43.6 KB |
| 9 | online-storage-and-backup | 1 | 11.9 KB |
| 10 | unknown | 1 | 5.22 KB |

**URL-Browsingübersicht**: Zeigt Ihre URL-Browsingübersicht einschließlich aller URLs an, auf die Sie nach Risiko zugegriffen haben. Sie können eine Aufschlüsselung von URLs nach Risiko (hoch, mittel oder niedrig) anzeigen und sehen, wie viele schädliche URLs Sie aufgerufen haben. Außerdem können Sie eine Liste der besuchten **Top 10 der URLs** anzeigen und sehen, wie oft Sie die einzelnen URLs besucht haben.


©2025 Palo Alto Networks, Inc.

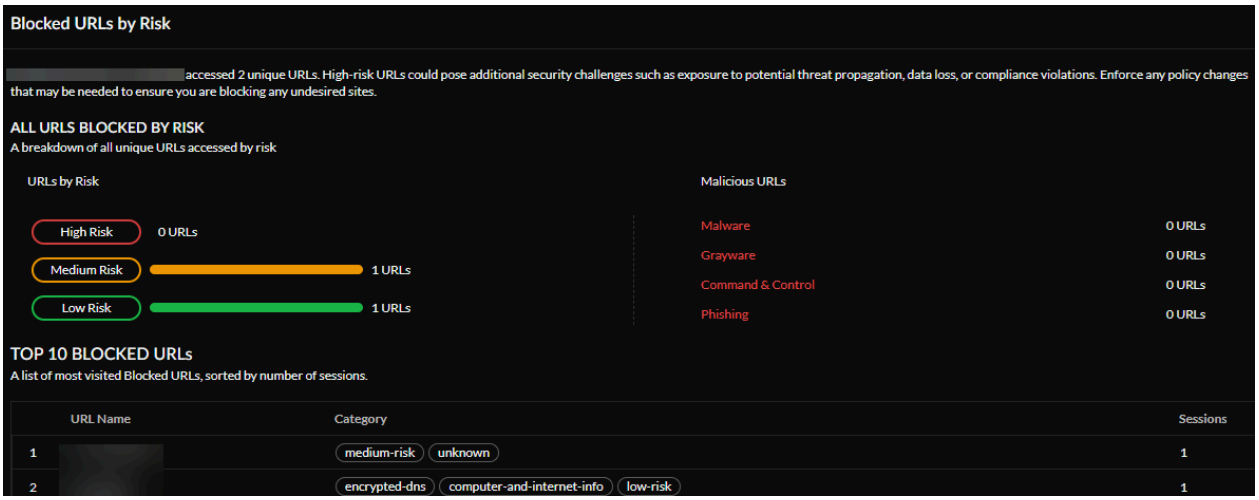



**URL-Filterungs-Protokolle anzeigen**: Wählen Sie **URL-Filterungs-Protokolle anzeigen**, um Details zu den übertragenen Gesamtdaten anzuzeigen. Der Protokoll-Viewer stellt einen Prüfpfad für System-, Konfigurations- und Netzwerkereignisse bereit. Netzwerkprotokolle zeichnen alle Ereignisse auf, bei denen Prisma Access auf Ihren Netzwerkverkehr einwirkt.

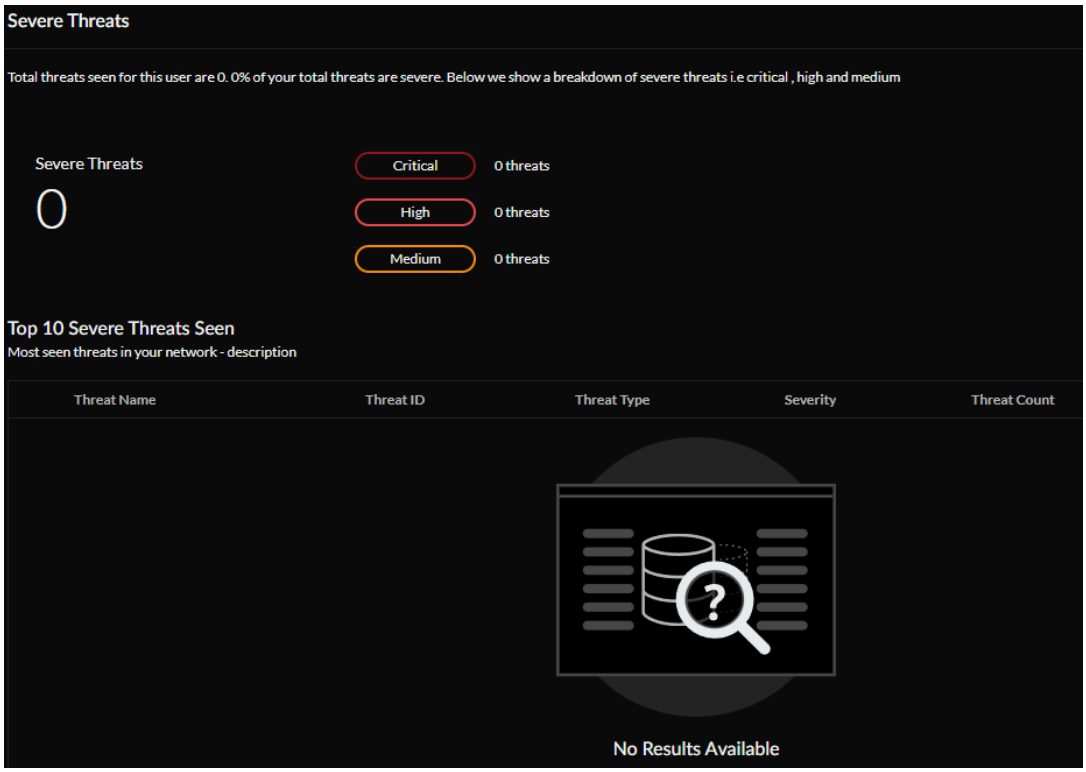
- Zeigen Sie alle Protokolldaten an oder verwenden Sie das Dropdown-Menü, um nach **Firewall/URL**, **Gemeinsam** oder **Endpunkt** zu filtern. Jeder dieser Filter hat mehrere Unterfilter zur Auswahl.
- Geben Sie eine Protokollabfrage ein. Klicken Sie in dieses Feld, um eine Auswahl von Abfragen anzuzeigen und Ihre Abfrage zu erstellen.
- Wählen Sie einen Zeitbereich aus. Standardmäßig sind 60 Minuten eingestellt.
- Wählen Sie **Protokolleinstellungen** aus, um das Dashboard von Strata Logging Service anzuzeigen. Strata Logging Service verwaltet den Zustellmechanismus für Protokolle.

**Blockierte URLs nach Risiko**: Hier sehen Sie, ob Sie auf alle nach Risiko blockierten URLs zugegriffen oder versucht haben, darauf zuzugreifen. URLs mit hohem Risiko können zusätzliche Sicherheitsherausforderungen mit sich bringen, z. B. die Gefahr vor potenzieller Ausbreitung von Bedrohungen, Datenverlust oder Compliance-Verstößen. Erzwingen Sie alle erforderlichen Richtlinienänderungen, um unerwünschte Websites zu blockieren. Sie können sich auch eine Liste der **Top 10 der blockierten URLs** ansehen, die Sie am häufigsten besucht haben, sortiert nach der Anzahl der Sitzungen.

 ©2025 Palo Alto Networks, Inc.




**Schwerwiegende Bedrohungen**: Zeigt an, wie viele Ihrer Bedrohungen schwerwiegend sind. Schwerwiegende Bedrohungen werden weiter in kritische, hohe und mittlere Bedrohungen unterteilt. Sie können auch eine Liste der **Top 10 der am häufigsten gesehenen schwerwiegenden Bedrohungen** in Ihrer Umgebung anzeigen.




## Konnektivität

Wählen Sie einen beliebigen **Benutzernamen** aus, um Informationen zur **Konnektivität** des Benutzers im ausgewählten **Zeitbereich** anzuzeigen.

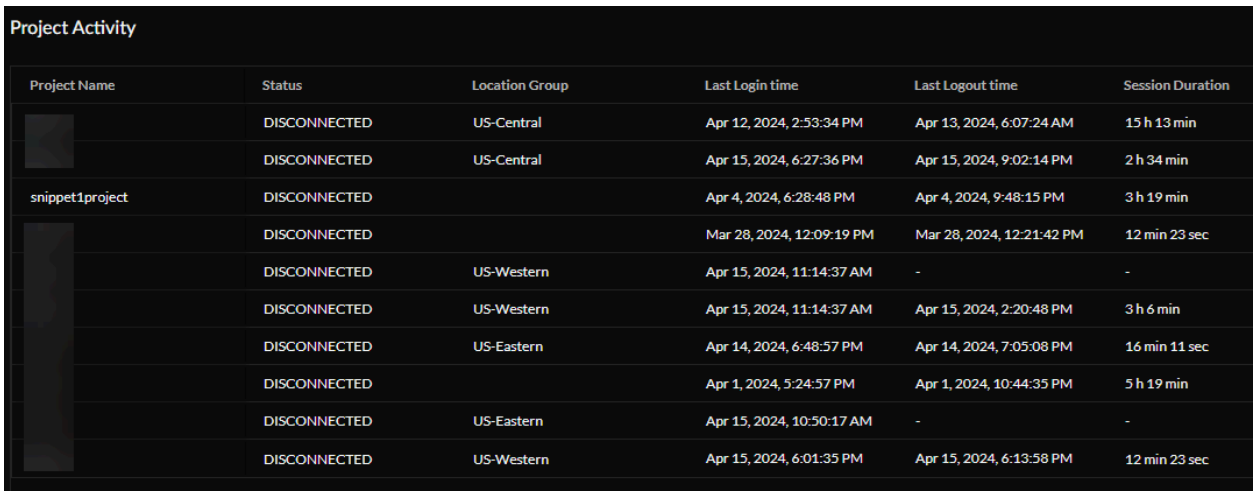
**Aktive Projekte**: Hier können Sie sehen, welche Projekte in dem von Ihnen ausgewählten Zeitraum aktiv waren und wann jedes Projekt aktiv wurde.

 ©2025 Palo Alto Networks, Inc.

**Gerätetrend eines verbundenen Benutzers und Geräte eines verbundenen Benutzers**: Auf der Benutzer-Hauptseite können Sie alle verbundenen Benutzer und ihre Projekte sehen. Zeigen Sie auf der Seite **Konnektivität** den Trend Ihrer individuellen **Geräte des verbundenen Benutzers** im ausgewählten Zeitraum sowie Details zu den **Geräten des verbundenen Benutzers** an, wie Gerätename, IP-Adresse der letzten Benutzerquelle, letzte private IP-Adresse, letzter Benutzerstandort, letzte Anmeldezeit, letzte Abmeldezeit und letzte Sitzungsdauer.




**Projektaktivität**: Zeigt die Projektaktivität eines Benutzers nach Sitzung an. Sie sehen den aktuellen Status einer Sitzung, wann sich der Benutzer bei jedem Projekt angemeldet hat, wann er sich abgemeldet hat und wie lange jede Sitzung gedauert hat.




**Gesamte Benutzeraktivität nach Projekt**: Zeigt die Zeit an, die ein Benutzer im ausgewählten Zeitraum für jedes Projekt verbracht hat.

 ©2025 Palo Alto Networks, Inc.

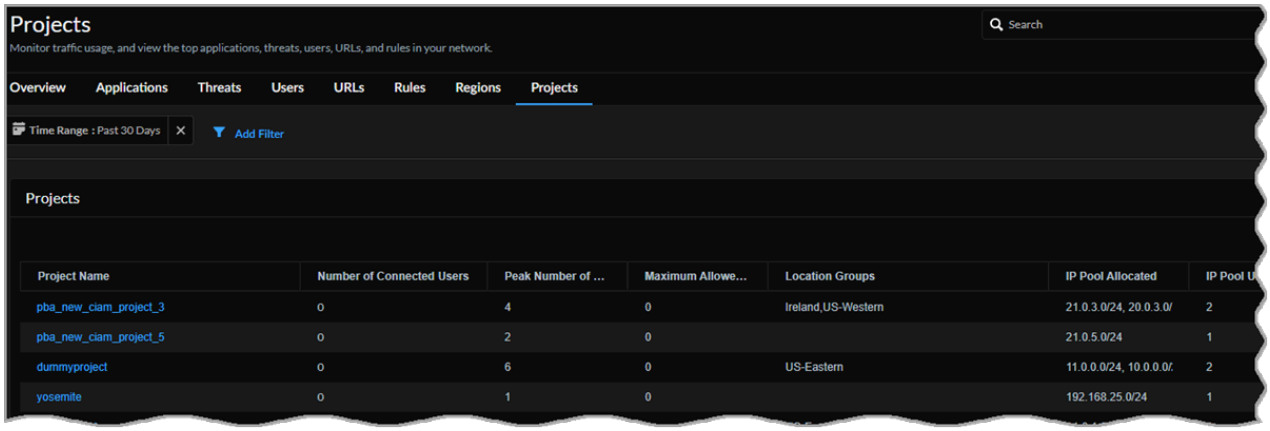
# Anzeigen und Überwachen von Projekten mit Zugriff mit dynamischen Rechten

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Verschaffen Sie sich einen Einblick in Ihre Prisma Access Agent-Bereitstellung, indem Sie Strata Cloud Manager verwenden, um die Projektaktivitäten Ihrer Benutzer zu überwachen. Navigieren Sie im Strata Cloud Manager Command Center zu **Activity Insights** > **Projekte**, um projektbasierte Zugriffsinformationen in Ihrer Umgebung anzuzeigen.

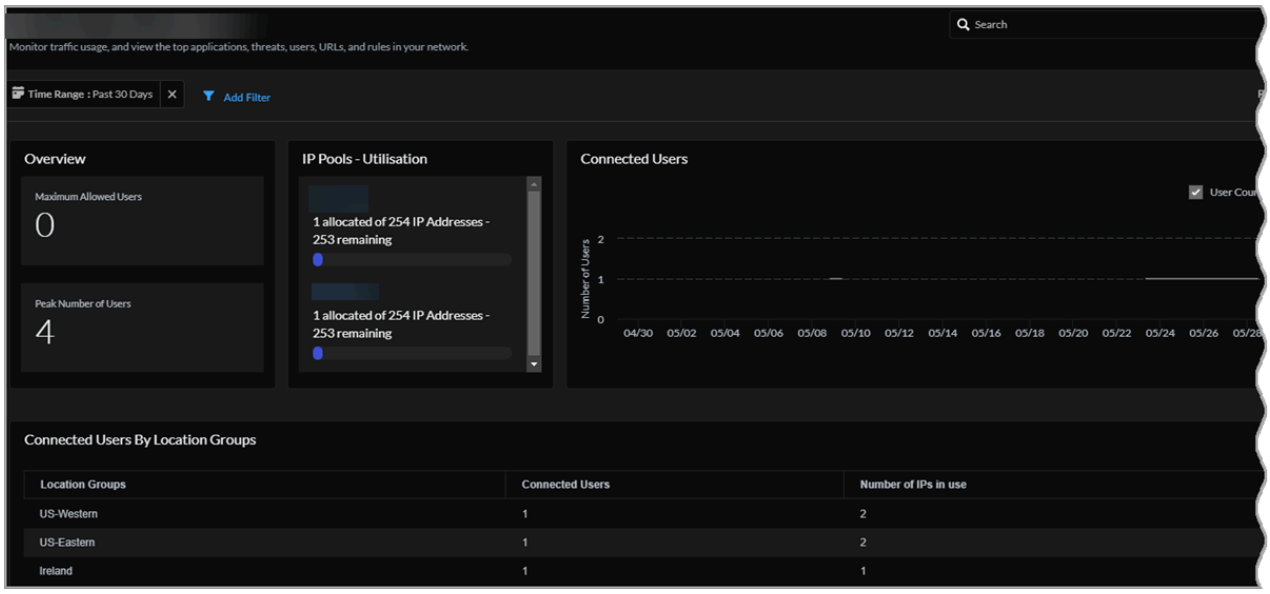
## Projekte

Die Tabelle **Projekte** bietet einen Gesamtüberblick über die Projekte, auf die Ihre Benutzer mit Prisma Access im ausgewählten Zeitraum zugreifen. Sie können die Anzahl der verbundenen Benutzer, die maximale Anzahl der Benutzer, die maximal zulässigen Benutzer, die Prisma Access-Standortgruppen, den zugewiesenen IP-Adresspool, den verwendeten IP-Pool, die Anzahl der verfügbaren IP-Adressen und den zuletzt verbundenen Prisma Access-Standort für jedes Projekt sehen.




Wählen Sie einen **Namen des Projekts** aus, um die Detailseite dieses Projekts aufzurufen. Der Projektname (in der folgenden Abbildung verschwommen dargestellt) wird oben links angezeigt.


©2025 Palo Alto Networks, Inc.

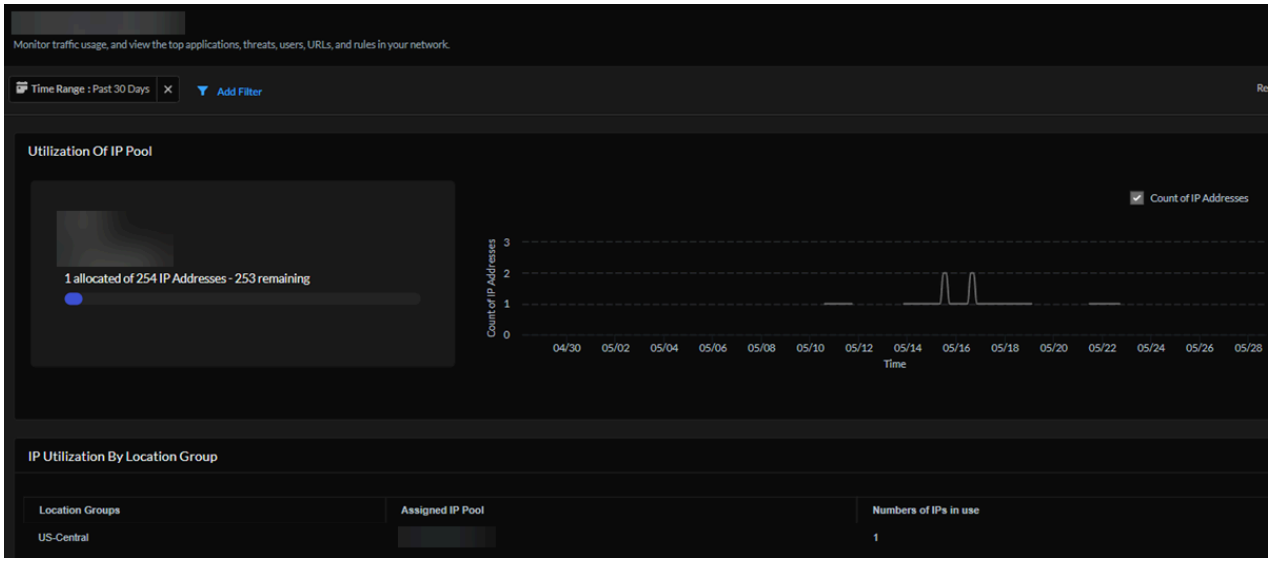



## Übersicht

Auf der Seite mit den Projektdetails werden unter **Überblick** die maximal zulässigen Benutzer für dieses Projekt und die maximale Anzahl von Benutzern im ausgewählten Zeitraum angezeigt.

## IP-Pool-Auslastung

Zeigen Sie die Anzahl der verwendeten IPs und die Anzahl der IPs an, die für die Pools in diesem Projekt noch verfügbar sind. Wählen Sie einen bestimmten IP-Pool aus, um zu seiner Detailseite zu gelangen (siehe folgende Abbildung). Dort sehen Sie die Auslastung dieses IP-Pools, die Anzahl der verwendeten IP-Adressen und die Auslastung der IP-Adressen nach Prisma Access-Standortgruppe.




 ©2025 Palo Alto Networks, Inc.

### Verbundene Benutzer

Zeigen Sie ein Diagramm der im ausgewählten Zeitbereich verbundenen Benutzer an. Bewegen Sie den Mauszeiger über einen beliebigen Punkt im Diagramm, um die Benutzeranzahl an dieser Stelle anzuzeigen.

### Verbundene Benutzer nach Standortgruppen

Zeigen Sie die Anzahl der Benutzer nach der Prisma Access-**Standortgruppe** an, der sie angehören. Sie können auch die Anzahl der verwendeten IP-Adressen für jede **Standortgruppe** anzeigen.

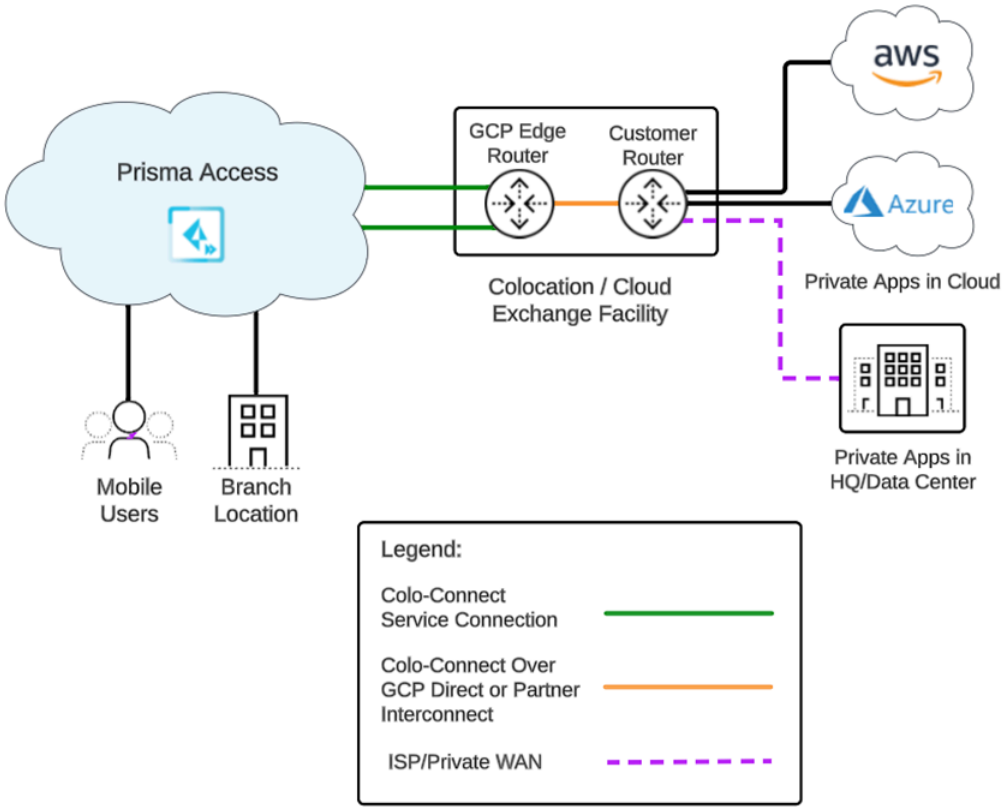

©2025 Palo Alto Networks, Inc.

# Prisma Access Colo-Connect

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Eine Prisma Access (Managed by Panorama)-Bereitstellung mit der Cloud-Services-Plug-in-Mindestversion 4.1 und der Dataplane-Mindestversion 10.2.4<br>❑ Eine Colo-Connect-Add-on-Lizenz |

Heute erstellen große Unternehmen Colo-basierte Leistungshubs, um private Anwendungen in hybriden Multicloud-Architekturen zu erreichen, da hohe Anforderungen in Bezug auf die Bandbreiten und niedrige Latenzzeiten bestehen. In der Regel umfassen diese Hubs Verbindungen zu einem oder auch mehreren Cloud-Anbietern und Verbindungen zu den lokalen Rechenzentren über ein privates oder gemietetes WAN. Leistungshubs können den Datenverkehr zwischen der Public Cloud und der lokalen Infrastruktur mit hoher Geschwindigkeit weiterleiten und sind aufgrund der zugrunde liegenden Verbindungsinfrastruktur stabil.

Colo-Connect baut auf dem Colo-basierten Leistungshub-Konzept auf und bietet private Verbindungen mit hoher Bandbreite (bis zu 20 Gb/s) sowie nahtlose Layer-2/3-Konnektivität zu Prisma Access über die bestehenden Leistungshubs. Die folgende Abbildung zeigt das Onboarding von Prisma Access in einer GCP-Instanz mithilfe von Dienstverbindungen und direkten Verbindungen oder Partnerverbindungen. Diese Einrichtung begrenzt die Gefährdung auf das Internet und ermöglicht die Verwendung privater Verbindungen für die Konnektivität privater Anwendungen.




Prisma Access Colo-Connect nutzt die Cloud-native GCP-Verbindungstechnologie, um Dienstverbindungen mit hoher Bandbreite für Ihre privaten Anwendungen mit den folgenden Funktionen bereitzustellen:

- Hoher Bandbreitendurchsatz (bis zu 20 Gb/s) pro Region für den Zugriff auf private Anwendungen
- Unterstützung sowohl für dedizierte Verbindungen als auch Partnerverbindungen mit Google Cloud Platform (GCP)
- Unterstützung für mehrere VLAN-Anschlüsse pro Interconnect-Link.
- Regionale Redundanz

 ©2025 Palo Alto Networks, Inc.

# Colo-Connect-Anwendungsfälle

Prisma Access Colo-Connect bietet bidirektionale Konnektivität mit hoher Bandbreite für sichere private Apps, wie in den folgenden Anwendungsfällen gezeigt.

## Zugriff auf private Apps mit hoher Bandbreite

Wenn Ihre Organisation über eine Netzwerkpräsenz in einem Colo verfügt und Sie Colo-Einrichtungen nutzen, um eine private Konnektivität zu den Apps aufzubauen, die vor Ort und/oder in der Public Cloud gehostet werden, kann Prisma Access über Colo-Connect in diese Colo-Infrastruktur integriert werden. Sie können Colo-Connect entweder mit einer dedizierten Verbindung oder einer Partnerverbindung konfigurieren, die von GCP bereitgestellt wird, um einen Durchsatz von bis zu 20 Gb/s pro Region für den privaten App-Zugriff zu erzielen.

Angenommen, Sie verfügen über ein oder mehrere Rechenzentren oder Zentralen, die über direkte Konnektivität zu Colo verfügen, und möchten eine Verbindung zu Prisma Access herstellen, um hohe Bandbreiten nutzen zu können und sicheren Zugriff auf private Apps zu erhalten. In diesem Fall können Sie eine Partner Interconnect-Verbindung mit Prisma Access Colo-Connect verwenden, um den Benutzern sicheren Zugriff auf die Apps zu ermöglichen. Da die Geräte in Colo sowohl mit der Public Cloud als auch mit Ihrem Rechenzentrum auf Peer-Ebene verbunden sind, können Sie auch Zugriff auf alle privaten Apps ermöglichen, die in der öffentlichen Cloud gehostet werden.

Colo-Connect koexistiert mit den vorhandenen tunnelbasierten IPSec-Dienstverbindungen. Wenn Sie also Zugriff auf private Apps für kleinere Rechenzentren bereitstellen müssen, die keinen Multi-Gigabit-Durchsatz mit hoher Bandbreite benötigen, können Sie auch Dienstverbindungen zu diesen Rechenzentren verwenden. Sie können Dienstverbindungen mithilfe von BGP-Routing konfigurieren, um Ihr Netzwerk mit Dienstverbindungen und Colo-Connect-Verbindungen kompatibel zu machen.

## Private Konnektivität für private Anwendungen

Colo-Connect kann ein privates Netzwerk nutzen, über das Benutzer auf private Apps zugreifen können, anstatt über das Internet. Hierdurch wird eine zusätzliche Ebene der Kontrolle und Sicherheit für die privaten Apps hinzugefügt.

## Verwenden eines NaaS-Drittanbieters

In diesem Anwendungsfall nutzen Sie NaaS-Drittanbieter (Network as a Service) wie Megaport und PacketFabric, um eine Verbindung zwischen Colo und Ihren Anwendungen herzustellen, die in öffentlichen Clouds oder mit SaaS-Anbietern wie beispielsweise salesforce.com oder Box ausgeführt werden. Sie möchten die Netzwerkkonnektivität zwischen den Netzwerken von Drittanbietern und Prisma Access herstellen, um Zugriff mit hoher Bandbreite auf die verbundenen Dienste, Clouds und Anwendungen zu ermöglichen. Mögliche Aktionen:

- Verwenden Sie Netzwerkgeräte eines NaaS-Anbieters als Hub, um Konnektivität zwischen Benutzern und Anwendungen bereitzustellen, die in VPCs in der öffentlichen Cloud oder über öffentliche SaaS-Anbieter in einer bestimmten Region ausgeführt werden.
- Richten Sie eine BGP-Sitzung zwischen den Netzwerkgeräten des NaaS-Anbieters und Prisma Access ein.

 ©2025 Palo Alto Networks, Inc.

*Die Verwendung von NaaS-Lösungen von Drittanbietern mit Prisma Access Colo-Connect wurde von Palo Alto Networks nicht validiert. Es wird empfohlen, die unterstützten Funktionen beim Drittanbieter zu evaluieren. Dabei sollte auch das Einrichten einer Verbindung mit GCP und das Erstellen von GRE-Tunneln zu Prisma Access für die Colo-Connect Dienstverbindungen bewertet werden.*

 ©2025 Palo Alto Networks, Inc.

# Wie unterscheidet sich Colo-Connect von Dienstverbindungen und ZTNA-Connector?

Palo Alto Networks bietet drei Möglichkeiten, den Zugriff auf private Anwendungen zu sichern: Dienstverbindungen, ZTNA-Connector und Colo-Connect. Sowohl über Dienstverbindungen als auch mit ZTNA-Connector können Sie den Zugriff auf private Anwendungen über das Internet sichern, während mit Colo-Connect eine private Verbindung zu Ihrem Rechenzentrum hergestellt wird. In der folgenden Tabelle finden Sie eine Gegenüberstellung der Bandbreite und der Unterscheidungsfaktoren.

| Bereitstellungstyp | | | |
|---|---|---|---|
| **Funktionalität** | **Colo-Connect** | **ZTNA-Connector** | **Dienstverbindungen** |
| Maximale Bandbreite pro Rechenregion | 20 Gb/s | 10 Gb/s | 5 Gb/s |
| Durchsatz | Bidirektionale private Konnektivität mit 20 Gb/s zum Rechenzentrum | Bis zu 10 Gb/s pro Rechenzentrum | 1 Gb/s pro Verbindung |
| Kompatibel mit SDN/ NaaS-Anbietern wie Equinix Cross-Connect und Megaport | Ja | Nein | Nein |
| Überlappende Netzwerke in den Rechenzentren | Nein | Ja | Nein |
| Weitere Vorteile | Einfaches Onboarding in bestehende Bereitstellungen, die über Colo im Hybrid- und Multicloud-Modus arbeiten können | Vereinfachtes Onboarding privater Anwendungen in Hybrid- und Multicloud-Bereitstellungen | Unterstützt lokales Active Directory |
| Erfordert eine lokale Bereitstellung? | Nein | Ja | Nein |


©2025 Palo Alto Networks, Inc.

# Von Colo-Connect nicht unterstützte Produktmerkmale und Funktionalität

Die folgenden Produktmerkmale und die folgende Funktionalität werden von Colo-Connect nicht unterstützt:

- Konfigurieren einer Colo-Connect-Dienstverbindung als Zieldienstverbindung bei Verwendung der Datenverkehrslenkung
- IPv6-Unterstützung für den privaten App-Zugriff
- eBGP-Peering über IPv6


©2025 Palo Alto Networks, Inc.

# Anforderungen und Voraussetzungen für Prisma Access Colo-Connect

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Eine Prisma Access (Managed by Panorama)-Bereitstellung mit der Cloud Services-Plug-in-Mindestversion 4.1 und der Dataplane-Mindestversion 10.2.4<br>❑ Eine Colo-Connect-Add-on-Lizenz |

Bevor Sie mit dem Onboarding und der Konfiguration von Colo-Connect beginnen, beachten Sie die erforderlichen Informationen und Voraussetzungen in folgender Checklist.

- ❑ Stellen Sie sicher, dass Sie Zugriff auf den Colo-Dienstanbieter haben (zum Beispiel, dass Sie Zugriff auf das Equinix-Kundenportal haben).
- ❑ Stellen Sie sicher, dass Ihr CPE GRE und BGP unterstützt.

  Colo-Connect-Dienstverbindungen verwenden GRE-Tunnel.
- ❑ Entscheiden Sie, welchen Interconnect-Typ Sie für Colo-Connect verwenden möchten (Partner Interconnect- oder dedizierte Interconnect-Verbindung).
  - **Partner Interconnect** – Für Partner Interconnects ist ein Kopplungsschlüssel von Prisma Access erforderlich. Sie erhalten diesen Schlüssel während des Onboardings in Prisma Access.

    Wenn Sie eine Partner Interconnect-Verbindung erstellen, stellen Sie sicher, dass der Dienstanbieter (Service Provider, kurz SP) ein genehmigter SP mit GCP ist und die Verbindung zwischen dem SP und GCP bereits hergestellt ist.
  - **Dedizierte Interconnect-Verbindung** –
    - Bestimmen Sie den Colo-Standort, an dem das Cross-Connect-Kabel angeschlossen wird, bevor Sie mit dem Onboarding in Prisma Access beginnen. Der Colo-Standort ist erforderlich, damit Palo Alto Networks die dedizierte Verbindung bestellen kann
    - Machen Sie sich mit den grundlegenden Netzwerkverbindungen vertraut, damit Sie die Schaltkreise konfigurieren können.
    - Nachdem Sie die dedizierte Interconnect-Verbindung bereitgestellt haben, müssen Sie sie testen.
- ❑ **Subnetzanforderungen** – Bestimmen Sie die RFC-1918 IPv4-Subnetze, die Sie für jede Colo-Connect-Verbindung pro Region verwenden. Prisma Access verwendet diese Subnetze für die interne Kommunikation und Vernetzung.

  Machen Sie die Subnetze in allen Colo-Connect-Regionen eines bestimmten Mandanten einzigartig. Das Colo-Connect-Subnetz darf sich nicht mit dem Infra-Subnetz von Prisma Access und dem Pool der mobilen Benutzer überschneiden. Verwenden Sie für das Subnetz eine Mindestgröße von /28.

 ©2025 Palo Alto Networks, Inc.

- **Link (Interconnect)-Anforderungen** – Befolgen Sie diese Richtlinien bei der Konfiguration von Links:
  - Jede Colo-Connect-Add-on-Lizenz umfasst einen Link mit einer Kapazität von 10 Gbit/s. Sie benötigen mindestens zwei Links. Das heißt, dass Sie mindestens zwei Lizenzen in einer Colo-Connect-Bereitstellung erwerben müssen.
  - Binden Sie in jeder Region zwei Links ein.

    Beide Links sollten sich in verschiedenen Verfügbarkeitszonen (Edge-Domänen) befinden.
  - (Nur dedizierte Interconnect-Bereitstellungen) Wenn Sie mehr als sechs Links in einem Mandanten einbinden möchten, wenden Sie sich an Ihren Ansprechpartner oder Partner von Palo Alto Networks. Dieser wird das Site Reliability Engineering(SRE)-Team kontaktieren und eine Anfrage zur Erhöhung des Kontingents für einen bestimmten Mandanten einreichen.

- **Verbindungsanforderungen** –
  - Binden Sie in jeder Region zwei Verbindungen ein.

    Beide Verbindungen sollten sich in unterschiedlichen Edge-Domänen befinden.
  - Verbindungen im Modus Aktiv/Backup oder Aktiv/Aktiv müssen die gleiche Bandbreite haben.
  - Entscheiden Sie, ob Sie Ihre Verbindungen in einer Konfiguration mit dem Modus Aktiv/Aktiv oder Aktiv/Backup einrichten möchten.
- **Anforderungen an Colo-Connect-Dienstverbindungen** –
  - Für jede Dienstverbindung sind zwei Verbindungen erforderlich.
  - Jede Verbindung für eine bestimmte Dienstverbindung muss sich auf einem anderen Link und einer anderen Edge-Domäne befinden.
  - Notieren Sie sich die Adressen, die Sie als BGP-IP-Adresse mit colo-router und den lokalen GRE-Tunnel-IP-Adressen verwenden werden. Sie verwenden diese Adressen während der Erstellung der Dienstverbindung.
  - Die Dienstverbindungen müssen denselben Linktyp aufweisen (Partner-Interconnect-Links oder dedizierte Interconnect-Links).
- **Interoperabilität mit bestehenden IPSec-basierten Dienstverbindungen** – Palo Alto Networks empfiehlt dringend, Colo-Connect und IPSec-tunnelbasierte Dienstverbindungen in verschiedenen Regionen bereitzustellen. Darüber hinaus müssen Sie ein Wartungsfenster planen, wenn Sie von einer auf IPSec-Tunneln basierenden Dienstverbindung zu einer Colo-Connect-Dienstverbindung migrieren. Wenn Sie von einer auf IPSec-Tunneln basierenden Dienstverbindung zu einer Colo-Connect-Dienstverbindung migriert sind, entfernen Sie die IPSec-basierte Dienstverbindung, nachdem die Colo-Connect-Dienstverbindung aktiv ist und bevor das Wartungsfenster abläuft.

 ©2025 Palo Alto Networks, Inc.

# Konfigurieren von Prisma Access Colo-Connect

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Eine Prisma Access (Managed by Panorama)-Bereitstellung mit der Cloud Services-Plug-in-Mindestversion 4.1 und der Dataplane-Mindestversion 10.2.4<br>❑ Eine Colo-Connect-Add-on-Lizenz |

Prisma Access Colo-Connect besteht aus folgenden Komponenten:

- **Colo** – Die Colocation-Einrichtung, die Rack-Platz, Stromversorgung und Konnektivität zu Hostnetzwerken sowie zu privaten und öffentlichen Cloud-Infrastrukturen wie beispielsweise Equinix bietet.
- **Dedizierte Interconnect-Verbindung** – Die dedizierte physische Layer-2- und Layer-3-Verbindung zwischen Ihrem Router und einem GCP-Edge-Router in einer bestimmten GCP-Rechenregion. Eine dedizierte Interconnect-Verbindung stellt eine direkte physische Verbindung zwischen Ihrem lokalen Netzwerk und dem Google-Netzwerk her.

  In der Prisma Access-Benutzeroberfläche werden Interconnect-Verbindungen als *Links* bezeichnet.
- **GCP-VLAN-Anhang** – Die logische Layer-2-Verbindung über den Link, der den Datenverkehr von allen anderen logischen Verbindungen trennt, die denselben Link teilen.

  VLAN-Anhänge werden in der Prisma Access-Benutzeroberfläche als *Verbindungen* bezeichnet.
- **Partner Interconnect** – Die physische Layer-3-Verbindung zwischen einem Router des Dienstanbieters und einem GCP-Edge-Router in einer bestimmten GCP-Rechenregion. Eine Partner Interconnect-Verbindung stellt die Konnektivität zwischen Ihren lokalen Netzwerken und VPC-Netzwerken über einen unterstützten Dienstanbieter bereit.

  Colo-Connect unterstützt sowohl dedizierte Interconnect-Verbindungen als auch Partner Interconnect-Verbindungen.
- **Colo-Router (Kunde)** – Das Routing-Gerät in der Colo-Einrichtung, das eBGP mit dem GCP-Cloud-Router über die Interconnect-Verbindung in der Colo-Einrichtung sowie eBGP mit einer Colo-Connect-Dienstverbindung über den GRE-Tunnel herstellt. Es handelt sich um einen Kundenrouter für eine dedizierte Interconnect-Verbindung. Wenn der Dienstanbieter über Layer-2-Konnektivität mit GCP verfügt, wird die Verbindung über Partner Interconnect hergestellt. Der Dienstanbieter ist der Eigentümer des Colo-Routers, wenn er über Layer-3-Konnektivität zum GCP-Cloud-Router verfügt.
- **GCP Edge-Router** – Das Netzwerk-Edge-Equipment von GCP dient zur Bereitstellung physischer Konnektivität zwischen GCP und dem Kunden-/Partnernetzwerk über das Colo.
- **Cloud-Router** – Das GCP-Softwarekonstrukt in der Cloud, das BGP-Sitzungen mit dem Netzwerkgerät (z. B. Router oder Layer-3-Firewall) im Colo einrichtet und den Datenverkehr zwischen Prisma Access und Ihrem Netzwerk routet. Sie müssen diese Komponente nicht konfigurieren; dieser Arbeitsschritt wird von Prisma Access automatisch durchgeführt.

 ©2025 Palo Alto Networks, Inc.

Um Colo-Connect zu konfigurieren, müssen Sie zunächst Informationen über Ihre bestehende Netzwerkumgebung sammeln und sicherstellen, dass Sie alle erforderlichen Netzwerkkomponenten installiert haben. Vergewissern Sie sich, dass alle Voraussetzungen erfüllt sind, und stellen Sie Colo-Connect dann entweder über eine Partner Interconnect-Verbindung oder eine dedizierte Interconnect-Verbindung im Netzwerk Ihres Unternehmens bereit.

- Strata Cloud Manager
- Panorama

# Konfigurieren von Prisma Access Colo-Connect (Strata Cloud Manager)

Um Colo-Connect zu konfigurieren, müssen Sie zunächst Informationen über Ihre bestehende Netzwerkumgebung sammeln und sicherstellen, dass Sie über alle erforderlichen Netzwerkkomponenten verfügen. Stellen Sie sicher, dass Sie alle Voraussetzungen erfüllen. Anschließend können Sie Colo-Connect im Netzwerk Ihrer Organisation entweder über eine Partner Interconnect-Verbindung oder eine dedizierte Interconnect-Verbindung bereitstellen.

## Konfigurieren Sie Prisma Access Colo-Connect-Bereitstellungen mit Partner Interconnect-Verbindungen.

Um Prisma Access Colo-Connect über eine Partner Interconnect-Verbindung zu konfigurieren, müssen Sie die folgenden Schritte ausführen.

**STEP 1 |** Erstellen Sie Subnetze für Ihre Colo-Connect-Verbindungen.

Sie verwenden die Subnetze, die Sie hier erstellen, in den Verbindungen und Dienstverbindungen, die Sie in späteren Schritten erstellen.

1. Rufen Sie in Strata Cloud Manager **Workflows** > **Einrichtung Prisma Access** > **Colo-Connect** auf.
2. Wählen Sie **Präfix hinzufügen** aus und fügen Sie einem Colo-Connect-Subnetz einen Prisma Access-Standort dafür hinzu.

   Eine Liste der unterstützten Colo-Connect-Standorte finden Sie hier. Verwenden Sie für das Subnetz eine Mindestgröße von /28.
3. (Optional) Wenn Sie planen, Colo-Connect-Instanzen für mehrere Standorte zu erstellen, fügen Sie für jeden Standort weitere Subnetze hinzu.

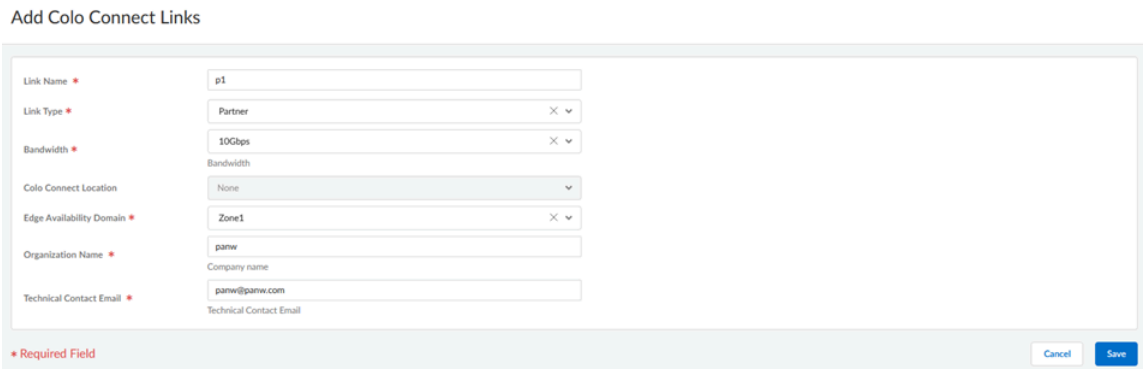
   Sie können ein Subnetz pro Standort konfigurieren.




 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Fügen Sie einen neuen Colo-Connect-Link hinzu (auch bekannt als *Interconnect*).

1. Wählen Sie **Workflows** > **Einrichtung Prisma Access** > **Colo-Connect** und **Link hinzufügen** aus.
2. Ordnen Sie dem Link einen eindeutigen **Linknamen** zu.
3. Wählen Sie **Partner** Interconnect als **Linktyp** aus.
4. Geben Sie die verbleibenden Colo-Connect-Linkparameter an.
   - Wählen Sie entweder **10 Gb/s** oder **20 Gb/s** als **Bandbreite** aus.
   - Wählen Sie entweder **Zone1** oder **Zone2** als **Edge-Verfügbarkeitsdomäne** aus. Entnehmen Sie diesen Wert der GCP-Zone, die für Ihre Edge-Verfügbarkeitsdomäne verwendet wird.
   - Geben Sie den **Namen der Organisation** ein, der für diesen Link verwendet werden soll.
   - Geben Sie die **E-Mail-Adresse** ein, die für diesen Link verwendet werden soll. Jede E-Mail-Adresse ist akzeptabel.




5. Wiederholen Sie die Schritte 2.a bis 2.d und erstellen Sie einen weiteren Link mit einer unterschiedlichen **Edge-Verfügbarkeitsdomäne**.

**STEP 3 |** Erstellen Sie die Verbindungen (auch bekannt als *VLAN-Anhänge*) für Colo-Connect.

1. Wählen Sie **Workflows** > **Einrichtung Prisma Access** > **Colo-Connect** und **Verbindung hinzufügen** aus.
2. Konfigurieren Sie die Verbindungseinstellungen.
   - Geben Sie einen eindeutigen **Verbindungsnamen** ein.
   - Wählen Sie aus den von Ihnen in einem vorangegangen Schritt konfigurierten Links einen **Linknamen** aus.

     Sie müssen keine **VLAN-ID** eingeben. Eine Konfiguration für VLANs, die über Partner Interconnect-Verbindungen erstellt wurden, ist nicht möglich.
   - Wählen Sie eine **Bandbreite** für die Verbindung aus.

     Sie können zwischen **1 Gb/s**, **2 Gb/s**, **5 Gb/s**, **10 Gb/s** oder **20 Gb/s** wählen.

     Wenn Sie für eine Interconnect-Verbindung mehrere Verbindungen konfigurieren, stellen Sie sicher, dass die Gesamtbandbreite der Verbindungen die Bandbreite der Interconnect-Verbindung nicht überschreitet. Beispiel: Für eine Partner Interconnect-Verbindung mit 10 Gb/s können Sie 10 Verbindungen mit jeweils 1 Gb/

 ©2025 Palo Alto Networks, Inc.

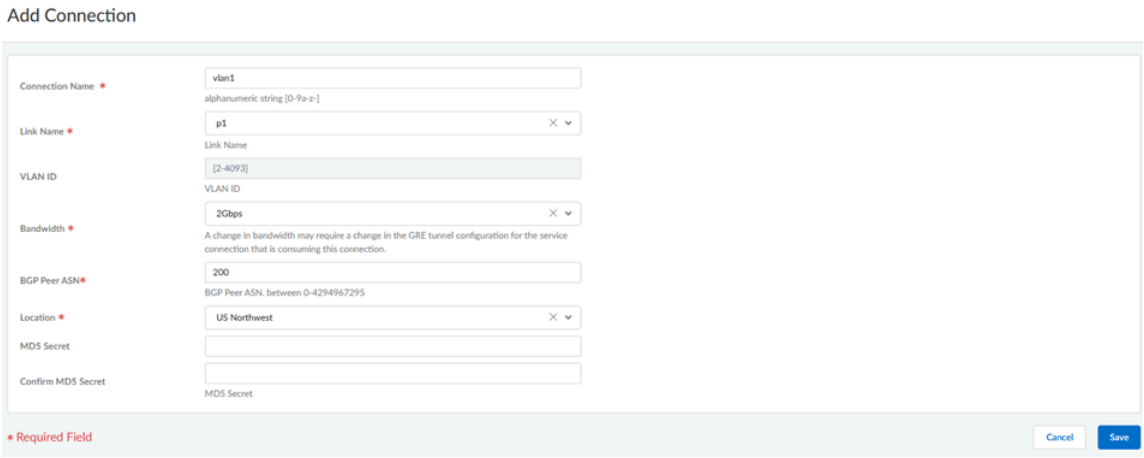
s konfigurieren, der Gesamtwert von insgesamt 10 Gb/s für alle Verbindungen darf jedoch nicht überschritten werden.

> *Wenn Ihre Bereitstellung mehr als 16 Verbindungen erfordert, wenden Sie sich an Ihr Palo Alto Networks-Account-Team, das einen SRE-Fall eröffnen wird, um die Anfrage zu bearbeiten.*

- Geben Sie eine **BGP-Peer-ASN** ein.

  Geben Sie die AS-Nummer (Autonomous System) für den Router des Kunden vor Ort im Colo ein. Der Bereich liegt zwischen 1 und 4294967295.
- Wählen Sie den **Standort** aus den Verbindungsnamen aus, die Sie in einem vorherigen Schritt erstellt haben.

  Sie müssen bereits ein Subnetz für alle von Ihnen angegebenen Standorte hinzugefügt haben.
- (Optional) Geben Sie den **Geheimen MD5-Schlüssel** für das BGP ein.




3. Fahren Sie mit der Erstellung von Verbindungen fort, bis alle erforderlichen Verbindungen erstellt wurden.

   Erstellen Sie zwei Verbindungen. Beide Verbindungen müssen sich in derselben Region befinden, und eine Verbindung muss sich in einer separaten Zone befinden. Sie verwenden diese Verbindungen in Dienstverbindungen, die Sie in einem späteren Schritt erstellen werden.

**STEP 4 |** Wählen Sie **Konfiguration übertragen** aus.

Aktualisieren Sie den Browser, nachdem der Commit-Job abgeschlossen ist, um die Kopplungsschlüssel unter **Verbindungen** anzuzeigen.

**STEP 5 |** Rufen Sie den**Kopplungsschlüssel** ab und schließen Sie Ihre Partner Interconnect-Konfiguration in GCP ab.

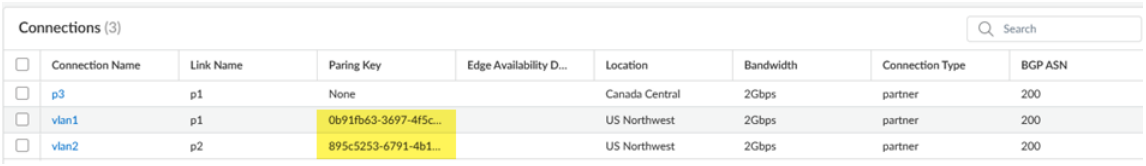
Sie verwenden diesen Kopplungsschlüssel, wenn Sie die Partner Interconnect-Verbindung im Colo einrichten.

Wenn Sie eine neue Verbindung zum ersten Mal einbinden, zeigt der **Status** im Bereich **Verbindungen** den **Status PENDING_PARTNER** und den **BGP-Status INAKTIV** an. Um den

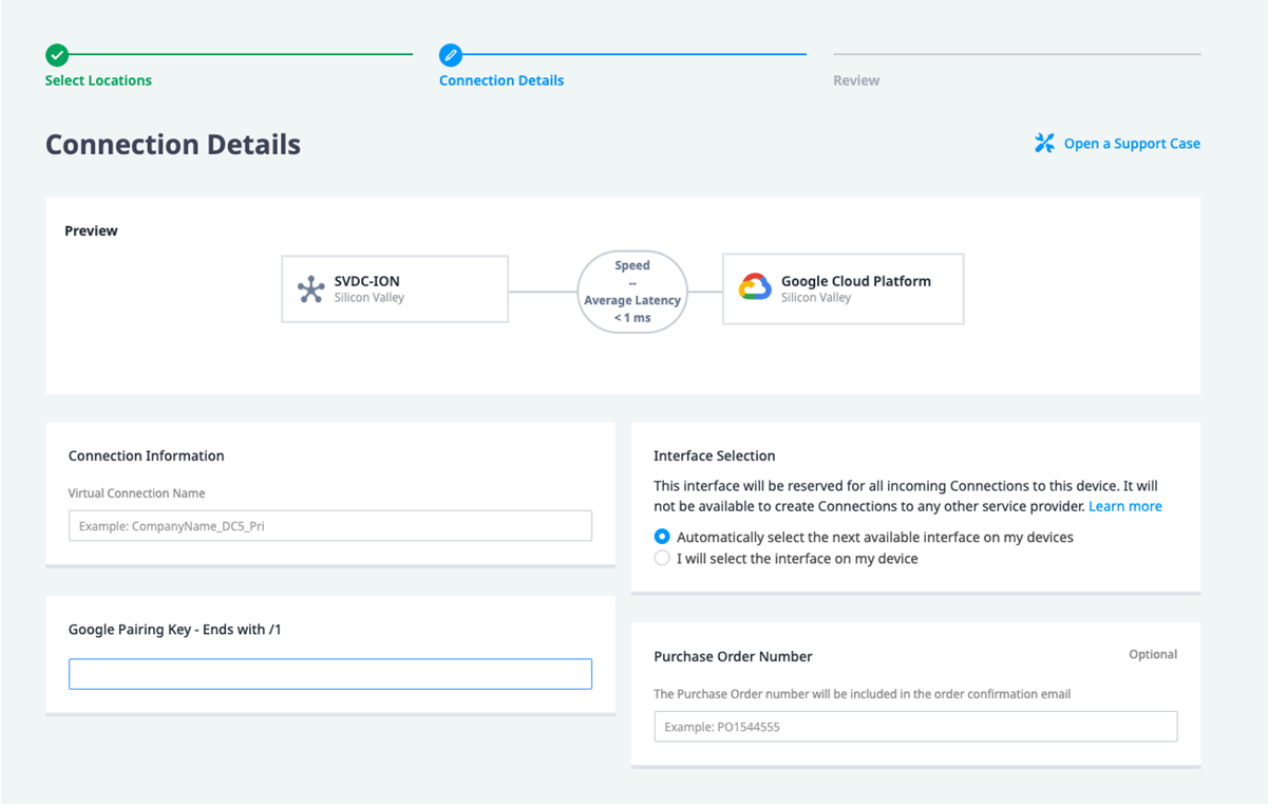
 ©2025 Palo Alto Networks, Inc.

Verbindungsstatus wieder auf **AKTIV** zu setzen, rufen Sie den Kopplungsschlüssel ab und geben Sie ihn in die Verbindung im Colo ein.

1. Wählen Sie **Workflows** > **Einrichtung Prisma Access** > **Colo-Connect** > **Verbindungen** aus und kopieren Sie den **Kopplungsschlüssel**.




2. Erstellen Sie eine neue VLAN-Verbindung im Colo.




3. Fügen Sie den Kopplungsschlüssel in das Colo-VLAN ein.

   GCP erkennt, wenn der Kopplungsschlüssel verarbeitet wird, setzt den VLAN-Status auf **AKTIV** und generiert die BGP-IP-Adresse, die Sie auf Ihrem lokalen Router im Colo konfigurieren können. Prisma Access verwendet diese IPs, um die eBGP-Nachbarschaft über jedes zugehörige VLAN zwischen dem Colo-Router und dem GCP-Cloud-Router zu initiieren.

**STEP 6 |** Erstellen Sie das eBGP-Routing auf dem Kundenrouter (Colo) für die Colo-Connect-Verbindung.

Sie müssen das BGP-Peering einrichten, um die Konnektivität zwischen dem Kundenrouter und dem Cloud-Router sicherzustellen.

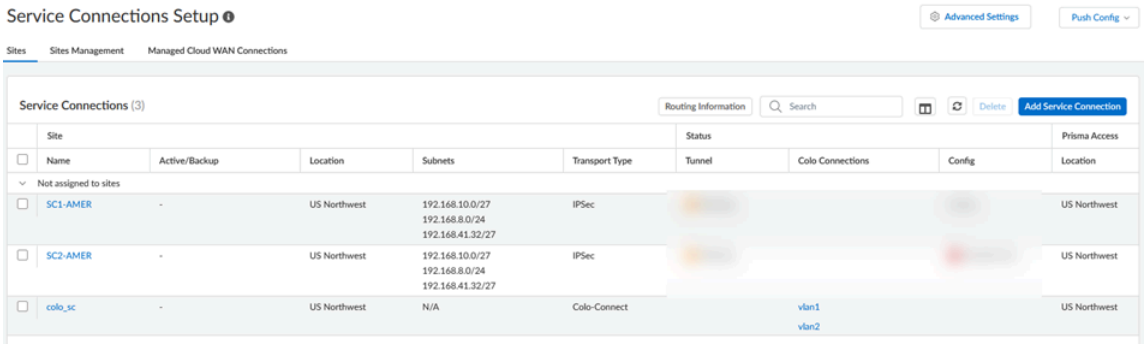
**STEP 7 |** Richten Sie die Dienstverbindungen ein, die Sie mit Colo-Connect verwenden möchten.

**STEP 8 |** Wählen Sie **Konfiguration übertragen** aus.

 ©2025 Palo Alto Networks, Inc.

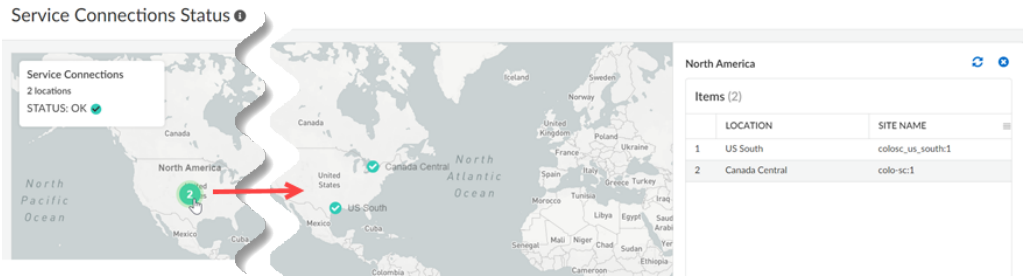
**STEP 9 |** Überprüfen Sie den Status der Colo-Connect-Verbindungen.

1. Um den Status einer von einer Colo-Connect-Verbindung verwendeten Dienstverbindung zu überprüfen, wählen Sie **Workflows** > **Einrichtung Prisma Access** > **Dienstverbindung** aus.




2. Wählen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** aus. Legen Sie für den **Konfigurationsumfang** die Einstellung **Prisma Access** fest. Wählen Sie den Status **Synchron** der **Dienstverbindungen** unter dem Prisma Access-Synchronisierungsstatus aus. Wählen Sie die Region aus, in der eine Colo-Connect-Verbindung bereitgestellt wurde.

   - Wenn die Colo-Connect-Verbindung und das BGP-Routing beide aktiv sind, wird der Status **OK** angezeigt.
   - Wenn die Colo-Connect-Verbindung aktiv ist, das BGP-Routing jedoch nicht, wird der Status **Warnung** angezeigt.
   - Wenn die Colo-Connect-Verbindung und das BGP-Routing beide inaktiv sind, wird der Status **INAKTIV** angezeigt.
   - Wenn die Colo-Connect-Verbindung inaktiv ist, das BGP-Routing jedoch aktiv, wird der Status **Fehler** angezeigt.




3. Zum Aufrufen weiterer Informationen klicken Sie auf das Regionsfeld und lesen sie die Informationen auf der Registerkarte **Status**.

**STEP 10 |** Überprüfen Sie die Verbindungsdetails der Colo-Connect-Verbindungen (einschließlich des Kopplungsschlüssels), indem Sie **Workflows** > **Einrichtung Prisma Access** > **Colo-Connect** auswählen.

## Konfigurieren Sie die Prisma Access Colo-Connect-Bereitstellungen mit dedizierten Interconnect-Verbindungen.

Um Prisma Access Colo-Connect über eine dedizierte Interconnect-Verbindung zu konfigurieren, müssen Sie die folgenden Schritte ausführen.

 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** Erstellen Sie Subnetze für Ihre Colo-Connect-Verbindungen.

Sie verwenden die Subnetze, die Sie hier erstellen, in den Verbindungen und Dienstverbindungen, die Sie in späteren Schritten erstellen.

1. Rufen Sie in Strata Cloud Manager **Workflows** > **Einrichtung Prisma Access** > **Colo-Connect** auf und klicken Sie dann auf das Zahnradsymbol, um die Einstellungen zu bearbeiten.
2. **Fügen Sie das Präfix** für das **Colo-Connect-Subnetz** hinzu und wählen Sie einen Prisma Access-Standort (**PA-Standort**) dafür aus.

   Verwenden Sie für das Subnetz eine Mindestgröße von /28.
3. (Optional) Wenn Sie die Erstellung von Colo-Connect-Instanzen für mehrere Standorte planen, fügen Sie für jeden Standort weitere Subnetze hinzu.

   Sie können nur ein Subnetz pro Standort konfigurieren.

**STEP 2 |** Fügen Sie einen neuen Colo-Connect-Link hinzu (auch bekannt als *Interconnect*).

1. Wählen Sie **Workflows** > **Einrichtung Prisma Access** > **Colo-Connect** und **Link hinzufügen** aus.
2. Ordnen Sie dem Link einen eindeutigen **Linknamen** zu.
3. Wählen Sie eine **dedizierte** Interconnect-Verbindung als **Linktyp** aus.
4. Geben Sie die verbleibenden Colo-Connect-Linkparameter an.
   - Wählen Sie entweder **10 Gb/s** oder **20 Gb/s** als **Bandbreite** aus.

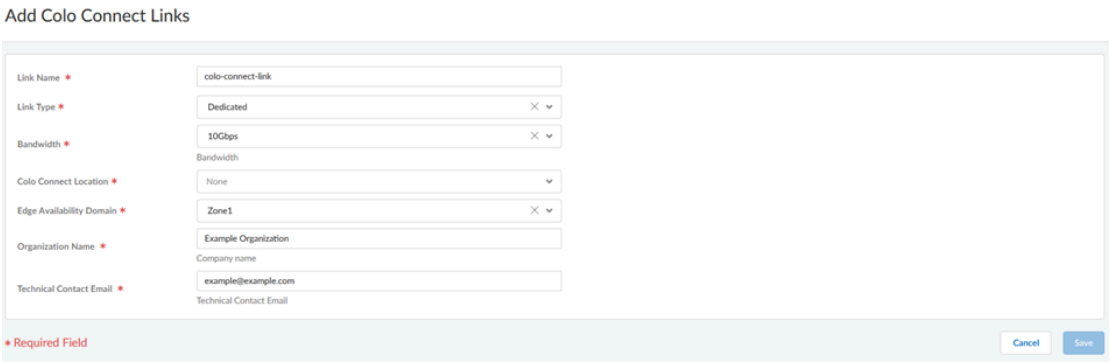
     *Wenn Sie 20 Gb/s auswählen, müssen Sie die dedizierte Interconnect-Verbindung zu zwei 10-Gb/s-Links zusammenfassen. Verwenden Sie dazu* LACP.

     Sie können die Bandbreite eines dedizierten Interconnect-Links nicht ändern, nachdem Sie sie festgelegt und Ihre Änderungen festgeschrieben und übertragen haben.
   - Wählen Sie einen **Colo-Connect-Standort** in der Dropdown-Liste aus.

     Stellen Sie sicher, dass Sie denselben Standort auswählen, den Sie für die dedizierte Interconnect-Verbindung verwendet haben.
   - Wählen Sie entweder **Zone1** oder **Zone2** als **Edge-Verfügbarkeitsdomäne** aus. Entnehmen Sie diesen Wert der GCP-Zone, die für Ihre Edge-Verfügbarkeitsdomäne verwendet wird.
   - Geben Sie den **Namen der Organisation** ein, der für diesen Link verwendet werden soll.
   - Geben Sie die **E-Mail-Adresse** ein, an die Sie die LOA-CFA-Details vom Cloud-Anbieter erhalten möchten.
     - GCP verwendet diese E-Mail, um das LOA-CFA (Letter of Authorization and Connecting Facility Assignment) zu senden. Stellen Sie sicher, dass das LOA-

 ©2025 Palo Alto Networks, Inc.

CFA an Ihren Colo-Anbieter gesendet wird, damit er mit der Installation Ihrer Verbindungen beginnen kann.



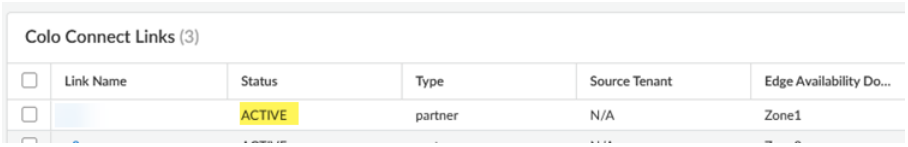

**STEP 3 |** Nachdem die dedizierte Verbindung hergestellt ist, führt die Colo-Einrichtung Tests für Ihre Verbindungen durch und informiert Sie darüber, dass die Tests durchgeführt wurden und die Verbindungen nun benutzt werden können.

Für diesen Schritt sind keine Prisma Access-Konfigurationen erforderlich. Erstellen Sie die Colo-Connect-Verbindungen nicht in Prisma Access, bis die Colo-Einrichtung Ihnen mitteilt, dass sie getestet wurden.

**STEP 4 |** Erstellen Sie die Verbindungen (auch bekannt als *VLAN-Anhänge*) für Colo-Connect.

1. Stellen Sie sicher, dass der dedizierte Linkstatus „Aktiv“ lautet. Rufen Sie hierzu **Workflows** > **Einrichtung Prisma Access** > **Colo-Connect** > **Colo-Connect-Links** auf.

   Bis der Status des dedizierten Links „Aktiv“ ist, können Sie keine Colo-Connect-Links erstellen.

2. Wählen Sie **Workflows** > **Einrichtung Prisma Access** > **Colo-Connect** und **Verbindung hinzufügen** aus.
3. Konfigurieren Sie die Verbindungseinstellungen.
   - Geben Sie einen eindeutigen **Namen** für die Verbindung ein.
   - Wählen Sie einen **Linknamen** aus den Links aus, die Sie in einem vorherigen Schritt konfiguriert haben.
   - (Optional) Geben Sie eine **VLAN-ID** für die Verbindung ein.

     VLAN-IDs werden vom Interconnect-Anbieter (GCP) generiert, wenn Sie manuell keinen Wert eingeben.
   - Wählen Sie eine **Bandbreite** für die Verbindung aus.

     Sie können zwischen **1 Gb/s**, **2 Gb/s**, **5 Gb/s**, **10 Gb/s** oder **20 Gb/s** wählen.

     Wenn Sie für eine Interconnect-Verbindung mehrere Verbindungen konfigurieren, stellen Sie sicher, dass die Gesamtbandbreite der Verbindungen die Bandbreite der Interconnect-Verbindung nicht überschreitet. Beispiel: Für eine dedizierte Interconnect-Verbindung mit 20 Gb/s können Sie 10 Verbindungen mit jeweils 2 Gb/

 ©2025 Palo Alto Networks, Inc.

s konfigurieren, der Gesamtwert von insgesamt 20 Gb/s für alle Verbindungen darf jedoch nicht überschritten werden.

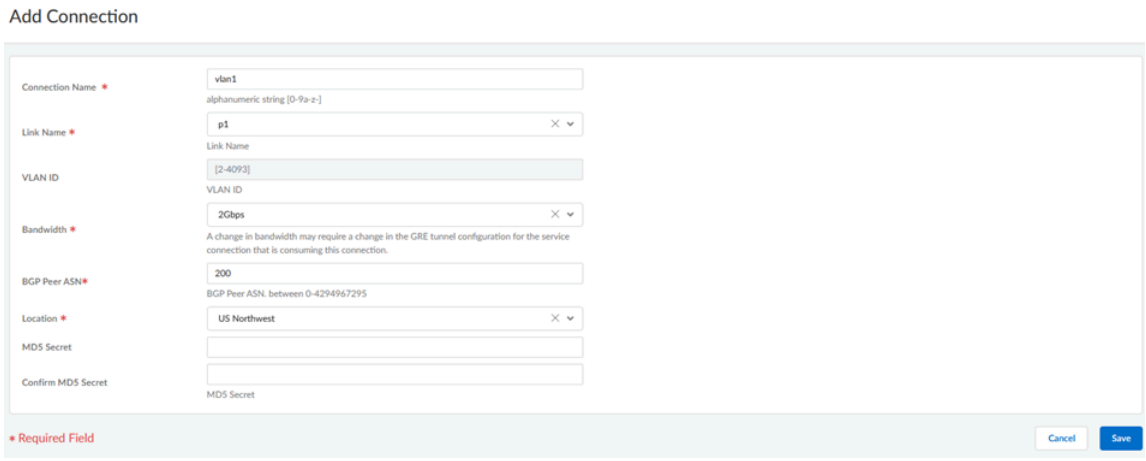
- Geben Sie eine **BGP-Peer-ASN** ein.

  Geben Sie die AS-Nummer (Autonomous System) für den Router des Kunden vor Ort im Colo ein. Der Bereich liegt zwischen 1 und 4294967295.

- Wählen Sie den **Standort** aus den Verbindungsnamen aus, die Sie in einem vorherigen Schritt erstellt haben.

  Sie müssen bereits ein Subnetz für alle von Ihnen angegebenen Standorte hinzugefügt haben.

- (Optional) Geben Sie den **Geheimen MD5-Schlüssel** für das BGP ein.




4. Fahren Sie mit der Erstellung von Verbindungen fort, bis alle erforderlichen Verbindungen erstellt wurden.

   Erstellen Sie zwei Verbindungen. Beide Verbindungen müssen sich in derselben Region befinden, und eine Verbindung muss sich in einer separaten Zone befinden. Sie verwenden diese Verbindungen in Dienstverbindungen, die Sie in einem späteren Schritt erstellen werden.

**STEP 5 |** Wählen Sie **Konfiguration übertragen** aus.

**STEP 6 |** Konfigurieren Sie das eBGP-Routing auf dem Kundenrouter.

Sie müssen das BGP-Peering einrichten, um die Konnektivität zum Kundenrouter sicherzustellen.

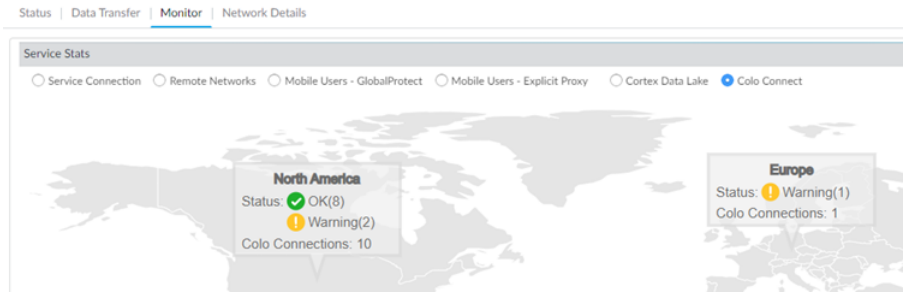
**STEP 7 |** Richten Sie die Dienstverbindungen ein, die Sie mit Colo-Connect verwenden möchten.

**STEP 8 |** Verwenden Sie **Commit und Push**, um Ihre Konfigurationsänderungen festzuschreiben und zu übertragen. Vergewissern Sie sich dabei, dass **Colo-Connect** im **Übertragungsumfang** ausgewählt wurde.


©2025 Palo Alto Networks, Inc.

**STEP 9 |** Überprüfen Sie den Status der Colo-Connect-Verbindungen.

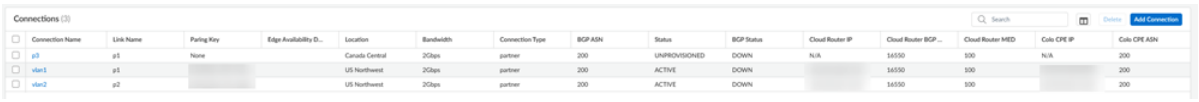
1. Um den Status einer Dienstverbindung zu überprüfen, die von einer Colo-Connect-Verbindung benutzt wird, wählen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** aus. Legen Sie für den **Konfigurationsumfang** die Einstellung **Prisma Access** fest.
2. Bewegen Sie den Mauszeiger über eine Region, in der eine Colo-Connect-Verbindung bereitgestellt wurde.
   - Wenn die Colo-Connect-Verbindung und das BGP-Routing beide aktiv sind, wird der Status **OK** angezeigt.
   - Wenn die Colo-Connect-Verbindung aktiv ist, das BGP-Routing jedoch nicht, wird der Status **Warnung** angezeigt.
   - Wenn die Colo-Connect-Verbindung und das BGP-Routing beide inaktiv sind, wird der Status **INAKTIV** angezeigt.
   - Wenn die Colo-Connect-Verbindung inaktiv ist, das BGP-Routing jedoch aktiv, wird der Status **Fehler** angezeigt.




3. Zum Aufrufen weiterer Informationen klicken Sie auf das Regionsfeld und lesen sie die Informationen auf der Registerkarte **Status**.

**STEP 10 |** Überprüfen Sie die Netzwerkinformationen der Colo-Connect-Verbindungen, indem Sie **Workflows** > **Einrichtung Prisma Access** > **Colo-Connect** > **Verbindungen** auswählen und dann die Details anzeigen.

Für dedizierte Links wird für den **Kopplungsschlüssel** der Wert **n. a.** angezeigt.



## Konfigurieren Sie das VLAN-eBGP-Routing auf dem Kundenrouter.

GCP erstellt während dieser Phasen Ihrer Bereitstellung IP-Adressen für den Kundenrouter (Colo-Router) und den Cloud-Router:

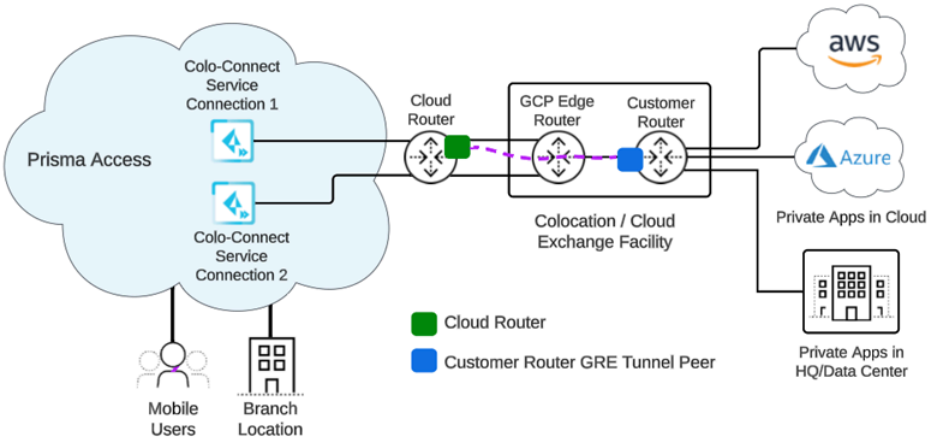
- Für Partner Interconnect-Verbindungen erstellt GCP die IP-Adressen, nachdem der Kopplungsschlüssel von Ihrem Colo (zum Beispiel Equinix) verarbeitet wurde.
- Für dedizierte Interconnect-Verbindungen erstellt GCP die IP-Adressen, nachdem Sie Ihre Colo-Connect-Verbindungen (VLAN-Anhänge) eingebunden und Ihre Änderungen festgeschrieben und übertragen haben.

Um ein korrektes Routing sicherzustellen, müssen Sie wie folgt vorgehen:

 ©2025 Palo Alto Networks, Inc.

- Konfigurieren Sie die IP-Adresse des Colo-Routers (die **Colo-CPE-IP** in Prisma Access) als die lokale eBGP-IP-Adresse
- Konfigurieren Sie die IP-Adresse des Cloud-Routers (**Cloud-Router-IP**) als die eBGP-Peer-Adresse auf Ihrem Colo-Router.

Nach Abschluss dieses Schrittes ist eBGP für die Verbindung (VLAN-Anhang) zwischen dem Colo-Router und dem Cloud-Router konfiguriert.




Das Erstellen dieses Routings ist der erste Schritt zur Einrichtung des GRE-Tunnel-Routings. Sie vervollständigen das GRE-Tunnel-Routing, wenn Sie die GRE-Tunnel während der Konfiguration der Dienstverbindung einrichten.

Führen Sie die folgenden Schritte aus, um das Routing zwischen dem Colo und dem Cloud-Router zu konfigurieren.

**STEP 1 |** Erstellen Sie in Strata Cloud Manager die Subnetze, Links und Verbindungen und wählen Sie dann **Konfiguration übertragen** aus.

Verwenden Sie den Workflow, der speziell für Ihren Interconnect-Typ definiert ist (entweder Partner oder Dediziert). Für Partner Interconnect-Verbindungen müssen Sie sich vergewissern, dass der Kopplungsschlüssel in das Colo-VLAN eingefügt wurde.

**STEP 2 |** Wählen Sie **Workflows** > **Einrichtung Prisma Access** > **Colo-Connect** > **Verbindungen** aus.

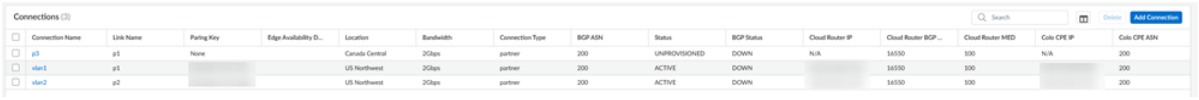
 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Notieren Sie die folgenden Verbindungselemente:

- **Colo-CPE-IP**
- **Cloud-Router-IP**
- **Cloud-Router-BGP-ASN**

Im folgenden Beispiel:

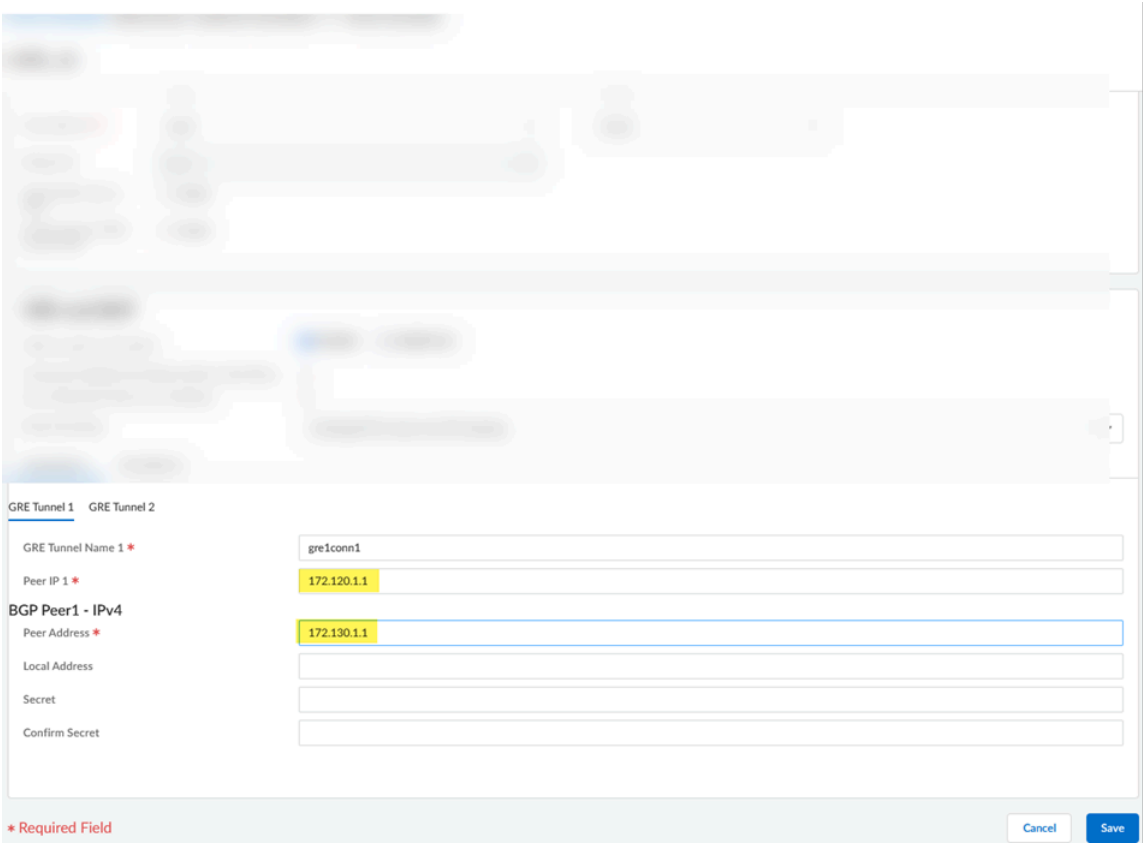
- Für die vlan-central-1-Verbindung lautet die **Colo-CPE-IP** 169.254.24.170/29, die **Cloud-Router-IP** ist 169.254.24.169/29 und als **Cloud-Router-BGP-ASN** ist 16550 angegeben
- Für die vlan-central-2-Verbindung lautet die **Colo-CPE-IP** 169.254.120.74/29, die **Cloud-Router-IP** ist 169.254.120.73/29 und als **Cloud-Router-BGP-ASN** ist 16550 angegeben.
- .




 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** Bestimmen Sie die IP-Adressen, die Sie für die lokalen GRE-IP-Adressen verwenden werden, wenn Sie die Colo-Connect-Dienstverbindungen einrichten.

Sie konfigurieren diese, wenn Sie eine Colo-Connect-Dienstverbindung (**Workflows** > **Einrichtung Prisma Access** > **Dienstverbindungen**) einrichten. In den Bereichen **Peer-IP 1** und ggf. **Peer-IP 2**.




Wenn Sie eine Dienstverbindung konfigurieren, um bis zu 10 Gb/s Durchsatz zu unterstützen, definieren Sie jeweils einen Tunnel in **Verbindung 1**und einen in **Verbindung 2**, insgesamt also zwei Tunnel in jeder Dienstverbindung.

Wenn Sie eine Dienstverbindung konfigurieren, um mehr als 10 Gb/s Durchsatz (bis zu 20 Gb/s) zu unterstützen, definieren Sie jeweils zwei Tunnel in **Verbindung 1**und **Verbindung 2**, insgesamt also vier Tunnel in jeder Dienstverbindung.

Die folgenden Beispiele zeigen, wie ein Tunnel für mehr als 10 Gb/s Durchsatz konfiguriert wird, sodass zwei Tunnel pro Verbindung verwendet werden, die die folgenden Peer-IP-Adressen benutzen:

- 172.120.1.1 für Verbindung 1
- 172.130.1.1 für Verbindung 1
- 172.121.1.1 für Verbindung 2
- 172.131.1.1 für Verbindung 2

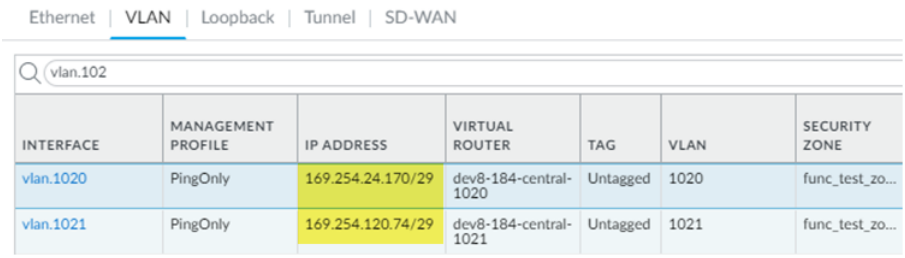
 ©2025 Palo Alto Networks, Inc.

**STEP 5 |** Melden Sie sich beim Colo-Router an.

In den folgenden Konfigurationsscreenshots wird eine Palo Alto Networks Next-Generation-Firewall als Colo-Router eingesetzt.

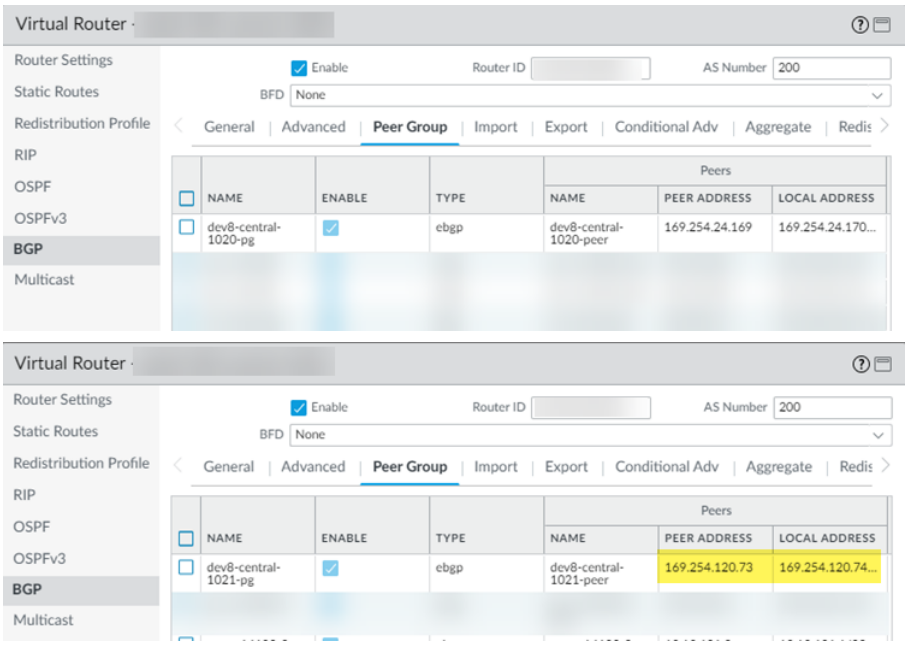
**STEP 6 |** Fügen Sie ein VLAN-Interface hinzu und geben Sie die **Colo-CPE-IP**-Adresse als IP-Adresse an.

Wenn Sie eine Next-Generation-Firewall als Colo-Router verwenden, dann wählen Sie **Netzwerk** > **Schnittstellen** > **VLAN** und **Hinzufügen** für die VLAN-Schnittstelle aus und geben Sie den Namen für den **Virtuellen Router** an.




**STEP 7 |** Konfigurieren Sie die Colo-Router-IP-Adresse (**Colo-CPE-IP**) als lokale eBGP-IP-Adresse und konfigurieren Sie die Cloud-Router-IP-Adresse (**Cloud-Router-IP**) als eBGP-Peer-Adresse auf Ihrem Colo-Router.

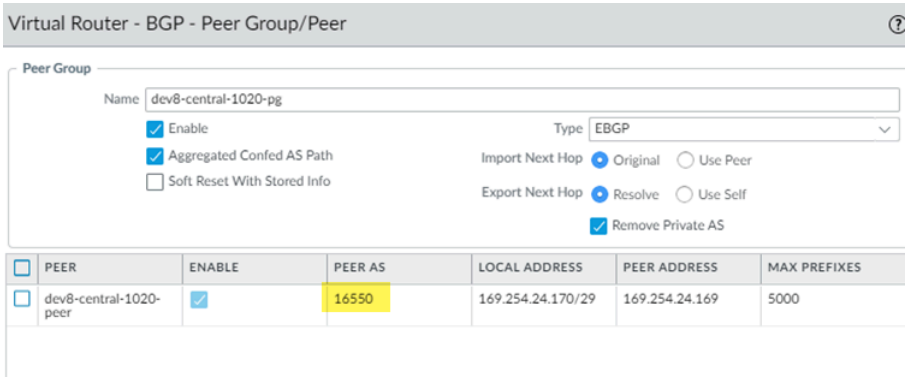
Wenn Sie eine Next-Generation-Firewall als Colo-Router verwenden, wählen Sie **Netzwerk** > **Virtuelle Router**, **Hinzufügen** für einen virtuellen Router aus. Wählen Sie anschließend **BGP** > **Peer-Gruppe** aus und geben Sie die **Colo-CPE-IP** als **Peer-Adresse** und die **Cloud-Router-IP** als **lokale Adresse** ein.




 ©2025 Palo Alto Networks, Inc.

**STEP 8 |** Konfigurieren Sie die **Cloud-Router-BGP-ASN** als die eBGP-Peer-ASN (Autonomous-System-Nummer).

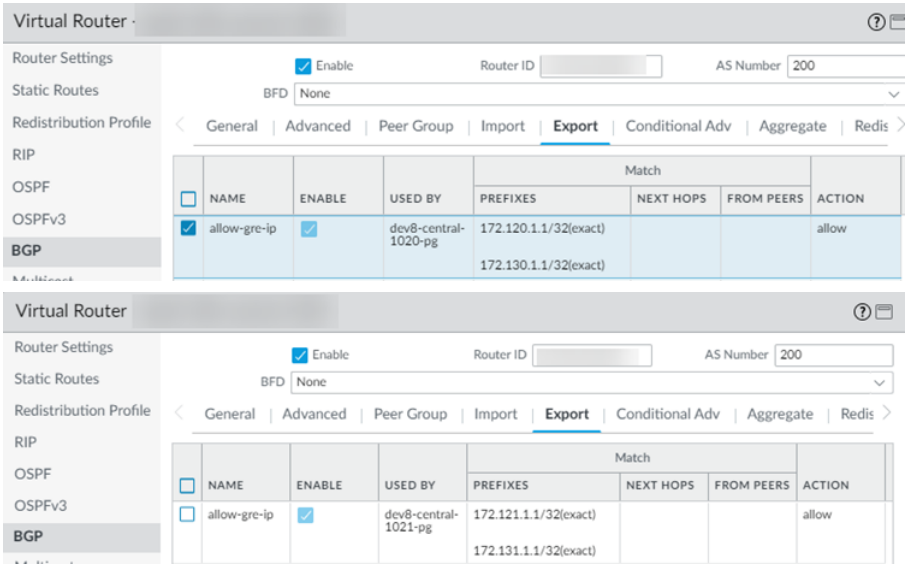
Wenn Sie eine Next-Generation-Firewall als Colo-Router verwenden, wählen Sie **Netzwerk** > **Virtuelle Router**, **Hinzufügen** für einen virtuellen Router aus. Wählen Sie anschließend **BGP** > **Peer-Gruppe** aus und **fügen Sie** eine Peer-Gruppe hinzu und wählen Sie ein **Peer-AS** mit dem Wert **16500** aus.




**STEP 9 |** Erstellen Sie eine BGP-Exportrichtlinie, mit der nur die lokale GRE-IP-Adresse an die Peer-IP-Adresse des Cloud-Routers mitgeteilt werden kann.

Da Cloud-Router nur eine begrenzte Anzahl von Routen empfangen können, müssen Sie Richtlinien erstellen, damit nur das Routing zwischen den IP-Adressen für die GRE-Tunnel der Dienstverbindung an den Cloud-Router gesendet wird.

Wenn Sie eine Next-Generation-Firewall als Colo-Router verwenden, wählen Sie **Netzwerk** > **Virtuelle Router**, **Hinzufügen** für einen virtuellen Router aus. Wählen Sie dann **BGP** > **Exportieren**, **Hinzufügen** für eine Exportregel aus und führen Sie einen **Abgleich** der IP-Adressen durch, die als Peer-IP-Adresse verwendet werden können. Erstellen Sie dann die **Aktion** des Typs **Zulassen**.




**STEP 10 |** Erstellen Sie die Colo-Connect-Dienstverbindungen.

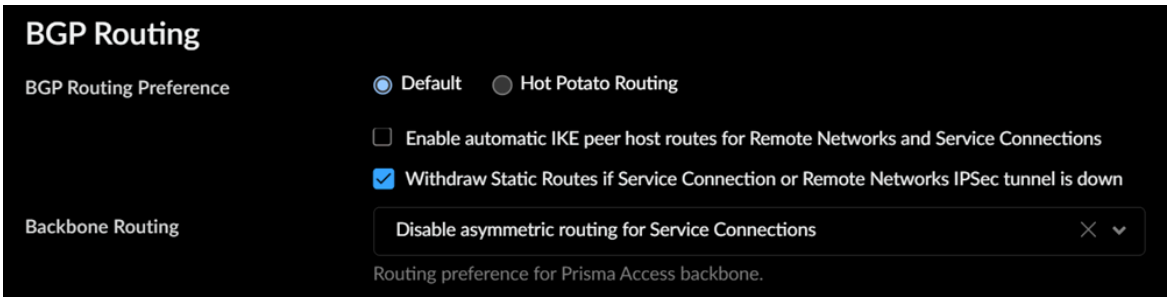
 ©2025 Palo Alto Networks, Inc.

## Erstellen Sie Colo-Connect-Dienstverbindungen

Colo-Connect verwendet Dienstverbindungen, die sich jedoch von Prisma Access-Dienstverbindungen dahingehend unterscheiden, dass sie anstelle von IPSec-Tunnel GRE-Tunnel und für das Routing immer BGP verwenden. Um Colo-Connect-Dienstverbindungen zu konfigurieren, führen Sie die folgenden Schritte aus.

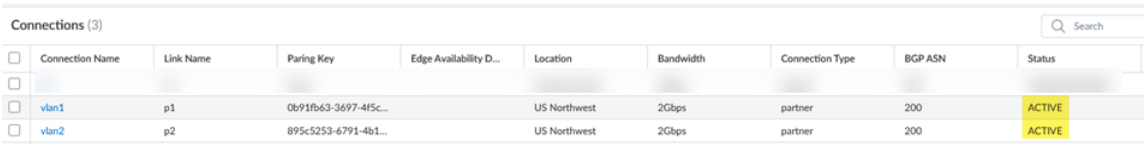
**STEP 1 |** Vergewissern Sie sich, dass Prisma Access statische Routen zurückzieht. Wählen Sie hierzu **Workflows** > **Einrichtung Prisma Access** > **Dienstverbindungen** > **Erweiterte Einstellungen** und dann **Statische Routen zurückziehen, wenn die Dienstverbindung oder der IPSec-Tunnel für Remote-Netzwerke ausgefallen ist** aus.

Die Auswahl dieser Option stellt sicher, dass bei Ausfall des GRE-Tunnels die vom GRE-Tunnel verwendete statische Route zurückgezogen wird.




**STEP 2 |** Wählen Sie die Registerkarte **Workflows** > **Einrichtung Prisma Access** > **Colo-Connect** > **Verbindungen** aus und vergewissern Sie sich, dass die Verbindungen den Status **Aktiv** aufweisen, indem sie ihren **Status** überprüfen.

Bis der **Status** der Verbindung **Aktiv** lautet, können Sie keine Dienstverbindungen konfigurieren.



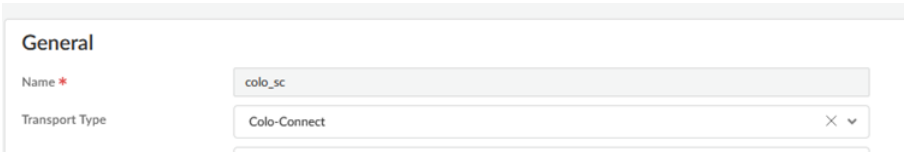

**STEP 3 |** Wählen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** aus und legen Sie als Konfigurationsumfang **Prisma Access** fest.

**STEP 4 |** Aktualisieren Sie den **Prisma Access-Synchronisierungsstatus**, damit die Colo-Connect-Konfiguration im Bereich der Dienstverbindungen bereitgestellt wird.

 ©2025 Palo Alto Networks, Inc.

**STEP 5 |** Wählen Sie **Workflows** > **Einrichtung Prisma Access** > **DienstverbindungDienstverbindung hinzufügen** aus und ordnen Sie einen eindeutigen **Namen** zu. Wählen Sie dann den **Transporttyp Colo-Connect** aus.

*Stellen Sie sicher, dass der eingegebene Name maximal 31 Zeichen lang ist; die Eingabe eines Namens mit 32 oder mehr Zeichen führt dazu, dass der Tunnel in der Prisma Access-Infrastruktur falsch zugeordnet wird.*




**STEP 6 |** Wählen Sie zwei Verbindungen aus, die mit den Dienstverbindungen (**Verbindung 1** und **Verbindung 2**) verwendet werden sollen.

Diese Verbindungen müssen sich in zwei verschiedenen Zonen befinden.




**STEP 7 |** Wählen Sie **Aktiv** oder **Backup** für **Verbindung 1** und **Verbindung 2** aus

Verwenden Sie beim Einrichten von Dienstverbindungen die folgenden Richtlinien:

- Sie können Verbindungen in diesen Modi konfigurieren:
  - **Aktiv/Aktiv**
  - **Aktiv/Backup**
  - **Backup/Aktiv**

  Die Konfiguration beider Verbindungen im Modus **Backup/Backup** ist ungültig und wird nicht unterstützt.
- Die Bandbreite der Verbindungen muss für alle Modi gleich sein.
- Die Verbindungen müssen sich in verschiedenen Zonen befinden.
- Die maximale Bandbreite, die Sie für eine Dienstverbindung angeben können, beträgt 20 Gb/s. Wenn Sie eine **Bandbreite** von **20 Gb/s** für eine Verbindung angeben, können Sie diese Verbindung nicht in einer **Aktiv/Aktiv**-Konfiguration verwenden. (Stattdessen müssen Sie **Aktiv/Backup** angeben.)
- Kombinieren Sie keine dedizierten Interconnect-Verbindungen und Partner Interconnect-Verbindungen innerhalb derselben Dienstverbindung und stellen Sie sicher, dass die Dienstverbindungen unterschiedliche Zonen verwenden. Diese Tabelle zeigt die erlaubten und nicht erlaubten Konfigurationen für Dienstverbindungen. Dies setzt allerdings voraus,

 ©2025 Palo Alto Networks, Inc.

dass Zonen, Standorte, Bandbreite und Rollen den Richtlinien und Anforderungen für Dienstverbindungen entsprechen:

| Verbindung 1 gehört zu | Verbindung 2 gehört zu | Gültige Colo-Connect-Dienstverbindungskonfiguratio |
|---|---|---|
| Partner-Connect 1 | Partner-Connect 2 | Ja |
| Dedizierte Connect 1 | Dedizierte Connect 2 | Ja |
| Partner- Connect 1 | Partner-Connect 1 | Nein |
| Dedizierte Connect 1 | Dedizierte Connect 1 | Nein |
| Partner-Connect | Dedizierte Connect | Nein |

**STEP 8 |** (Optional und nur für Hot-Potato-Routing-Bereitstellungen) Wählen Sie eine Dienstverbindung aus, die als bevorzugte Backup-Verbindung verwendet werden soll. Hierbei handelt es sich um die **Backup-SC** in der Hot-Potato-Routing-Konfiguration.

Sie können nur eine Dienstverbindung auswählen, die als Colo-Connect-Dienstverbindung konfiguriert wurde. Prisma Accessverwendet die von Ihnen ausgewählte Backup-SC als bevorzugte Dienstverbindung im Falle eines Verbindungsfehlers. Durch Auswahl einer Backup-Dienstverbindung (Backup-SC) können Probleme aufgrund asymmetrischen Routings verhindert werden, wenn Sie mehr als zwei Dienstverbindungen erstellt haben.

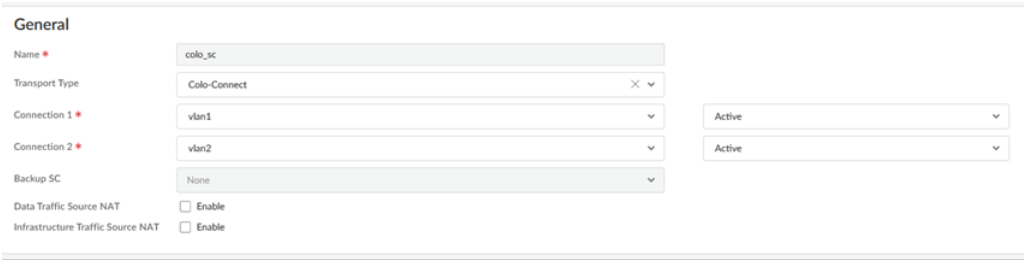
**STEP 9 |** (Optional) Aktivieren Sie die Quell-NAT für IP-Pooladressen für Mobile Benutzer – GlobalProtect und/oder für IP-Adressen im Infrastruktursubnetz.

Sie können ein Subnetz an einer oder mehreren Dienstverbindungen angeben, die für den NAT-Datenverkehr zwischen mobilen Prisma Access GlobalProtect-Benutzern und privaten Anwendungen und Ressourcen in einem Rechenzentrum verwendet werden.

- **Quell-NAT des Datenverkehrs aktivieren** – Führt die NAT für Adressen des IP-Adresspools mobiler Benutzer aus, sodass diese nicht ans Rechenzentrum mitgeteilt werden und nur die von Ihnen bei den Dienstverbindungen angegebenen Subnetze im Rechenzentrum mitgeteilt und geroutet werden.
- **Quell-NAT des Infrastrukturdatenverkehrs aktivieren** – Führt die NAT für Adressen aus dem Infrastruktursubnetz aus, sodass diese nicht ans Rechenzentrum mitgeteilt werden und nur die von Ihnen bei den Dienstverbindungen angegebenen Subnetze im Rechenzentrum mitgeteilt und geroutet werden.
- **IP-Pool** – Geben Sie den IP-Adresspool an, der zum Ausführen der NAT im IP-Adresspool für mobile Benutzer und/oder im Infrastruktursubnetz verwendet wird. Verwenden Sie ein privates IP-Subnetz (RFC 1918) oder ein geeignetes Subnetz, das in Ihrer Routingdomäne routingfähig ist und sich nicht mit dem GlobalProtect-IP-Adresspool für mobile Benutzer

 ©2025 Palo Alto Networks, Inc.

oder dem Infrastruktursubnetz überschneidet. Geben Sie ein Subnetz zwischen /25 und /32 ein.




**STEP 10 |** Konfigurieren Sie im Bereich **GRE und BGP** den GRE-Tunnel und die BGP-Einstellungen für die Dienstverbindung.

BGP ist immer auf **Aktivieren** gesetzt.

1. (Optional) Wählen Sie zwischen den folgenden Optionen:

   - Um eine Community des Typs **No-Export** für Corporate Access Nodes (Dienstverbindungen) den ausgehenden Präfixen von den eBGP-Peers im Customer Premises Equipment (CPE) hinzuzufügen, legen Sie für **No-Export-Community hinzufügen** die Einstellung **Aktiviert Aus** fest. Diese Funktion ist standardmäßig auf **Deaktiviert** eingestellt.

     Verwenden Sie diese Funktionalität nicht im Hot-Potato-Routing-Modus.

   - Um die Anzahl der IP-Subnetzmitteilungen für mobile Benutzer über BGP zu Ihrem Customer Premises Equipment (CPE) zu reduzieren, wählen Sie **Mobile Benutzerrouten vor dem Mitteilen zusammenfassen** aus.

     Standardmäßig teilt Prisma Access die IP-Adresspools der mobilen Benutzer in Blöcken von /24-Subnetzen mit. Wenn Sie sie zusammenfassen, teilt Prisma Access den Pool basierend auf dem von Ihnen angegebenen Subnetz mit. Beispiel: Prisma Access teilt einen öffentlichen mobilen IP-Pool für Benutzer mit der Angabe 10.8.0.0/20 unter Verwendung des Subnetzes /20 mit, anstatt den Pool in die Subnetze 10.8.1.0/24, 10.8.2.0/24, 10.8.3.0/24 usw. zu unterteilen, bevor sie mitgeteilt werden. Durch die Zusammenfassung dieser Mitteilungen kann die Anzahl der in den CPE-Routingtabellen gespeicherten Routen reduziert werden. Sie können die Zusammenfassung von IP-Pools z. B. mit Cloud-VPN-Gateways (Virtual Private Gateways (VGWs) oder Transit Gateways (TGWs)) verwenden, die eine begrenzte Anzahl von Routen akzeptieren können.

     *Wenn Sie das Hot-Potato-Routing aktiviert haben und die Routen-Zusammenfassung aktivieren, fügt Prisma Access keine weiteren AS-PATH-Voranstellungen mehr hinzu, was zu asymmetrischem Routing führen kann. Stellen Sie sicher, dass Ihr Rückkehrdatenverkehr vom Rechenzentrum oder der Zentrale eine symmetrische Rückkehr garantiert, bevor Sie die Routenzusammenfassung mit Hot-Potato-Routing aktivieren.*

   - Um zu verhindern, dass der Prisma Access-BGP-Peer Routen in das Netzwerk Ihrer Organisation weiterleitet. **Keine Prisma Access-Routen mitteilen**.

     Standardmäßig teilt Prisma Access alle BGP-Routinginformationen einschließlich der Informationen zu lokalen Routen und allen Präfixen mit, die von anderen Dienstverbindungen, Remote-Netzwerken und den Subnetzen mobiler Benutzer

 ©2025 Palo Alto Networks, Inc.

empfangen werden. Aktivieren Sie dieses Kontrollkästchen, um Prisma Access daran zu hindern, BGP-Mitteilungen zu senden. Die empfangenen BGP-Informationen werden aber weiterhin verwendet, um Informationen zu Routen anderer BGP-Nachbarn zu erhalten.

*Da Prisma Access keine BGP-Mitteilungen sendet, wenn Sie diese Option auswählen, müssen Sie statische Routen auf dem lokalen Gerät konfigurieren, um Routen zurück zu Prisma Access einzurichten.*

- Was bedeutet die Einstellung „Routenaustausch“?

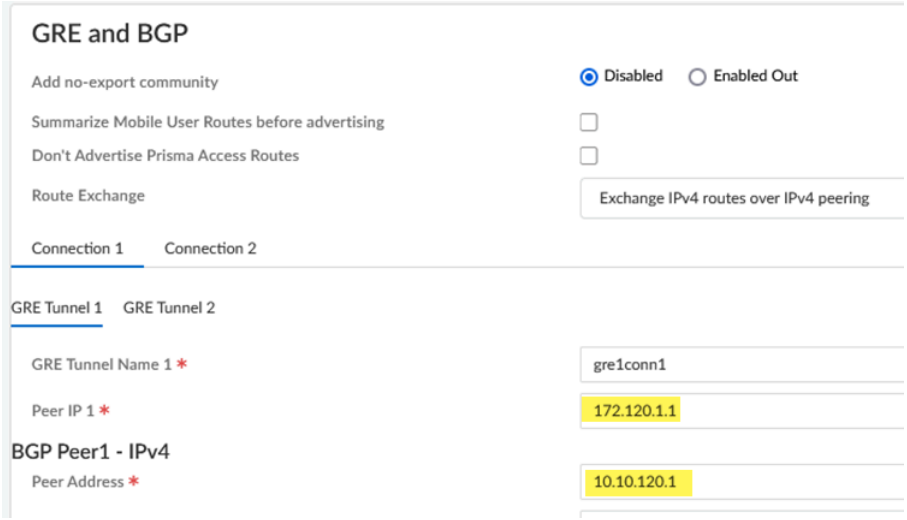
2. Richten Sie das Routing für die Dienstverbindung mit GRE-Tunneln ein.
3. Rufen Sie in Strata Cloud Manager wieder **Workflows** > **Einrichtung Prisma Access** > **Dienstverbindung** und einen GRE-Tunnel für **Verbindung 1** auf, indem Sie einen **Namen des GRE-Tunnels 1** und eine **Peer-IP 1** für **Verbindung 1** angeben. Wenn mehr als 10 Gb/s Bandbreite erforderlich sind, geben Sie den **Namen des GRE-Tunnels 2** und **Peer-IP 2** für den zweiten Tunnel für Verbindung 1 ein. Erstellen Sie dann einen GRE-Tunnel für **Verbindung 2**, indem Sie die gleichen Schritte wiederholen.

   Jedes Paar von GRE-Tunneln in einer Verbindung unterstützt eine maximale Bandbreite von 10 Gb/s. Wenn Sie mehr als 10 Gb/s Bandbreite benötigen, konfigurieren Sie zwei Tunnel pro Verbindung. Beispiel:

   Für die Peer-IP geben Sie die GRE-IP-Adresse des lokalen Routers im Colo ein.

   Verwenden Sie IPv4-Adressen für die BGP-Werte; IPv6 wird nicht unterstützt.
4. Geben Sie die **Peer-Adresse** und die **lokale Adresse** für den BGP-Peer 1 und, falls ein zweiter für die Verbindung 1 erforderlich ist, den BGP-Peer 2 ein.

   Für die **Peer-Adresse** geben Sie die BGP-Peer-IP-Adresse des Colo-Routers ein; für die **lokale Adresse** geben Sie die Adresse ein, die für die BGP-Netzwerkeinrichtung über den GRE-Tunnel verwendet wird.
5. (Optional) Um einen geheimen BGP-Schlüssel zu konfigurieren, geben Sie die Werte für **Geheimer Schlüssel** und **Geheimen Schlüssel bestätigen** ein.

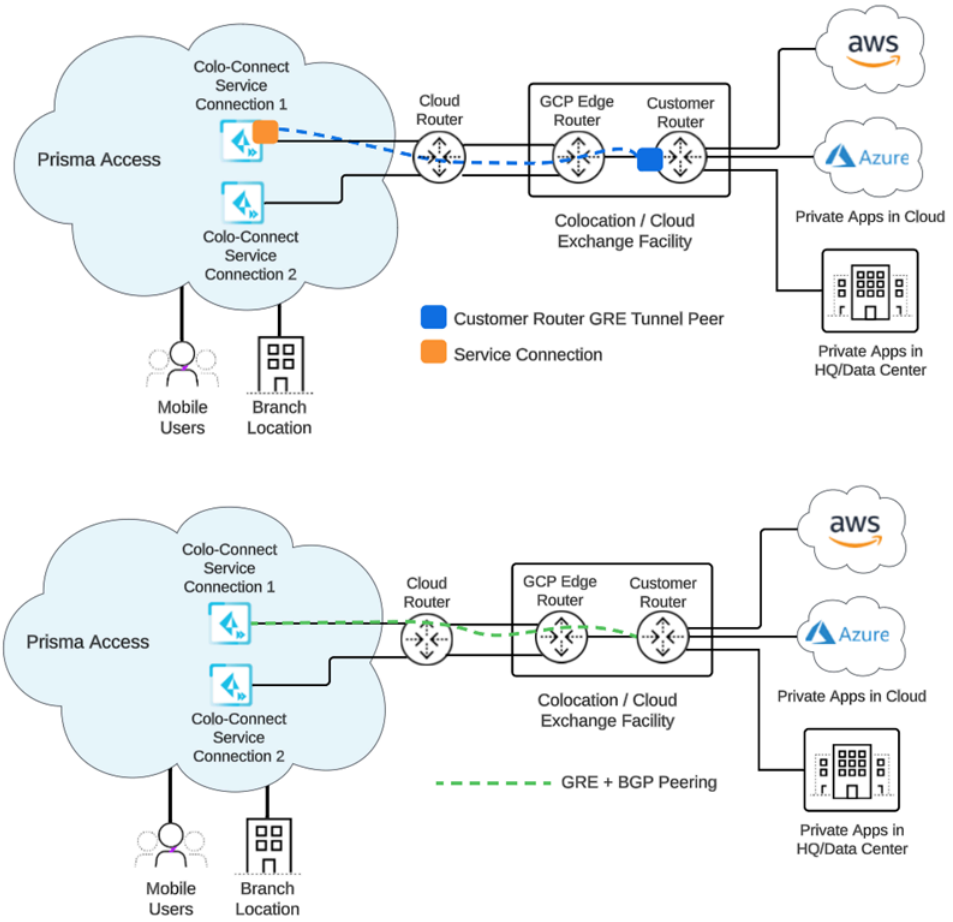



 ©2025 Palo Alto Networks, Inc.

**STEP 11 |** Verwenden Sie **Commit und Push**, um Ihre Konfigurationsänderungen festzuschreiben und zu übertragen. Vergewissern Sie sich dabei, dass **Colo-Connect** im **Übertragungsumfang** ausgewählt wurde.

## Richten Sie das Routing für die Dienstverbindung mithilfe von GRE-Tunneln ein.

Der Colo-Router teilt seine GRE-Tunnel-Peer-IP-Adresse an den Cloud-Router mit und erhält die Informationen zum Subnetz für den GRE-Tunnel vom Cloud-Router. Bei der Erstkonfiguration für das eBGP-Routing über das VLAN auf dem Kundenrouter haben Sie die lokale Erreichbarkeit für die GRE-Tunnel mitgeteilt. Nachdem der Cloud-Router und der Colo-Router die Routen für das Colo-Subnetz und die lokalen GRE-IP-Adressen gegenseitig mitgeteilt und erhalten haben, werden die von der Dienstverbindung verwendeten GRE-Tunnel aktiviert (up).




Um das Routing einzurichten und GRE-Tunnel zu den Dienstverbindungen hinzuzufügen, führen Sie die folgenden Schritte aus.

 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** Notieren Sie die IP-Adressen, die für die **Peer-Adresse** verwendet werden sollen, und außerdem die **lokale Adresse** für BGP-Peer 1 und, falls ein zweiter für Verbindung 1 benötigt wird, für BGP-Peer 2.

Die hier aufgeführten Beispiele verwenden die folgenden Peer-Adressen und lokalen Adressen:

- **Peer-Adresse** – 10.10.120.0 und 10.10.130.1 für Verbindung 1, 10.10.120.2 und 10.10.130.2 für Verbindung 2
- **Lokale Adresse** – 10.10.120.2 und 10.10.130.2 für Verbindung 1, 10.10.121.2 und 10.10.131.2 für Verbindung 2

**STEP 2 |** Notieren Sie die IP-Adressen, die Sie für die **Peer-IP 1**- und, falls erforderlich, für die **Peer-IP 2**-Adresse in den Dienstverbindungen verwenden wollen.

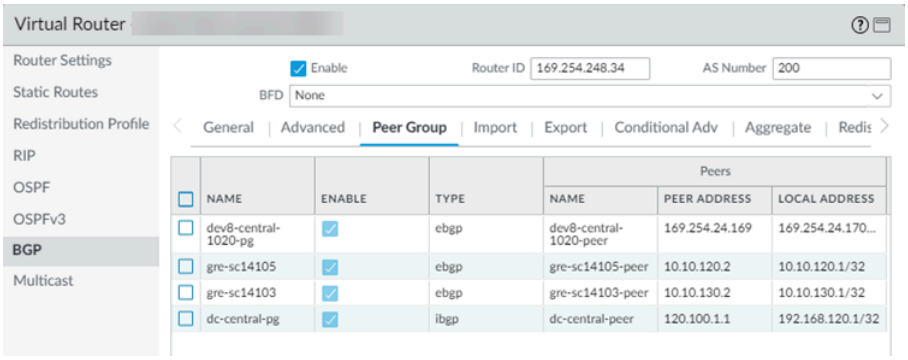
Sie verwenden diese IP-Adressen, um eine Ablehnungsrichtlinie zu erstellen, die verhindert, dass die lokale GRE-IP-Adresse an die Colo-Connect-Dienstverbindung mitgeteilt wird.

Alle Beispiele in diesem Dokument verwenden diese IP-Adressen:

- 172.120.1.1 für Verbindung 1
- 172.121.1.1 für Verbindung 2

**STEP 3 |** Konfigurieren Sie Peer-Gruppen für die Peer- und die lokalen IP-Adressen.

Wenn Sie eine Next-Generation-Firewall als Colo-Router verwenden, wählen Sie **Netzwerk** > **Virtuelle Router**, **Hinzufügen** aus, um einen virtuellen Router hinzuzufügen. Rufen Sie dann **BGP** > **Peer-Gruppe** auf und geben Sie die Peer-Adresse als **Peer-Adresse** und die **lokale Adresse** als **lokale Adresse** an.



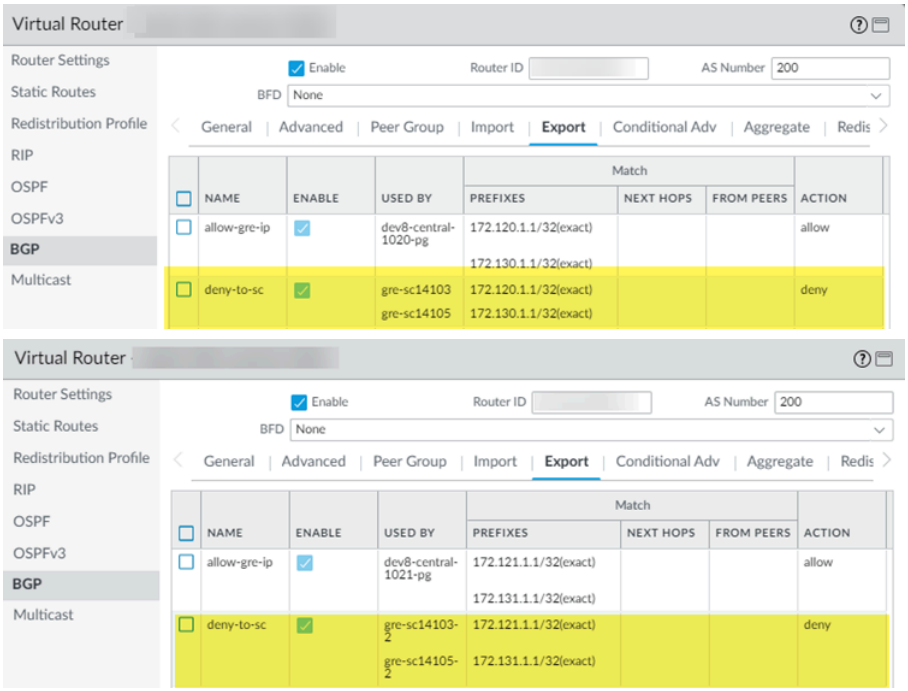

**STEP 4 |** Erstellen Sie eine BGP-Exportrichtlinie, um die Peer-IP-Adressen, die Sie konfiguriert haben (172.120.1.1, 172.130.1.1, 172.121.1.1 und 172.131.1.1), abzulehnen und sie auf die von Ihnen erstellten Peer-Gruppen anzuwenden.

Diese Exportrichtlinie legt eine Ablehnungsregel für die lokalen GRE-Tunnel-Peer-IP-Adressen fest und erlaubt, dass alle anderen Routen an die Dienstverbindung mitgeteilt werden.

Wenn Sie eine Next-Generation-Firewall als Colo-Router verwenden, wählen Sie **Netzwerk** > **Virtuelle Router**, **Hinzufügen** für einen virtuellen Router aus. Wählen Sie dann **BGP** > **Exportieren**, **Hinzufügen** für eine Exportregel aus und führen Sie einen **Abgleich** der IP-

 ©2025 Palo Alto Networks, Inc.

Adressen durch, die als Peer-IP-Adresse verwendet werden können. Erstellen Sie dann die **Aktion** des Typs **Ablehnen**.




## Erhöhen oder Verringern der Bandbreite einer Colo-Connect-Dienstverbindung

Wenn Sie Dienstverbindungen konfigurieren, konfigurieren Sie die Bandbreite basierend auf den Verbindungen (VLAN-Anhängen), die Sie zuordnen. Sie weisen zwei Verbindungen pro Dienstverbindung zu und dann entweder einen oder zwei GRE-Tunnel pro Verbindung.

Während jede Colo-Connect-Dienstverbindung maximal 20 Gb/s unterstützt, unterstützt jeder GRE-Tunnel in der Dienstverbindung 10 Gb/s. Aus diesem Grund müssen Sie möglicherweise die GRE-Tunnel in der Colo-Connect-Dienstverbindung hinzufügen oder löschen, um die gesamte Bandbreite in einem Link zu ändern. Dies kann dazu führen, dass die Bandbreite der Dienstverbindung dann die Grenze von 10 Gb/s über- oder unterschreitet.

### Erhöhen der Bandbreite einer Colo-Connect-Dienstverbindung

Um die Bandbreite einer bestehenden Dienstverbindung über 10 Gb/s zu erhöhen, führen Sie die folgenden Schritte aus:

**STEP 1 |** Rufen Sie **Workflows** > **Einrichtung Prisma Access** > **Colo-Connect** auf.

**STEP 2 |** Wählen Sie den **Linknamen** aus, der der Dienstverbindung zugeordnet ist.

**STEP 3 |** Erhöhen Sie die **Bandbreite** des Links (Interconnect).

**STEP 4 |** Wählen Sie **Konfiguration übertragen** aus.

**STEP 5 |** Wählen Sie **Workflows** > **Einrichtung Prisma Access** > **Dienstverbindung** aus.

**STEP 6 |** Fügen Sie den zusätzlichen GRE-Tunnel zur Colo-Connect-Dienstverbindung hinzu.

**STEP 7 |** Wählen Sie **Konfiguration übertragen** aus.

 ©2025 Palo Alto Networks, Inc.

**STEP 8 |** Fügen Sie die lokalen GRE-IP-Adressen (Peer) zu Ihren Exportrichtlinien für das VLAN-eBGP-Routing und das Dienstverbindungsrouting für die GRE-Tunnel hinzu.

#### Verringern der Bandbreite einer Colo-Connect-Dienstverbindung

Um die Bandbreite einer bestehenden Dienstverbindung unter 10 Gb/s zu verringern, führen Sie die folgenden Schritte aus:

**STEP 1 |** Wählen Sie **Workflows** > **Einrichtung Prisma Access** > **Colo-Connect** aus.

**STEP 2 |** Wählen Sie den **Linknamen** aus, der der Dienstverbindung zugeordnet ist.

**STEP 3 |** Reduzieren Sie die **Bandbreite** des Links (Interconnect).

**STEP 4 |** Wählen Sie **Konfiguration übertragen** aus.

Sie müssen die Dienstverbindung nicht neu konfigurieren, um den zusätzlichen GRE-Tunnel zu entfernen. Prisma Access erkennt und senkt die Bandbreite der Verbindung und entfernt den zusätzlichen Tunnel, wenn Sie Ihre Änderungen im Übertragungsumfang der Dienstverbindung festschreiben und sie übertragen.

### Löschen einer Colo-Connect-Verbindung

Um eine Colo-Connect-Verbindung zu löschen, befolgen Sie die umgekehrte Reihenfolge der Konfiguration, indem Sie die folgenden Schritte ausführen:

**STEP 1 |** Löschen Sie die Dienstverbindungen, die der Verbindung zugeordnet sind, und wählen Sie hierzu **Workflows** > **Einrichtung Prisma Access** > **Dienstverbindungen** aus. Wählen Sie dann die Dienstverbindung und anschließend **Löschen** aus.

**STEP 2 |** Wählen Sie **Konfiguration übertragen** aus.

**STEP 3 |** Löschen Sie die Colo-Connect-Verbindungen, die der Verbindung zugeordnet sind. Wählen Sie hierzu **Workflows** > **Einrichtung Prisma Access** > **Colo-Connect**und **Verbindungsname** im Bereich für das **Onboarding** sowie **Löschen** aus.

**STEP 4 |** Löschen Sie den Colo-Connect-Link, indem Sie den **Linknamen** und dann **Löschen** auswählen.

**STEP 5 |** Löschen Sie die lokalen GRE-IP-Adressen (Peer) auf Basis Ihrer Exportrichtlinien für das VLAN-eBGP-Routing und das Dienstverbindungsrouting für die GRE-Tunnel.

## Konfigurieren von Prisma Access Colo-Connect (Panorama)

### Konfigurieren Sie Prisma Access Colo-Connect-Bereitstellungen mit Partner Interconnect-Verbindungen.

Um Prisma Access Colo-Connect über eine Partner Interconnect-Verbindung zu konfigurieren, müssen Sie die folgenden Schritte ausführen.

 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** Erstellen Sie Subnetze für Ihre Colo-Connect-Verbindungen.

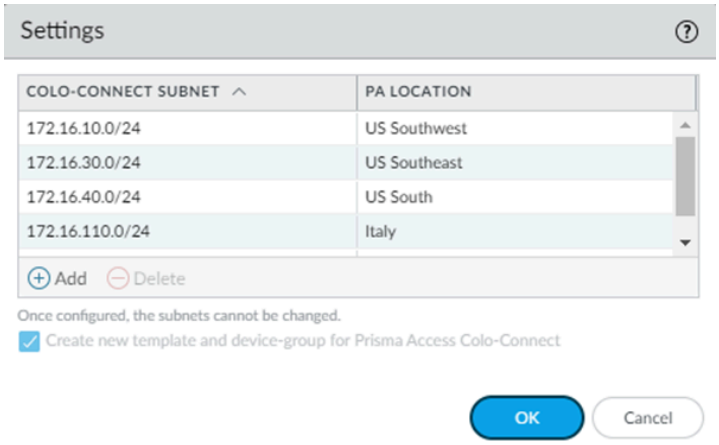
Sie verwenden die Subnetze, die Sie hier erstellen, in den Verbindungen und Dienstverbindungen, die Sie in späteren Schritten erstellen.

1. Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Colo-Connect** aus und klicken Sie dann auf das Zahnradsymbol, um die Einstellungen zu bearbeiten.
2. **Fügen Sie** ein **Colo-Connect-Subnetz** hinzu und wählen Sie einen Prisma Access-Standort (**PA-Standort**) für es aus.

   Verwenden Sie für das Subnetz eine Mindestgröße von /28.
3. (Optional) Wenn Sie die Erstellung von Colo-Connect-Instanzen für mehrere Standorte planen, fügen Sie für jeden Standort weitere Subnetze hinzu.

   Sie können ein Subnetz pro Standort konfigurieren.
4. Wählen Sie **Neue Vorlagen und Gerätegruppe für Prisma Access Colo-Connect erstellen** aus.

   Wählen Sie bei der Erstkonfiguration einer Colo-Connect-Bereitstellung dieses Kontrollkästchen aus, damit Vorlagen und Gerätegruppen (Colo_Connect_Template bzw. Colo_Connect_Device_Group) für Colo-Connect erstellt werden. Nachdem Sie diese Vorlagen und Gerätegruppen erstellt haben, wird dieses Kontrollkästchen ausgegraut.



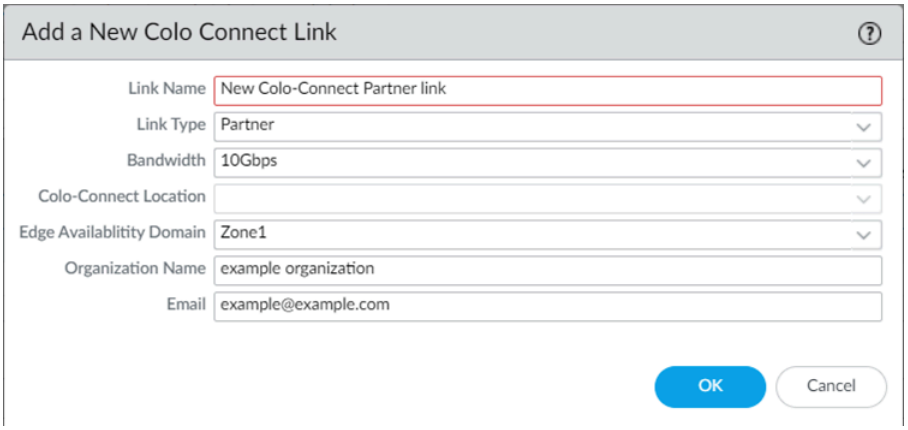

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Fügen Sie einen neuen Colo-Connect-Link hinzu (auch bekannt als *Interconnect*).

1. Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Colo-Connect** > **Colo-Connect-Link** und **Hinzufügen** aus, um einen Colo-Connect-Link hinzuzufügen.
2. Ordnen Sie dem Link einen eindeutigen **Linknamen** zu.
3. Wählen Sie eine **Partner Interconnect-Verbindung** aus.

   Sie müssen keine **VLAN-ID** eingeben, da Ihr Colo eine solche ID bereitstellt, wenn es die Konfiguration Ihres VLAN-Anhangs mit dem Kopplungsschlüssel abschließt.
4. Geben Sie die verbleibenden Colo-Connect-Linkparameter an.
   - Wählen Sie entweder **10 Gb/s** oder **20 Gb/s** als **Bandbreite** aus.

     Sie können die Bandbreite eines dedizierten Interconnect-Links nicht ändern, nachdem Sie ihn angegeben und Ihre Änderungen übertragen haben.
   - Wählen Sie entweder **Zone1** oder **Zone2** als **Edge-Verfügbarkeitsdomäne** aus. Entnehmen Sie diesen Wert der GCP-Zone, die für Ihre Edge-Verfügbarkeitsdomäne verwendet wird.
   - Geben Sie den **Namen der Organisation** ein, der für diesen Link verwendet werden soll.
   - Geben Sie die **E-Mail-Adresse** ein, die für diesen Link verwendet werden soll. Jede E-Mail-Adresse ist akzeptabel.




**STEP 3 |** Erstellen Sie die Verbindungen (auch bekannt als *VLAN-Anhänge*) für Colo-Connect.

1. Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Colo-Connect** > **Onboarding** und **Hinzufügen** aus, um eine neue Verbindung hinzuzufügen.
2. Konfigurieren Sie die Verbindungseinstellungen.
   - Geben Sie einen eindeutigen **Namen** für die Verbindung ein.
   - Wählen Sie einen **Linknamen** aus den Links aus, die Sie in einem vorherigen Schritt konfiguriert haben.
   - Wählen Sie eine **Bandbreite** für die Verbindung aus.

     Sie können zwischen **1 Gb/s**, **2 Gb/s**, **5 Gb/s**, **10 Gb/s** oder **20 Gb/s** wählen.

     Wenn Sie für eine Interconnect-Verbindung mehrere Verbindungen konfigurieren, stellen Sie sicher, dass die Gesamtbandbreite der Verbindungen die Bandbreite der Interconnect-Verbindung nicht überschreitet. Beispiel: Für eine Partner Interconnect-

 ©2025 Palo Alto Networks, Inc.

Verbindung mit einer Kapazität von 10 Gb/s können Sie 10 Verbindungen mit jeweils 1 Gb/s konfigurieren, der Gesamtwert von insgesamt 10 Gb/s für alle Verbindungen darf jedoch nicht überschritten werden.

*Wenn Ihre Bereitstellung mehr als 16 Verbindungen erfordert, wenden Sie sich an Ihr Palo Alto Networks-Account-Team, das einen SRE-Fall eröffnen wird, um die Anfrage zu bearbeiten.*

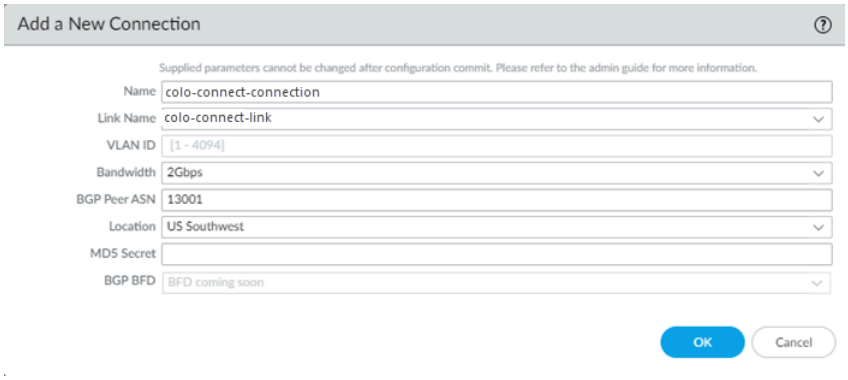
- Geben Sie eine **BGP-Peer-ASN** ein.

  Geben Sie die AS-Nummer (Autonomous System) für den Router des Kunden vor Ort im Colo ein. Der Bereich liegt zwischen 1 und 4294967295.
- Wählen Sie den **Standort** aus den Verbindungsnamen aus, die Sie in einem vorherigen Schritt erstellt haben.

  Sie müssen bereits ein Subnetz für alle von Ihnen angegebenen Standorte hinzugefügt haben.
- (Optional) Geben Sie den **Geheimen MD5-Schlüssel** für das BGP ein.

*Lassen Sie das Feld **BGP-BFD** leer; es ist für ein zukünftiges Colo-Connect-Release reserviert*

.



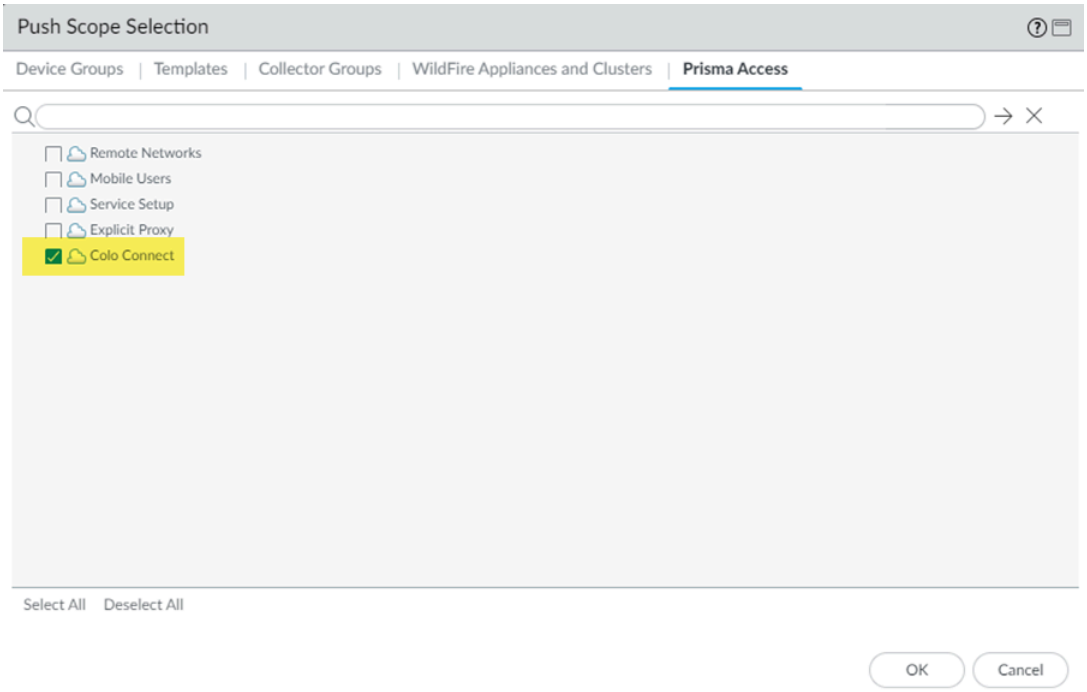

3. Fahren Sie mit der Erstellung von Verbindungen fort, bis alle erforderlichen Verbindungen erstellt wurden.

   Sie müssen zwei Verbindungen erstellen. Beide Verbindungen müssen sich in derselben Region befinden, und eine Verbindung muss sich in einer separaten Zone befinden. Sie verwenden diese Verbindungen in Dienstverbindungen, die Sie in einem späteren Schritt erstellen werden.

 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** Führen Sie einen Commit aus und übertragen Sie die Änderung per Push.

1. Klicken Sie auf **Commit** > **Commit und Push**.
2. Verwenden Sie die Option **Auswahlen bearbeiten** und stellen Sie sicher, dass Colo-Connect im Übertragungsumfang ausgewählt ist.



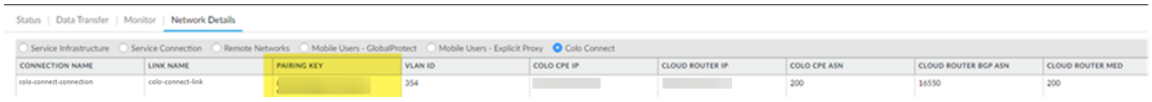

3. Klicken Sie auf **OK**, um Ihre Änderungen im Übertragungsumfang zu speichern.
4. Führen Sie für Ihre Änderungen die Aktion **Commit und Push** aus.

**STEP 5 |** Rufen Sie den**Kopplungsschlüssel** ab und schließen Sie Ihre Partner Interconnect-Konfiguration in GCP ab.

Sie verwenden diesen Kopplungsschlüssel, wenn Sie die Partner Interconnect-Verbindung im Colo einrichten.

Wenn Sie eine neue Verbindung zum ersten Mal einbinden, wird im Bereich für das Colo-Connect-Onboarding der **Status PENDING_PARTNER** und der **BGB-StatusINAKTIV** angezeigt. Um den Verbindungsstatus auf **AKTIV** zu setzen, rufen Sie den Kopplungsschlüssel ab und geben Sie ihn in die Verbindung im Colo ein.

1. Wählen Sie **Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Colo-Connect** aus und kopieren Sie den **Kopplungsschlüssel**.




2. Erstellen Sie eine neue VLAN-Verbindung im Colo (z. B. Equinix).
3. Fügen Sie den Kopplungsschlüssel in das Colo-VLAN ein.

   GCP erkennt, wenn der Kopplungsschlüssel verarbeitet wird, setzt den VLAN-Status auf **AKTIV** und generiert die BGP-IP-Adresse, die Sie auf Ihrem lokalen Router im Colo konfigurieren können. Diese Aktionen starten das eBGP-Routing über das VLAN zwischen dem Colo-Router und dem GCP-Cloud-Router.

 ©2025 Palo Alto Networks, Inc.

**STEP 6 |** Erstellen Sie das eBGP-Routing auf dem Kundenrouter (Colo) für die Colo-Connect-Verbindung.

Sie müssen das BGP-Peering einrichten, um die Konnektivität zwischen dem Kundenrouter und dem Cloud-Router zu gewährleisten.

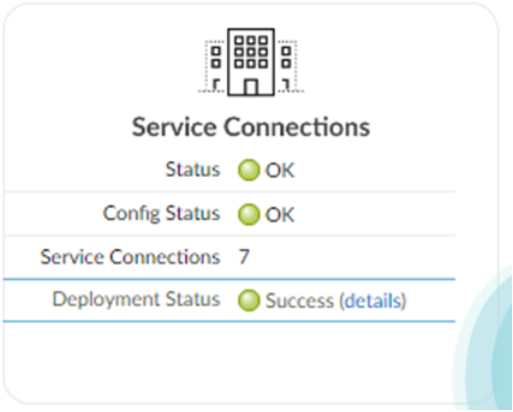
**STEP 7 |** Richten Sie die Dienstverbindungen ein, die Sie mit Colo-Connect verwenden möchten.

**STEP 8 |** Verwenden Sie **Commit und Push**, um Ihre Konfigurationsänderungen festzuschreiben und zu übertragen. Vergewissern Sie sich dabei, dass **Colo-Connect** im **Übertragungsumfang** ausgewählt wurde.

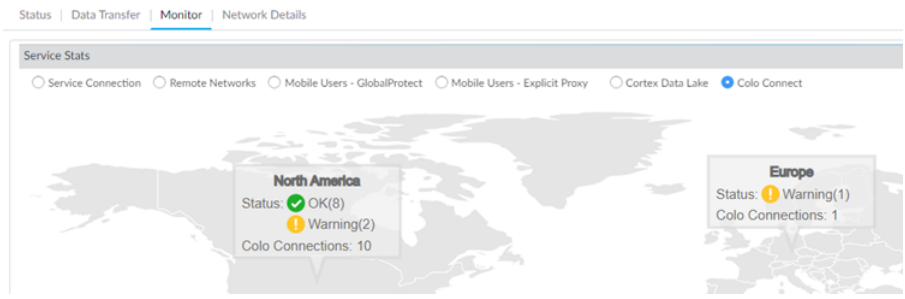

©2025 Palo Alto Networks, Inc.

**STEP 9 |** Überprüfen Sie den Status der Colo-Connect-Verbindungen.

1. Um den Status einer von einer Colo-Connect-Verbindung verwendeten Dienstverbindung zu überprüfen, wählen Sie **Panorama** > **Cloud Services** > **Status** > > **Colo-Connect** > **Überwachen** aus




2. Bewegen Sie den Mauszeiger über eine Region, in der eine Colo-Connect-Verbindung bereitgestellt wurde.
   - Wenn die Colo-Connect-Verbindung und das BGP-Routing beide aktiv sind, wird der Status **OK** angezeigt.
   - Wenn die Colo-Connect-Verbindung aktiv ist, das BGP-Routing aber nicht, wird der Status **Warnung** angezeigt.
   - Wenn die Colo-Connect-Verbindung und das BGP-Routing beide inaktiv sind, wird der Status **INAKTIV** angezeigt.
   - Wenn die Colo-Connect-Verbindung inaktiv ist, das BGP-Routing jedoch aktiv, wird der Status **Fehler** angezeigt.




3. Zum Aufrufen weiterer Informationen klicken Sie auf das Regionsfeld und lesen sie die Informationen auf der Registerkarte **Status**.

**STEP 10 |** Überprüfen Sie die Netzwerkdetails einschließlich des Kopplungsschlüssels der Colo-Connect-Verbindungen, indem Sie **Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Colo-Connect** aufrufen und die Informationen in den folgenden Feldern anzeigen.

## Konfigurieren Sie die Prisma Access Colo-Connect-Bereitstellungen mit dedizierten Interconnect-Verbindungen.

Um Prisma Access Colo-Connect über eine dedizierte Interconnect-Verbindung zu konfigurieren, müssen Sie die folgenden Schritte ausführen.

 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** Erstellen Sie Subnetze für Ihre Colo-Connect-Verbindungen.

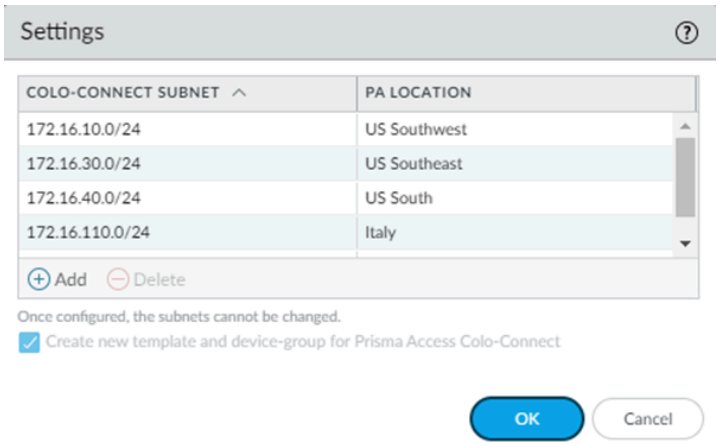
Sie verwenden die Subnetze, die Sie hier erstellen, in den Verbindungen und Dienstverbindungen, die Sie in späteren Schritten erstellen.

1. Rufen Sie in Panorama, das Prisma Access verwaltet, **Panorama** > **Cloud Services** > **Konfiguration** > **Colo-Connect** auf und klicken Sie dann auf das Zahnradsymbol, um die Einstellungen zu bearbeiten.
2. **Fügen Sie** ein **Colo-Connect-Subnetz** hinzu und wählen Sie einen Prisma Access-Standort (**PA-Standort**) für es aus.

   Verwenden Sie für das Subnetz eine Mindestgröße von /28.
3. (Optional) Wenn Sie die Erstellung von Colo-Connect-Instanzen für mehrere Standorte planen, fügen Sie für jeden Standort weitere Subnetze hinzu.

   Sie können nur ein Subnetz pro Standort konfigurieren.
4. Wählen Sie **Neue Vorlagen und Gerätegruppe für Prisma Access Colo-Connect erstellen** aus.

   Wählen Sie bei der Erstkonfiguration einer Colo-Connect-Bereitstellung dieses Kontrollkästchen aus, damit Vorlagen und Gerätegruppen (Colo_Connect_Template bzw. Colo_Connect_Device_Group) für Colo-Connect erstellt werden. Nachdem Sie diese Vorlagen und Gerätegruppen erstellt haben, wird dieses Kontrollkästchen ausgegraut.




 ©2025 Palo Alto Networks, Inc.

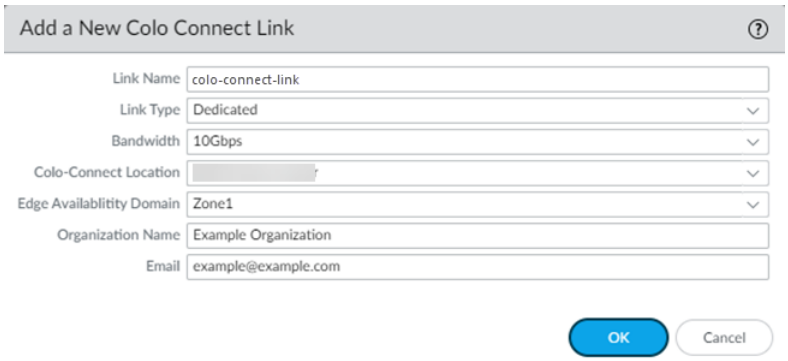
**STEP 2 |** Fügen Sie einen neuen Colo-Connect-Link hinzu (auch bekannt als *Interconnect*).

1. Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Colo-Connect** > **Colo-Connect-Link** und **Hinzufügen** aus, um einen Colo-Connect-Link hinzuzufügen.
2. Ordnen Sie dem Link einen eindeutigen **Linknamen** zu.
3. Wählen Sie eine **dedizierte** Interconnect-Verbindung aus.
4. Geben Sie die verbleibenden Colo-Connect-Linkparameter an.
   - Wählen Sie entweder **10 Gb/s** oder **20 Gb/s** als **Bandbreite** aus.

     *Wenn Sie 20 Gb/s auswählen, müssen Sie die dedizierte Interconnect-Verbindung zu zwei 10-Gb/s-Links zusammenfassen. Verwenden Sie dazu LACP.*

     Sie können die Bandbreite eines dedizierten Interconnect-Links nicht ändern, nachdem Sie ihn angegeben und Ihre Änderungen festgeschrieben und übertragen haben.
   - Wählen Sie einen **Colo-Connect-Standort** in der Dropdown-Liste aus.

     Stellen Sie sicher, dass Sie denselben Standort auswählen, den Sie für die dedizierte Interconnect-Verbindung verwendet haben.
   - Wählen Sie entweder **Zone1** oder **Zone2** als **Edge-Verfügbarkeitsdomäne** aus. Entnehmen Sie diesen Wert der GCP-Zone, die für Ihre Edge-Verfügbarkeitsdomäne verwendet wird.
   - Geben Sie den **Namen der Organisation** ein, der für diesen Link verwendet werden soll.
   - Geben Sie die **E-Mail-Adresse** ein, an die Sie die LOA-CFA-Details vom Cloud-Anbieter erhalten möchten.
     - GCP verwendet diese E-Mail, um das LOA-CFA (Letter of Authorization and Connecting Facility Assignment) zu senden. Stellen Sie sicher, dass das LOA-CFA an Ihren Colo-Anbieter gesendet wird, damit er mit der Installation Ihrer Verbindungen beginnen kann.




 ©2025 Palo Alto Networks, Inc.

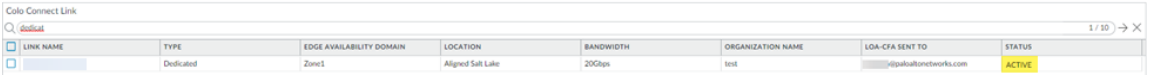
**STEP 3 |** Nachdem die dedizierte Verbindung hergestellt ist, führt die Colo-Einrichtung Tests für Ihre Verbindungen durch und informiert Sie darüber, dass die Tests durchgeführt wurden und die Verbindungen nun benutzt werden können.

Für diesen Schritt sind keine Prisma Access-Konfigurationen erforderlich. Erstellen Sie die Colo-Connect-Verbindungen nicht in Prisma Access, bis die Colo-Einrichtung Ihnen mitteilt, dass sie getestet wurden.

**STEP 4 |** Erstellen Sie die Verbindungen (auch bekannt als *VLAN-Anhänge*) für Colo-Connect.

1. Stellen Sie sicher, dass der Status des dedizierten Links „Aktiv“ ist, indem Sie zu **Panorama** > **Cloud Services** > **Konfiguration** > **Colo-Connect** > **Colo-Connect-Link** wechseln.

   Solange der Status des dedizierten Links nicht „Aktiv“ ist, können Sie keine Colo-Connect-Links erstellen.

2. Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Colo-Connect** > **Onboarding** und **Hinzufügen** aus, um eine neue Verbindung hinzuzufügen.
3. Konfigurieren Sie die Verbindungseinstellungen.
   - Geben Sie einen eindeutigen **Namen** für die Verbindung ein.
   - Wählen Sie einen **Linknamen** aus den Links aus, die Sie in einem vorherigen Schritt konfiguriert haben.
   - (Optional) Geben Sie eine **VLAN-ID** für die Verbindung ein.

     VLAN-IDs werden vom Interconnect-Anbieter (GCP) generiert, wenn Sie nicht manuell einen Wert eingeben.
   - Wählen Sie eine **Bandbreite** für die Verbindung aus.

     Sie können zwischen **1 Gb/s**, **2 Gb/s**, **5 Gb/s**, **10 Gb/s** oder **20 Gb/s** wählen.

     Wenn Sie für eine Interconnect-Verbindung mehrere Verbindungen konfigurieren, stellen Sie sicher, dass die Gesamtbandbreite der Verbindungen die Bandbreite der Interconnect-Verbindung nicht überschreitet. Beispiel: Für eine dedizierte Interconnect-Verbindung mit einer Kapazität von 20 Gb/s können Sie

 ©2025 Palo Alto Networks, Inc.

10 Verbindungen mit jeweils 2 Gb/s konfigurieren, der Gesamtwert von insgesamt 20 Gb/s für alle Verbindungen darf jedoch nicht überschritten werden.

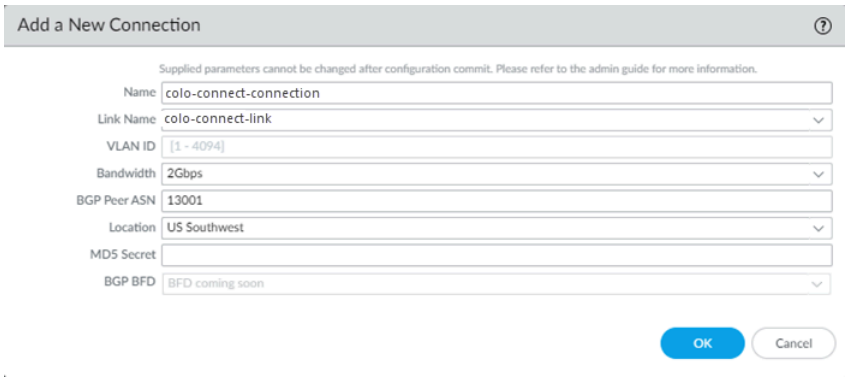
- Geben Sie eine **BGP-Peer-ASN** ein.

  Geben Sie die AS-Nummer (Autonomous System) für den Router des Kunden vor Ort im Colo ein. Der Bereich liegt zwischen 1 und 4294967295.

- Wählen Sie den **Standort** aus den Verbindungsnamen aus, die Sie in einem vorherigen Schritt erstellt haben.

  Sie müssen bereits ein Subnetz für alle von Ihnen angegebenen Standorte hinzugefügt haben.

- (Optional) Geben Sie den **Geheimen MD5-Schlüssel** für das BGP ein.



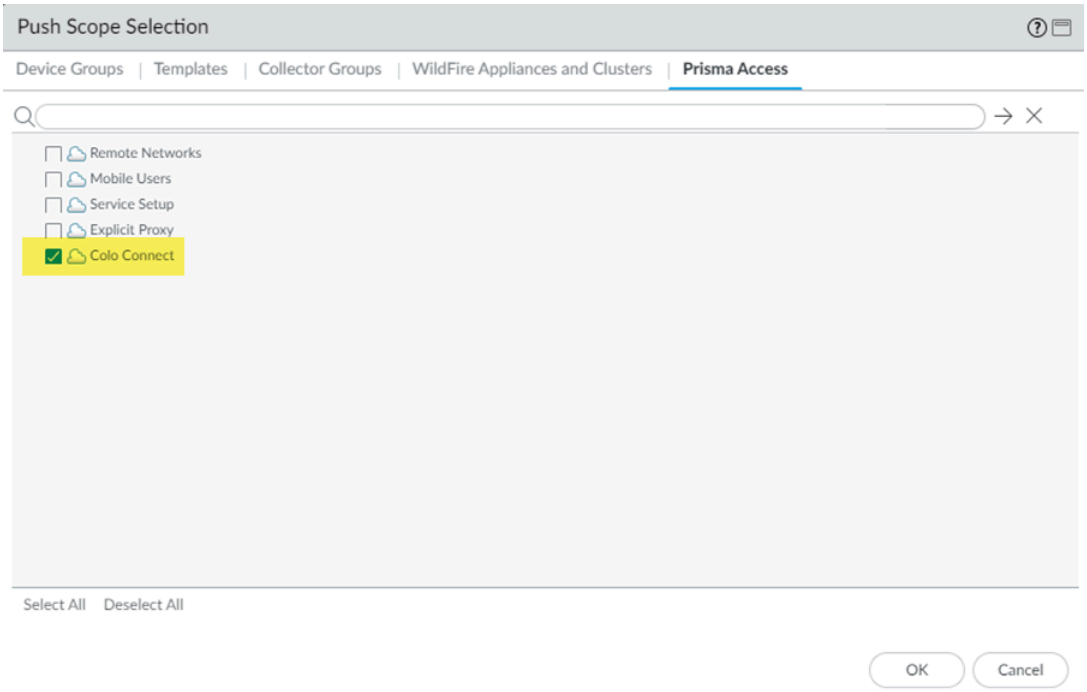

4. Fahren Sie mit der Erstellung von Verbindungen fort, bis alle erforderlichen Verbindungen erstellt wurden.

   Sie müssen zwei Verbindungen erstellen. Beide Verbindungen müssen sich in derselben Region befinden, und eine Verbindung muss sich in einer separaten Zone befinden. Sie verwenden diese Verbindungen in Dienstverbindungen, die Sie in einem späteren Schritt erstellen werden.


©2025 Palo Alto Networks, Inc.

**STEP 5 |** Führen Sie einen Commit aus und übertragen Sie die Änderung per Push.

1. Klicken Sie auf **Commit** > **Commit und Push**.
2. Verwenden Sie die Option **Auswahlen bearbeiten** und stellen Sie sicher, dass Colo-Connect im Übertragungsumfang ausgewählt ist.




3. Klicken Sie auf **OK**, um Ihre Änderungen im Übertragungsumfang zu speichern.
4. Führen Sie für Ihre Änderungen die Aktion **Commit und Push** aus.

**STEP 6 |** Konfigurieren Sie das eBGP-Routing auf dem Kundenrouter.

Sie müssen das BGP-Peering einrichten, um die Konnektivität zum Kundenrouter sicherzustellen.

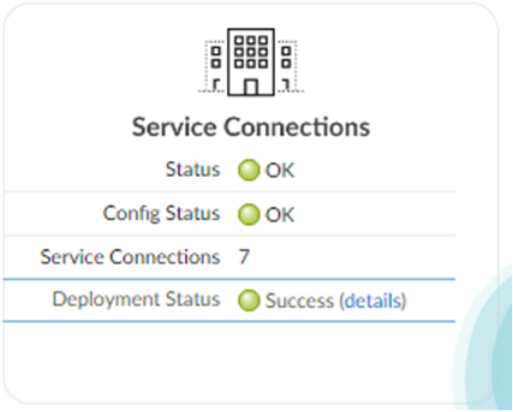
**STEP 7 |** Richten Sie die Dienstverbindungen ein, die Sie mit Colo-Connect verwenden möchten.

**STEP 8 |** Verwenden Sie **Commit und Push**, um Ihre Konfigurationsänderungen festzuschreiben und zu übertragen. Vergewissern Sie sich dabei, dass **Colo-Connect** im **Übertragungsumfang** ausgewählt wurde.

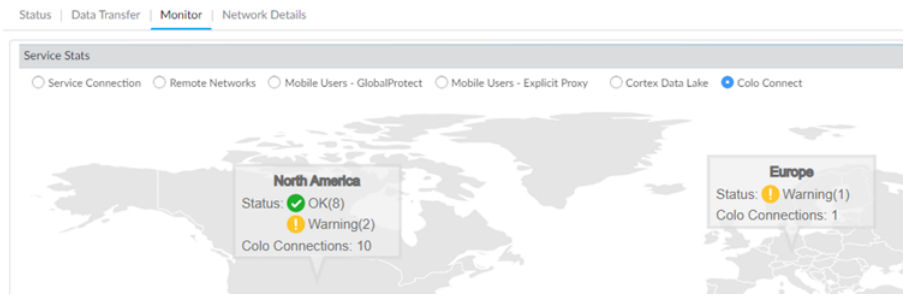

©2025 Palo Alto Networks, Inc.

**STEP 9 |** Überprüfen Sie den Status der Colo-Connect-Verbindungen.

1. Um den Status einer von einer Colo-Connect-Verbindung benutzten Dienstverbindung zu überprüfen, wählen Sie **Panorama** > **Cloud Services** > **Status** > > **Colo-Connect** > **Überwachen** aus.




2. Bewegen Sie den Mauszeiger über eine Region, in der eine Colo-Connect-Verbindung bereitgestellt wurde.
   - Wenn die Colo-Connect-Verbindung und das BGP-Routing beide aktiv sind, wird der Status **OK** angezeigt.
   - Wenn die Colo-Connect-Verbindung aktiv ist, das BGP-Routing aber nicht, wird der Status **Warnung** angezeigt.
   - Wenn die Colo-Connect-Verbindung und das BGP-Routing beide inaktiv sind, wird der Status **INAKTIV** angezeigt.
   - Wenn die Colo-Connect-Verbindung inaktiv ist, das BGP-Routing jedoch aktiv, wird der Status **Fehler** angezeigt.

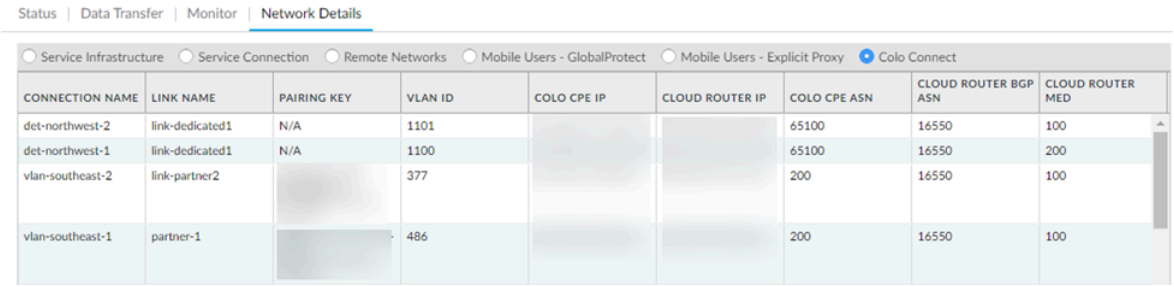



3. Zum Aufrufen weiterer Informationen klicken Sie auf das Regionsfeld und lesen sie die Informationen auf der Registerkarte **Status**.

 ©2025 Palo Alto Networks, Inc.

**STEP 10 |** Überprüfen Sie die Netzwerkdetails der Colo-Connect-Verbindungen, indem Sie **Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Colo-Connect** aufrufen und die Informationen anzeigen.

Für dedizierte Links wird für den **Kopplungsschlüssel** der Wert **n. a.** angezeigt.




## Führen Sie die Konfiguration für das VLAN-eBGP-Routing auf dem Kundenrouter durch.

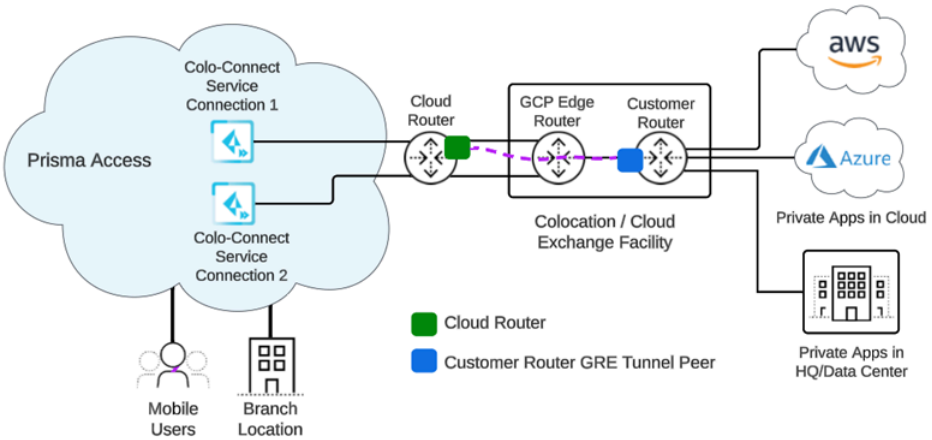
GCP erstellt während dieser Phasen Ihrer Bereitstellung IP-Adressen für den Kundenrouter (Colo-Router) und den Cloud-Router:

- Für Partner Interconnect-Verbindungen erstellt GCP die IP-Adressen, nachdem der Kopplungsschlüssel von Ihrem Colo (zum Beispiel Equinix) verarbeitet wurde.
- Für dedizierte Interconnect-Verbindungen erstellt GCP die IP-Adressen, nachdem Sie Ihre Colo-Connect-Verbindungen (VLAN-Anhänge) eingebunden und Ihre Änderungen festgeschrieben und übertragen haben.

Um ein korrektes Routing sicherzustellen, müssen Sie wie folgt vorgehen:

- Konfigurieren Sie die IP-Adresse des Colo-Routers (die **Colo-CPE-IP** in der Prisma Access-Benutzerschnittstelle) als die lokale VLAN-IP-Adresse und die lokale eBGP-IP-Adresse
- Konfigurieren Sie die IP-Adresse des Cloud-Routers (**Cloud-Router-IP**) als die eBGP-Peer-Adresse auf Ihrem Colo-Router.

Nach Abschluss dieses Schrittes ist eBGP für die Verbindung (VLAN-Anhang) zwischen dem Colo-Router und dem Cloud-Router konfiguriert.




 ©2025 Palo Alto Networks, Inc.

Das Erstellen dieses Routings ist der erste Schritt zur Einrichtung des GRE-Tunnel-Routings. Sie vervollständigen das GRE-Tunnel-Routing, wenn Sie die GRE-Tunnel während der Konfiguration der Dienstverbindung einrichten.

Führen Sie die folgenden Schritte aus, um das Routing zwischen dem Colo und dem Cloud-Router zu konfigurieren.

**STEP 1 |** Erstellen Sie aus dem Panorama, das zur Verwaltung von Prisma Access benutzt wird, die Subnetze, Links und Verbindungen und verwenden Sie dann **Commit und Push**, um Ihre Änderungen festzuschreiben und zu übertragen.

Verwenden Sie den Workflow, der speziell für Ihren Interconnect-Typ definiert ist (entweder Partner oder Dediziert). Für Partner Interconnect-Verbindungen müssen Sie sich vergewissern, dass der Kopplungsschlüssel in das Colo-VLAN eingefügt wurde.

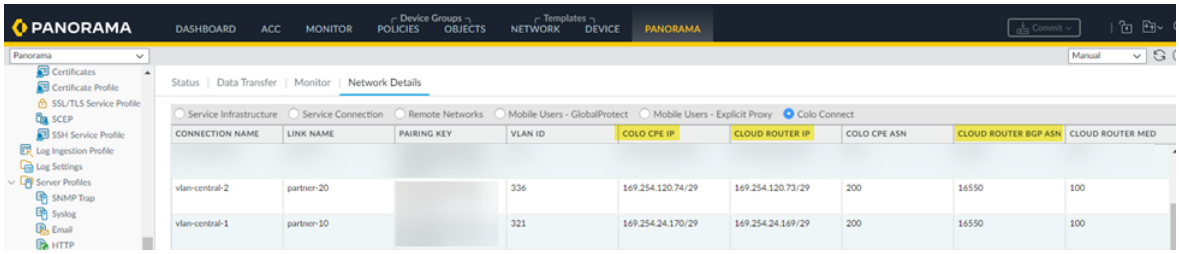
**STEP 2 |** Wählen Sie **Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Colo-Connect** aus.

**STEP 3 |** Notieren Sie die folgenden Verbindungselemente:

- **Colo-CPE-IP**
- **Cloud-Router-IP**
- **Cloud-Router-BGP-ASN**

Im folgenden Beispiel:

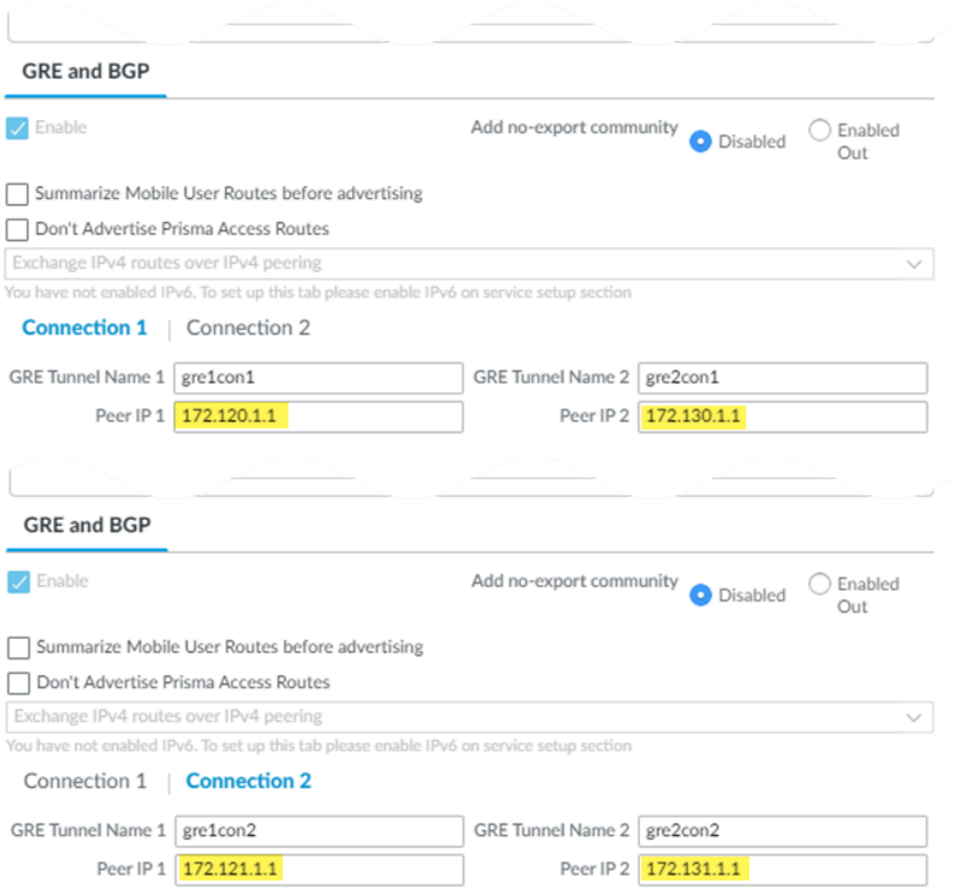
- Für die vlan-central-1-Verbindung lautet die **Colo-CPE-IP** 169.254.24.170/29, die **Cloud-Router-IP** ist 169.254.24.169/29 und als **Cloud-Router-BGP-ASN** ist 16550 angegeben
- Für die vlan-central-2-Verbindung lautet die **Colo-CPE-IP** 169.254.120.74/29, die **Cloud-Router-IP** ist 169.254.120.73/29 und als **Cloud-Router-BGP-ASN** ist 16550 angegeben.
- .




 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** Bestimmen Sie die IP-Adressen, die Sie für die lokalen GRE-IP-Adressen verwenden werden, wenn Sie die Colo-Connect-Dienstverbindungen einrichten.

Diese konfigurieren Sie beim Einrichten einer Colo-Connect-Dienstverbindung (**Panorama** > **Cloud Services** > **Konfiguration** > **Dienstverbindung**) im Bereich **Peer-IP 1** und **Peer-IP 2**.




Wenn Sie eine Dienstverbindung so konfigurieren, dass ein Durchsatz von bis zu 10 Gb/s unterstützt wird, definieren Sie jeweils einen Tunnel in **Verbindung 1**und einen in **Verbindung 2**, insgesamt also zwei Tunnel in jeder Dienstverbindung.

Wenn Sie eine Dienstverbindung so konfigurieren, dass ein Durchsatz über 10 Gb/s (bis zu 20 Gb/s) unterstützt wird, definieren Sie jeweils zwei Tunnel in **Verbindung 1**und **Verbindung 2**, insgesamt also vier Tunnel in jeder Dienstverbindung.

Die folgenden Beispiele zeigen, wie ein Tunnel für mehr als 10 Gb/s Durchsatz konfiguriert wird, sodass zwei Tunnel pro Verbindung verwendet werden, die die folgenden Peer-IP-Adressen benutzen:

- 172.120.1.1 für Verbindung 1
- 172.130.1.1 für Verbindung 1
- 172.121.1.1 für Verbindung 2
- 172.131.1.1 für Verbindung 2

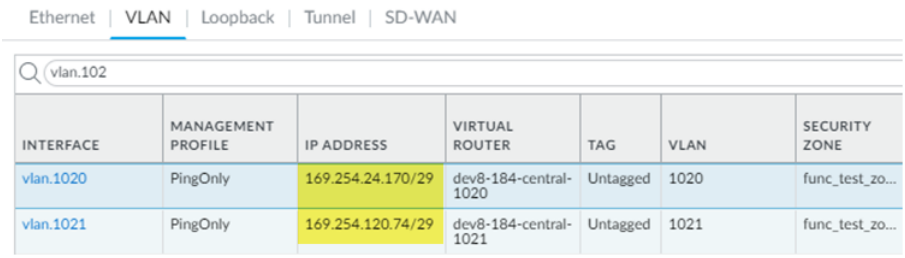
 ©2025 Palo Alto Networks, Inc.

**STEP 5 |** Melden Sie sich beim Colo-Router an.

In den folgenden Screenshots zur Konfiguration wird eine Palo Alto Networks Next-Generation-Firewall als Colo-Router eingesetzt.

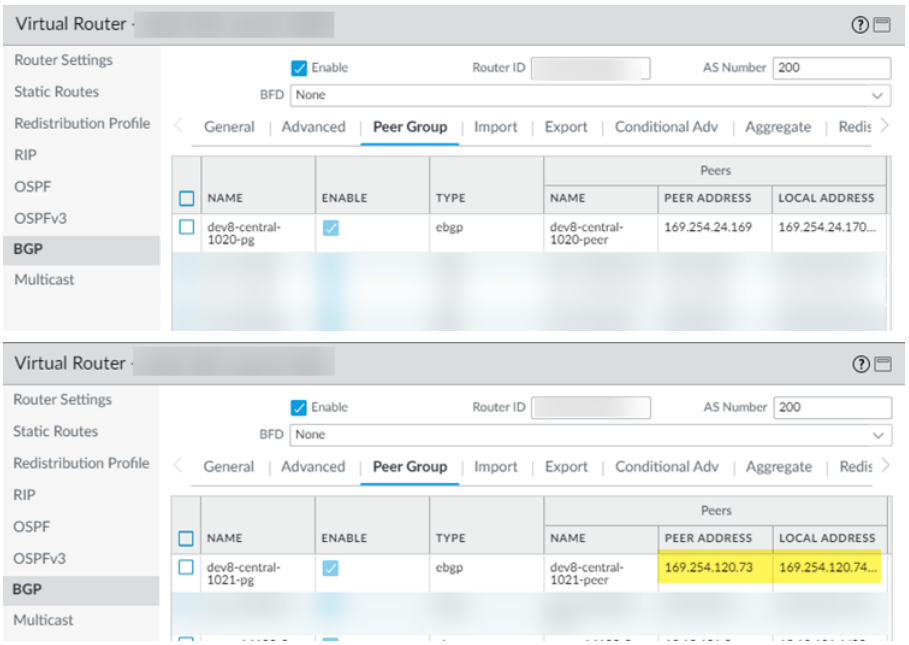
**STEP 6 |** Fügen Sie ein VLAN-Interface hinzu und geben Sie die **Colo-CPE-IP**-Adresse als IP-Adresse an.

Wenn Sie als Colo-Router eine Next-Generation-Firewall verwenden, dann wählen Sie **Netzwerk** > **Schnittstellen** > **VLAN** und **Hinzufügen** für die VLAN-Schnittstelle aus und geben Sie den Namen für den **Virtuellen Router** an.




**STEP 7 |** Konfigurieren Sie die Colo-Router-IP-Adresse (**Colo-CPE-IP**) als lokale eBGP-IP-Adresse und konfigurieren Sie die Cloud-Router-IP-Adresse (**Cloud-Router-IP**) als eBGP-Peer-Adresse auf Ihrem Colo-Router.

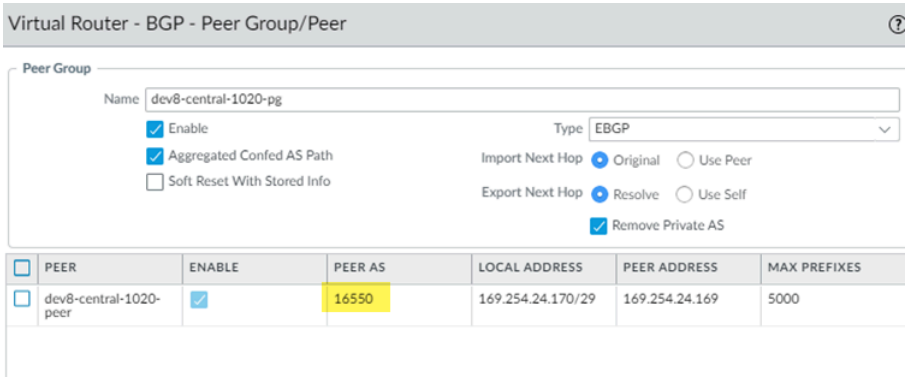
Wenn Sie eine Next-Generation-Firewall als Colo-Router verwenden, wählen Sie **Netzwerk** > **Virtuelle Router** und dann für einen virtuellen Router **Hinzufügen** aus. Wählen Sie anschließend **BGP** > **Peer-Gruppe** aus und geben Sie die **Colo-CPE-IP** als **Peer-Adresse** und die **Cloud-Router-IP** als **lokale Adresse** ein.




 ©2025 Palo Alto Networks, Inc.

**STEP 8 |** Konfigurieren Sie die **Cloud-Router-BGP-ASN** als die eBGP-Peer-ASN (Autonomous-System-Nummer).

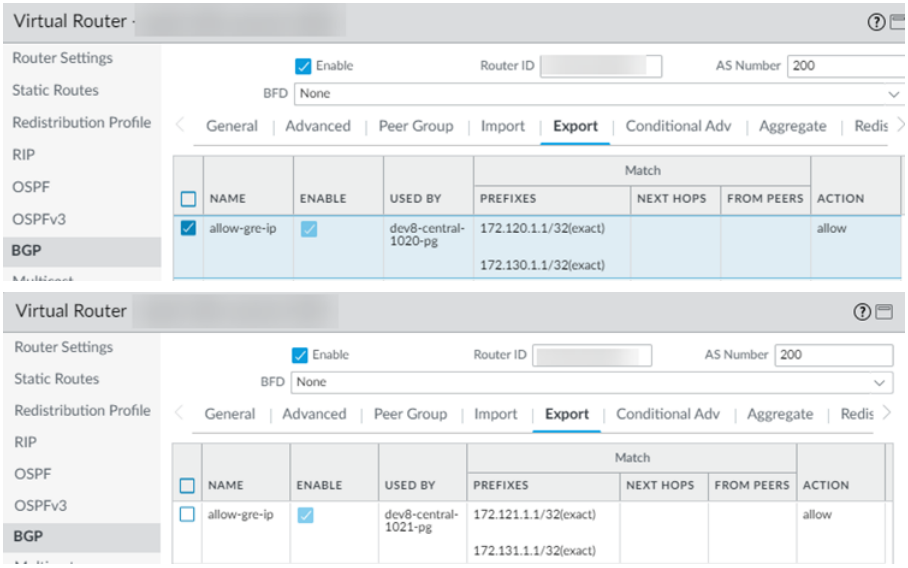
Wenn Sie eine Next-Generation-Firewall als Colo-Router verwenden, wählen Sie **Netzwerk** > **Virtuelle Router** und dann für einen virtuellen Router **Hinzufügen** aus. Wählen Sie anschließend **BGP** > **Peer-Gruppe** aus und **fügen Sie** eine Peer-Gruppe hinzu und wählen Sie ein **Peer-AS** mit dem Wert **16500** aus.




**STEP 9 |** Erstellen Sie eine BGP-Exportrichtlinie, mit der nur die lokale GRE-IP-Adresse an die Peer-IP-Adresse des Cloud-Routers mitgeteilt werden kann.

Da Cloud-Router nur eine begrenzte Routenanzahl empfangen können, müssen Sie Richtlinien erstellen, damit nur das Routing zwischen den IP-Adressen für die GRE-Tunnel der Dienstverbindung an den Cloud-Router gesendet wird.

Wenn Sie eine Next-Generation-Firewall als Colo-Router verwenden, wählen Sie **Netzwerk** > **Virtuelle Router** und für einen virtuellen Router **Hinzufügen** aus. Wählen Sie dann **BGP** > **Exportieren**, **Hinzufügen** für eine Exportregel aus und führen Sie einen **Abgleich** der IP-Adressen durch, die als Peer-IP-Adresse verwendet werden können. Erstellen Sie dann die **Aktion** des Typs **Zulassen**.




**STEP 10 |** Erstellen Sie die Colo-Connect-Dienstverbindungen.

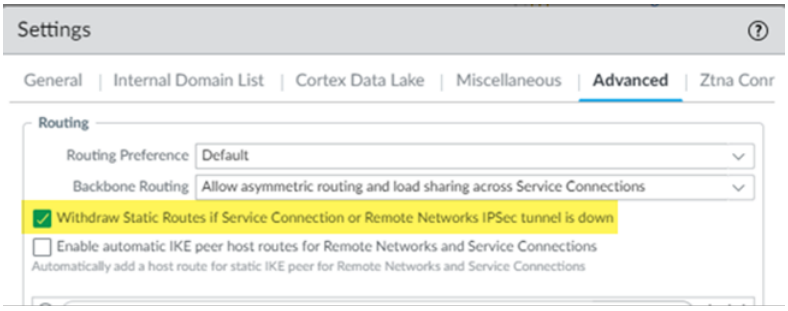
 ©2025 Palo Alto Networks, Inc.

## Erstellen Sie Colo-Connect-Dienstverbindungen

Colo-Connect verwendet Dienstverbindungen, die sich jedoch von Prisma Access-Dienstverbindungen dahingehend unterscheiden, dass sie anstelle von IPSec-Tunnel GRE-Tunnel und für das Routing immer BGP verwenden. Um Colo-Connect-Dienstverbindungen zu konfigurieren, führen Sie die folgenden Schritte aus.

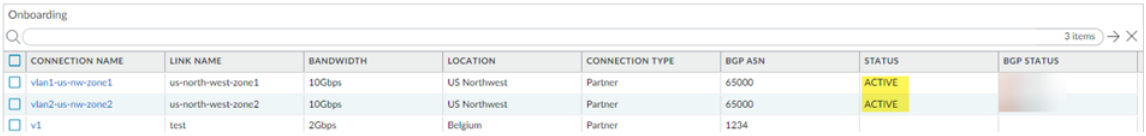
**STEP 1 |** Vergewissern Sie sich in der zur Verwaltung von Prisma Access verwendeten Panorama-Instanz, dass Prisma Access statische Routen zurückzieht. Rufen Sie hierzu **Panorama** > **Cloud Services** > **Konfiguration** > **Diensteinrichtung** auf und klicken Sie auf das Zahnradsymbol, um die **Einstellungen** zu bearbeiten. Wählen Sie dann **Statische Routen zurückziehen, wenn die Dienstverbindung oder der Remote Network IPSec-Tunnel ausgefallen ist**.

Die Auswahl dieser Option stellt sicher, dass bei einem Ausfall des GRE-Tunnels die vom GRE-Tunnel verwendete statische Route zurückgezogen wird.



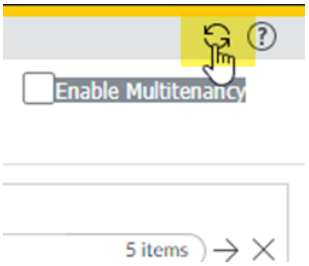

**STEP 2 |** Wählen Sie die Registerkarte **Colo-Connect** aus und prüfen Sie dort, ob die Verbindungen sich im Status **Aktiv** befinden. Überprüfen Sie dazu das Feld **Status** im Onboarding-Bereich.

Erst wenn der **Status** der Verbindung **Aktiv** lautet, können Sie Dienstverbindungen konfigurieren.




**STEP 3 |** Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Dienstverbindung** aus.

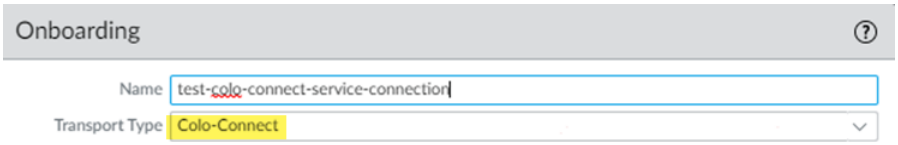
**STEP 4 |** Klicken Sie oben rechts in der Panorama-Benutzeroberfläche auf **Aktualisieren**, damit die Colo-Connect-Konfiguration im Bereich für Dienstverbindungen bereitgestellt wird.




 ©2025 Palo Alto Networks, Inc.

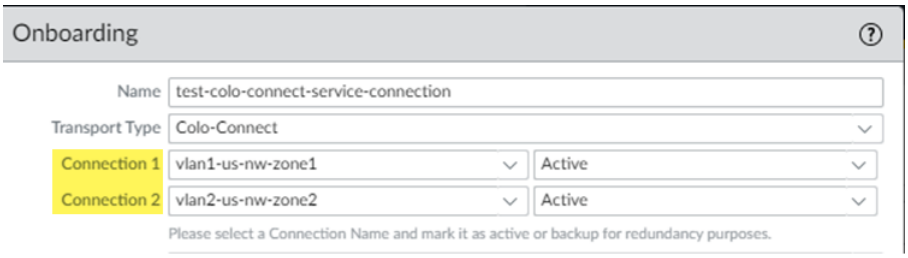
**STEP 5 |** **Fügen Sie** eine Dienstverbindung hinzu, geben Sie ihr einen eindeutigen **Namen** und wählen Sie den **Transporttyp Colo-Connect** aus.

*Stellen Sie sicher, dass der eingegebene Name maximal 31 Zeichen lang ist; die Eingabe eines Namens mit 32 oder mehr Zeichen führt dazu, dass der Tunnel in der Prisma Access-Infrastruktur falsch zugeordnet wird.*




**STEP 6 |** Wählen Sie zwei Verbindungen aus, die mit den Dienstverbindungen (**Verbindung 1** und **Verbindung 2**) verwendet werden sollen.

Diese Verbindungen müssen sich in zwei verschiedenen Zonen befinden.




**STEP 7 |** Wählen Sie **Aktiv** oder **Backup** für **Verbindung 1** und **Verbindung 2** aus

Verwenden Sie beim Einrichten von Dienstverbindungen die folgenden Richtlinien:

- Sie können Verbindungen in diesen Modi konfigurieren:
  - **Aktiv/Aktiv**
  - **Aktiv/Backup**
  - **Backup/Aktiv**

  Die Konfiguration beider Verbindungen im Modus **Backup/Backup** ist ungültig und wird nicht unterstützt.
- Die Bandbreite der Verbindungen muss für alle Modi gleich sein.
- Die Verbindungen müssen sich in verschiedenen Zonen befinden.
- Die maximale Bandbreite, die Sie für eine Dienstverbindung angeben können, beträgt 20 Gb/s. Wenn Sie für eine Verbindung eine **Bandbreite** von **20 Gb/s** angeben, können Sie diese Verbindung nicht in einer **Aktiv/Aktiv**-Konfiguration verwenden. (Stattdessen müssen Sie **Aktiv/Backup** angeben).
- Kombinieren Sie keine dedizierten Interconnect-Verbindungen und Partner Interconnect-Verbindungen innerhalb derselben Dienstverbindung und stellen Sie sicher, dass die Dienstverbindungen unterschiedliche Zonen verwenden. Diese Tabelle zeigt die erlaubten und nicht erlaubten Konfigurationen für Dienstverbindungen. Dies setzt allerdings voraus,

 ©2025 Palo Alto Networks, Inc.

dass Zonen, Standorte, Bandbreite und Rollen den Richtlinien und Anforderungen für Dienstverbindungen entsprechen:

| Verbindung 1 gehört zu | Verbindung 2 gehört zu | Gültige Colo-Connect-Dienstverbindungskonfiguratio |
|---|---|---|
| Partner-Connect 1 | Partner-Connect 2 | Ja |
| Dedizierte Connect 1 | Dedizierte Connect 2 | Ja |
| Partner- Connect 1 | Partner-Connect 1 | Nein |
| Dedizierte Connect 1 | Dedizierte Connect 1 | Nein |
| Partner-Connect | Dedizierte Connect | Nein |

**STEP 8 |** (Optional, nur Hot-Potato-Routing-Bereitstellungen) Wählen Sie eine Dienstverbindung aus, die als bevorzugte Backup-Dienstverbindung (Backup SC) verwendet werden soll.

Sie können nur eine Dienstverbindung auswählen, die als Colo-Connect-Dienstverbindung konfiguriert wurde. Prisma Access verwendet die von Ihnen ausgewählte Backup-Dienstverbindung (Backup-SC) als bevorzugte Dienstverbindung für den Fall eines Verbindungsfehlers. Durch Auswahl einer Backup-Dienstverbindung (Backup-SC) können Probleme aufgrund asymmetrischen Routings verhindert werden, wenn Sie mehr als zwei Dienstverbindungen erstellt haben.

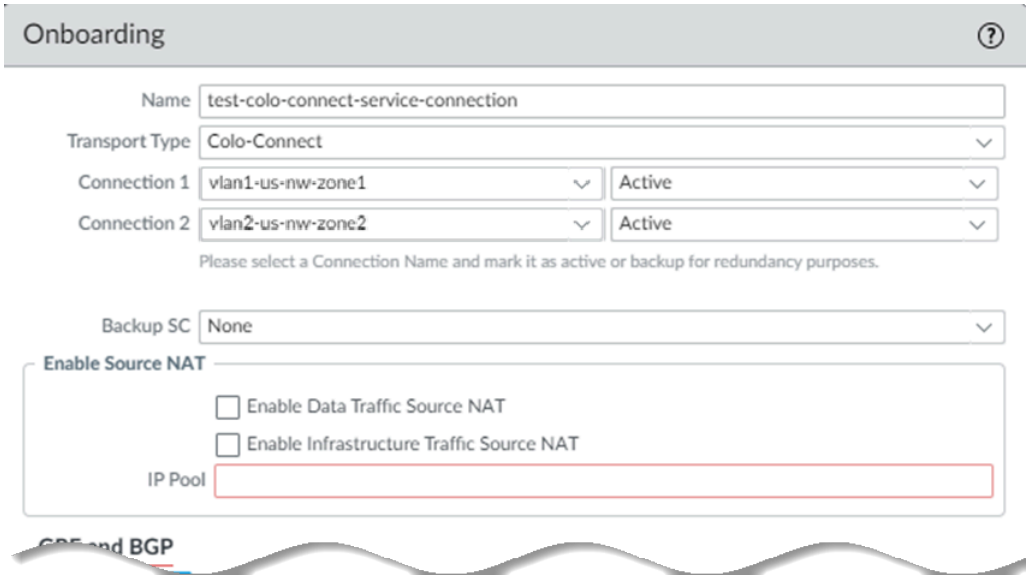
**STEP 9 |** (Optional) Aktivieren Sie die Quell-NAT für IP-Pooladressen für mobile GlobalProtect-Benutzer und/oder für IP-Adressen im Infrastruktursubnetz.

Sie können ein Subnetz an einer oder mehreren Dienstverbindungen angeben, die für den NAT-Datenverkehr zwischen mobilen Prisma Access GlobalProtect-Benutzern und privaten Anwendungen und Ressourcen in einem Rechenzentrum verwendet werden.

- **Quell-NAT des Datenverkehrs aktivieren** – Führt die NAT für Adressen des IP-Adresspools mobiler Benutzer aus, sodass diese nicht ans Rechenzentrum mitgeteilt werden und nur die von Ihnen bei den Dienstverbindungen angegebenen Subnetze im Rechenzentrum mitgeteilt und geroutet werden.
- **Quell-NAT des Infrastrukturdatenverkehrs aktivieren** – Führt die NAT für Adressen aus dem Infrastruktursubnetz aus, sodass diese Adressen nicht ans Rechenzentrum mitgeteilt werden und nur die von Ihnen bei den Dienstverbindungen angegebenen Subnetze im Rechenzentrum mitgeteilt und geroutet werden.
- **IP-Pool** – Geben Sie den IP-Adresspool an, der zum Ausführen der NAT für den IP-Adresspool mobiler Benutzer und/oder im Infrastruktursubnetz verwendet wird. Verwenden Sie ein privates IP-Subnetz (RFC 1918) oder ein geeignetes Subnetz, das innerhalb Ihrer Routingdomäne routingfähig ist und sich nicht mit dem GlobalProtect-IP-

 ©2025 Palo Alto Networks, Inc.

Adresspool für mobile Benutzer oder dem Infrastruktursubnetz überschneidet. Geben Sie ein Subnetz zwischen /25 und /32 ein.




**STEP 10 |** Konfigurieren Sie im Bereich **GRE und BGP** den GRE-Tunnel und die BGP-Einstellungen für die Dienstverbindung.

BGP ist immer auf **Aktivieren** gesetzt.

1. (Optional) Wählen Sie zwischen den folgenden Optionen:

   - Um eine Community des Typs **No-Export** für Corporate Access Nodes (Dienstverbindungen) den ausgehenden Präfixen von den eBGP-Peers im Customer Premises Equipment (CPE) hinzuzufügen, legen Sie für **No-Export-Community hinzufügen** die Einstellung **Aktiviert Aus** fest. Diese Funktion ist standardmäßig auf **Deaktiviert** eingestellt.

     Verwenden Sie diese Funktionalität im Hot-Potato-Routing-Modus nicht.

   - Um zu verhindern, dass der Prisma Access-BGP-Peer Routen in das Netzwerk Ihrer Organisation weiterleitet. **Keine Prisma Access-Routen mitteilen**.

     Standardmäßig teilt Prisma Access alle BGP-Routinginformationen einschließlich der Informationen zu lokalen Routen und allen Präfixen mit, die von anderen Dienstverbindungen, Remote-Netzwerken und den Subnetzen mobiler Benutzer empfangen werden. Aktivieren Sie dieses Kontrollkästchen, um Prisma Access daran zu hindern, BGP-Mitteilungen zu senden. Die empfangenen BGP-Informationen werden aber weiterhin verwendet, um Informationen zu Routen anderer BGP-Nachbarn zu erhalten.

     *Da Prisma Access keine BGP-Mitteilungen sendet, wenn Sie diese Option auswählen, müssen Sie statische Routen auf dem lokalen Gerät konfigurieren, um Routen zurück zu Prisma Access einzurichten.*


©2025 Palo Alto Networks, Inc.

- Um die Anzahl der IP-Subnetzmitteilungen für mobile Benutzer über BGP zu Ihrem Customer Premises Equipment (CPE) zu reduzieren, wählen Sie **Mobile Benutzerrouten vor dem Mitteilen zusammenfassen** aus.

  Standardmäßig teilt Prisma Access die IP-Adresspools der mobilen Benutzer in Blöcken von /24-Subnetzen mit. Wenn Sie sie zusammenfassen, teilt Prisma Access den Pool basierend auf dem von Ihnen angegebenen Subnetz mit. Beispiel: Prisma Access teilt einen öffentlichen mobilen IP-Pool für Benutzer mit der Angabe 10.8.0.0/20 unter Verwendung des Subnetzes /20 mit, anstatt den Pool in die Subnetze 10.8.1.0/24, 10.8.2.0/24, 10.8.3.0/24 usw. zu unterteilen, bevor sie mitgeteilt werden. Durch die Zusammenfassung dieser Mitteilungen kann die Anzahl der in den CPE-Routingtabellen gespeicherten Routen reduziert werden. Sie können die Zusammenfassung von IP-Pools z. B. mit Cloud-VPN-Gateways (Virtual Private Gateways (VGWs) oder Transit Gateways (TGWs)) verwenden, die eine begrenzte Anzahl von Routen akzeptieren können.

  *Wenn Sie das Hot-Potato-Routing aktiviert haben und die Routen-Zusammenfassung aktivieren, fügt Prisma Access keine weiteren AS-PATH-Voranstellungen mehr hinzu, was zu asymmetrischem Routing führen kann. Stellen Sie sicher, dass Ihr Rückkehrdatenverkehr vom Rechenzentrum oder der Zentrale eine symmetrische Rückkehr garantiert, bevor Sie die Routenzusammenfassung mit Hot-Potato-Routing aktivieren.*

2. Routing für die Dienstverbindung mit GRE-Tunneln einrichten.
3. Kehren Sie in der zur Verwaltung von Prisma Access verwendeten Panorama-Instanz zu **Panorama** > **Cloud Service** > **Konfiguration** > **Dienstverbindung** zurück und richten Sie einen GRE-Tunnel für **Verbindung 1** ein, indem Sie einen **GRE-Tunnelnamen 1** und eine **Peer-IP 1** für **Verbindung 1** eingeben. Wenn mehr als 10 Gb/s Bandbreite benötigt werden, geben Sie den **GRE-Tunnelnamen 2** und die **Peer-IP 2** für den zweiten Tunnel für Verbindung 1 ein. Erstellen Sie dann einen GRE-Tunnel für **Verbindung 2**, indem Sie dieselben Schritte wiederholen.

   Jedes Paar von GRE-Tunneln in einer Verbindung unterstützt eine maximale Bandbreite von 10 Gb/s. Wenn Sie mehr als 10 Gb/s Bandbreite benötigen, konfigurieren Sie zwei Tunnel pro Verbindung. Beispiel:

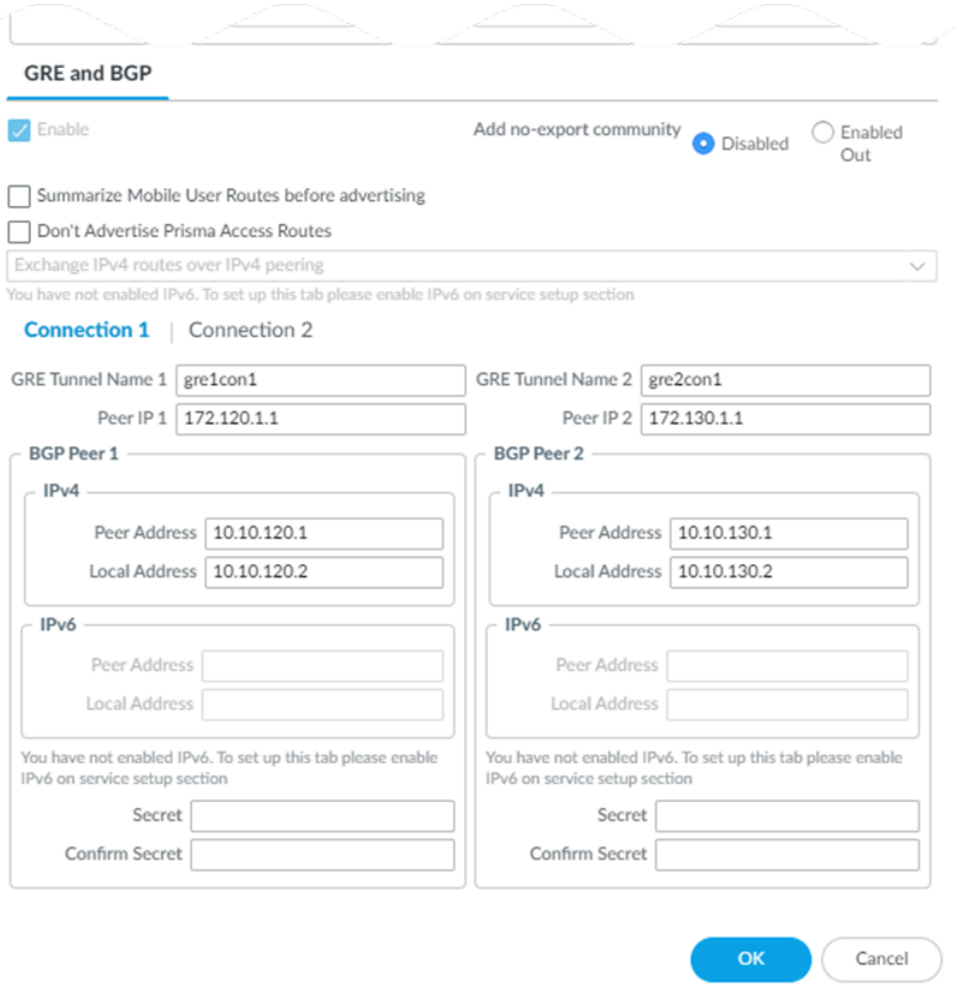
   Für die Peer-IP geben Sie die GRE-IP-Adresse des lokalen Routers im Colo ein.

   Verwenden Sie IPv4-Adressen für die BGP-Werte; IPv6 wird nicht unterstützt.
4. Geben Sie die **Peer-Adresse** und die **lokale Adresse** für den BGP-Peer 1 und, falls ein zweiter Tunnel für Verbindung 1 erforderlich war, BGP-Peer 2 ein.

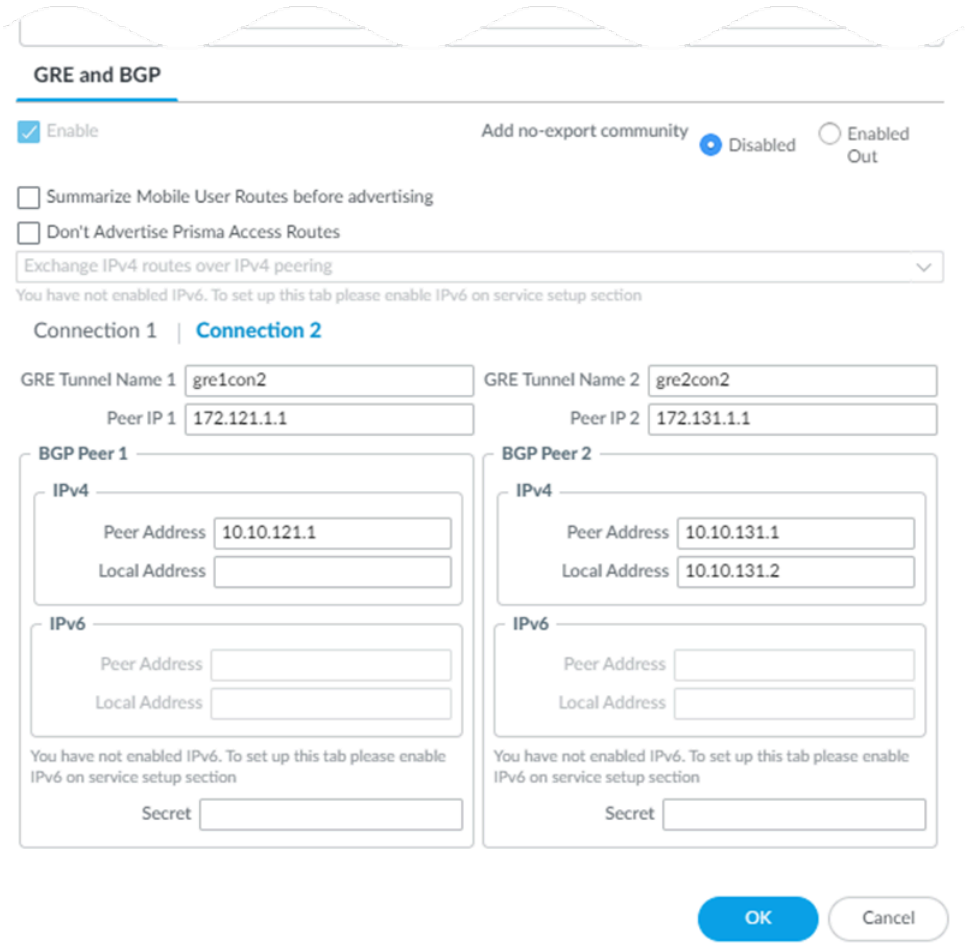
   Für die **Peer-Adresse** geben Sie die BGP-Peer-IP-Adresse des Colo-Routers ein; für die **lokale Adresse** geben Sie die Adresse ein, die für die BGP-Netzwerkeinrichtung über den GRE-Tunnel verwendet wird.

 ©2025 Palo Alto Networks, Inc.

5. (Optional) Um einen geheimen BGP-Schlüssel zu konfigurieren, geben Sie die Werte für **Geheimer Schlüssel** und **Geheimen Schlüssel bestätigen** ein.




 ©2025 Palo Alto Networks, Inc.

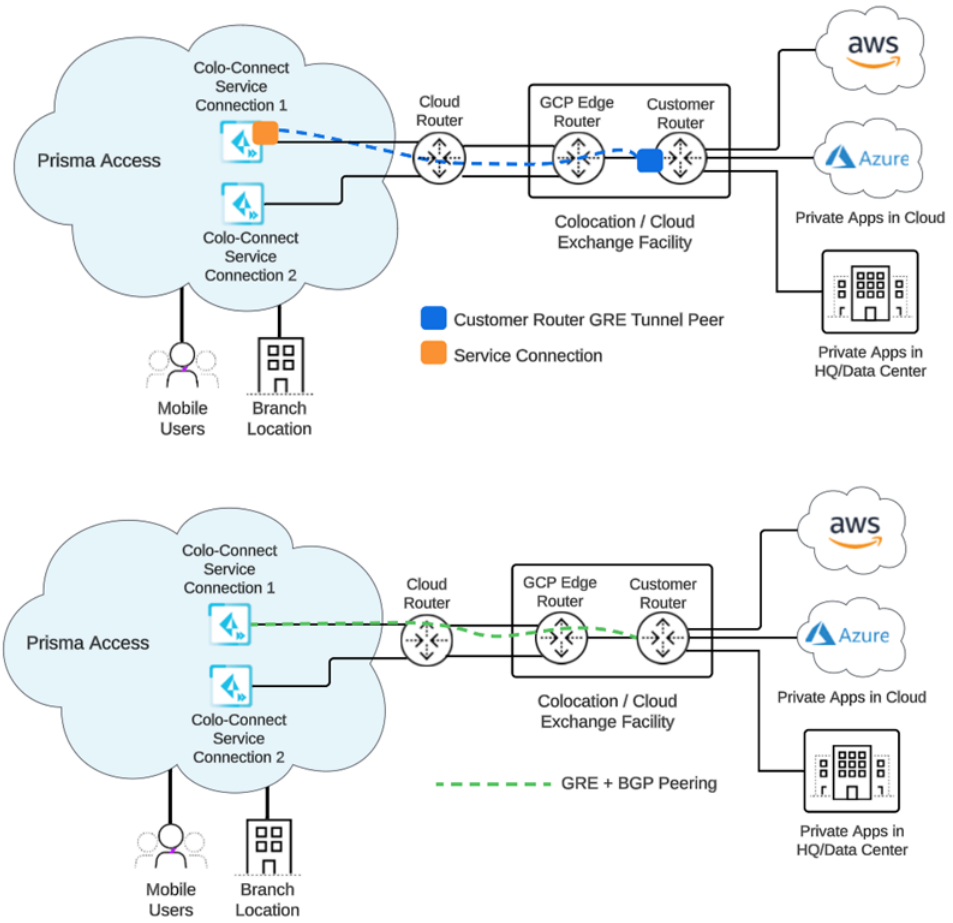



**STEP 11 |** Verwenden Sie **Commit und Push**, um Ihre Konfigurationsänderungen festzuschreiben und zu übertragen. Vergewissern Sie sich dabei, dass **Colo-Connect** im **Übertragungsumfang** ausgewählt wurde.

## Richten Sie das Routing für die Dienstverbindung mithilfe von GRE-Tunneln ein.

Der Colo-Router teilt seine GRE-Tunnel-Peer-IP-Adresse an den Cloud-Router mit und erhält die Informationen zum Subnetz für den GRE-Tunnel vom Cloud-Router. Bei der Erstkonfiguration für das eBGP-Routing über das VLAN auf dem Kundenrouter haben Sie die lokale Erreichbarkeit für die GRE-Tunnel mitgeteilt. Nachdem der Cloud-Router und der Colo-Router die Routen für das Colo-Subnetz und die lokalen GRE-IP-Adressen gegenseitig mitgeteilt und erhalten haben, werden die von der Dienstverbindung verwendeten GRE-Tunnel aktiviert (up).

 ©2025 Palo Alto Networks, Inc.




Um das Routing einzurichten und GRE-Tunnel zu den Dienstverbindungen hinzuzufügen, führen Sie die folgenden Schritte aus.

**STEP 1 |** Notieren Sie die IP-Adressen, die für die **Peer-Adresse** verwendet werden sollen, und außerdem die **lokale Adresse** für BGP-Peer 1 und, falls ein zweiter Tunnel für Verbindung 1 benötigt wird, für BGP-Peer 2.

Die hier aufgeführten Beispiele verwenden die folgenden Peer-Adressen und lokalen Adressen:

- **Peer-Adresse** – 10.10.120.0 und 10.10.130.1 für Verbindung 1, 10.10.120.2 und 10.10.130.2 für Verbindung 2
- **Lokale Adresse** – 10.10.120.2 und 10.10.130.2 für Verbindung 1, 10.10.121.2 und 10.10.131.2 für Verbindung 2

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Notieren Sie die IP-Adressen, die Sie für die **Peer-IP 1**- und, falls erforderlich, für die **Peer-IP 2**-Adresse in den Dienstverbindungen verwenden wollen.

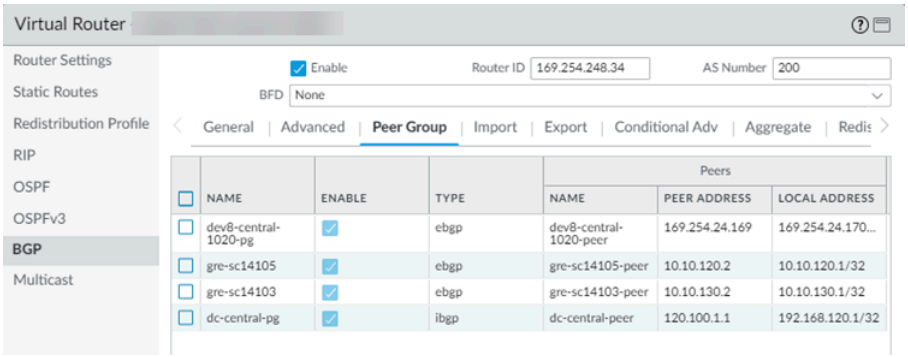
Sie verwenden diese IP-Adressen, um eine Ablehnungsrichtlinie zu erstellen, die verhindert, dass die lokale GRE-IP-Adresse an die Colo-Connect-Dienstverbindung mitgeteilt wird.

Alle Beispiele in diesem Dokument verwenden diese IP-Adressen:

- 172.120.1.1 für Verbindung 1
- 172.130.1.1 für Verbindung 1
- 172.121.1.1 für Verbindung 2
- 172.131.1.1 für Verbindung 2

**STEP 3 |** Konfigurieren Sie Peer-Gruppen für die Peer- und die lokalen IP-Adressen.

Wenn Sie eine Next-Generation-Firewall als Colo-Router benutzen, wählen Sie **Netzwerk** > **Virtuelle Router**, **Hinzufügen** aus, um einen virtuellen Router hinzuzufügen. Rufen Sie dann **BGP** > **Peer-Gruppe** auf und geben Sie die Peer-Adresse als **Peer-Adresse** und die **lokale Adresse** als **lokale Adresse** ein.



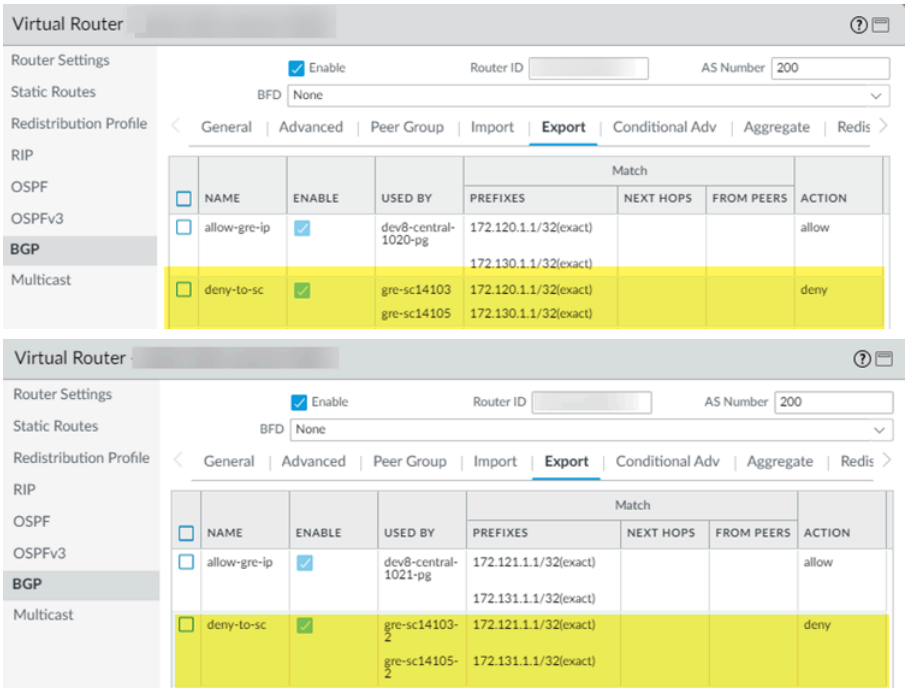

**STEP 4 |** Erstellen Sie eine BGP-Exportrichtlinie, um die Peer-IP-Adressen, die Sie konfiguriert haben (172.120.1.1, 172.130.1.1, 172.121.1.1 und 172.131.1.1), abzulehnen und sie auf die von Ihnen erstellten Peer-Gruppen anzuwenden.

Diese Exportrichtlinie legt eine Ablehnungsregel für die lokalen GRE-Tunnel-Peer-IP-Adressen fest und erlaubt, dass alle anderen Routen an die Dienstverbindung mitgeteilt werden.

Wenn Sie eine Next-Generation-Firewall als Colo-Router verwenden, wählen Sie **Netzwerk** > **Virtuelle Router** und für einen virtuellen Router **Hinzufügen** aus. Wählen Sie dann **BGP** > **Exportieren**, **Hinzufügen** für eine Exportregel aus und führen Sie einen **Abgleich** der IP-

 ©2025 Palo Alto Networks, Inc.

Adressen durch, die als Peer-IP-Adresse verwendet werden können. Erstellen Sie dann die **Aktion** des Typs **Ablehnen**.




## Erhöhen oder Verringern der Bandbreite einer Colo-Connect-Dienstverbindung

Wenn Sie Dienstverbindungen konfigurieren, konfigurieren Sie die Bandbreite basierend auf den Verbindungen (VLAN-Anhängen), die Sie zuordnen. Sie weisen zwei Verbindungen pro Dienstverbindung zu und dann entweder einen oder zwei GRE-Tunnel pro Verbindung.

Während jede Colo-Connect-Dienstverbindung maximal 20 Gb/s unterstützt, unterstützt jeder GRE-Tunnel in der Dienstverbindung 10 Gb/s. Aus diesem Grund müssen Sie möglicherweise die GRE-Tunnel in der Colo-Connect-Dienstverbindung hinzufügen oder löschen, um die gesamte Bandbreite in einem Link zu ändern. Dies kann dazu führen, dass die Bandbreite der Dienstverbindung dann die Grenze von 10 Gb/s über- oder unterschreitet.

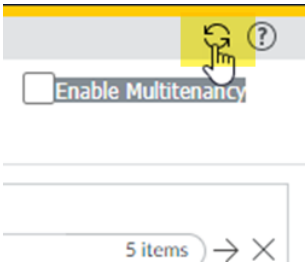
### Erhöhen der Bandbreite einer Colo-Connect-Dienstverbindung

Um die Bandbreite einer bestehenden Dienstverbindung über 10 Gb/s zu erhöhen, führen Sie die folgenden Schritte aus:

**STEP 1 |** Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Colo-Connect** aus.

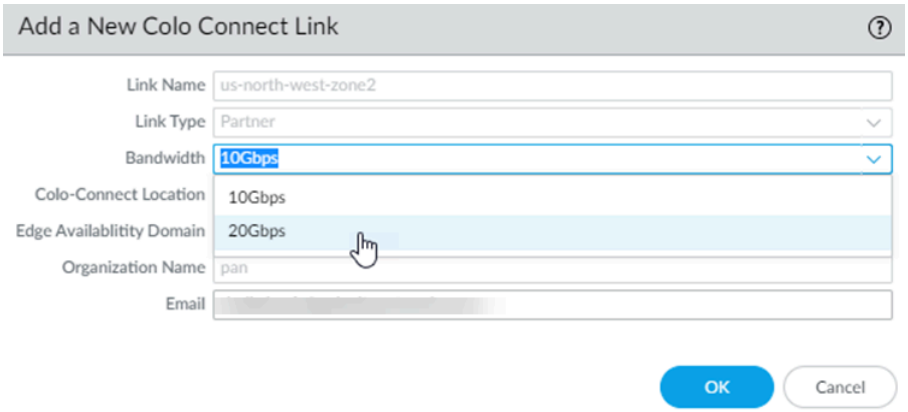
 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Rufen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Dienstverbindung** auf und klicken Sie oben rechts in der Panorama-Benutzeroberfläche auf **Aktualisieren**, damit die Colo-Connect-Konfiguration im Bereich für Dienstverbindungen bereitgestellt wird.




**STEP 3 |** Wählen Sie den **Linknamen** aus, der der Dienstverbindung zugeordnet ist.

**STEP 4 |** Erhöhen Sie die **Bandbreite** des Links (Interconnect).

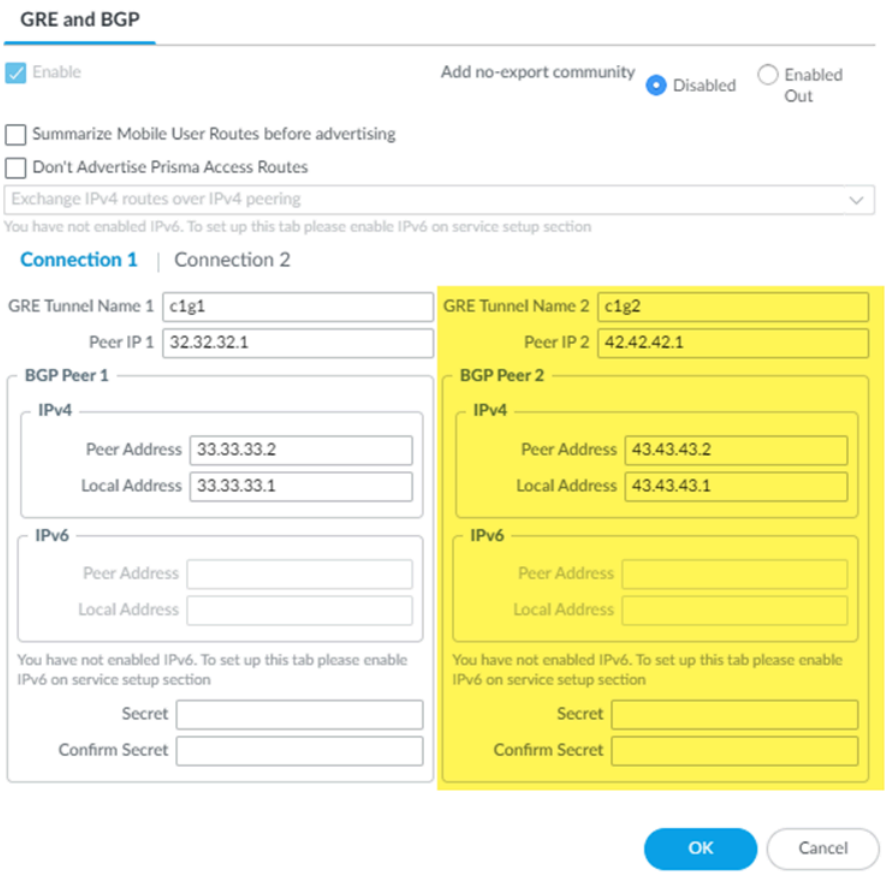



**STEP 5 |** Führen Sie die Aktion **Commit und Push** aus, um Ihre Änderungen festzuschreiben und zu übertragen. Wählen Sie im **Übertragungsumfang** nur **Colo-Connect** aus.

**STEP 6 |** Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Dienstverbindung** > ***<service-connection-name>*** > **Onboarding** aus.


©2025 Palo Alto Networks, Inc.

**STEP 7 |** Fügen Sie den zusätzlichen GRE-Tunnel zur Colo-Connect-Dienstverbindung hinzu.




**STEP 8 |** Führen Sie die Aktion **Commit und Push** aus, um Ihre Änderungen festzuschreiben und zu übertragen. Wählen Sie im **Übertragungsumfang** die Option **Dienstverbindungen** aus.

**STEP 9 |** Fügen Sie den Exportrichtlinien für das VLAN-eBGP-Routing und das Dienstverbindungsrouting für die GRE-Tunnel die lokalen GRE-IP-Adressen (Peer) hinzu.

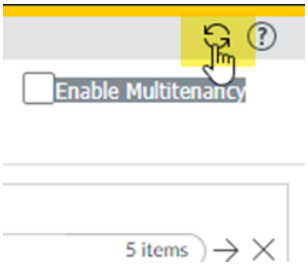
### Verringern der Bandbreite einer Colo-Connect-Dienstverbindung

Um die Bandbreite einer bestehenden Dienstverbindung unter 10 Gb/s zu verringern, führen Sie die folgenden Schritte aus:

**STEP 1 |** Rufen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Colo-Connect** auf.

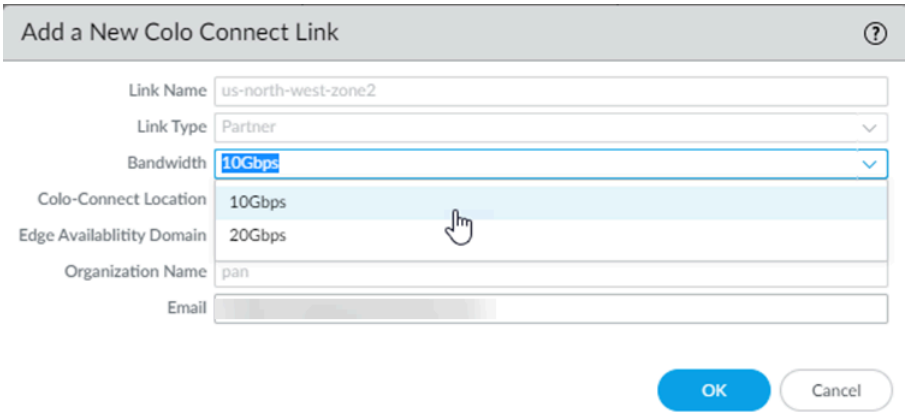
 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Rufen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Dienstverbindung** auf und klicken Sie oben rechts in der Panorama-Benutzeroberfläche auf **Aktualisieren**, damit die Colo-Connect-Konfiguration im Bereich für Dienstverbindungen bereitgestellt wird.




**STEP 3 |** Wählen Sie den **Linknamen** aus, der der Dienstverbindung zugeordnet ist.

**STEP 4 |** Reduzieren Sie die **Bandbreite** des Links (Interconnect).




**STEP 5 |** Führen Sie die Aktion **Commit und Push** aus, um Ihre Änderungen festzuschreiben und zu übertragen. Wählen Sie im **Übertragungsumfang** nur **Colo-Connect** aus.

**STEP 6 |** Führen Sie die Aktion **Commit und Push** aus, um Ihre Änderungen festzuschreiben und zu übertragen. Wählen Sie im **Übertragungsumfang** die Option **Dienstverbindungen** aus.

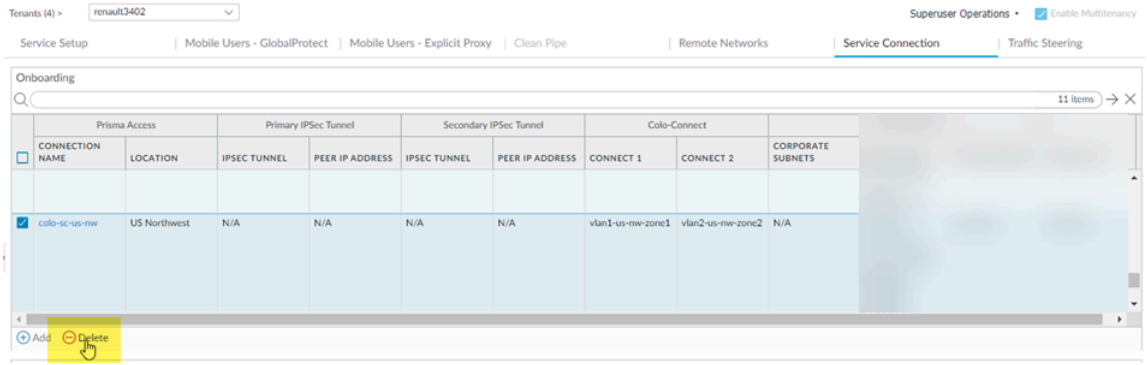
Sie müssen die Dienstverbindung nicht neu konfigurieren, um den zusätzlichen GRE-Tunnel zu entfernen. Prisma Access erkennt und senkt die Bandbreite des Links und entfernt den zusätzlichen Tunnel, wenn Sie Ihre Änderungen im Übertragungsumfang der Dienstverbindung festschreiben und sie übertragen.

## Löschen einer Colo-Connect-Verbindung

Um eine Colo-Connect-Verbindung zu löschen, befolgen Sie die umgekehrte Reihenfolge der Konfiguration, indem Sie die folgenden Schritte ausführen:

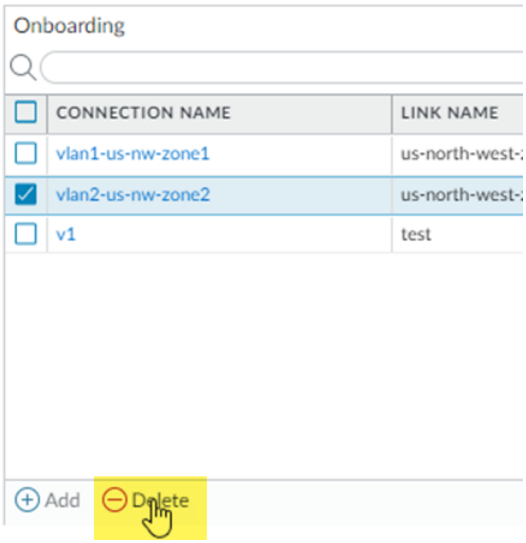
 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** Löschen Sie die der Verbindung zugeordneten Dienstverbindungen, indem Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Dienstverbindung** aufrufen, die Dienstverbindung auswählen und auf **Löschen** klicken.



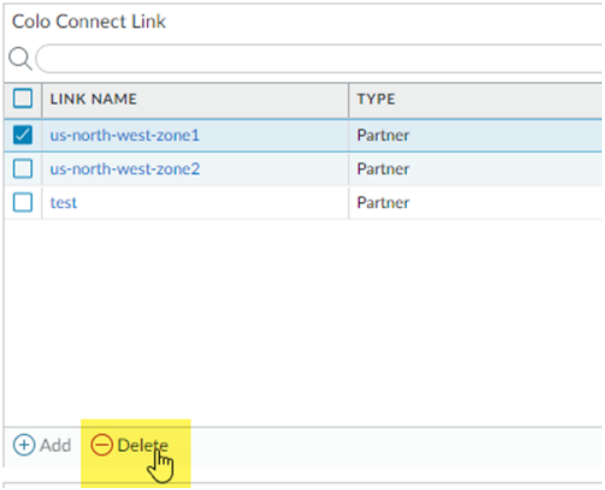

**STEP 2 |** Führen Sie die Aktion **Commit und Push** aus, um Ihre Änderungen festzuschreiben und zu übertragen. Wählen Sie im **Übertragungsumfang** die Option **Dienstverbindungen** aus.

**STEP 3 |** Löschen Sie die Colo-Connect-Verbindungen, die der Verbindung zugeordnet sind. Wählen Sie hierzu **Panorama** > **Cloud Services** > **Konfiguration** > **Colo-Connect** und dann im Abschnitt **Onboarding** den **Verbindungsnamen** sowie **Löschen** aus.




 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** Löschen Sie den Colo-Connect-Link, indem Sie den **Linknamen** und dann **Löschen** auswählen.




**STEP 5 |** Löschen Sie die lokalen GRE-IP-Adressen (Peer) auf Basis Ihrer Exportrichtlinien für das VLAN-eBGP-Routing und das Dienstverbindungsrouting für die GRE-Tunnel.

 ©2025 Palo Alto Networks, Inc.

# App-Beschleunigung in Prisma Access

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Mindestens Prisma Access Version 5.0 Innovation<br>❑ Prisma Access-Lizenz<br>❑ Für die App-Beschleunigung wird Prisma Access Dataplane Version 10.2.10 benötigt.<br>❑ Add-on-Lizenz für App-Beschleunigung<br>Die Lizenz für die App-Beschleunigung umfasst eine 30-Tage-Evaluierungslizenz für Autonomous DEM (ADEM), sodass Sie Leistungskennzahlen für die App-Beschleunigung von ADEM abrufen können. |

Durch die App-Beschleunigung können Sie die Ursachen einer schlechten App-Leistung direkt beseitigen. Sie arbeitet im Echtzeitmodus, um die Auswirkungen der Ursachen zu mildern. Dadurch wird die Benutzererfahrung für Prisma Access-GlobalProtect- und Remote-Netzwerk-Benutzer drastisch verbessert.

Die Hauptursachen für die schlechte Benutzererfahrung beim Zugriff auf Apps sind dynamische Inhalte (Inhalte, die für jeden Benutzer einzeln und auf Abruf verarbeitet werden müssen) und Probleme mit der Netzwerkverbindung.

Die App-Beschleunigung bietet Ihnen folgende Funktionalität:

**Beschleunigung für Top-SaaS-Apps** – Die App-Beschleunigung für Prisma SASE beschleunigt dynamische Inhalte, um die Reaktionszeit der Top-SaaS-Apps zu verbessern. Die Funktion bereitet die dynamischen Inhalte, die jeder Benutzer benötigt, sicher und intelligent auf, bevor der Benutzer sie anfordert.

Als Ergebnis reduziert die App-Beschleunigung die Reaktionszeit von Anwendungen und APIs drastisch, sodass die Benutzererfahrung verbessert und die Produktivität erheblich gesteigert werden kann.

Beschleunigte Anwendungen werden im Abschnitt Unterstützte Apps aufgelistet.

**Netzwerkbeschleunigung** – Wenn Ihre Benutzer auf Apps zugreifen, kann es zu einer schlechten App-Performance kommen, die durch verringerten Durchsatz verursacht wird, was wiederum durch Paketverlust, verschlechterte drahtlose Konnektivität, Netzwerküberlastung und andere Faktoren verursacht werden kann. Diese Netzwerkprobleme können ihrerseits die Erfahrung der Mitarbeiter beeinträchtigen und ihre Produktivität verringern.

Als das Internet konzipiert wurde, waren die Netzwerke homogen und die drahtlose Konnektivität steckte noch in den Kinderschuhen. Grundlegende Protokolle wie TCP wurden ursprünglich für diese Netzwerke erstellt. Heute sind Netzwerke nicht mehr homogen und die drahtlose Konnektivität schafft eine sehr variable Benutzererfahrung. Wenn Benutzer unter verschlechterten Netzwerkbedingungen leiden, kann TCP nicht unterscheiden, ob das Problem aufgrund von Geräteeinschränkungen, Netzwerkbeschränkungen oder physischen Einschränkungen aufgetreten ist.

Ohne dass dazu Änderungen an Ihrer Clientkonfiguration oder Ihren Anwendungen erforderlich werden, liefert die App-Beschleunigung Daten, die Ihnen zu einem soliden Verständnis in den folgenden Bereichen verhelfen:

- **Gerätefähigkeit** – Die Art des Client-Endpunkts
- **Netzwerkfähigkeit** – Die Art des Netzwerks
- **App-Kontext** – Die Art der verwendeten App

Die App-Beschleunigung nutzt ihre verfügbaren Daten zu Geräten, Netzwerken und zum Anwendungskontext, die dazu eingesetzt werden, den Durchsatz Ihres Systems zu maximieren und es in Echtzeit an sich verändernde Netzwerkbedingungen anzupassen.

Im Vergleich zum direkten Internetzugang bietet die App-Beschleunigung eine deutliche Durchsatzverbesserung für den TCP-Datenverkehr bei der Verbindung über Prisma Access.

Sie können Durchsatzverbesserungen durch die App-Beschleunigung in Prisma SASE-Vorfällen und -Benachrichtigungen anzeigen. KI-gestütztes autonomes DEM (ADEM) ermöglicht die Integration mit der App-Beschleunigung und liefert Ihnen Metriken wie die Anzahl der Anwendungen, die beschleunigt wurden, und die insgesamt erzielte Leistungssteigerung.

 ©2025 Palo Alto Networks, Inc.

# Anforderungen und Richtlinien für die App-Beschleunigung

Beachten Sie bei der Konfiguration der App-Beschleunigung die folgenden Richtlinien und Anforderungen:

- **Unterstützte Apps** – Die App-Beschleunigung unterstützt die folgenden Apps:
  - Amazon S3
  - Azure Storage
  - Box
  - Google Drive
  - Microsoft 365:
    - My Content
  - Microsoft OneDrive
  - Salesforce
  - SAP Ariba
  - ServiceNow
  - Slack (*Dateidownloads*)
  - Zoom:
    - Dateidownloads aus Chat
    - Cloud-Aufnahme-Downloads
    - Zoom Team Chat
- **Unterstützte Standorte** – App-Beschleunigung ist für alle Prisma Access-Standorte mit Ausnahme der folgenden Standorte verfügbar:
  - Alle lokalen Zonen
  - Bahrain
  - China
  - Irland
  - Südafrika (West)
  - Schweden
  - Vereinigte Arabische Emirate
- **Upload über vertrauenswürdige Stammzertifizierungsstelle** – Sie müssen eine vertrauenswürdige Stammzertifizierungsstelle einrichten und die Aktion „Commit und Push“ ausführen und diese dann während der Einrichtung der App-Beschleunigung auswählen. Dieser Vorgang wird in den folgenden Verfahren gezeigt. Wenn Sie Strata Cloud Manager zum Konfigurieren der App-Beschleunigung verwenden, richten Sie die Stammzertifizierungsstelle im Prisma Access-Geltungsbereich ein. Wenn Sie das verwendete Zertifikat ändern, müssen Sie das geänderte Zertifikat vor seiner Auswahl auch mit „Commit und Push“ festschreiben und übertragen.

 ©2025 Palo Alto Networks, Inc.

- **Forward-Trust-Zertifikat und vertrauenswürdige Stammzertifizierungsstelle –** Aktivieren Sie die Zertifizierungsstelle und das Zertifikat, die Sie als Forward-Trust-Zertifikat und vertrauenswürdige Stammzertifizierungsstelle hochgeladen haben, wie in den folgenden Verfahren gezeigt. Wenn die SSL-Entschlüsselung auf beschleunigte Apps angewendet wird, müssen Sie das Zertifikat als Forward-Trust-Zertifikat und vertrauenswürdige Stammzertifizierungsstelle markieren, da andernfalls SSL-Fehler auftreten, wenn Benutzer versuchen, auf diese Apps zuzugreifen.
- **Nicht unterstützte Prisma Access-Funktionalität** – Die folgende Funktionalität unterstützt keine App-Beschleunigung und Prisma Access-Bereitstellungen, in denen diese Funktionen aktiviert wurden, können nicht beschleunigt werden:
  - IPv6

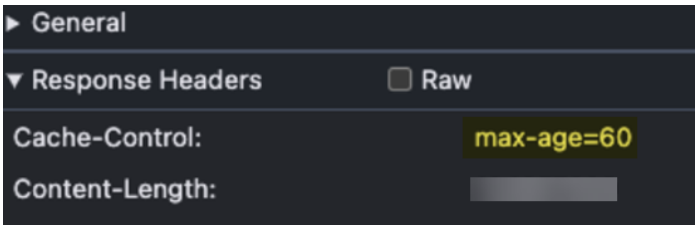
    Die App-Beschleunigung koexistiert mit der IPv6-Vernetzung, wenn IPv6 konfiguriert ist; es wird jedoch nur der IPv4-TCP-Datenverkehr beschleunigt. Der IPv6-Datenverkehr wird nicht beschleunigt, funktioniert aber normal.
  - Remote-Netzwerke, die überlappende Subnetze verwenden (standardmäßig in Prisma Access (Managed by Strata Cloud Manager)-Bereitstellungen unterstützt und in Prisma Access (Managed by Panorama)-Bereitstellungen konfigurierbar).
- **Richtlinien für die App-Beschleunigung**:
  - **-QUIC-Protokollunterstützung** – Einige Browser (wie Google Chrome) verwenden standardmäßig das QUIC-Protokoll (Quick UDP Internet Connections). Die App-Beschleunigung für Layer 7 kann für Datenverkehr, für den QUIC eingesetzt wird, nicht verwendet werden. Um dieses Problem zu umgehen, können Sie das QUIC-Protokoll deaktivieren, wenn Sie die App-Beschleunigung konfigurieren.
  - **SaaS Apps und Zy-* Antwortheader** – Benutzer, die eine Verbindung zu Prisma Access-Bereitstellungen herstellen, in denen die App-Beschleunigung für Top-SaaS-Apps aktiviert ist, können erwarten, dass Antwortheader mit einem Namen nach dem Muster Zy-* angezeigt werden, z. B. Zy-Server und Zy-Accelerated sowie ein zy_sid-Sitzungscookie.

    Wenn der Antwortheader Zy-Accelerated ist, zeigt der Wert **1** an, dass die Antwort beschleunigt wurde, und der Wert **0** zeigt an, dass die Antwort nicht beschleunigt wurde.
  - **Inhaltslokalisierung** – Wenn eine beschleunigte SaaS-App Inhalte ausschließlich auf der Grundlage der IP-Adresse oder Benutzer-ID des Benutzers lokalisiert, wird der Inhalt nicht lokalisiert, wenn die Beschleunigung für diese App aktiviert ist.
  - **Zum Standardverhalten für Sicherheitsrichtlinienregeln mit einer Aktion wechseln, die auf „Ablehnen“ gesetzt ist** – Wenn Sie über eine Sicherheitsrichtlinienregel mit einer Aktion verfügen, die auf **Ablehnen** gesetzt ist und die auf den Datenverkehr angewendet wird, der über die App-Beschleunigung mit einer Regel auf Basis von Quell- oder Zieladresse, Anwendung oder Dienst ausgeführt wird, wird für den Datenverkehr ein Drei-Wege-Handshake ausgeführt. Prisma Access blockiert diesen Vorgang jedoch und die Richtlinie mit **Ablehnen** funktioniert wie konfiguriert.
  - **Amazon S3 und Azure Blob Storage `cache-control`** – Amazon S3 und Azure-Blob-Storage-Buckets und -Dateien verfügen über eine Reihe von verknüpften HTTP-Antwortheadern. Einer dieser Werte ist `cache-control`. Dateien werden nicht beschleunigt, wenn der Wert für `cache-control` wie folgt lautet:
    - Nicht gesetzt

 ©2025 Palo Alto Networks, Inc.

- Gesetzt auf den Wert `max-age=0`
- Gesetzt auf den Wert `max-age=no-cache`

Zur Nutzung der Vorteile der App-Beschleunigung für Amazon S3 und Azure Blob Storage setzen Sie den Wert `cache-control` `max-age` auf einen Wert größer Null.




- **Apps mit gemeinsam genutzter Domäne in Activity Insights** – Bei Verwendung der App-Beschleunigung basiert die Beschleunigung in Layer 7 auf der Domäne. Wenn zwei Apps dieselbe Domäne teilen, kann die App, die in Activity Insights berichtet, unter bestimmten Bedingungen den Layer-7-Datenverkehr einer App einer anderen App zuordnen. Wenn z. B. Datenverkehr der MS-Teams- und der OneDrive-App dieselbe Domäne gemeinsam nutzt, wird die Berichterstattung der MS-Teams-App unter OneDrive angezeigt.
- **Langlebige Verbindungen und Systemprotokolle** – Die App-Beschleunigung schreibt Layer-4-Protokolle, wenn eine einzelne TCP-Verbindung beendet wird. Bei kurzlebigen Verbindungen ist dieses Verhalten transparent, da kurzlebige Verbindungen häufig von Anwendungen erstellt werden.

  Die App-Beschleunigung erfasst Metriken für den gesamten Zeitraum, in dem die Verbindung aktiv ist. Für langlebige Verbindungen, wie sie von angehängten SMB-Netzlaufwerken verwendet werden, kann dieses Verhalten zu dem Eindruck führen, dass Metriken nur während der Beendigung der Verbindungen erfasst werden.

 ©2025 Palo Alto Networks, Inc.

# App-Beschleunigung konfigurieren

Um die App-Beschleunigung in Prisma Access zu konfigurieren, wählen Sie abhängig von Ihrer Bereitstellung (Prisma Access (Managed by Strata Cloud Manager) oder Prisma Access (Managed by Panorama)) eine der folgenden Registerkarten aus.

- Strata Cloud Manager
- Panorama

 ©2025 Palo Alto Networks, Inc.

# Konfigurieren der App-Beschleunigung in Prisma Access (Strata Cloud Manager)

Zum Konfigurieren der App-Beschleunigung in einer Prisma Access (Managed by Strata Cloud Manager)-Bereitstellung führen Sie diese Task aus.

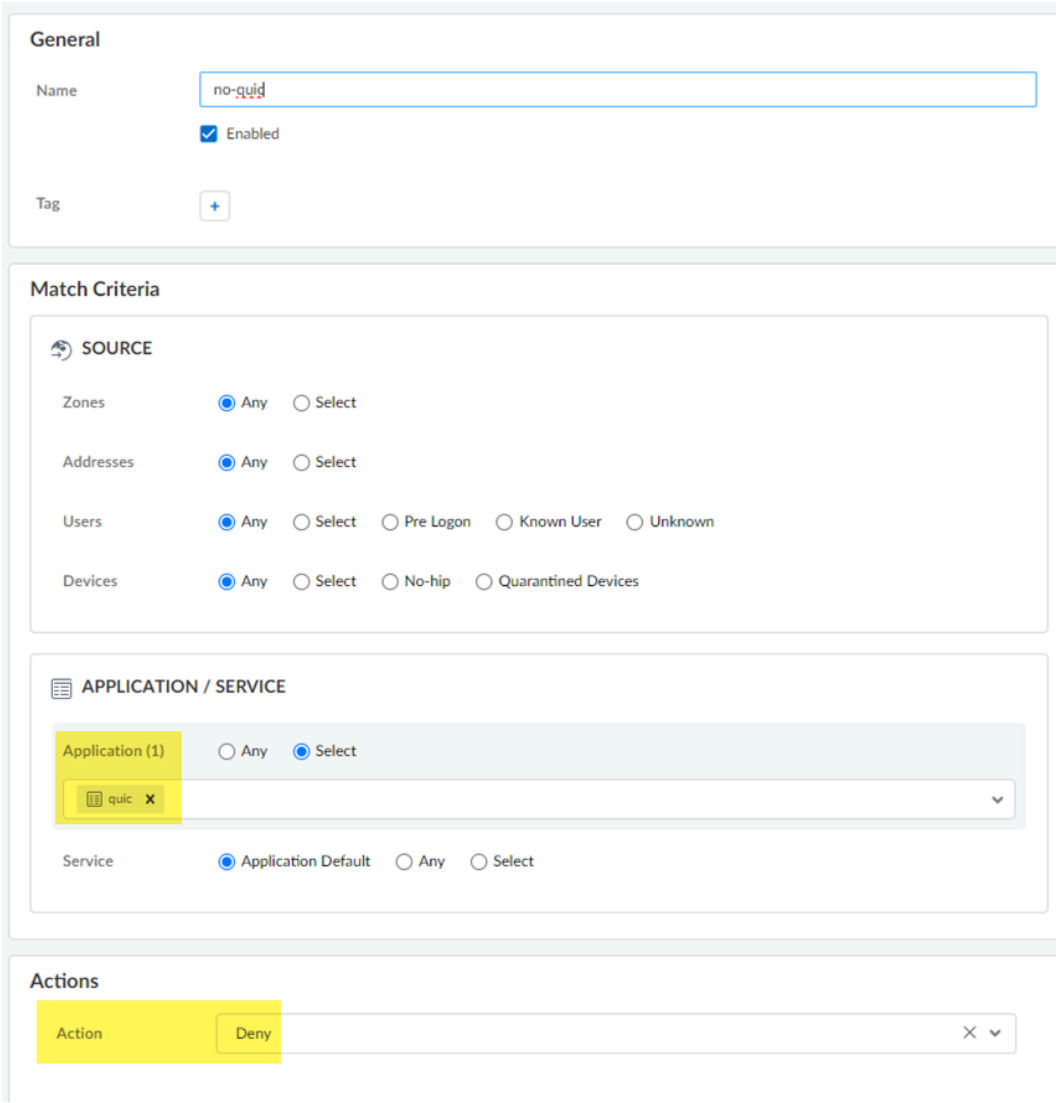

©2025 Palo Alto Networks, Inc.

**STEP 1 |** (Optional) Deaktivieren Sie das QUIC-Protokoll (Quick UDP Internet Connections).

Die App-Beschleunigung kann Apps in Layer 7 nur beschleunigen, wenn QUIC deaktiviert wird.

1. Rufen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Sicherheitsdienste** > **Sicherheitsrichtlinie** und **Regel hinzufügen** > **Vor-Regeln** auf.

   Erstellen Sie diese Sicherheitsrichtlinienregel im Konfigurationsumfang **Global**.
2. Wählen Sie für **Anwendung/Dienst** die Einstellung **quic** und für **Aktionen** die Einstellung **Ablehnen** aus.

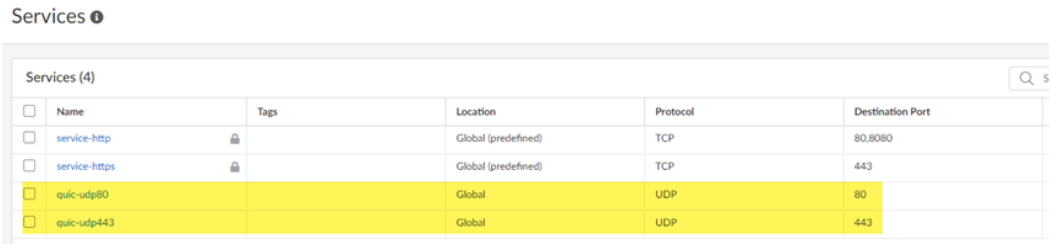



3. **Save (Speichern)** Sie Ihre Änderungen.
4. Rufen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Objekte** > **Dienste** > **Dienst** und **Hinzufügen** auf, um Dienste für UDP-Port 80 und UDP-Port 443 hinzuzufügen.

   Palo Alto Networks empfiehlt, Dienste für den UDP-Port 80 und den UDP-Port 443 hinzuzufügen und eine zusätzliche Sicherheitsrichtlinie zu erstellen, um UDP-

 ©2025 Palo Alto Networks, Inc.

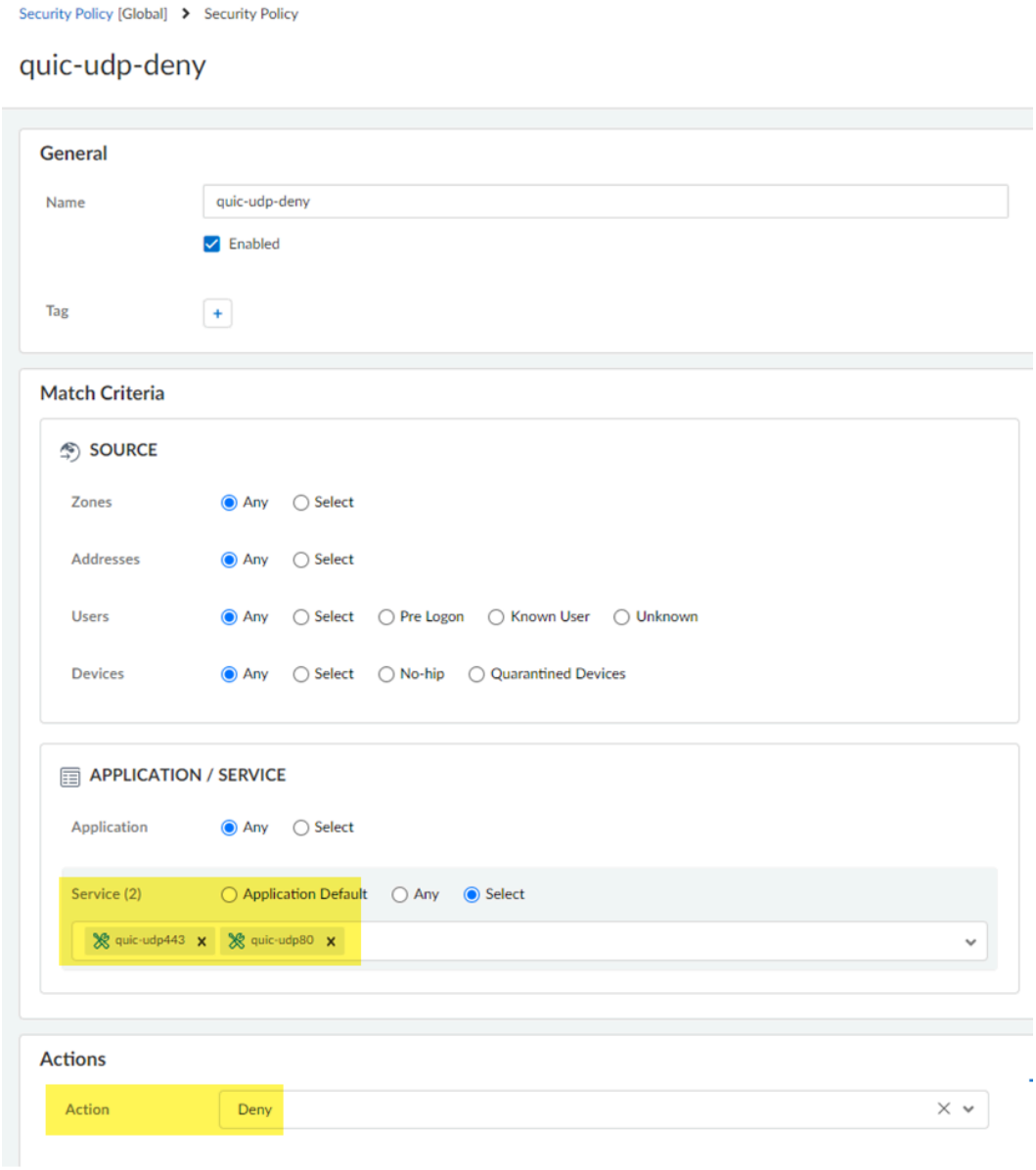
Datenverkehr an diesen Ports zu blockieren, da neuere Versionen von QUIC sonst möglicherweise als **unknown-udp** identifiziert werden.




5. Rufen Sie wieder **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Sicherheitsdienste** > **SicherheitsrichtlinieRegel hinzufügen** für eine zweite

 ©2025 Palo Alto Networks, Inc.

Sicherheitsrichtlinie auf, indem Sie die Dienste unter **Anwendung/Dienste** und als **Aktion Ablehnen** angeben.




Nach Abschluss dieser Arbeitsschritte verfügen Sie über zwei Sicherheitsrichtlinien: Eine dient zum Blockieren des QUIC-Protokolls, die andere zum Blockieren von Datenverkehr über die UDP-Ports 80 und 443.




 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Importieren Sie ein Zertifikat der Stammzertifizierungsstelle (Certificate Authority – CA) und einen privaten Schlüssel in Strata Cloud Manager in den Prisma Access-Geltungsbereich, um diese Komponenten für die App-Beschleunigung zu verwenden. Übertragen Sie Ihre Änderungen anschließend mit einer Push-Aktion.

Ein selbstsigniertes Zertifikat der Stammzertifizierungsstelle stellt innerhalb einer Zertifikatkette das höchste Zertifikat dar. Die App-Beschleunigung verwendet die Stammzertifizierungsstelle und die entsprechenden Zertifikate zur Erstellung von Zertifikaten für die beschleunigten Apps. Übertragen Sie die Stammzertifizierungsstelle und die entsprechenden Zertifikate an Prisma Access, damit die App-Beschleunigung mit der Erstellung der App-spezifischen Zertifikate beginnen kann.

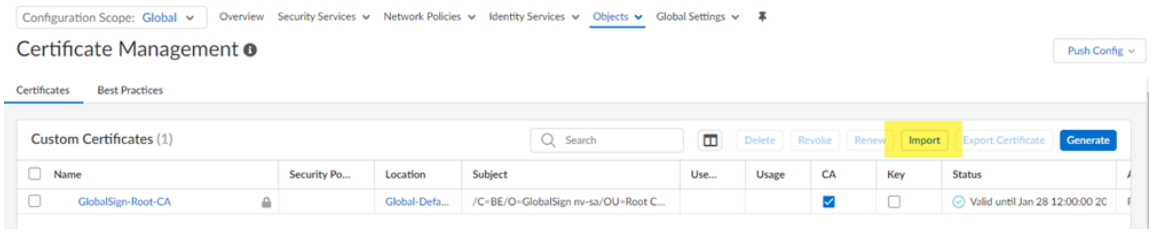
Die Stammzertifizierungsstelle und die entsprechenden Zertifikate müssen folgende Merkmale aufweisen:

- Bei der Zertifizierungsstelle (CA) muss es sich um eine vertrauenswürdige Zertifizierungsstelle handeln.
- (Empfohlen) Die Zertifizierungsstelle sollte eindeutig sein und ausschließlich für die App-Beschleunigung verwendet werden.
- Die Zertifizierungsstelle darf nicht abgelaufen sein. Notieren Sie sich das Ablaufdatum der Zertifizierungsstelle und erneuern Sie das Zertifikat vor seinem Ablauf. Wenn ein CA-Zertifikat, das für die App-Beschleunigung verwendet wird, abläuft, erhalten Benutzer einen SSL-Fehler, wenn sie versuchen, auf beschleunigte Apps zuzugreifen. Es ist von zentraler Bedeutung, dass die Zertifizierungsstelle (CA) gültig ist, wenn die App-Beschleunigung von Ihrer Organisation verwendet wird.
- Sie muss einen Schlüssel enthalten.
- Sie muss eine Passphrase verwenden.
- Sie muss sich im Geltungsbereich von **Prisma Access** befinden.
- (Mobile Benutzer – Nur GlobalProtect-Bereitstellungen) Sie muss im lokalen Stammzertifikatspeicher installiert werden.

  Sie können diese Installation durchführen, indem Sie das Zertifikat wie beschrieben der Liste der vertrauenswürdigen Zertifikate hinzufügen. Wenn Sie mit ActiveDirectory arbeiten, können Sie die Stammzertifizierungsstelle über AD mithilfe eines ActiveDirectory-Gruppenrichtlinienobjekts (Group Policy Object – GPO) verteilen.

Wenn Sie die Stammzertifizierungsstelle und die entsprechenden Zertifikate ändern müssen, dann müssen Sie die Änderungen hochladen und festschreiben. Erst danach kann das geänderte Zertifikat verwendet werden.

1. Navigieren Sie zu **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Objekte** > **Zertifikatsverwaltung**.
2. **Importieren** Sie ein Zertifikat.




 ©2025 Palo Alto Networks, Inc.

3. Wählen Sie die folgenden Parameter aus:
   - Geben Sie unter **Zertifikatname** einen eindeutigen Namen für das Zertifikat ein (z. B. `AppAcceleration_CA`).

     Bei diesem Namen wird zwischen Groß- und Kleinschreibung unterschieden. Er kann bis zu 31 Zeichen lang sein. Verwenden Sie ausschließlich Buchstaben, Zahlen, Bindestriche und Unterstriche im Namen.
   - Verwenden Sie **Datei auswählen** und suchen Sie dann nach der **Zertifikatsdatei**, die Sie von der Zertifizierungsstelle (CA) erhalten haben. Klicken Sie dann auf **Öffnen**, um die Datei zu öffnen.
   - Wählen Sie ein **Format** aus:
     - **Verschlüsselter privater Schlüssel und Zertifikat (PKCS12)** – Dies ist das Standardformat und gebräuchlichste Format, bei dem sich der Schlüssel und das Zertifikat in einem einzigen Container (Zertifikatsdatei) befinden.
     - **Base64-codiertes Zertifikat (PEM)** – Bei diesem Format müssen Sie den Schlüssel getrennt vom Zertifikat importieren. Sie müssen eine **Schlüsseldatei** auswählen, wenn Sie dieses Format auswählen.
     - Geben Sie eine **Passphrase** ein und wählen Sie dann **Passphrase bestätigen** aus.
4. **Save (Speichern)** Sie Ihre Änderungen.

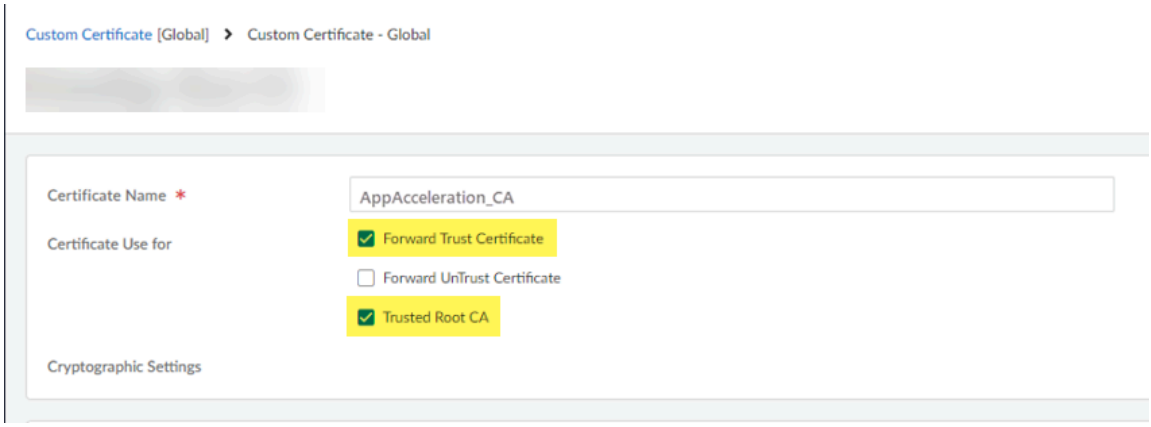



 ©2025 Palo Alto Networks, Inc.

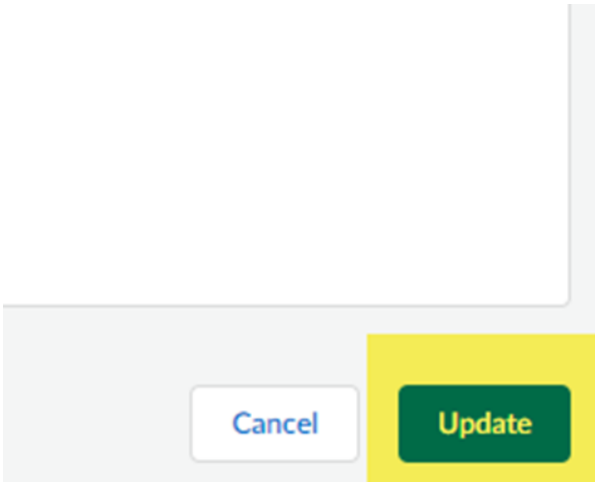
**STEP 3 |** Markieren Sie die Stammzertifizierungsstelle und das entsprechende Zertifikat, die Sie hinzugefügt haben, als Forward-Trust-Zertifikat und vertrauenswürdige Stammzertifizierungsstelle.

Wenn Sie das Zertifikat nicht als Forward-Trust-Zertifikat und CA nicht als vertrauenswürdige Stammzertifizierungsstelle angeben, treten SSL-Fehler auf, wenn Benutzer versuchen, bei Verwendung der SSL-Entschlüsselung auf beschleunigte Apps zuzugreifen.

1. Wählen Sie die von Ihnen hinzugefügte Stammzertifizierungsstelle und das entsprechende Zertifikat aus.
2. Wählen Sie für das Zertifikat **Forward-Trust-Zertifikat** und **Vertrauenswürdige Stammzertifizierungsstelle** aus.

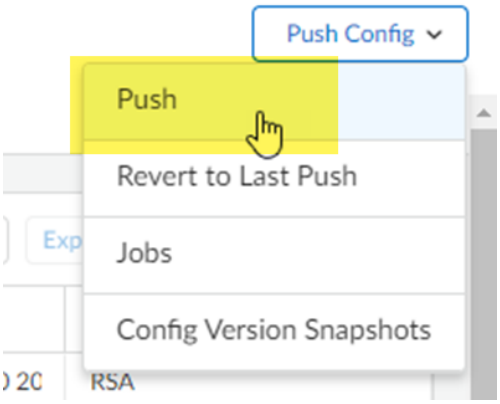



3. **Aktualisieren** Sie das Zertifikat.




 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** Übertragen Sie Ihre Änderungen mit der Aktion **Push**.



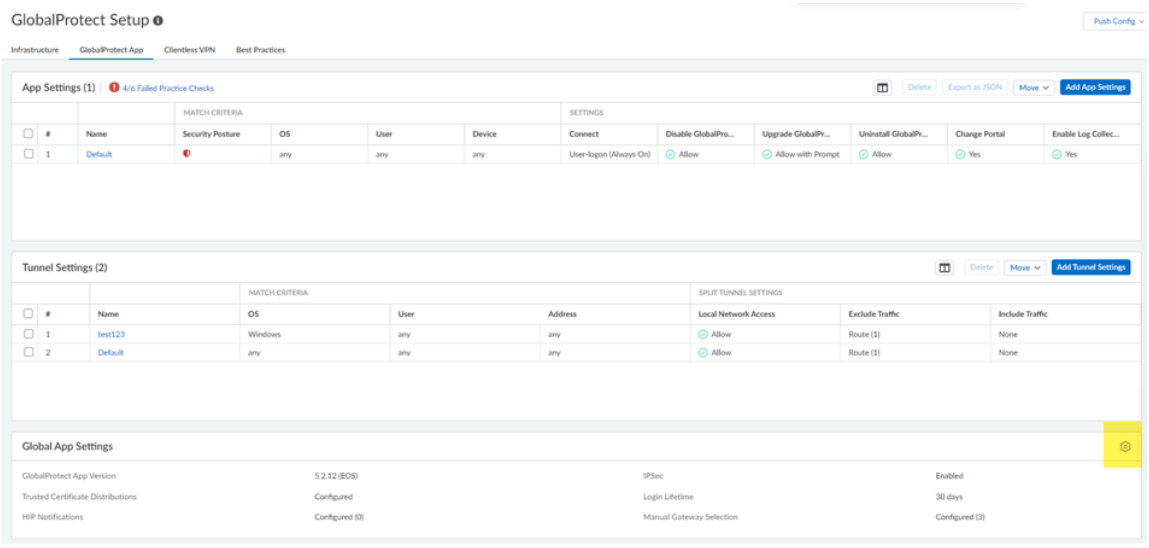

**STEP 5 |** (Mobile Benutzer – Nur GlobalProtect-Bereitstellungen) Fügen Sie die Stammzertifizierungsstelle und das entsprechende Zertifikat hinzu, die Sie der Liste der

 ©2025 Palo Alto Networks, Inc.

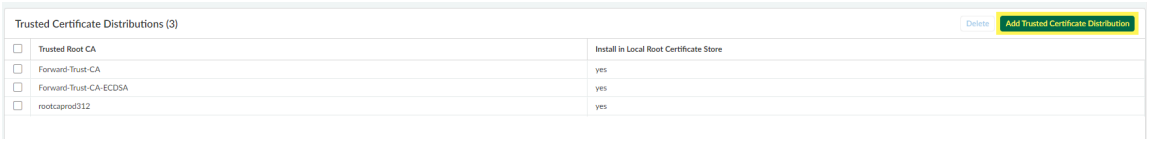
vertrauenswürdigen GlobalProtect-Zertifikate hinzugefügt haben, und installieren Sie die Komponenten im lokalen Stammzertifikatspeicher.

*Wenn Sie ActiveDirectory verwenden, können Sie die Stammzertifizierungsstelle alternativ mithilfe eines ActiveDirectory-Gruppenrichtlinienobjekts (GPO) über AD verteilen.*

1. Rufen Sie **Workflows** > **Einrichtung Prisma Access** > **GlobalProtect** > **GlobalProtect-App** > **Globale App-Einstellungen** auf.
2. Klicken Sie auf das Zahnradsymbol, um die **Einstellungen** zu bearbeiten.




3. **Verteilung vertrauenswürdiger Zertifikate hinzufügen.**




4. Wählen Sie unter **Vertrauenswürdige Stammzertifizierungsstelle** die von Ihnen zuvor erstellte vertrauenswürdige Stammzertifizierungsstelle und anschließend **Im lokalen Stammzertifikatspeicher installieren** aus.

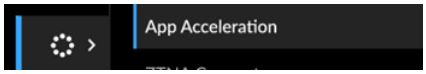



5. **Save (Speichern)** Sie Ihre Änderungen.
6. Übertragen Sie Ihre Änderungen mit der Aktion **Push**.

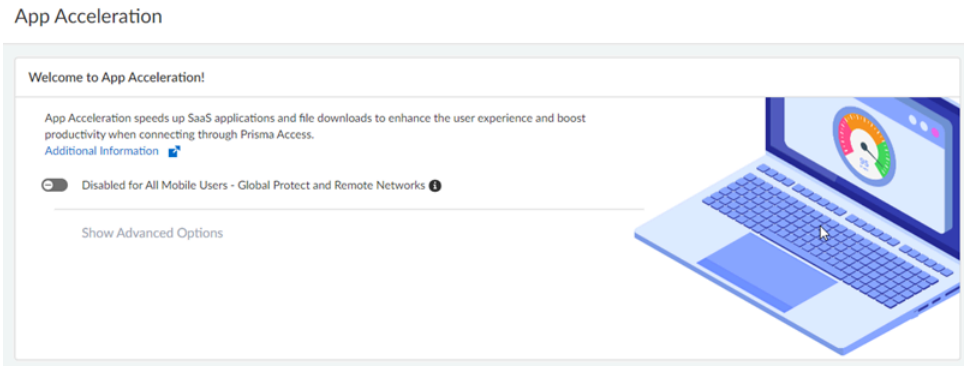
 ©2025 Palo Alto Networks, Inc.

**STEP 6 |** Aktivieren Sie die App-Beschleunigung und wählen Sie die von Ihnen erstellte Zertifikatsdatei aus.

1. Wählen Sie in der linken Navigationsleiste **Workflows** > **App-Beschleunigung** aus.

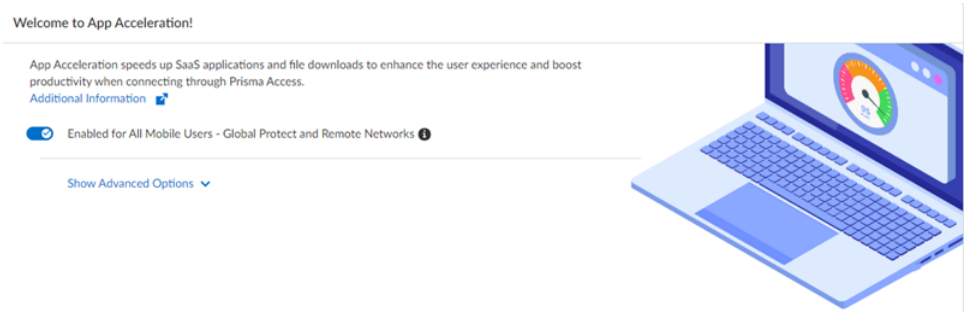



Daraufhin wird das Fenster für die App-Beschleunigung angezeigt.




2. Bewegen Sie den Schieberegler nach rechts, damit für die App-Beschleunigung die Option **Aktiviert für alle mobilen Benutzer – GlobalProtect und Remote-Netzwerke** festgelegt wird.

*Wenn momentan noch Commit-Aktionen ausgeführt werden, dann werden die Einstellungen für die App-Beschleunigung wirksam, nachdem alle Commits abgeschlossen sind.*



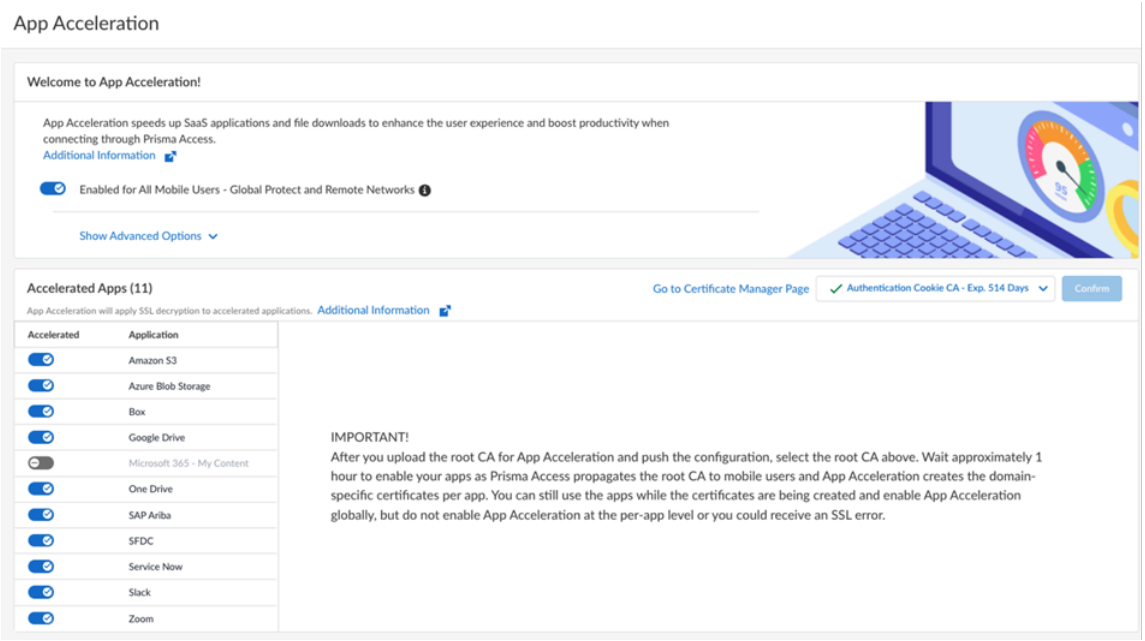

Die App-Beschleunigung wird für den gesamten TCP-Datenverkehr aktiviert. Wenn Sie SaaS-Anwendungen beschleunigen möchten, müssen Sie eine Stammzertifizierungsstelle und das entsprechende Zertifikat auswählen. Siehe hierzu den nächsten Schritt.

**STEP 7 |** Wählen Sie das Zertifikat aus, das Sie in einem vorherigen Schritt erstellt haben.

Wenn Sie das Zertifikat basierend auf einem vorhandenen Zertifikat ändern müssen, vergewissern Sie sich, dass Sie das Zertifikat mit „Commit und Push“ an Ihre Firewalls und

 ©2025 Palo Alto Networks, Inc.

Benutzer übertragen haben, und wählen Sie es dann hier aus. Sie müssen das neue Zertifikat mit Commit festschreiben, bevor Sie es auswählen können.




*Nachdem Sie das Zertifikat importiert haben, müssen Sie warten, bis die App-Beschleunigung domänenspezifische Zertifikate für jede App generiert. Dieser Vorgang kann bis zu einer Stunde dauern. In der Zwischenzeit können Sie den Schieberegler für* ***Beschleunigte Apps*** *nach links bewegen, um die App-Beschleunigung vorübergehend zu deaktivieren und auf die Apps zuzugreifen, bis die Zertifikate generiert sind. Wenn Sie dies nicht tun, erhalten Sie möglicherweise so lange einen SSL-Fehler, bis die Zertifikate generiert wurden.*

*Die Aktivierung der Beschleunigung kann bis zu 10 Minuten dauern, nachdem Sie sie für eine bestimmte Anwendung eingeschaltet haben.*

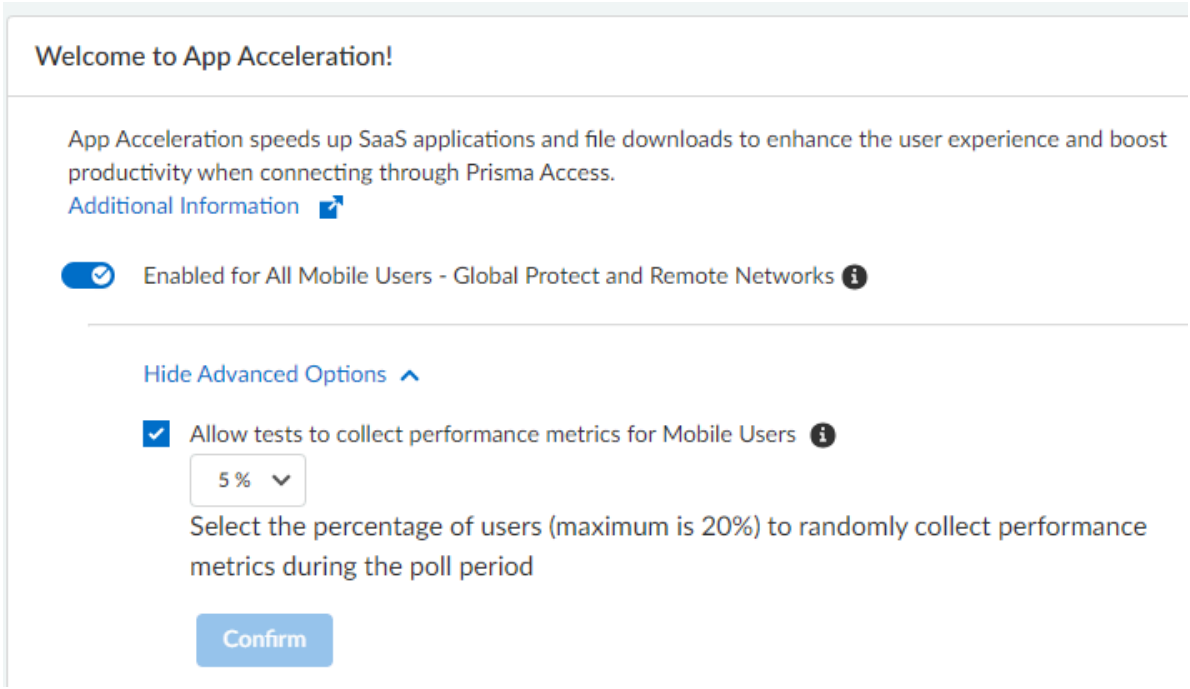
**STEP 8 |** (Optional) Rufen Sie **Erweiterte Optionen anzeigen** auf und ändern Sie die Parameter für den Metriktest.

- (Optional) Um die Erfassung von Metriken zum Abrufen von Leistungsinformationen zu deaktivieren, wählen Sie die Option **Tests zum Erfassen von Leistungsmetriken für mobile Benutzer zulassen** ab.

  Palo Alto Networks empfiehlt, die Metrikerfassung zu aktivieren, um die Verbesserungen der App-Leistung bei Verwendung der App-Beschleunigung anzuzeigen.
- (Optional) Um den Prozentsatz der Benutzer, für die prädiktive Tests verarbeitet werden, abweichend von der Standardeinstellung von 5 % zu ändern, wählen Sie in der Dropdown-

 ©2025 Palo Alto Networks, Inc.

Liste einen anderen Prozentsatz und dann **Bestätigen** aus, um die Änderungen zu bestätigen.




 ©2025 Palo Alto Networks, Inc.

# Konfigurieren der App-Beschleunigung in Prisma Access (Panorama)

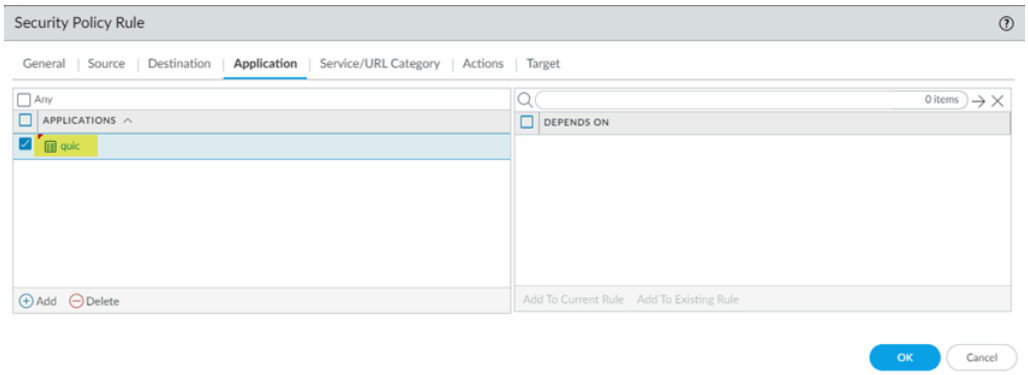
Zum Konfigurieren der App-Beschleunigung in einer Prisma Access (Managed by Panorama)-Bereitstellung führen Sie diese Task aus.

**STEP 1 |** (Optional) Deaktivieren Sie das QUIC-Protokoll (Quick UDP Internet Connections).

Die App-Beschleunigung kann Apps in Layer 7 nur beschleunigen, wenn QUIC deaktiviert wird.

1. Rufen Sie **Richtlinien** > **Sicherheit** > **Vor-Regeln** und dann **Hinzufügen** auf, um eine Sicherheitsrichtlinie hinzuzufügen.

   Erstellen Sie diese Sicherheitsrichtlinienregel in der Gerätegruppe **Freigegeben**.
2. Wählen Sie eine **Anwendung** mit der Angabe **quic** und die **Aktion** mit der Angabe **Ablehnen** aus.




3. Verwenden Sie **Hinzufügen**, um eine zweite Sicherheitsrichtlinie hinzuzufügen.

   Eventuell werden neuere Versionen von QUIC fälschlicherweise als **unknown-udp** identifiziert. Aus diesem Grund empfiehlt Palo Alto Networks, Dienste für UDP-Port 80 und UDP-Port 443 hinzuzufügen und eine zusätzliche Sicherheitsrichtlinie zu erstellen, um den UDP-Datenverkehr auf diesen Ports zu blockieren.
4. Fügen Sie unter **Dienst/URL-Kategorie** durch Auswahl von **Hinzufügen** neue Dienste für UDP-Port 80 und UDP-Port 443 hinzu. Fügen Sie außerdem eine **Aktion** mit der Angabe **Ablehnen** hinzu.

   Nach Abschluss dieser Arbeitsschritte verfügen Sie über zwei Sicherheitsrichtlinien: Die eine dient zum Blockieren des QUIC-Protokolls, die andere zum Blockieren des Datenverkehrs auf den UDP-Ports 80 und 443.

| | NAME | LOCATION | APPLICATION | TAGS | ACTION | SERVICE | PROFILE |
|---|---|---|---|---|---|---|---|
| 1 | quic-deny | Shared | quic | none | Deny | application-... | none |
| 2 | quic-udp-deny | Shared | any | none | Deny | quic-udp80<br>quic-udp443 | none |

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Importieren Sie das Zertifikat einer Stammzertifizierungsstelle (CA) und einen privaten Schlüssel in Panorama, um diese Komponenten für die App-Beschleunigung zu verwenden. Anschließend müssen Sie Ihre Änderungen mit der Aktion „Commit und Push“ festschreiben und übertragen.

Ein selbstsigniertes Zertifikat der Stammzertifizierungsstelle stellt innerhalb einer Zertifikatkette das höchste Zertifikat dar. Die App-Beschleunigung verwendet die Stammzertifizierungsstelle und die entsprechenden Zertifikate zur Erstellung von Zertifikaten für die beschleunigten Apps. Übertragen Sie die Stammzertifizierungsstelle und das entsprechende Zertifikat an Prisma Access, damit die App-Beschleunigung mit der Erstellung der App-spezifischen Zertifikate beginnen kann.

Die Stammzertifizierungsstelle und das entsprechende Zertifikat müssen die folgenden Eigenschaften aufweisen:

- Bei der Zertifizierungsstelle muss es sich um eine vertrauenswürdige Zertifizierungsstelle handeln.
- (Empfohlen) Die Zertifizierungsstelle sollte eindeutig sein und ausschließlich für die App-Beschleunigung verwendet werden.
- Die Zertifizierungsstelle darf nicht abgelaufen sein. Notieren Sie sich das Ablaufdatum der Zertifizierungsstelle und erneuern Sie das Zertifikat vor seinem Ablauf. Wenn ein CA-Zertifikat, das für die App-Beschleunigung verwendet wird, abläuft, erhalten Benutzer einen SSL-Fehler, wenn sie versuchen, auf beschleunigte Apps zuzugreifen. Es ist von zentraler Bedeutung, dass die Zertifizierungsstelle (CA) gültig ist, wenn die App-Beschleunigung von Ihrer Organisation verwendet wird.
- Sie muss einen Schlüssel enthalten.
- Sie muss eine Passphrase verwenden.
- (Mobile Benutzer – Nur GlobalProtect-Bereitstellungen) Sie muss im lokalen Stammzertifikatspeicher installiert werden.

  Sie können diese Installation durchführen, indem Sie das Zertifikat wie beschrieben der Liste der vertrauenswürdigen Zertifikate hinzufügen. Wenn Sie mit ActiveDirectory arbeiten, können Sie die Stammzertifizierungsstelle über AD mithilfe eines ActiveDirectory-Gruppenrichtlinienobjekts (Group Policy Object – GPO) verteilen.

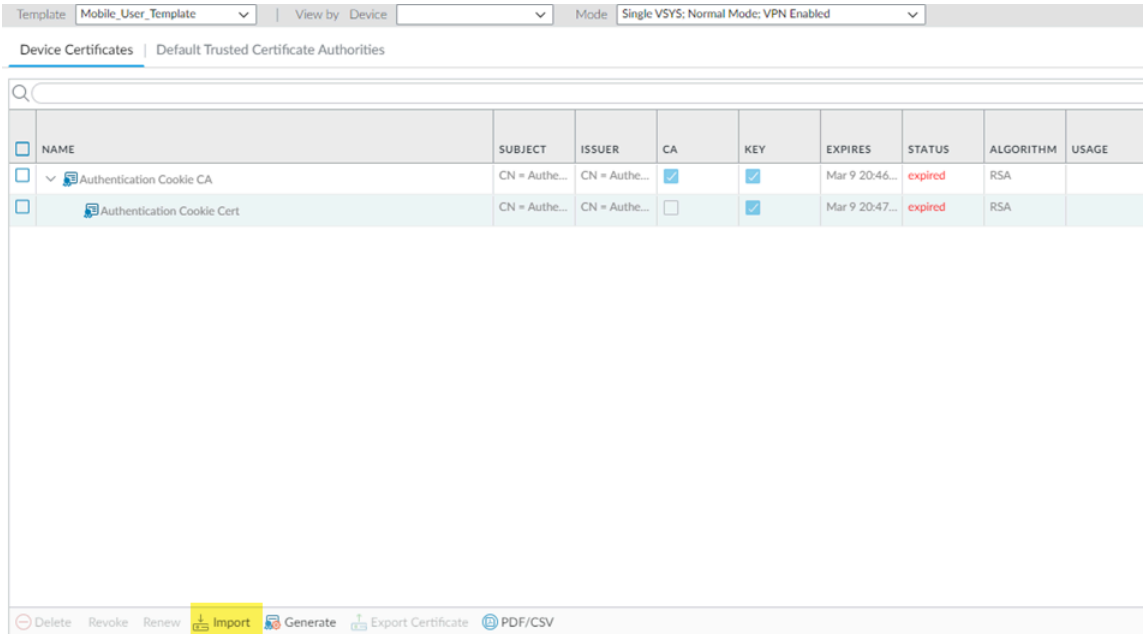
Wenn Sie die Stammzertifizierungsstelle und das entsprechende Zertifikat ändern müssen, dann müssen Sie diese Komponenten hochladen und Ihre Änderungen mit der Aktion „Commit und Push“ festschreiben und übertragen, bevor Sie das geänderte Zertifikat verwenden können.

1. Rufen Sie **Gerät** > **Zertifikate** > **Zertifikatverwaltung** auf.

   Vergewissern Sie sich, dass Sie mit Mobile_User_Template arbeiten.

 ©2025 Palo Alto Networks, Inc.

2. **Importieren** Sie ein Zertifikat.



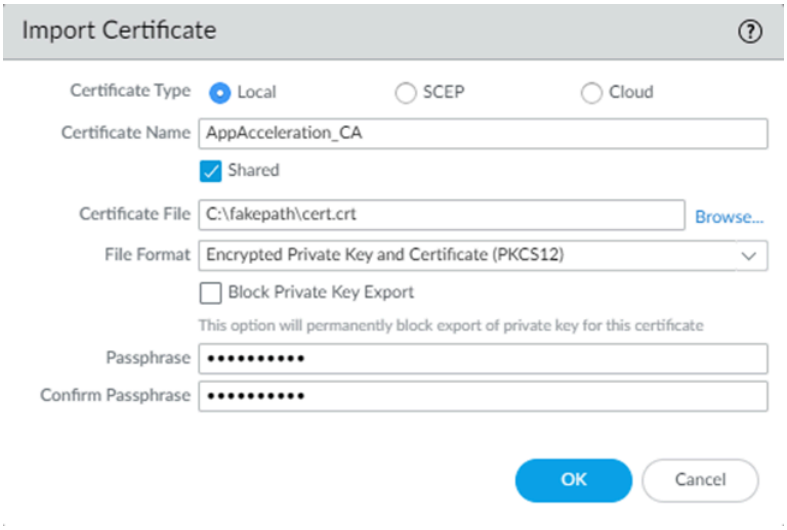

3. Wählen Sie die folgenden Parameter aus:

   - Geben Sie unter **Zertifikatname** einen eindeutigen Namen für das Zertifikat ein (z. B. `AppAcceleration_CA`).

     Bei diesem Namen wird zwischen Groß- und Kleinschreibung unterschieden. Er kann bis zu 31 Zeichen lang sein. Verwenden Sie ausschließlich Buchstaben, Zahlen, Bindestriche und Unterstriche im Namen.
   - Suchen Sie nach der **Zertifikatsdatei**, die Sie von der Zertifizierungsstelle erhalten haben, und klicken Sie dann auf **Öffnen**, um die Datei zu öffnen.
   - Wählen Sie ein **Format** aus:
     - **Verschlüsselter privater Schlüssel und Zertifikat (PKCS12)** – Dies ist das Standardformat und gebräuchlichste Format, bei dem sich der Schlüssel und das Zertifikat in einem einzigen Container (Zertifikatsdatei) befinden.
     - **Base64-codiertes Zertifikat (PEM)** – Bei diesem Format müssen Sie den Schlüssel getrennt vom Zertifikat importieren. Sie müssen die Option **Privaten Schlüssel importieren** und eine **Schlüsseldatei** auswählen, wenn Sie dieses Format auswählen.
     - Geben Sie eine **Passphrase** ein und wählen Sie dann **Passphrase bestätigen** aus.

 ©2025 Palo Alto Networks, Inc.

4. Klicken Sie auf **OK**.




5. Wiederholen Sie diese Schritte und ersetzen Sie dabei Mobile_User_Template durch Remote_Network_Template.

   Sie müssen diese Zertifikate sowohl in Mobile_User_Template als auch in Remote_Network_Template importieren, um Apps für Ihre mobilen Benutzer und Benutzer an Remote-Netzwerkstandorten zu beschleunigen.

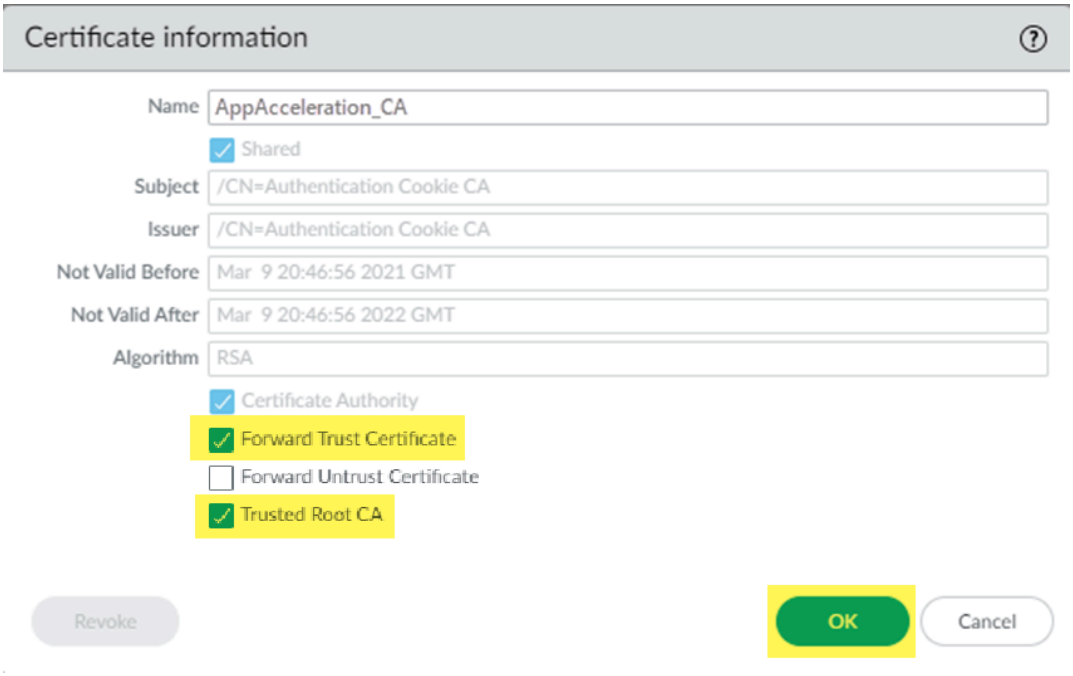
**STEP 3 |** Markieren Sie die Stammzertifizierungsstelle und das entsprechende Zertifikat, die Sie hinzugefügt haben, als Forward-Trust-Zertifikat und vertrauenswürdige Stammzertifizierungsstelle.

Wenn Sie das Zertifikat nicht als Forward-Trust-Zertifikat und CA nicht als vertrauenswürdige Stammzertifizierungsstelle angeben, treten SSL-Fehler auf, wenn Benutzer versuchen, bei Verwendung der SSL-Entschlüsselung auf beschleunigte Apps zuzugreifen. Wenn Zertifikate in Mobile_User_Template und Remote_Network_Template enthalten sind, führen Sie diesen Schritt in beiden Vorlagen aus.

1. Wählen Sie die von Ihnen hinzugefügte Stammzertifizierungsstelle und das entsprechende Zertifikat aus.

 ©2025 Palo Alto Networks, Inc.

2. Wählen Sie das Zertifikat als **Forward-Trust-Zertifikat** und **Vertrauenswürdige Stammzertifizierungsstelle** aus und klicken Sie dann auf **OK**.




**STEP 4 |** Führen Sie für Ihre Änderungen die Aktion **Commit und Push** aus.

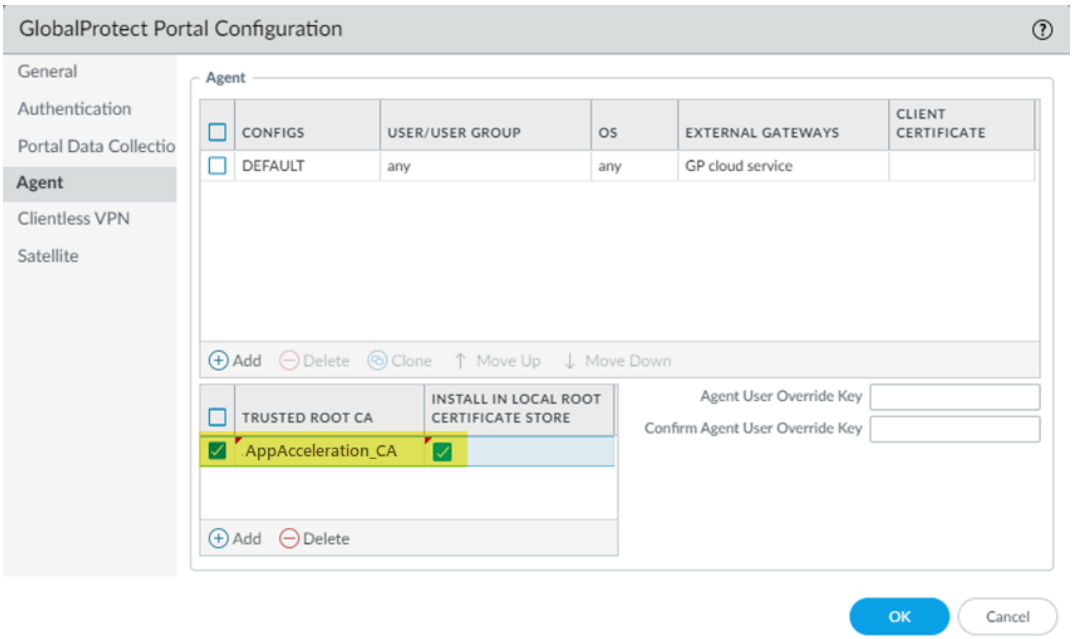
**STEP 5 |** (Mobile Benutzer – Nur GlobalProtect-Bereitstellungen) Fügen Sie die Stammzertifizierungsstelle und das entsprechende Zertifikat hinzu, die Sie der Liste der

 ©2025 Palo Alto Networks, Inc.

vertrauenswürdigen GlobalProtect-Zertifikate in der GlobalProtect-Portalkonfiguration hinzugefügt haben.

*Wenn Sie ActiveDirectory verwenden, können Sie die Stammzertifizierungsstelle alternativ mithilfe eines ActiveDirectory-Gruppenrichtlinienobjekts (GPO) über AD verteilen.*

1. Rufen Sie **Netzwerk** > **GlobalProtect** > **Portale** > **GlobalProtect_Portal** > **Agent** auf. Vergewissern Sie sich, dass Sie mit Mobile_User_Template arbeiten.
2. Verwenden Sie **Hinzufügen**, um die vertrauenswürdige Stammzertifizierungsstelle hinzuzufügen, die Sie in einem vorherigen Schritt erstellt haben.
3. Wählen Sie **Im lokalen Stammzertifikatspeicher installieren** aus.
4. Klicken Sie auf **OK**.

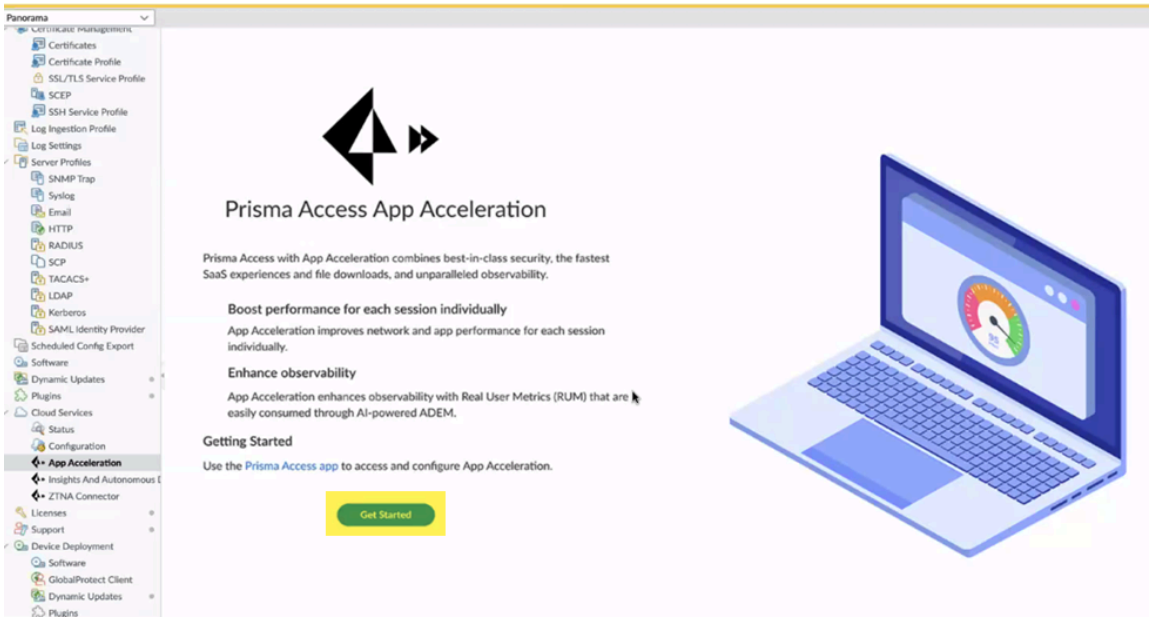



5. Führen Sie für Ihre Änderungen die Aktion **Commit und Push** aus.

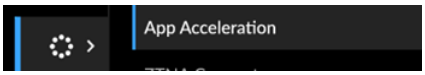
 ©2025 Palo Alto Networks, Inc.

**STEP 6 |** Aktivieren Sie die App-Beschleunigung und wählen Sie die von Ihnen erstellte Zertifikatsdatei aus.

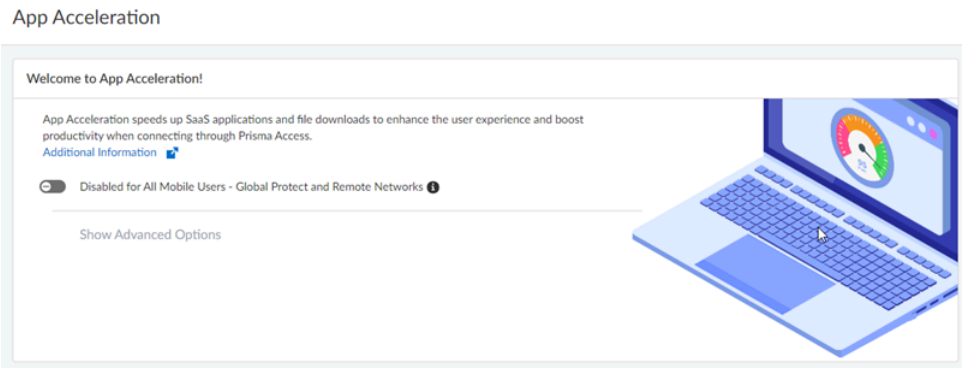
1. Rufen Sie **Panorama** > **Cloud Services** > **App-Beschleunigung** auf und verwenden Sie **Erste Schritte**, um sich mit der App-Beschleunigung vertraut zu machen.




2. Wählen Sie in der linken Navigationsleiste **Workflows** > **App-Beschleunigung** aus.



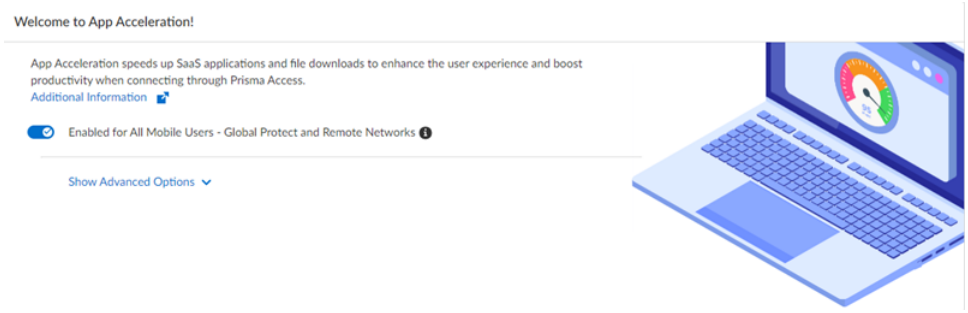

Daraufhin wird das Fenster „App-Beschleunigung“ angezeigt.




3. Bewegen Sie den Schieberegler nach rechts, damit für die App-Beschleunigung die Option **Aktiviert für alle mobilen Benutzer – GlobalProtect und Remote-Netzwerke** festgelegt wird.

*Wenn momentan noch Commit-Aktionen ausgeführt werden, dann werden die Einstellungen für die App-Beschleunigung wirksam, nachdem alle Commits abgeschlossen sind.*

 ©2025 Palo Alto Networks, Inc.




Die App-Beschleunigung wird für den gesamten TCP-Datenverkehr aktiviert. Wenn Sie SaaS-Anwendungen beschleunigen möchten, müssen Sie eine Stammzertifizierungsstelle und das entsprechende Zertifikat auswählen. Siehe hierzu den nächsten Schritt.

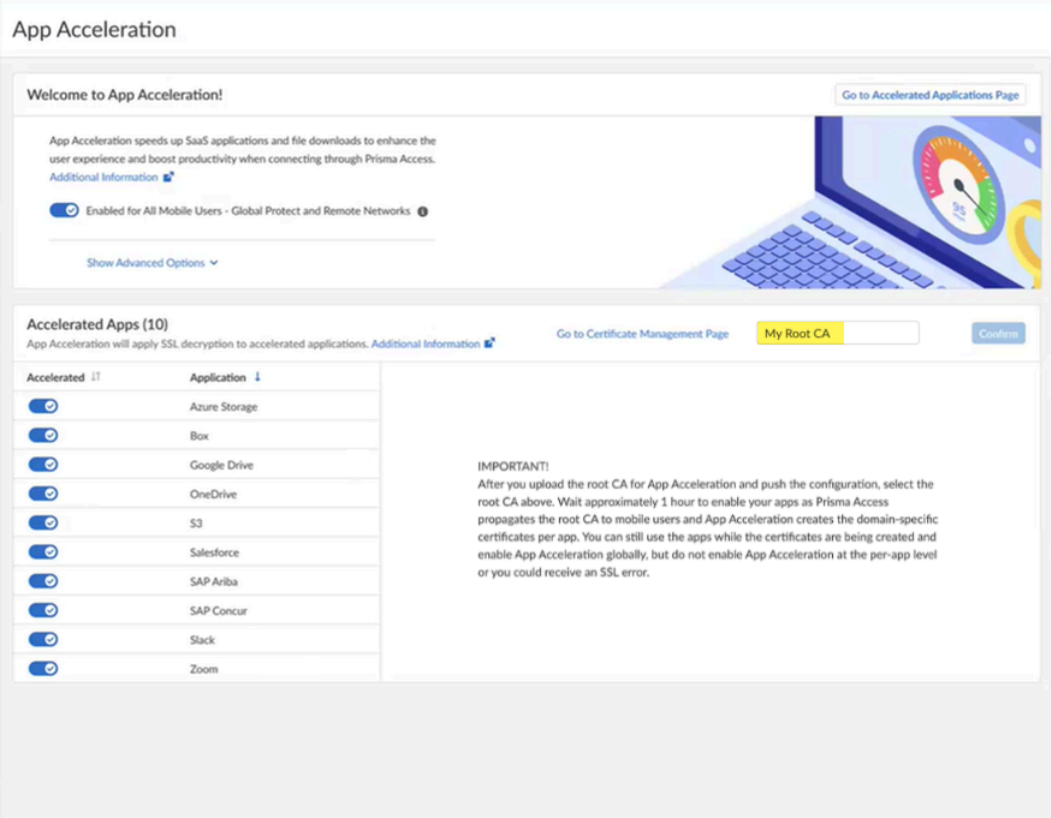
**STEP 7 |** Geben Sie in der Konfiguration der App-Beschleunigung den Namen des in einem früheren Schritt erstellten Zertifikats genau so ein, wie er in Panorama aufgeführt wird.

*Vergewissern Sie sich, dass Sie das Zertifikat mit „Commit und Push“ festgeschrieben und übertragen haben, bevor Sie ihn eingeben.*

Wenn Sie das Zertifikat durch Änderung eines bereits vorhandenen Zertifikats erstellen möchten, dann geben Sie den neuen Namen ein. Sie müssen den Namen eingeben (Sie können

 ©2025 Palo Alto Networks, Inc.

ihn nicht in einer Liste auswählen) und Sie müssen das neue Zertifikat mit „Commit und Push“ festschreiben und übertragen, bevor Sie den Namen eingeben.




*Nachdem Sie das Zertifikat importiert haben, müssen Sie warten, bis die App-Beschleunigung domänenspezifische Zertifikate für jede App generiert. Dieser Vorgang kann bis zu einer Stunde dauern. In der Zwischenzeit können Sie den Schieberegler für* ***Beschleunigte Apps*** *nach links bewegen, um die App-Beschleunigung vorübergehend zu deaktivieren und auf die Apps zuzugreifen, bis die Zertifikate generiert sind. Wenn Sie dies nicht tun, erhalten Sie möglicherweise so lange einen SSL-Fehler, bis die Zertifikate generiert wurden.*

*Die Aktivierung der Beschleunigung kann bis zu 10 Minuten dauern, nachdem Sie sie für eine bestimmte Anwendung eingeschaltet haben.*

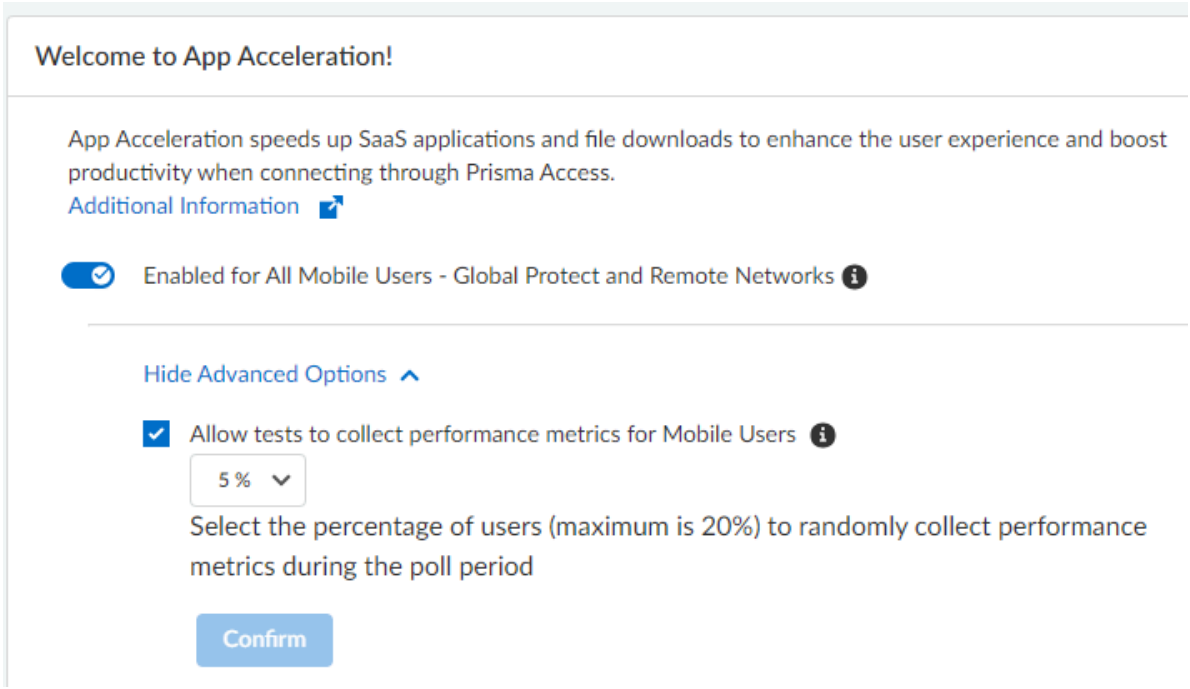
**STEP 8 |** (Optional) Rufen Sie **Erweiterte Optionen anzeigen** auf und ändern Sie die Parameter für den Metriktest.

- (Optional) Um die Erfassung von Metriken zum Abrufen von Leistungsinformationen zu deaktivieren, wählen Sie die Option **Tests zum Erfassen von Leistungsmetriken für mobile Benutzer zulassen** ab.

  Palo Alto Networks empfiehlt, die Metrikerfassung zu aktivieren, um die Verbesserungen der App-Leistung bei Verwendung der App-Beschleunigung anzuzeigen.
- (Optional) Um den Prozentsatz der Benutzer, für die prädiktive Tests verarbeitet werden, abweichend von der Standardeinstellung von 5 % zu ändern, wählen Sie in der Dropdown-

 ©2025 Palo Alto Networks, Inc.

Liste einen anderen Prozentsatz und dann **Bestätigen** aus, um die Änderungen zu bestätigen.




 ©2025 Palo Alto Networks, Inc.

# Prisma Access Mobile Benutzer

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

Prisma Access bietet zwei Verbindungsmethoden an, um mobile Benutzer zu schützen: Benutzer können sich über die GlobalProtect-App oder über eine Proxy-Autokonfiguration(PAC)-Datei mit Prisma Access verbinden.

- **Mobile Benutzer mit der GlobalProtect-App schützen**

  Sie können GlobalProtect in den folgenden Modi verwenden:

  - Tunnelmodus – Der Standard-Agentenmodus für GlobalProtect in Prisma Access. Richtet einen Tunnel (IPSec oder SSL) zu Prisma Access ein, um den Zugriff mobiler Benutzer auf alle Anwendungen, Ports und Protokolle zu sichern und gleichbleibende Sicherheit zu erhalten, unabhängig davon, ob sich der Benutzer innerhalb oder außerhalb Ihres Netzwerks befindet.

    Die auf dem Endgerät der Benutzer installierte GlobalProtect-App sichert den Benutzerdatenverkehr zum Internet, zu SaaS-Anwendungen sowie zu Ihren internen und öffentlichen Cloud-Ressourcen. Stellen Sie die GlobalProtect-App für Ihre Benutzer bereit (verfügbar für Smartphones, Tablets oder Laptops mit Microsoft Windows, Apple macOS und iOS, Android, Google Chrome OS und Linux), damit sie den Datenverkehr zur Durchsetzung von Richtlinien und zur Bedrohungsprävention an Prisma Access tunneln können. Die GlobalProtect-App stellt auch HIP-Berichte (Host Information Profile) bereit, damit Sie basierend auf dem Gerätestatus detaillierte Regeln erstellen können, um sicherzustellen, dass Endpunkte Ihre Sicherheitsstandards einhalten – beispielsweise bei den aktuellen Patches, Verschlüsselungs- und Virendefinitionen –, um auf Ihre sensibelsten Anwendungen zuzugreifen. Um sicheren Zugriff für Benutzer auf nicht verwalteten Geräten zu ermöglichen, können Sie auch Clientless VPN aktivieren. Prisma Access wird je nach Region dynamisch ein- und ausgeschaltet, abhängig davon, wo sich Ihre Benutzer gerade befinden.
  - Proxy-Modus – Mit diesem Modus können Sie den VPN-Agenten eines Drittanbieters verwenden, während Sie Prisma Access weiterhin als sicheres Web-Gateway für konsistente und überlegene SaaS-Sicherheit verwenden. Diese Verbindungsmethode ist ideal, wenn Sie noch nicht bereit sind, Ihr bestehendes privates App-VPN zu ersetzen, aber Ihr sicheres Web-Gateway ersetzen möchten. Sie verwenden beispielsweise den VPN-Agenten eines Drittanbieters für den privaten Zugriff, möchten aber nur Prisma Access für Ihre Internetsicherheit verwenden. Diese Verbindungsmethode bringt folgende Vorteile mit sich:
    - Erfüllt Compliance- oder Netzwerkanforderungen, die einen Proxy erfordern
    - Reduziert die Belastung durch PAC-Dateiverwaltung und unterstützt Proxy-basierte Apps über den Browser hinaus

    - Verbessert die Benutzererfahrung, indem es die Notwendigkeit eines Backhauls auf einen lokalen Web-Proxy vermeidet
  - Tunnel- und Proxymodus – Mit diesem Modus können Sie den Zugriff auf das Internet und SaaS-Anwendungen über den Proxymodus und den Zugriff auf private Apps über den Tunnelmodus sichern. Dies ist besonders hilfreich, wenn Sie den schnellsten Zugriff mit der niedrigsten Latenz auf eine private App benötigen und sich Ihr Prisma Access-Standort nicht in Ihrer Region befindet.

    In diesem Modus wertet die GlobalProtect-App zunächst die von Ihnen definierten Regeln für die Weiterleitung von expliziten Proxys aus und sendet den gesamten internetbasierten Datenverkehr an den expliziten Proxy von Prisma Access. Für den gesamten restlichen Datenverkehr bestimmt die App, welcher Datenverkehr durch den Tunnel an das GlobalProtect-Gateway gesendet und welcher Datenverkehr aus dem Tunnel ausgeschlossen werden soll, basierend auf allen von Ihnen definierten Split-Tunnel-Regeln. Sie können den Tunnel auch verwenden, um nicht proxyfähige Anwendungen zu sichern.

- **Mobile Benutzer mit PAC-Datei schützen**

  Zusätzlich zum Schutz mobiler Benutzer mit GlobalProtect können Sie mit Prisma Access einen expliziten Proxy konfigurieren. Mit einem expliziten Proxy verwendet ein Endpunkt eine PAC-Datei, die einen Webbrowser und proxyfähige Apps anweist, den Datenverkehr an den Web-Proxy-Server statt an den Zielserver weiterzuleiten und so Ihren webbasierten Internet-Verkehr (HTTP und HTTPS) zu schützen.

  Wenn das bestehende Netzwerk Ihres Unternehmens bereits explizite Proxys verwendet und PAC-Dateien auf Ihren Client-Endpunkten und -Servern bereitstellt, können Sie problemlos von älteren proxybasierten SWG-Lösungen zu Prisma Access migrieren, um den ausgehenden Internet-Verkehr mobiler Benutzer zu schützen. Sie können auch einen expliziten Proxy verwenden, wenn Sie einen Proxy für Audit- oder Compliance-Zwecke verwenden müssen.

- **Mobile Benutzer mit Prisma Access Browser Mobile schützen**

  Prisma Access Browser Mobile vereinfacht die Sicherung mobiler Benutzer durch die Kombination starker Zugriffskontrollen mit einer übersichtlichen, intuitiven Oberfläche. Es ermöglicht Benutzern den sicheren Zugriff auf private Anwendungen, ohne auf VPNs, Zertifikate oder Mobile-Device-Management(MDM)-Systeme angewiesen zu sein. Dadurch werden die Komplexität reduziert und die Konnektivität erleichtert.

  Es wurde für BYOD-Umgebungen (Bring Your Own Device) entwickelt und gewährleistet sicheren Zugriff auf private Anwendungen auf nicht verwalteten Geräten. So können Unternehmen kritische Ressourcen auf sämtliche Mitarbeiter ausweiten. Tablets werden durch Prisma Access Browser Mobile zu vielseitigen Desktop-Alternativen und bieten das gleiche Maß an Sicherheit und Zugriff wie herkömmliche Endgeräte.

  Mit Prisma Access Browser Mobile kann Ihr Unternehmen den Zugriff auf private Apps optimieren, die Produktivität auf Tablets steigern und zuverlässige Sicherheit auf verschiedenen mobilen Plattformen gewährleisten.

 ©2025 Palo Alto Networks, Inc.

# Mobile Benutzer: GlobalProtect

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

Mit GlobalProtect können Sie mobile Benutzer schützen, indem Sie die GlobalProtect-App auf deren Endpunkten installieren und GlobalProtect-Einstellungen in Prisma Access konfigurieren. GlobalProtect ermöglicht es Ihnen, den Zugriff mobiler Benutzer auf alle Anwendungen, Ports und Protokolle abzusichern und konsistente Sicherheit zu erhalten, unabhängig davon, ob sich der Benutzer innerhalb oder außerhalb Ihres Netzwerks befindet.

Wenn Sie mobile Benutzer mit GlobalProtect absichern, müssen Sie die Einstellungen definieren, um das Portal und die Gateways in der Cloud zu konfigurieren. Sie definieren beispielsweise einen Portal-Hostnamen, richten den IP-Adresspool für Ihre mobilen Benutzer ein und konfigurieren DNS-Einstellungen für Ihre internen Domänen. Möglicherweise können Sie vorhandene Konfigurationen für einige der erforderlichen Einstellungen verwenden, z. B. welches Authentifizierungsprofil zur Authentifizierung mobiler Benutzer verwendet werden soll. Wenn Sie bereits über eine Vorlage mit Ihren Authentifizierungsprofilen, Zertifikaten, Zertifikatprofilen und Serverprofilen verfügen, können Sie diese Vorlage während des Onboardings dem vordefinierten Vorlagenstack hinzufügen, um den Einrichtungsprozess zu vereinfachen.

Wenn Sie möchten, dass Ihre mobilen Benutzer eine Verbindung zu Ihren Remote-Netzwerkstandorten herstellen können, oder wenn Ihre mobilen Benutzer in verschiedenen geografischen Gebieten arbeiten und direkten Zugriff auf die Endpunkte des anderen benötigen, müssen Sie mindestens eine Dienstverbindung mit Platzhalterwerten konfigurieren, auch wenn Sie nicht planen, die Verbindung zu verwenden, um Zugriff auf die Standorte Ihres Rechenzentrums oder Ihrer Zentrale bereitzustellen. Dies ist erforderlich, weil zwar alle Remote-Netzwerkstandorte vollständig vernetzt sind, Prisma Access-Gateways (auch *Standorte* genannt) sich jedoch mit der Dienstverbindung in einer Hub-and-Spoke-Architektur verbinden, um Zugriff auf die internen Netzwerke in Ihrer Prisma Access-Infrastruktur zu gewähren.

- Planungscheckliste für GlobalProtect auf Prisma Access
- GlobalProtect für mobile Benutzer einrichten
- GlobalProtect — Tunneleinstellungen anpassen
- Ticketanforderung zur Deaktivierung von GlobalProtect (Strata Cloud Manager)
- GlobalProtect für mobile Benutzer überwachen
- IP-Adresspools für eine GlobalProtect-Bereitstellung für mobile Benutzer
- Wie die GlobalProtect-App Prisma Access-Standorte für mobile Benutzer auswählt
- Zulassungslisten mobiler GlobalProtect-Benutzer erstellen
- GlobalProtect-App-Upgrades
- Prisma Access mit lokalen GlobalProtect-Gateways integrieren


©2025 Palo Alto Networks, Inc.

# Planungscheckliste für GlobalProtect auf Prisma Access

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

Wenn Sie GlobalProtect zum Sichern mobiler Benutzer verwenden, stellen Sie anhand der folgenden Checkliste sicher, dass Sie den Dienst erfolgreich aktivieren und konsistente Richtlinien für Ihre mobilen Benutzer durchsetzen können (Schutz von Benutzern mit der auf deren Endpunkten installierten GlobalProtect-App und sicheres Zugreifen auf Anwendungen mit clientlosem VPN).

- ☐ **Checkliste zur Installationsvorbereitung:**
  - **IP-Adresspool** – Wenn Sie Prisma Access für Benutzer konfigurieren möchten, müssen Sie einen IP-Adresspool bereitstellen, der nicht andere, intern verwendete IP-Adressen oder den für das Infrastruktursubnetz festgelegten IP-Adresspool überlappt.

    *Wir empfehlen die Verwendung eines RFC-1918-konformen IP-Adresspools. Obwohl die Verwendung nicht RFC-1918-konformer (öffentlicher) IP-Adressen unterstützt wird, raten wir aufgrund möglicher Konflikte mit dem öffentlichen Internet-IP-Adressraum davon ab.*

    Geben Sie keine Subnetze an, die sich mit den folgenden IP-Adressen und Subnetzen überschneiden, da Prisma Access diese IP-Adressen und Subnetze für den internen Gebrauch reserviert:

    169.254.0.0/16 und 100.64.0.0/10

    Prisma Access verwendet diesen IP-Adresspool, um den virtuellen Netzwerkadaptern von Endpunkten IP-Adressen zuzuweisen, wenn sie sich mithilfe der GlobalProtect-App mit Prisma Access verbinden. Jedes Gerät, das eine Verbindung mit einem Gateway für mobile Prisma Access-Benutzer herstellt, benötigt eine eigene IP-Adresse. Sie legen diese Pools während des Onboarding-Prozesses für mobile Benutzer fest.

    Palo Alto Networks empfiehlt, die Anzahl der IP-Adressen im Pool auf das Zweifache der Anzahl mobiler Benutzergeräte festzulegen, die eine Verbindung zu Prisma Access Prisma Access herstellen. Wenn Ihre Organisation über eine Bring Your Own Device(BYOD)-Richtlinie verfügt oder ein einzelner Benutzer mehrere Benutzerkonten hat, stellen Sie sicher, dass Sie diese zusätzlichen Geräte und Konten bei der Zuweisung Ihrer IP-Pools berücksichtigen. Wenn der IP-Adresspool sein Limit erreicht, können keine weiteren mobilen Benutzergeräte mehr Verbindungen herstellen.

    Wenn mobile Benutzergeräte eine Verbindung zu einem Gateway herstellen, übernimmt Prisma Access IP-Adressen aus den von Ihnen angegebenen Pools und weist sie dem Gateway in /24-Blöcken zu. Sobald ein /24-Block sein Limit erreicht, wenn sich mehr Benutzergeräte anmelden, weist Prisma Access dem Gateway mehr /24-Blöcke aus dem Pool zu. Prisma Access kündigt diese /24-Subnetze in seinem Backbone an, da sie basierend auf den Gateway-Zuweisungen zugeordnet werden.

 ©2025 Palo Alto Networks, Inc.

- **Vorlage** – Die Prisma Access GlobalProtect-Bereitstellung erstellt automatisch einen Vorlagenstack und eine Vorlage auf oberster Ebene. Wenn Sie GlobalProtect bereits vor Ort ausführen und Ihre vorhandene Konfiguration nutzen möchten, können Sie dem Stack zusätzliche Vorlagen hinzufügen, um vorhandene Konfigurationen für GlobalProtect-Portal, GlobalProtect-Gateway, Benutzer-ID, Serverprofil (z. B. für die Verbindung mit Ihrem Authentifizierungsdienst), Zertifikat und SSL/TLS-Dienstprofil in Prisma Access für Benutzer per Push zu übertragen. Wenn Ihnen keine Vorlagen mit vorhandenen Konfigurationseinstellungen vorliegen, können Sie die erforderlichen Konfigurationseinstellungen manuell eingeben, wenn Sie GlobalProtect auf Prisma Access (Managed by Panorama) einrichten. Darüber hinaus muss jede Vorlage, die Sie dem Stack hinzufügen, die Zonenkonfiguration für die Zonen enthalten, die Sie verwenden, um Sicherheitsrichtlinien für Ihre mobilen Benutzer durchzusetzen.
- **Übergeordnete Gerätegruppe** – Wenn Sie Prisma Access für Benutzer konfigurieren, müssen Sie eine übergeordnete Gerätegruppe angeben, die verwendet werden soll, wenn Sie Ihre Adressgruppen und Sicherheitsrichtlinien, Sicherheitsprofile, andere Richtlinienobjekte (z. B. Anwendungsgruppen und -objekte), HIP-Objekte und -Profile sowie Authentifizierungsrichtlinien per Push übertragen, die der Dienst benötigt, um konsistente Richtlinien für Ihre Remote-Benutzer durchzusetzen.
- **Einzubindende Standorte** – Prisma Access bietet Ihnen weltweit Standorte, an denen Sie GlobalProtect auf Prisma Access (Managed by Panorama) einrichten können. Bevor Sie Ihre Standorte einbinden, sehen Sie sich diese Liste an, um zu bestimmen, welche Standorte Sie für die Bereitstellung mobiler Benutzer einbinden sollten.

  Wählen Sie Standorte aus, die sich in nächster Nähe zu Ihren Benutzern oder im selben Land wie Ihre Benutzer befinden. Wenn ein Standort in dem Land, in dem sich Ihre mobilen Benutzer befinden, nicht verfügbar ist, können Sie einen Standort auswählen, der dieselbe Sprache wie Ihre mobilen Benutzer verwendet.

  Sie können die Standorte auch nach geografischen Regionen unterteilen. Wenn Sie alle Standorte in einer Region beibehalten, können Sie nur für diese Region einen IP-Adresspool angeben. Dies kann nützlich sein, wenn Ihnen eine begrenzte Anzahl von IP-Adressen zur Verfügung steht, die Sie dem Pool zuweisen können. Ein einziger regionaler IP-Adresspool bietet zudem eine detailliertere Kontrolle über bereitgestellte Regionen und ermöglicht es Ihnen, Regionen auszuschließen, wenn dies Ihre Richtlinien oder Branchenvorschriften erfordern.

  Wenn Sie über eine lokale Lizenz für Prisma Access für Benutzer und über eine GlobalProtect-Bereitstellung sowie eine Bereitstellung des Typs „Expliziter Proxy“ verfügen, können Sie maximal fünf Standorte für beide Bereitstellungen kombiniert bereitstellen. Sie müssen die fünf Standorte zwischen beiden Bereitstellungen zuweisen (z. B. zwei Standorte für „Mobile Benutzer – GlobalProtect“ und drei Standorte für „Mobile Benutzer – Expliziter Proxy“). Wenn Sie eine weltweite Lizenz besitzen, gibt es keine Einschränkungen für die maximale Anzahl von Standorten.
- **Portal-Hostname** –Prisma Access für Benutzer ermöglicht es Ihnen, den Portal-Hostnamen schnell und einfach mit einem Standarddomänennamen (`.gpcloudservice.com`) einzurichten. In diesem Fall veröffentlicht der Cloud-Dienst den Hostnamen automatisch auf öffentlichen DNS-Servern und übernimmt die gesamte Zertifikatgenerierung. Sie können sich jedoch dafür entscheiden, Ihren eigenen Firmendomänennamen im Portalhostnamen zu verwenden. Wenn Sie Ihren Firmendomänennamen verwenden möchten, müssen Sie vor dem Konfigurieren des Dienstes eigene Zertifikate für das Portal erwerben und

 ©2025 Palo Alto Networks, Inc.

ein SSL/TLS-Dienstprofil konfigurieren, das auf das Zertifikat verweist. Wenn Sie Ihren eigenen Domänennamen im Portal-Hostnamen verwenden, müssen Sie außerdem Ihre DNS-Server so konfigurieren, dass sie auf den Portal-DNS-CNAME zeigen, der während des Konfigurationsprozesses bereitgestellt wird.

- **Dienstverbindung** – Sie müssen eine Dienstverbindung erstellen und konfigurieren, wenn Sie Ihren mobilen Benutzern den Zugriff auf Ressourcen, z. B. Authentifizierungsserver, in Ihrem internen Netzwerk (z. B. einen Authentifizierungsserver am Standort Ihres Rechenzentrums oder Ihrer Zentrale) oder auf Ihre Remote-Netzwerkstandorte ermöglichen möchten.

  Selbst wenn Sie nicht planen, die Verbindung zu verwenden, um Zugriff auf Ihre internen Ressourcen zu gewähren, müssen Sie mindestens eine Dienstverbindung mit Platzhalterwerten konfigurieren, wenn Ihre mobilen Benutzer eine Verbindung zu Ihren Remote-Netzwerkstandorten herstellen können oder wenn sich Ihre mobilen Benutzer in verschiedenen geografischen Gebieten befinden und direkten Zugriff auf die Endpunkte der jeweils anderen Benutzer benötigen.
- **IPv6-Nutzung in Ihrem Netzwerk** – Bestimmen Sie, ob Sie eine Bedrohungsminderung für den IPv6-Datenverkehr in Ihrem Netzwerk durchführen möchten, um die Angriffsfläche zu reduzieren. In einem Dual-Stack-Endpunkt, der sowohl IPv4- als auch IPv6-Datenverkehr verarbeiten kann, wird IPv6-Datenverkehr für mobile Benutzer standardmäßig nicht an Prisma Access, sondern an den lokalen Netzwerkadapter auf dem Endpunkt gesendet. Aus diesem Grund empfiehlt Palo Alto Networks, Prisma Access für Sinkhole-IPv6-Datenverkehr zu konfigurieren.
- **Protokollierung für GlobalProtect-Endpunkte** – Sie haben zwei Möglichkeiten, Protokolle von mobilen Benutzern zu erfassen, die die GlobalProtect-App verwenden:
  - **Manuelle Protokollerfassung von GlobalProtect-Endpunkten** – Lassen Sie die mobilen Benutzer die Protokolle von der GlobalProtect-App für Windows-, macOS- und Linux-Geräte erfassen. Diese Option erfordert keine zusätzliche Konfiguration.
  - **Protokollerfassung durch die GlobalProtect-App zur Fehlerbehebung** – Erlauben Sie der GlobalProtect App, End-to-End-Diagnosetests durchzuführen, um Verbindungs-, Leistungs- und Zugriffsprobleme zu beheben und Fehlerbehebungs- sowie Diagnoseprotokolle zu generieren, die zur weiteren Analyse an Strata Logging Service gesendet werden. Sie müssen ein Zertifikat generieren, damit sich die GlobalProtect-App mit Strata Logging Service authentifizieren kann, um Protokolle zur Fehlerbehebung zu erfassen. Mit **Prisma Access (Managed by Strata Cloud Manager)** können Sie der GlobalProtect-App ermöglichen, Protokolle von Strata Logging Service zu Fehlerbehebungszwecken zu erfassen. Für **Prisma Access (Managed by Panorama)** befindet sich diese Funktionalität unter **Panorama** > **Cloud Services** > **Konfiguration** > **Diensteinrichtung** > **Zertifikat für GlobalProtect-App-Protokollerfassung und Autonomous DEM generieren**. Konfigurationsdetails finden Sie unter Protokollerfassung durch die GlobalProtect-App.

❑ **Checkliste nach der Installation:**

- **Öffentliche IP-Adressen zu einer Zulassungsliste in Ihrem Netzwerk hinzufügen** – Nachdem Sie Ihre Standorte eingebunden haben, müssen Sie die von jedem Standort verwendeten öffentlichen Adressen und IP-Adressen bestimmen und diese zu einer Zulassungsliste in Ihrem Netzwerk hinzufügen, um mobilen Benutzern den Zugriff auf SaaS oder öffentliche Anwendungen zu ermöglichen. Wenn Sie weitere Standorte

 ©2025 Palo Alto Networks, Inc.

hinzufügen, müssen Sie auch die neuen IP-Adressen abrufen, die Prisma Access für die neu hinzugefügten Standorte zuweist.

- **Gateway-Namenskonsistenz** – Wenn Sie über eine bestehende Bereitstellung des Typs „Mobile Benutzer – GlobalProtect“ verfügen und es in Ihrem Unternehmen Fusions- und Übernahmeaktivitäten (Merger and Acquisition, M&A) gibt, müssen Sie möglicherweise vorhandene Gateways verwenden, um nicht auf einen früheren Markennamen oder einen neuen Markennamen zu verweisen. In diesem Fall wenden Sie sich an Ihr Palo Alto Networks Account-Team, das einen SRE-Fall zur Bearbeitung Ihrer Anfrage eröffnen wird. Palo Alto Networks empfiehlt, dass Sie diese Konfigurationsänderung während eines Wartungsfensters oder außerhalb der Spitzenzeiten vornehmen. Palo Alto Networks aktualisiert während des Wartungsfensters alle Gateways in Ihrer Bereitstellung, die eine Namensänderung erfordern.

# GlobalProtect für mobile Benutzer einrichten

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

Stellen Sie vor der Konfiguration mobiler Benutzer sicher, dass Sie über die erforderlichen Lizenzen verfügen (Prisma Access-Lizenz für mobile Benutzer und eine Strata Logging Service-Lizenz mit entsprechendem Firewall-Speicherplatz). Wenn mobile Benutzer eine Verbindung zu anderen verbundenen Netzwerken herstellen, benötigen Sie entweder eine ZTNA- (Zero Trust Network Access) oder eine Enterprise Edition Prisma Access-Lizenz, die den für die Verbindung erforderlichen Corporate Access Node (CAN) bereitstellt.

Zum Konfigurieren von Prisma Access für mobile Benutzer benötigen Sie Folgendes:

- Prisma Access-Lizenz für mobile Benutzer: Überprüfen Sie, ob die Prisma Access-Lizenz für mobile Benutzer aktiviert wurde.
- IP-Adresspool für mobile Benutzer: Stellen Sie sicher, dass Ihnen ein oder mehrere sich nicht überschneidende IP-Adresspools für mobile Benutzer zur Verfügung stehen.
- Portal-Hostname: Stellen Sie sicher, dass Sie den vollqualifizierten Domänennamen (FQDN) des Portals kennen.
- GlobalProtect-Agent für mobile Benutzer: Prisma Access für mobile Benutzer erfordert, dass die GlobalProtect-App auf jedem unterstützten Endpunkt installiert ist. Sie benötigen eine Bereitstellungsstrategie für die Installation des GlobalProtect-Agenten auf mobilen Benutzergeräten.
- Informationen zu Sicherheitsrichtlinienregeln: Sie werden Sicherheitsrichtlinienregeln implementieren, um Datenverkehr über Prisma Access zuzulassen oder zu verweigern. Sie müssen wissen, welche Regeln bereitzustellen sind, wenn Sie Prisma Access für Ihre mobilen Benutzer konfigurieren.
- Geografische Standorte Ihrer mobilen Benutzer: Wenn Sie mobile Benutzer unterstützen, sollten Sie einen verfügbaren geografischen Standort auswählen, der sich in der Nähe Ihrer mobilen Benutzer befindet.

 ©2025 Palo Alto Networks, Inc.

Erfahren Sie, wie Sie mobile GlobalProtect-Benutzer in Prisma Access einbinden.

- Strata Cloud Manager
- Panorama

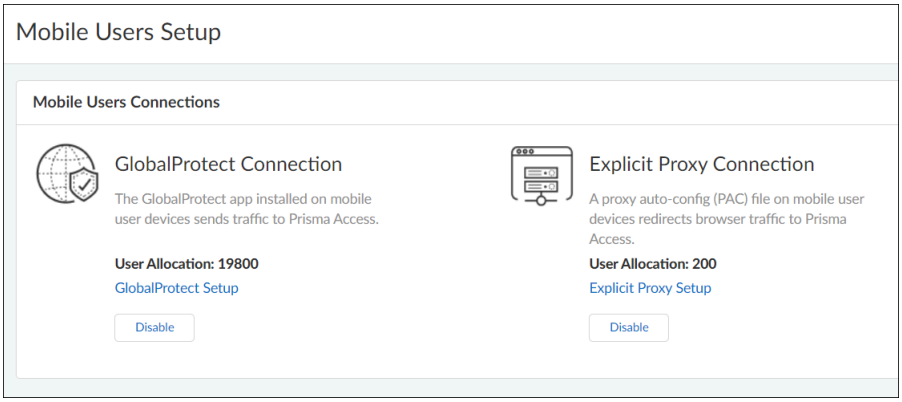
## GlobalProtect für mobile Benutzer einrichten (Strata Cloud Manager)

In nur wenigen Schritten können Sie damit beginnen, mobile Benutzer in Prisma Access einzubinden.

1. **GlobalProtect als Verbindungstyp für mobile Benutzer aktivieren**

   Gehen Sie zu **Workflows** > **Einrichtung Prisma Access** > **Mobile Benutzer**.

   Sie können Ihre Lizenz für mobile Benutzer zwischen GlobalProtect-Verbindungen und Verbindungen mit explizitem Proxy aufteilen. Einige Benutzer können die Verbindung über GlobalProtect und andere über einen expliziten Proxy herstellen. Mit einer **GlobalProtect-Verbindung** sendet die auf mobilen Endgeräten installierte GlobalProtect-App Datenverkehr an Prisma Access.

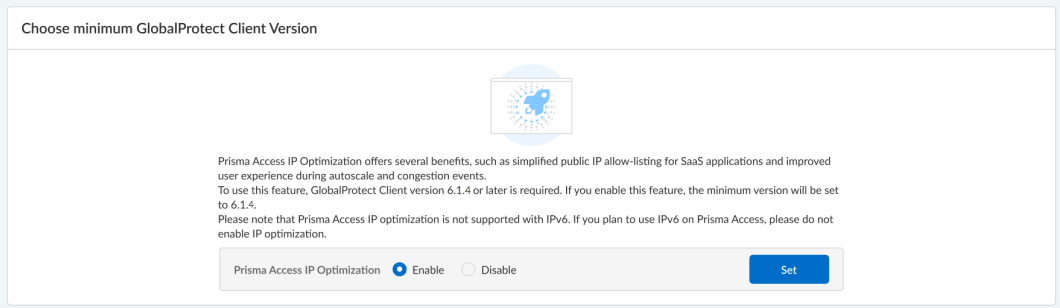



 ©2025 Palo Alto Networks, Inc.

2. **Grundlegende Infrastruktureinstellungen einrichten**

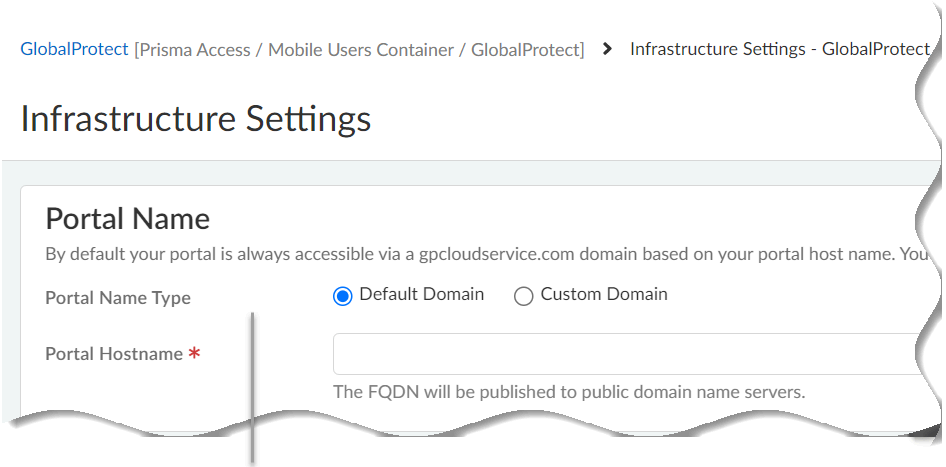
   Konfigurieren Sie die Infrastruktureinstellungen, die für GlobalProtect spezifisch sind. Zu Anfang müssen Sie einige erforderliche Einstellungen eingeben, damit Prisma Access die Umgebung für Ihre mobilen Benutzer bereitstellen kann.

   - *Wenn Sie GlobalProtect zum ersten Mal einrichten, entscheiden Sie, ob Sie die Prisma Access-IP-Optimierung aktivieren möchten. Um die IP-Optimierung zu aktivieren, sind GlobalProtect-Clientversion 6.1.4 und neuer, 6.2.3 und neuer oder 6.3.0 und neuer erforderlich und IPv6 wird nicht unterstützt. Gehen Sie bei der Auswahl sorgfältig vor, da Sie diese Einstellung später nicht mehr ändern können.*
   - *Die IP-Optimierungsfunktion ist nur für neue GlobalProtect-Bereitstellungen von Prisma Access vorgesehen. Bestehende GlobalProtect-Bereitstellungen, einschließlich neuer Mandanten, die Sie aus einer bestehenden Bereitstellung mit mehreren Mandanten erstellen, sind nicht berechtigt.*
   - *Wenn Sie Ihre GlobalProtect-Bereitstellung zu Prisma Access migrieren (und keine lokalen Gateways und Portale mehr verwenden), stellen Sie sicher, dass alle Benutzer die GlobalProtect-App Version 6.1.4 und neuer, 6.2.3 und neuer oder 6.3 und neuer verwenden, bevor Sie diese Funktionalität aktivieren.*

   Gehen Sie zu **Workflows** > **Einrichtung Prisma Access** > **GlobalProtect** > **Infrastruktur** > **Infrastruktureinstellungen**.

 ©2025 Palo Alto Networks, Inc.




**GlobalProtect Infrastructure Settings**

- Geben Sie den **Portalnamen** an.
  - **Standarddomäne** – Wenn Sie diese Option auswählen, verwendet Ihr Portal-Hostname den Standarddomänennamen: `.gpcloudservice.com`. Geben Sie in diesem Fall einfach einen **Portal-Hostnamen** ein, der an den Standarddomänennamen angehängt wird. Prisma Access für Benutzer erstellt automatisch die erforderlichen Zertifikate und veröffentlicht den Hostnamen auf den öffentlichen DNS-Servern.
  - **Benutzerdefinierte Domäne** – Sie können auch die Portaladresse anpassen, wenn Sie möchten, dass die Domäne im Portal-Hostnamen mit Ihrem Firmendomänennamen übereinstimmt (z. B. myportal.mydomain.com).
- Geben Sie die Auflösungseinstellungen für das **Client-DNS** Ihrer GlobalProtect-Bereitstellung ein.
  - Wählen Sie eine Region für die **DNS-Server** aus (**Region hinzufügen**).

    Wählen Sie **Weltweit** oder einen Schauplatz aus. Wenn Sie mehrere Proxy-Einstellungen mit einer Kombination aus „Weltweit“- und „Schauplatz“-Einstellungen angeben, verwendet Prisma Accessdie Einstellungen für die Standortgruppe, dann die für den Schauplatz und dann die für „Weltweit“. Prisma Access wertet die Regeln in der Liste von oben nach unten aus.
  - Wählen Sie aus, ob Prisma Access **interne Domänen auflösen** soll oder nicht. Falls ja, müssen Sie mindestens eine **interne Domänenauflösungsregel hinzufügen**.
  - Geben Sie einen eindeutigen **Namen** für die Regel ein.
  - Wählen Sie **Prisma Access Standard** aus, um den Standard-Prisma Access-DNS-Server zur Auflösung interner Domänen zu verwenden. Wenn Ihr interner DNS-Server nur die von Ihnen angegebenen Domänen auflösen soll, geben Sie die aufzulösenden Domänen in die **Domänenliste** ein. Geben Sie vor der Domäne ein Sternchen an, z. B. *.acme.com. Sie können maximal 1.024 Domäneneinträge angeben.
  - Wenn Sie über einen **benutzerdefinierten** DNS-Server verfügen, der auf Ihre internen Domänen zugreifen kann, geben Sie die IP-Adressen des **primären** und **sekundären DNS**-Servers an.
  - Wenn Ihr interner DNS-Server nur die von Ihnen angegebenen Domänen auflösen soll, geben Sie die aufzulösenden Domänen in die **Domänenlisten** ein. Geben Sie vor der

 ©2025 Palo Alto Networks, Inc.

Domäne ein Sternchen an, z. B. *.acme.com. Sie können maximal 1.024 Domäneneinträge angeben.

- **Speichern** Sie abschließend Ihre Änderungen.

- (Optional) Geben Sie einen **Client-IP-Pool** an.

  Standardmäßig stellt Ihnen Prisma Access einen Standardpool für mobile Benutzer mit IP-Adressen von 100.127.0.0/16 zur Verfügung, der an jedem beliebigen Standort weltweit verwendet werden kann. Prisma Access weist jedem mit GlobalProtect verbundenen Gerät eine IP-Adresse aus diesem Pool zu. Optional können Sie hier einen IP-Adresspool pro Region hinzufügen.

  - Sie können pro Standort ein minimal erforderliches Subnetz von /23 (512 IP-Adressen) eingeben. Zusätzliche Standorte erfordern mindestens ein /23-Subnetz. Wenn Sie ein weltweites Subnetz angeben, ist das minimal erforderliche Subnetz /23. Wir empfehlen jedoch IP-Adresspools für eine GlobalProtect-Bereitstellung für mobile Benutzer, um einen IP-Adresspool zuzuweisen, der der Anzahl der lizenzierten mobilen Benutzer entspricht oder größer ist, damit sich diese gleichzeitig anmelden können.

    Geben Sie keine Adressen an, die sich mit anderen intern verwendeten Netzwerken überschneiden, oder mit den Pools, die Sie beim Konfigurieren Sie die Prisma Access-Dienstinfrastruktur (Panorama) zugewiesen haben. Verwenden Sie außerdem nicht die folgenden IP-Adressen und Subnetze, da Prisma Access diese IP-Adressen und Subnetze für die interne Verwendung reserviert:

    - 169.254.0.0/16
    - 100.64.0.0/10

    *Wir empfehlen die Verwendung eines RFC-1918-konformen IP-Adresspools. Nicht mit RFC 1918 konforme (öffentliche) IP-Adressen für mobile Benutzer werden von uns zwar unterstützt, doch wir raten von deren Verwendung ab, da sie möglicherweise zu Konflikten mit dem öffentlichen IP-Adressraum des Internets führen.*

- Geben Sie die DNS-Einstellungen für **Primäre DNS für öffentliche Domänen** und **Sekundäre DNS für öffentliche Domänen** an.

  - **Prisma Access Standard** – Verwenden Sie den Standard-DNS-Server von Prisma Access.
  - **Internes DNS** – Verwenden Sie denselben Server, den Sie zum Auflösen interner Domänen verwenden.
  - **Benutzerdefiniert** – Wenn Sie über einen DNS-Server verfügen, der auf Ihre öffentlichen (externen) Domänen zugreifen kann, geben Sie in dieses Feld die primäre DNS-Serveradresse ein.
  - Sie können eine **Suffixliste für Client-DNS** hinzufügen, um das Suffix anzugeben, das der Client lokal verwenden soll, wenn ein nicht qualifizierter Hostname eingegeben wird, den er nicht auflösen kann, z. B. acme.local. Geben Sie vor dem Domänensuffix (z. B. acme.com) kein Platzhalterzeichen (*) ein. Sie können mehrere Suffixe hinzufügen.

 ©2025 Palo Alto Networks, Inc.

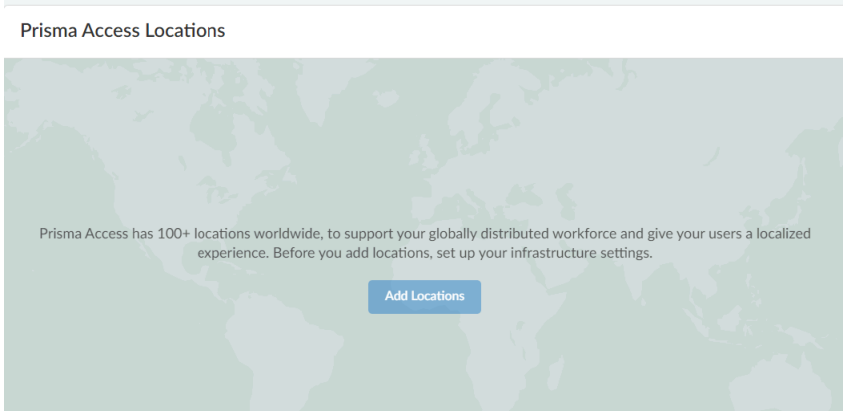
3. Richten Sie **erweiterte Einstellungen** ein.
   - (Optional) Verwenden Sie **Statische Einträge**, um FQDNs an bestimmte IP-Adressen aufzulösen.

     Diese Funktionalität kann nützlich sein, wenn in Ihrer Organisation Gast-Internetdienste vorhanden sind und Sie möchten, dass Ihre Gäste Suchmaschinen sicher verwenden, damit verhindert wird, dass diese nach potenziell unangemessenem oder anstößigem Material suchen, das gegen die Unternehmensrichtlinie verstoßen könnte. Geben Sie dazu einen eindeutigen **Namen** für die Regel für statische Einträge, einen **FQDN** und die IP-**Adresse** ein, an die die FQDN-Anfragen gerichtet werden soll.

   - Wenn Sie möchten, dass Prisma Access als Proxy für DNS-Anfragen fungiert, konfigurieren Sie Werte für **Wiederholung von UDP-Abfragen** (das **Intervall in Sek.)**, um die Abfrage nach einer bestimmten Anzahl von Sekunden zu wiederholen, sowie die Anzahl der durchzuführenden **Wiederholversuche**.
4. **Wählen Sie den Prisma Access-Standort aus, mit dem sich Ihre GlobalProtect-Benutzer verbinden werden**

   Fügen Sie die Prisma Access-Standorte hinzu, an denen Sie GlobalProtect-Benutzer unterstützen möchten. Gehen Sie zu **Workflows** > **Einrichtung Prisma Access** > **GlobalProtect** > **Infrastruktur** > **Prisma Access-Standorte**.

   Die Karte zeigt die globalen Regionen, in denen Sie Prisma Access für Benutzer bereitstellen können. Darüber hinaus bietet Prisma Access mehrere Standorte innerhalb der einzelnen Regionen, um sicherzustellen, dass Ihre Benutzer eine Verbindung zu einem Standort herstellen können, der eine auf den Standort des Benutzers zugeschnittene Benutzererfahrung bietet. Für eine optimale Leistung wählen Sie **Alles auswählen** aus. Wählen Sie alternativ bestimmte Standorte innerhalb der einzelnen ausgewählten Regionen aus, für die Ihre Benutzer Zugriffsrechte benötigen. Indem Sie Ihre Bereitstellung auf eine einzelne Region

 ©2025 Palo Alto Networks, Inc.

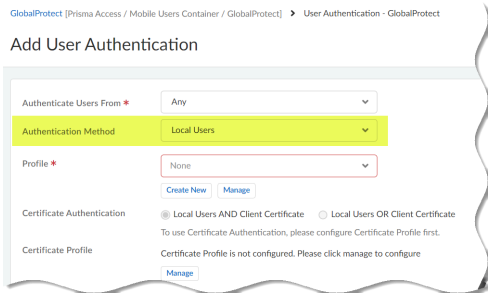
beschränken, können Sie die von Ihnen bereitgestellten Regionen genauer steuern und Regionen ausschließen, wenn Ihre Richtlinien oder Branchenvorschriften dies erfordern.

Wenn Sie die Anzahl der Standorte begrenzen, wählen Sie für ein optimales Benutzererlebnis die Standorte aus, die Ihren Benutzern am nächsten sind oder die sich im selben Land wie Ihre Benutzer befinden. Wenn ein Standort in dem Land, in dem sich Ihre mobilen Benutzer befinden, nicht verfügbar ist, wählen Sie für eine optimale Leistung den Standort aus, der Ihren Benutzern am nächsten ist.

5. **GlobalProtect-Benutzer authentifizieren**

   Richten Sie die Benutzerauthentifizierung ein, damit nur legitime Benutzer Zugriff auf Ihre Dienste und Anwendungen erhalten. Gehen Sie zu **Workflows** > **Einrichtung Prisma Access** > **GlobalProtect** > **Infrastruktur** > **Benutzerauthentifizierung**.

   Um Ihr Setup zu testen, können Sie Benutzer hinzufügen, die Prisma Access lokal authentifiziert. Alternativ können Sie direkt mit der Einrichtung der Authentifizierung auf Unternehmensebene fortfahren. Erfahren Sie mehr zum Thema Mobilen Benutzern die Authentifizierung bei Prisma Access ermöglichen.




6. Prisma Access setzt standardmäßig Best-Practice-Sicherheitsrichtlinienregeln durch. Diese Regeln ermöglichen es Ihren Benutzern, sicher auf allgemeine Internetseiten zu navigieren. Für die Benutzer gilt Folgendes:

   - Der Besuch bekannter bösartiger Websites wird basierend auf der URL blockiert
   - Bekanntermaßen bösartige Dateien können nicht hoch- oder heruntergeladen werden
   - Sie werden vor unbekannten, nie zuvor gesehenen Bedrohungen geschützt
   - Sie werden vor Malware, Spyware (Command-and-Control-Angriffen) und Sicherheitslücken geschützt

   Nach der Ersteinrichtung können Sie diese Standardregeln überprüfen und aktualisieren, um Ihren Unternehmensanforderungen zu entsprechen.

7. **Überprüfen, ob der Standort des mobilen Benutzers aktiv ist**

   Nachdem Sie Ihre anfängliche Konfiguration an Prisma Access übertragen haben, beginnt Prisma Access mit der Bereitstellung der GlobalProtect-Umgebung Ihrer mobilen Benutzer. Dies kann bis zu 15 Minuten dauern.

   *Sie können Ihre Einrichtung auch überprüfen, indem Sie **Workflows** > **Einrichtung Prisma Access** > **Prisma Access** > **Infrastruktureinstellungen** auswählen und Infrastruktureinstellungen bearbeiten, um zu bestätigen, dass an jedem der von Ihnen bereitgestellten Standorte ein Gateway eingerichtet ist.*

 ©2025 Palo Alto Networks, Inc.

### GlobalProtect – Portaladresse anpassen

Prisma Access erfordert nur die minimalen Einstellungen, um die Umgebung Ihres mobilen Benutzers bereitzustellen, damit Sie sie testen können. Wenn Sie Ihre Unternehmensdomäne lieber in der Portaladresse verwenden möchten, können Sie die Adresse nach der ersten Umgebungseinrichtung ändern.

Standardmäßig verwendet Prisma Access die Domäne *gpcloudservice.com*, um die Prisma Access-Portaladresse einzurichten, mit der Ihre mobilen Benutzer eine Verbindung herstellen müssen, um sicheren Zugang zum Internet, zu Ihrer Zentrale und zu Ihren Rechenzentren zu erhalten. Sie müssen diese Standarddomäne verwenden, wenn Sie Ihre Umgebung zum ersten Mal einrichten und testen. Wenn Sie den Domänennamen nach der Ersteinrichtung anpassen möchten, um Ihre Unternehmensdomäne zu verwenden, können Sie zurückgehen und die Umgebungseinstellungen so bearbeiten, dass die Portaladresse, mit der Ihre Benutzer eine Verbindung herstellen, Ihre eigene Unternehmensdomäne enthält (z. B. prisma-access.acme.com).

*Die Domäne *.gpcloudservice.com ist der Palo Alto Networks-Anwendung zugeordnet.*

Um Prisma Access so zu konfigurieren, dass Ihre eigene Domäne verwendet wird, müssen Sie wie folgt vorgehen:

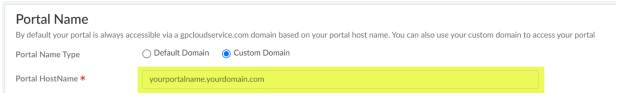
- Rufen Sie Zertifikate für den Dienst ab.
- Erstellen Sie auf Ihren DNS-Servern einen DNS-CNAME-Eintrag, der die Standardportaladresse mithilfe der Standarddomäne der benutzerdefinierten Portaladresse zuordnet, die Ihre Unternehmensdomäne verwendet. Dies ist erforderlich, da Prisma Access die von Ihnen eingerichtete Portaladresse bei der Erstbereitstellung auf Servern der öffentlichen Domäne veröffentlicht.

**STEP 1 |** Wählen Sie **Workflows** > **Einrichtung Prisma Access** > **GlobalProtect** > **Infrastruktur** aus und ändern Sie die **Infrastruktureinstellungen**.

*In Strata Cloud Manager ist Netzwerkredundanz standardmäßig zwischen Portalen oder Gateways und Dienstverbindungen aktiviert, wodurch redundante Verbindungen für mobile Benutzer zu zugänglichen Diensten und Anwendungen gewährleistet sind.*

**STEP 2 |** Legen Sie den Portal-Namenstyp auf **Benutzerdefinierte Domäne** fest.

**STEP 3 |** Geben Sie den gewünschten **Portal-Hostnamen** ein.




**STEP 4 |** Fügen Sie den **Portal-DNS-CNAME** hinzu, dem die DNS-Servereinträge zugeordnet werden sollen.

 ©2025 Palo Alto Networks, Inc.

**STEP 5 |** **Importieren** Sie das **Zertifikat**, das Sie für Ihre benutzerdefinierte Domänenportaladresse bereitgestellt haben.

1. Wählen Sie das **Format** für das zu importierende Zertifikat aus:
   - **Verschlüsselter privater Schlüssel und Zertifikat (PKCS12)** – Schlüssel und Zertifikat befinden sich in einem einzelnen Container (Zertifikatdatei). Klicken Sie auf **Datei auswählen** und navigieren Sie zu der PKCS12-Datei, die importiert werden soll.
   - **Base64-codiertes Zertifikat (PEM)** – Wenn Sie diese Option auswählen, müssen Sie die **Schlüsseldatei** getrennt vom Zertifikat importieren. Um das PEM-Zertifikat und die Schlüsseldatei zu importieren, klicken Sie auf **Datei auswählen**.
2. Geben Sie die **Passphrase** ein, um den Schlüssel zu verschlüsseln, bestätigen Sie die **Passphrase** und klicken Sie dann auf **Speichern**.

**STEP 6 |** Falls noch nicht geschehen, konfigurieren Sie Ihre DNS-Server so, dass sie auf den von Ihnen definierten Prisma Access-DNS-CNAME verweisen.

**STEP 7 |** **Speichern** Sie die Umgebungseinrichtung und wählen Sie **Konfiguration übertragen** aus, um sie auf Prisma Access zu übertragen.

Vergewissern Sie sich, dass die Konfigurationsumfänge für **Expliziter Proxy** und **GlobalProtect** ausgewählt sind.

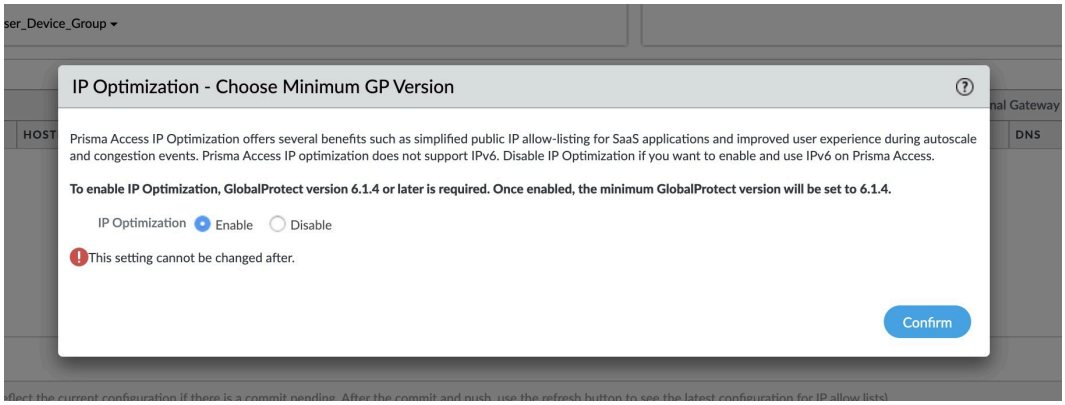
## GlobalProtect für mobile Benutzer einrichten (Panorama)

Gehen Sie wie folgt vor, um eine Bereitstellung des Typs „Mobile Benutzer – GlobalProtect“ zu konfigurieren. Sie müssen vor Beginn verstanden haben, wie Prisma Access funktioniert und mithilfe der Checkliste Ihre GlobalProtect-Bereitstellung planen.

 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Mobile Benutzer – GlobalProtect** aus.

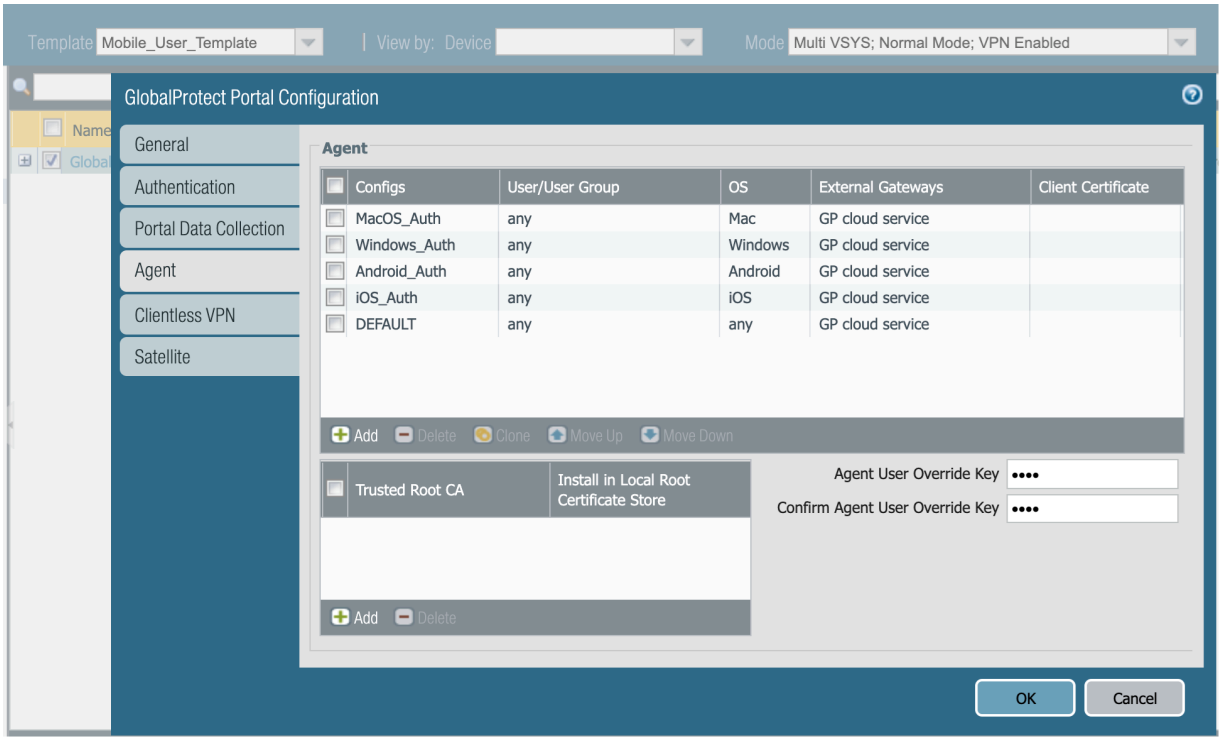
- *Wenn Sie GlobalProtect zum ersten Mal einrichten, werden Sie gefragt, ob Sie die Prisma Access-IP-Optimierung aktivieren möchten. Um die IP-Optimierung zu aktivieren, sind GlobalProtect-Clientversion 6.1.4 und neuer, 6.2.3 und neuer oder 6.3.0 und neuer erforderlich und IPv6 wird nicht unterstützt. Gehen Sie bei der Auswahl sorgfältig vor, da Sie diese Einstellung später nicht mehr ändern können.*
- *Die IP-Optimierungsfunktion ist nur für neue GlobalProtect-Bereitstellungen von Prisma Access vorgesehen. Bestehende GlobalProtect-Bereitstellungen, einschließlich neuer Mandanten, die Sie aus einer bestehenden Bereitstellung mit mehreren Mandanten erstellen, sind nicht berechtigt.*
- *Wenn Sie Ihre GlobalProtect-Bereitstellung zu Prisma Access migrieren (und keine lokalen Gateways und Portale mehr verwenden), stellen Sie sicher, dass alle Benutzer die GlobalProtect-App Version 6.1.4 und neuer, 6.2.3 und neuer oder 6.3 und neuer verwenden, bevor Sie diese Funktionalität aktivieren*




**STEP 2 |** (Optional) Wenn Sie die Agent-Konfiguration anpassen möchten, die Prisma Access per Push an Clients überträgt, bearbeiten Sie die GlobalProtect-Portalkonfiguration in der Vorlage „Mobile_User_Template“, um eine neue Agent-Konfiguration hinzuzufügen. Verschieben Sie die Agent-Konfiguration nach der Konfiguration über die in der Vorlage vordefinierte Agent-Konfiguration STANDARD, um sicherzustellen, dass Ihre Einstellungen Vorrang vor

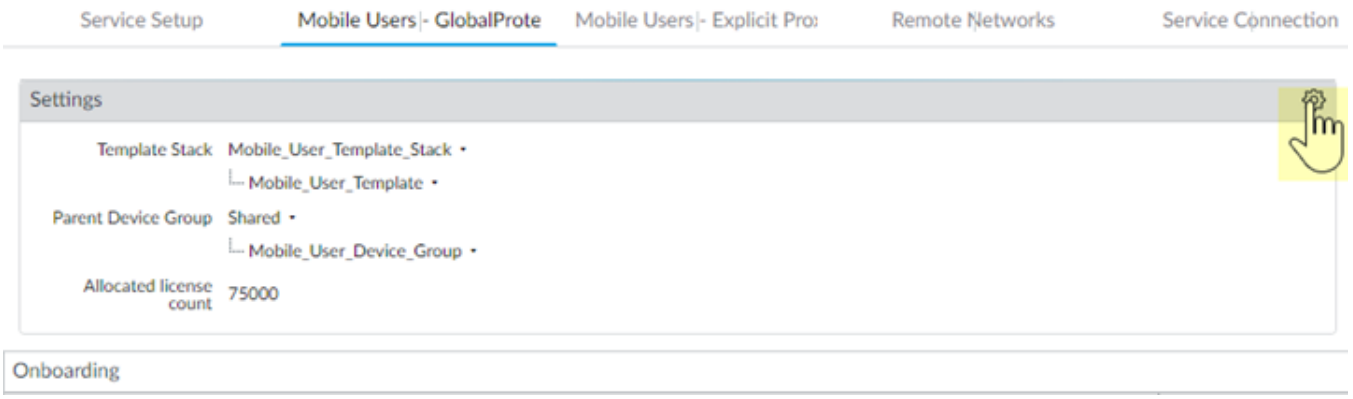
 ©2025 Palo Alto Networks, Inc.

den Standardeinstellungen haben. Entfernen oder ändern Sie beim Bearbeiten dieser Vorlage nicht den Eintrag „Externes Gateway“.




**STEP 3 |** Konfigurieren Sie die Gerätegruppenhierarchie, die der Cloud-Dienst per Push an das Portal und das Gateway überträgt.

1. Ändern Sie die **Einstellungen**.



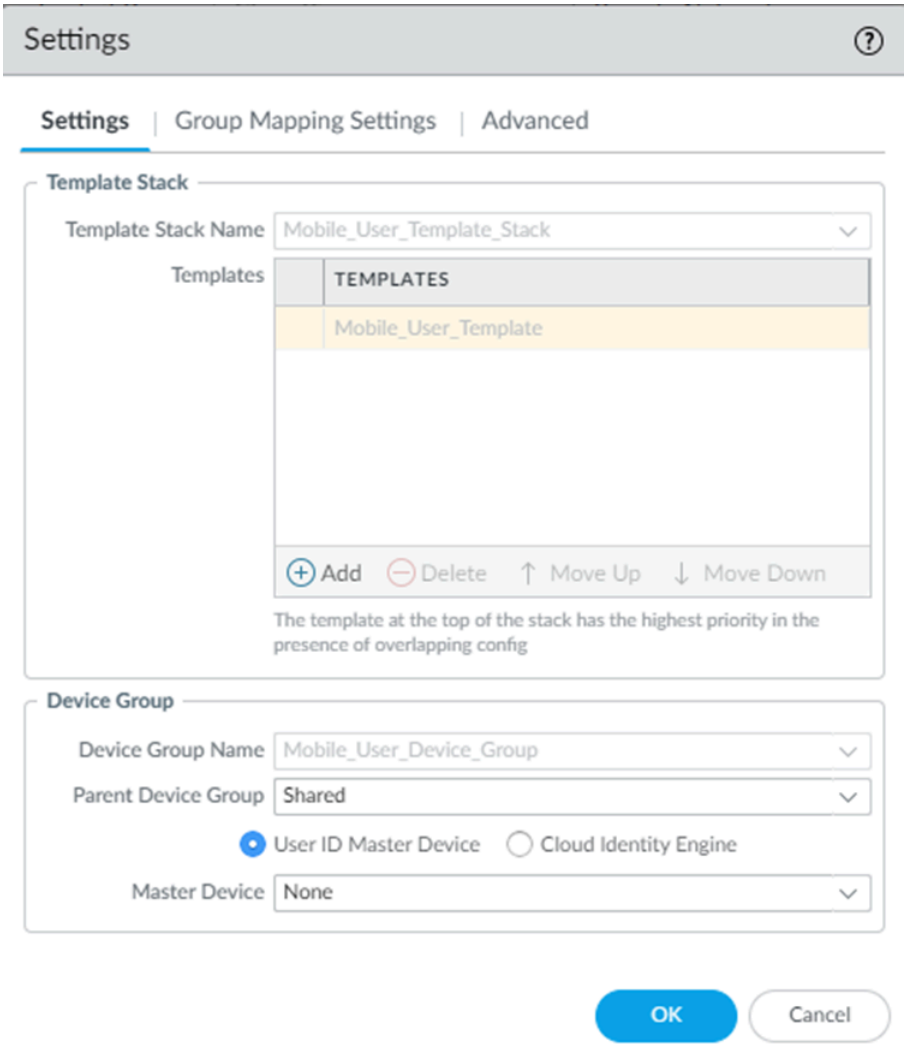

2. Wählen Sie im Abschnitt „Gerätegruppe“ die **übergeordnete Gerätegruppe** aus, die die Konfigurationseinstellungen enthält, die Sie per Push an Prisma Access für Benutzer

 ©2025 Palo Alto Networks, Inc.

übertragen möchten, oder belassen Sie die übergeordnete Gerätegruppe als **freigegeben**, um die freigegebene Hierarchie der Prisma Access-Gerätegruppe zu verwenden.

Sie werden die gesamte Konfiguration per Push übertragen – einschließlich der Adressgruppen, der Sicherheitsrichtlinie, der Sicherheitsprofile und anderer Richtlinienobjekte (z. B. Anwendungsgruppen und -objekte), der HIP-Objekte und -Profile und Authentifizierungsrichtlinien –, die Prisma Access für Benutzer benötigt, um konsistente Richtlinien für Ihre mobilen Benutzer mithilfe der hier angegebenen Gerätegruppenhierarchie durchzusetzen. Darüber hinaus müssen Sie sicherstellen, dass Sie ein Protokollweiterleitungsprofil konfiguriert haben, das die gewünschten Protokolltypen an den **Panorama/Strata-Protokollierungsdienst** in einer Gerätegruppe weiterleitet, die an Prisma Access für Benutzer weitergeleitet wird. Nur so weiß der Cloud-Dienst, welche Protokolle an Strata Logging Service weitergeleitet werden sollen.

3. (Optional) Wenn Sie eine Firewall der nächsten Generation als Mastergerät konfiguriert oder ein Cloud Identity Engine-Profil hinzugefügt haben, um Benutzer- und Gruppeninformationen in Sicherheitsrichtlinien auswählbar zu machen, wählen Sie **Benutzer-ID-Mastergerät** oder **Cloud Identity Engine** aus. Anschließend wählen Sie entweder das Mastergerät oder das Cloud Identity Engine-Profil aus, das Sie erstellt haben.




 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** (Optional) Konfigurieren Sie Prisma Access so, dass die Komponente „Verzeichnissynchronisierung“ der Cloud Identity Engine zum Abrufen von Benutzer- und Gruppeninformationen verwendet werden kann.

Konfigurieren Sie die Verzeichnissynchronisierungskomponente der Cloud Identity Engine so, dass Benutzer- und Gruppeninformationen aus dem Cloud-Verzeichnis oder Active Directory (AD) abgerufen werden können, bevor Sie die Integration der Verzeichnissynchronisierung in Prisma Access-**Einstellungen für die Gruppenzuordnung** aktivieren und konfigurieren.

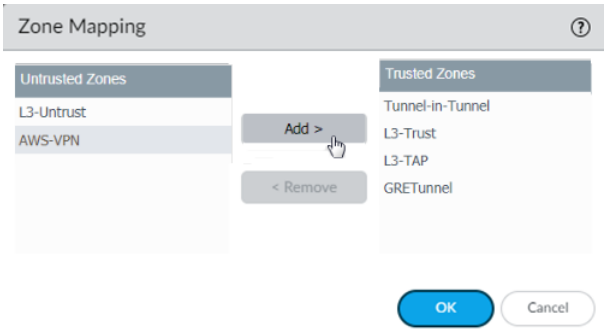
**STEP 5 |** Klicken Sie auf **OK**, um die Einstellungen für mobile Benutzer zu speichern.

**STEP 6 |** Weisen Sie die innerhalb des Vorlagenstacks konfigurierten Zonen als vertrauenswürdig oder nicht vertrauenswürdig zu.

Auf einer Palo Alto Networks-Firewall der nächsten Generation wird die Sicherheitsrichtlinie zwischen Zonen durchgesetzt, die physischen oder virtuellen Schnittstellen auf der Firewall zugeordnet sind. Mit Prisma Access für Benutzer wird die Netzwerkinfrastruktur jedoch automatisch für Sie eingerichtet, sodass Sie keine Schnittstellen mehr konfigurieren und Zonen zuordnen müssen. Um eine konsistente Durchsetzung von Sicherheitsrichtlinien zu ermöglichen, müssen Sie jedoch die Zonen, die Sie innerhalb Ihrer Organisation verwenden, als vertrauenswürdig oder nicht vertrauenswürdig zuordnen, damit Prisma Access für Benutzer die Richtlinienregeln, die Sie per Push an den Cloud-Dienst übertragen, in die internen Zonen innerhalb der Netzwerkinfrastruktur übersetzen kann.

1. Ändern Sie die Einstellungen für die Zonenzuordnung.

   Standardmäßig sind alle Zonen im Vorlagenstack „Mobile_User_Template_Stack“ als nicht vertrauenswürdige Zonen klassifiziert.
2. Wählen Sie jede Zone aus, die Sie als vertrauenswürdig festlegen möchten, und klicken Sie auf **Hinzufügen**, um sie in die Liste der **vertrauenswürdigen Zonen** zu verschieben.




3. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

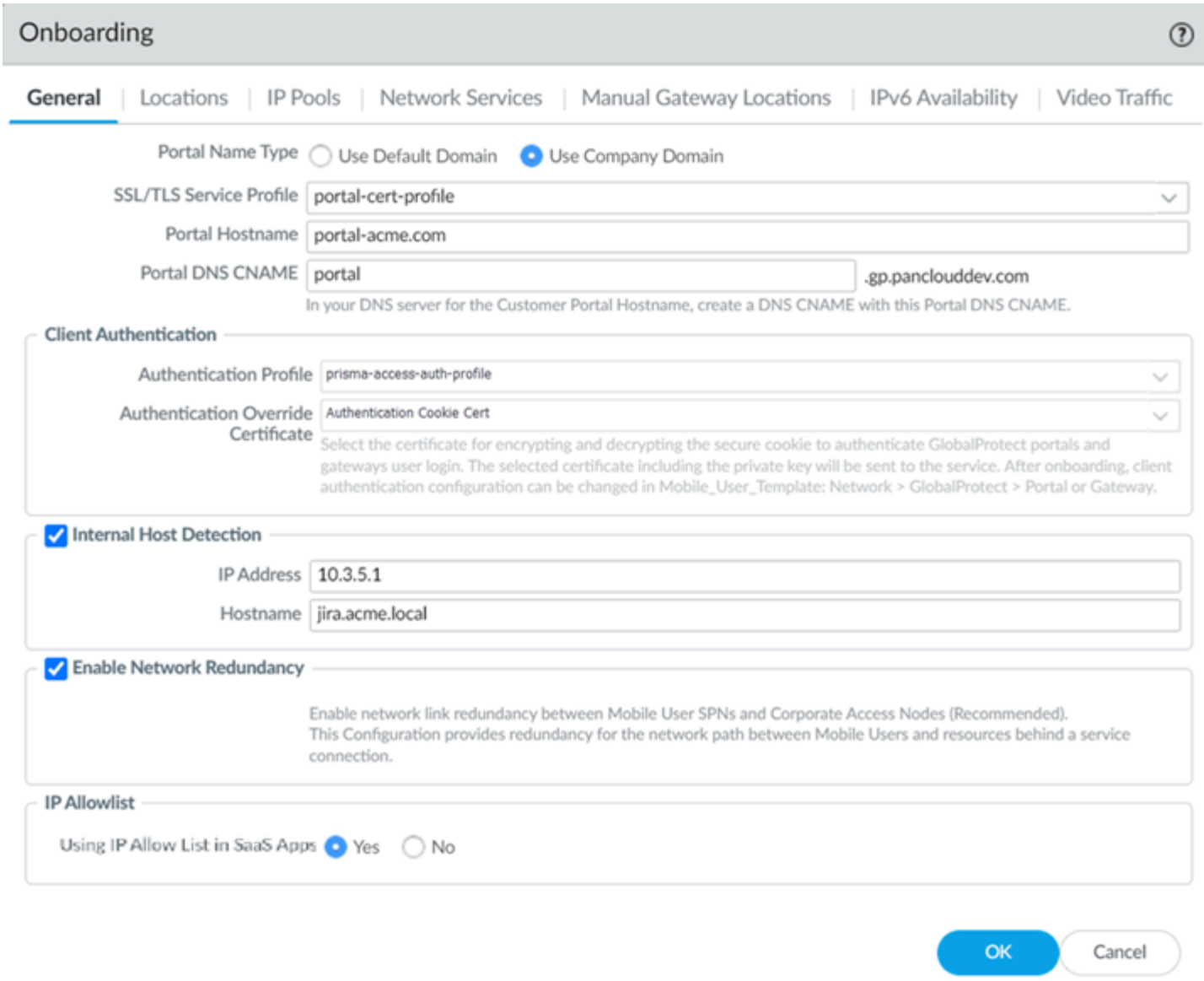
**STEP 7 |** Konfigurieren Sie die Einstellungen für das GlobalProtect-Portal und externe Gateways.

Sie können Prisma Access-Gateways nur als externe Gateways konfigurieren – nicht als interne Gateways.

1. Klicken Sie im Abschnitt „Onboarding“ auf **Konfigurieren**.
2. Geben Sie auf der Registerkarte **Allgemein** den **Portal-Namenstyp** an:
   - **Standarddomäne verwenden** – Wenn Sie diese Option auswählen, verwendet Ihr Portal-Hostname den Standarddomänennamen: `.gpcloudservice.com`. Geben Sie in diesem Fall einfach einen Wert für **Portal-Hostname** ein, der an

 ©2025 Palo Alto Networks, Inc.

den Standarddomänennamen angefügt wird. Prisma Access für Benutzer erstellt automatisch die erforderlichen Zertifikate und veröffentlicht den Hostnamen auf den öffentlichen DNS-Servern.




Wenn Sie bereits über eine GlobalProtect-Bereitstellung mit einem vorhandenen Portalnamen verfügen und diesen Portalnamen weiterhin verwenden möchten, fügen Sie einen CNAME-Eintrag hinzu, der den Prisma Access-Portalnamen Ihrem vorhandenen Portalnamen zuordnet. Wenn beispielsweise ein bestehendes Portal mit dem Namen portal.acme.com vorliegt und Sie das neue Prisma Access-Portal diesem Namen zuordnen möchten, können Sie dem DNS-Eintrag für Ihr bestehendes Portal den CNAME „gpcs2.gpcloudservice.com“ hinzufügen.

*Die Domäne *.gpcloudservice.com ist der Palo Alto Networks-Anwendung zugeordnet.*

- **Firmendomäne verwenden** – Wählen Sie diese Option aus, wenn die Domäne im Portal-Hostnamen mit Ihrem Unternehmensdomänennamen übereinstimmen soll

 ©2025 Palo Alto Networks, Inc.

(z. B. myportal.mydomain.com). Wenn Sie diese Option verwenden möchten, müssen Sie zunächst ein eigenes Zertifikat erwerben und ein darauf verweisendes SSL/TLS-Dienstprofil konfigurieren. Anschließend können Sie den Portalnamen konfigurieren, indem Sie das **SSL/TLS-Dienstprofil** auswählen und den **Portal-Hostnamen** eingeben. Wenn Sie diese Option verwenden, müssen Sie Ihre internen DNS-Server auf den **Portal-DNS-CNAME** verweisen, also auf den Hostnamen des Portals mit der Domäne `.gpcloudservice.com`. Wenn Sie beispielsweise den DNS-Hostnamen „acme-portal.acme.com“ angegeben haben, müssen Sie einen DNS-CNAME-Eintrag erstellen, der diesen Hostnamen „acme-portal.gpcloudservice.com“ auf Ihren internen DNS-Servern zuordnet.

*Wenn Sie ein neues Zertifikat hochladen müssen, importieren Sie das Zertifikat und den privaten Schlüssel. Anschließend sehen Sie sich den von Prisma Access verwendeten SSL/TLS-Dienst an (unter **Netzwerk** > **GlobalProtect** > **Portale** > **GlobalProtect_Portal** > **Authentifizierung**) und überprüfen den Namen des **SSL/TLS-Dienstprofils**. Dieses Feld wird nur angezeigt, wenn Sie eine Unternehmensdomäne anstelle der Standarddomäne verwenden. Sie können dann **Gerät** > **Zertifikatverwaltung** > **SSL/TLS-Zertifikatprofil** auswählen und das Zertifikat im SSL/TLS-Profil, das vom Portal verwendet wird, durch das importierte Zertifikat ersetzen.*

3. Wählen Sie ein **Authentifizierungsprofil** aus, das angibt, wie Prisma Access mobile Benutzer authentifizieren soll, oder erstellen Sie ein neues Profil.

   Wenn Sie eine übergeordnete Gerätegruppe hinzugefügt haben, die eine Authentifizierungsprofilkonfiguration enthält, sollte diese in der Liste der verfügbaren Profile angezeigt werden. Wenn Sie das Profil in der Gerätegruppe nicht per Push übertragen haben, können Sie jetzt ein Authentifizierungsprofil erstellen.

   *Nachdem Sie Ihre Änderungen festgeschrieben und per Push übertragen haben, können Sie in diesem Bereich keine Änderungen am Authentifizierungsprofil und am Authentifizierungsüberschreibungszertifikat vornehmen, und die Optionen sind nun schreibgeschützt. Um nach dem ersten Onboarding Änderungen vorzunehmen, können Sie eine oder mehrere GlobalProtect-Clientauthentifizierungskonfigurationen unter der Vorlage **Mobile_User_Template** ändern oder hinzufügen.*

4. Wählen Sie ein **Authentifizierungsüberschreibungszertifikat** aus, um die sicheren Cookies zu verschlüsseln, die mobile Benutzer gegenüber dem Portal und dem Gateway authentifizieren.

   Wenn Sie eine übergeordnete Gerätegruppe hinzugefügt haben, die das Zertifikat enthält, das Sie zum Verschlüsseln von Authentifizierungscookies verwenden möchten, sollten Sie es in der Liste der verfügbaren Zertifikate sehen. Wenn Sie kein Zertifikat per Push in die Gerätegruppe übertragen haben, können Sie jetzt eines importieren oder generieren.

5. (Optional) Um sicherzustellen, dass Ihre mobilen Benutzer immer Zugriff auf die Dienste und Anwendungen haben, auf die über Dienstverbindungen zugegriffen werden kann, können Sie zwischen den Portalen oder Gateways und Dienstverbindungen die **Netzwerkredundanz aktivieren**.

   Diese Funktionalität bietet redundante Netzwerkpfade zwischen der Dataplane der mobilen Benutzer und den Dienstverbindungen an verschiedenen Compute-Standorten.

 ©2025 Palo Alto Networks, Inc.

Durch die Aktivierung der Redundanz erhalten Benutzer einen zuverlässigeren Zugriff auf die Ressourcen, die hinter den Dienstverbindungen in einem Rechenzentrum oder in der Zentrale stehen. Da für den Zugriff mobiler Benutzer auf Ressourcen aus Remote-Netzwerken eine Dienstverbindung erforderlich ist, ist auch der Zugriff auf Ressourcen an Remote-Netzwerkstandorten für Benutzer zuverlässiger.

6. (Optional) Wenn Sie keine Tunnelverbindungen für GlobalProtect-Endpunkte im internen Netzwerk benötigen, aktivieren Sie die **interne Hosterkennung**.
   1. Aktivieren Sie das Kontrollkästchen **Interne Hosterkennung**.
   2. Geben Sie die **IP-Adresse** eines Hosts ein, den Benutzer nur aus dem internen Netzwerk erreichen können.
   3. Geben Sie den DNS-**Hostnamen** für die eingegebene IP-Adresse ein. Clients, die versuchen, eine Verbindung herzustellen, führen einen Reverse DNS-Lookup an der angegebenen Adresse durch. Wenn die Suche fehlschlägt, stellt der Client fest, dass er eine Tunnelverbindung zu Prisma Access für Benutzer benötigt.

   > *Prisma Access kopiert die internen Hosterkennungseinstellungen, die Sie hier angeben, auf die Standard-Agent-Einstellungen in Ihrer* GlobalProtect-Portalkonfiguration *(**Netzwerk** > **GlobalProtect** > **Portale** > **<Portalkonfiguration>** > **Agent** > **STANDARD** > **Intern**). Wenn Sie interne Hosterkennungseinstellungen für den Standardagenten im GlobalProtect-Portal eingegeben haben, können Sie die Optionen hier nicht ändern, sondern müssen sie im Portal ändern. Wenn Sie mehrere Agent-Konfigurationen benötigen, geben Sie im GlobalProtect-Portal Einstellungen für die Standard-Agent-Konfiguration ein und verwenden Sie diese Einstellungen für Prisma Access. Wählen Sie anschließend **Netzwerk** > **GlobalProtect** > **Portale** > **<Portalkonfiguration>** > **Agent** aus, um eine vom Standard abweichende Konfiguration **hinzuzufügen**, und geben Sie diese Konfiguration in anderen Teilen Ihrer Bereitstellung an.*

7. (Optional) Wenn Ihre Organisation Zulassungslisten verwendet, um den Zugriff auf öffentliche oder SaaS-Anwendungen zu steuern, geben Sie an, ob Sie **IP-Zulassungslisten in SaaS-Apps verwenden** oder nicht.

   Damit Sie die öffentlichen (Ausgangs-)IP-Adressen für Ihre Bereitstellung des Typs „GlobalProtect – Mobile Benutzer“ zu allen Zulassungslisten Ihrer SaaS-Anwendungen hinzufügen können, die Sie in Ihrer Organisation verwenden, stellt Prisma Access Ihnen die IP-Adressen bereit und ermöglicht es Ihnen, zu überprüfen, ob Sie sie zu Ihrer Zulassungsliste hinzugefügt haben, bevor Sie sie in Ihrer Umgebung verwenden. Sie können Zulassungslisten für Ausgangs-IP-Adressen von Prisma Access für bestehende und für neue Bereitstellungen implementieren.

8. (Optional) Passen Sie die Einstellungen der GlobalProtect-App an (geben Sie z. B. die Verbindungsmethode an, die von GlobalProtect verwendet wird), indem Sie **Netzwerk** > **GlobalProtect** > **Portale** > **GlobalProtect_Portal** > **Agent** auswählen, die anzupassende Konfiguration oder **STANDARD** und anschließend **App** auswählen, um die GlobalProtect-App anzupassen.

 ©2025 Palo Alto Networks, Inc.

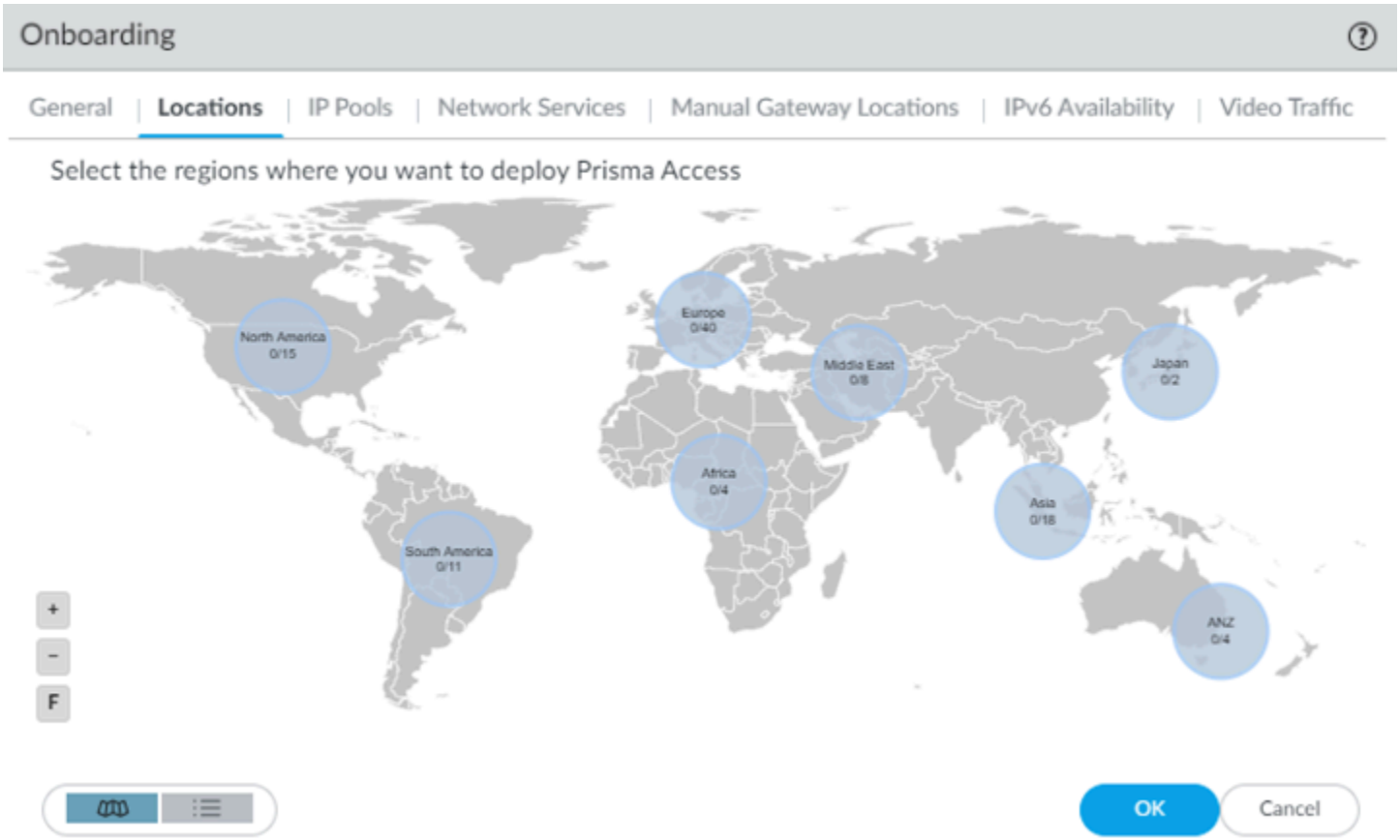
**STEP 8 |** Wählen Sie die **Standorte** und Regionen aus, die den Standorten zugeordnet sind, an denen Sie Ihre mobilen Benutzer bereitstellen möchten.

Auf der Registerkarte **Standorte** wird eine Karte angezeigt. Wenn Sie die Karte hervorheben, werden die globalen Regionen (Amerika, Europa und Asien-Pazifik) und die verfügbaren Standorte innerhalb der einzelnen Region angezeigt. Wählen Sie eine Region und anschließend die Standorte aus, die Sie in jeder Region bereitstellen möchten. Indem Sie Ihre Bereitstellung auf eine einzelne Region beschränken, können die bereitgestellten Regionen genauer gesteuert und Regionen ausgeschlossen werden, wenn Ihre Richtlinien oder Branchenvorschriften dies erfordern. Sie können einen Standort in einer Region auswählen, die Ihren mobilen Benutzern am nächsten liegt, oder einen Standort auswählen, wie es in Ihren Richtlinien oder Branchenvorschriften vorgeschrieben ist.

*Prisma Access nutzt die Standorte „Hongkong“, „Niederlande (Mitte)“ und „USA (Nordwest)“ als Fallback-Standorte für mobile Benutzer, wenn andere Standorte nicht verfügbar sind. Aus diesem Grund empfiehlt Palo Alto Networks dringend, mindestens einen dieser Standorte während des Onboardings mobiler Benutzer zu aktivieren.*

Standorte, die mit zwei Sternchen angegeben werden, sind **lokale Zonen**. Diese Standorte platzieren Rechen-, Speicher-, Datenbank- und Infrastrukturdienste in der Nähe großer Bevölkerungs- und Industriezentren. Allerdings gelten für sie auch einige Einschränkungen. Um eine lokale Zone hinzuzufügen, wenden Sie sich an Ihren Palo Alto Networks-Ansprechpartner.

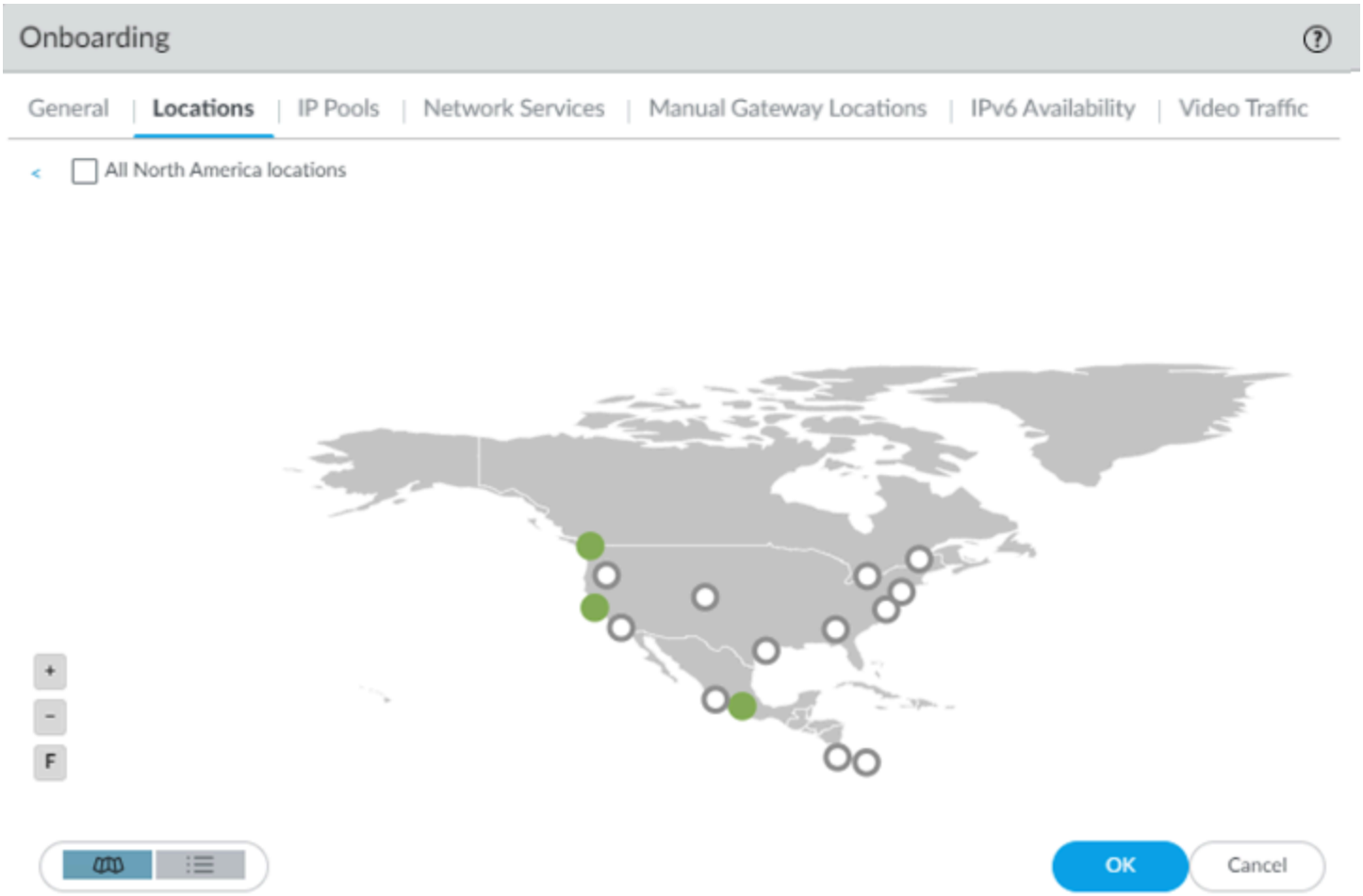
1. Klicken Sie auf die Registerkarte **Standorte** und wählen Sie eine Region aus.




 ©2025 Palo Alto Networks, Inc.

2. Wählen Sie mithilfe der Karte ein oder mehrere Prisma Access-Gateways innerhalb Ihrer ausgewählten Region aus.

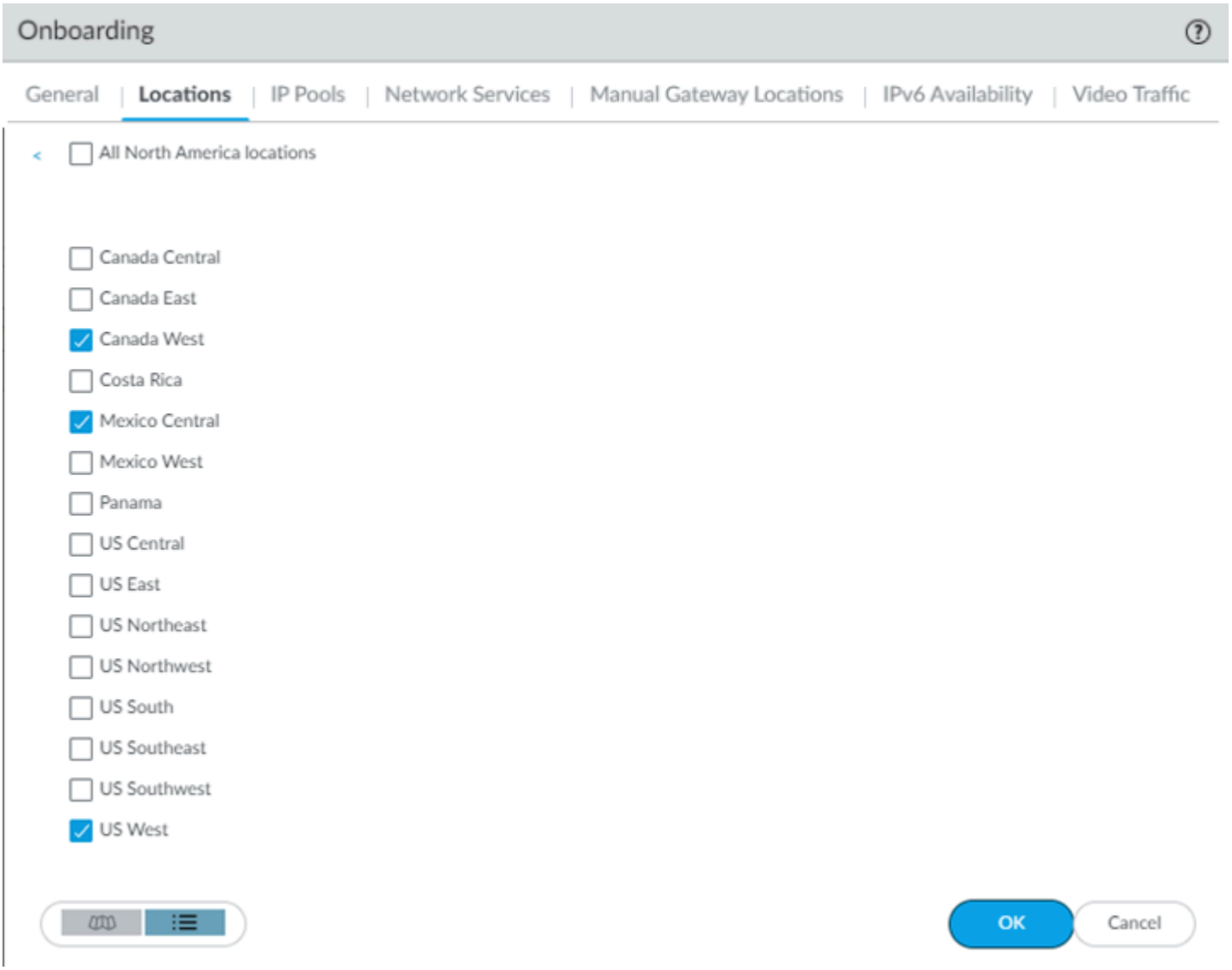
   Wenn Sie den Cursor über einen Standort bewegen, wird dieser hervorgehoben. Weiße Kreise zeigen einen verfügbaren Standort an, grüne Kreise zeigen an, dass Sie diesen Standort ausgewählt haben.




   Zusätzlich zur Kartenansicht können Sie eine Liste von Regionen und Standorten anzeigen. Sie können in der unteren linken Ecke zwischen der Karten- und der Listenansicht umschalten. In der Listenansicht werden Regionen nach Spalten sortiert

 ©2025 Palo Alto Networks, Inc.

angezeigt, wobei alle Orte nach Regionen angeordnet sind. Sie können **alle** Standorte innerhalb einer Region auswählen (oben im Dialogfenster).




**STEP 9 |** Richten Sie die IP-Adresspools ein, mit denen IP-Adressen GlobalProtect-Endpunkten zugewiesen werden, indem Sie die Registerkarte **IP-Pools** auswählen und einen IP-Adresspool **hinzufügen**.

1. Geben Sie eine **Region** für den IP-Adresspool an.

   Sie können einen einzigen IP-Adresspool für alle GlobalProtect-Endpunkte weltweit verwenden (**Weltweit**), Sie können separate Pools für jeden Schauplatz verwenden, in dem mobile Benutzer vorliegen, oder Sie können Pools pro Standortgruppe angeben (eine Gruppe von Standorten, die kleiner als der Schauplatz ist). Sie können auch eine Kombination aus weltweiten IP-Pools, IP-Pools pro Schauplatz oder IP-Pools pro Standortgruppe angeben. Beispielsweise können Sie einen Pool für eine bestimmte

 ©2025 Palo Alto Networks, Inc.

Standortgruppe hinzufügen und dann einen **weltweiten** Pool hinzufügen, der für alle anderen Standorte verwendet werden soll.

Verwenden Sie standortgruppenspezifische IP-Adresspools, wenn Sie über Dienste verfügen, die von der Quell-IP-Adresse des Benutzers abhängen, um die Details des Benutzers zu identifizieren (z. B. standortbasierte Dienste oder Dienste, die auf einer Benutzergruppe oder -funktion basieren), damit Sie Zugriffssteuerungsrichtlinien anwenden können oder um Routing- bzw. Richtlinienvorgänge für verschiedene Länder durchzuführen, wenn sich die Länder in unterschiedlichen Rechenregionen befinden. Sie könnten beispielsweise einen separaten IP-Adresspool für Kanada und einen für Brasilien verwenden, die sich an verschiedenen Compute-Standorten befinden, um unterschiedliche Zugriffs- und Sicherheitskontrollen bereitzustellen.

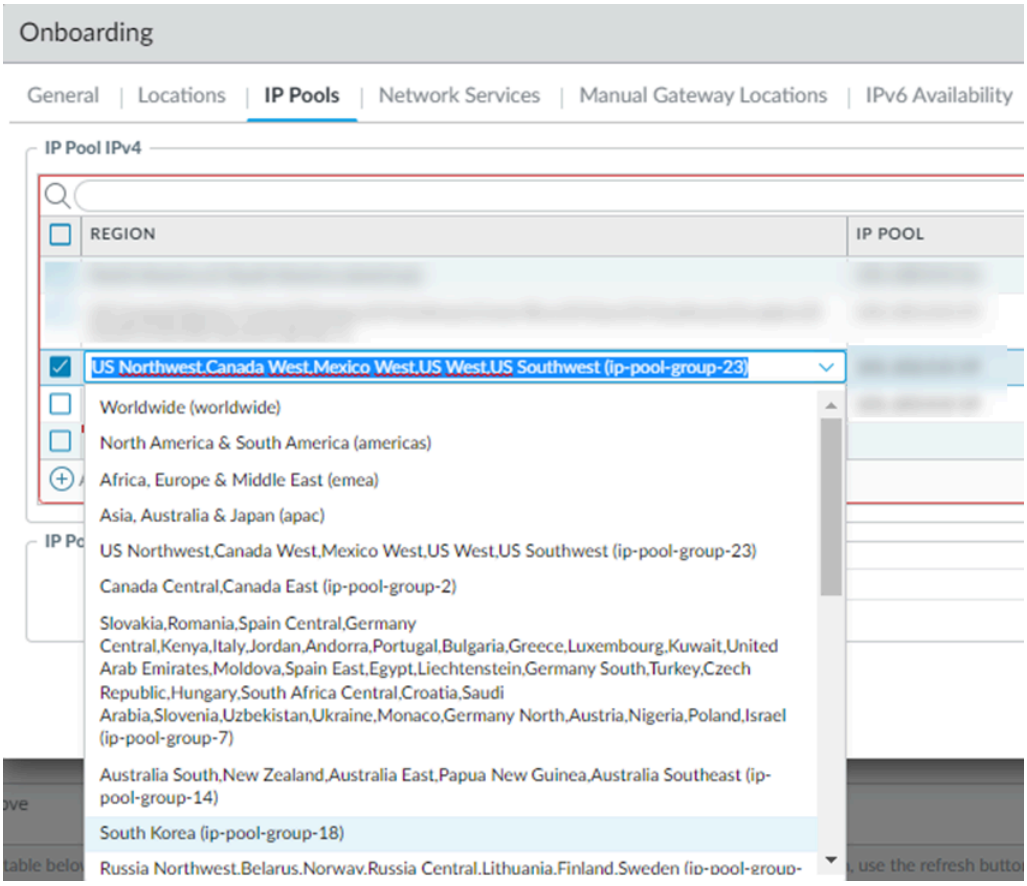
*Um standortgruppenspezifische IP-Adresspools zu verwenden, müssen Sie auch einen weltweiten oder schauplatzspezifischen Pool angeben.*

Mobile Benutzer von GlobalProtect verwenden zuerst die IP-Adressen in der Standortgruppe, dann die schauplatzspezifischen IP-Adressen und dann die weltweiten IP-Adressen. Wenn Sie beispielsweise einen Pool für eine Standortgruppe und „Weltweit“ angeben und dann die verfügbaren IP-Adressen im Pool der Standortgruppe aufgebraucht sind, verwendet Prisma Access für diese Standortgruppe IP-Adressen aus dem Pool **Weltweit**.

- Um IP-Pools anzugeben, die von allen mobilen GlobalProtect-Benutzern verwendet werden können, wählen Sie **Weltweit** aus.
- Um IP-Pools anzugeben, die von GlobalProtect-Benutzern in einem bestimmten Schauplatz verwendet werden können, wählen Sie den Schauplatz aus.

 ©2025 Palo Alto Networks, Inc.

- Um IP-Pools anzugeben, die für die Standortgruppe spezifisch sind, wählen Sie diese aus der Liste aus.




2. Geben Sie einen **IP-Pool** ein, um die Endpunkte in der von Ihnen ausgewählten Region zuzuweisen.

   - Sie können pro Standort ein minimal erforderliches Subnetz von /23 (512 IP-Adressen) eingeben. Zusätzliche Standorte erfordern mindestens ein /23-Subnetz. Wenn Sie ein weltweites Subnetz angeben, ist das minimal erforderliche Subnetz /23. Wir empfehlen jedoch IP-Adresspools für eine GlobalProtect-Bereitstellung für mobile Benutzer, um einen IP-Adresspool zuzuweisen, der der Anzahl der lizenzierten mobilen Benutzer entspricht oder größer ist, damit sich diese gleichzeitig anmelden können.

     Geben Sie keine Adressen an, die sich mit anderen intern verwendeten Netzwerken überschneiden, oder mit den Pools, die Sie beim Konfigurieren Sie die Prisma Access-Dienstinfrastruktur (Panorama) zugewiesen haben. Verwenden Sie außerdem nicht die folgenden IP-Adressen und Subnetze, da Prisma Access diese IP-Adressen und Subnetze für die interne Verwendung reserviert:

     - 169.254.0.0/16

 ©2025 Palo Alto Networks, Inc.

- 100.64.0.0/10

> *Wir empfehlen die Verwendung eines RFC-1918-konformen IP-Adresspools. Nicht mit RFC 1918 konforme (öffentliche) IP-Adressen für mobile Benutzer werden von uns zwar unterstützt, doch wir raten von deren Verwendung ab, da sie möglicherweise zu Konflikten mit dem öffentlichen IP-Adressraum des Internets führen.*

**STEP 10 |** Um die DNS-Auflösungseinstellungen für Ihre internen und externen (öffentlichen) Domänen festzulegen, wählen Sie die Registerkarte **Netzwerkdienste** aus, um die Einstellungen **hinzuzufügen**.

GlobalProtect-Endpunkte mit aktiver Tunnelverbindung verwenden ihre virtuellen Netzwerkadapter anstelle ihrer physischen Netzwerkadapter und benötigen daher separate Einstellungen für die DNS-Auflösung.

Konfigurieren Sie Netzwerkeinstellungen im Fenster **Netzwerkdienste**.

- Wählen Sie aus dem Dropdown-Menü eine **Region** aus.

  Wählen Sie **Weltweit**, einen Schauplatz oder eine Standortgruppe aus, um die DNS-Einstellungen global anzuwenden. Wenn Sie mehrere Proxy-Einstellungen mit einer Kombination aus „Weltweit“-, schauplatz- und standortspezifischen Einstellungen angeben, verwendet Prisma Access die Einstellungen für die Standortgruppe, dann die für den Schauplatz, dann die für „Weltweit“. Prisma Access wertet die Regeln von oben nach unten in der Liste aus.
- Sie können eine oder mehrere Regeln **hinzufügen**, um die DNS-Einstellungen für **Interne Domänen** zu konfigurieren.
  - Geben Sie einen eindeutigen **Regelnamen** für die Regel ein.
  - Geben Sie keine 127.0.0.1-Adresse ein, da dies zu internen Routingproblemen in Prisma Access führen kann.
  - Wenn Ihr interner DNS-Server nur die von Ihnen angegebenen Domänen auflösen soll, geben Sie die aufzulösenden Domänen in die **Domänenliste** ein. Geben Sie vor der Domäne ein Sternchen an, z. B. *.acme.com. Sie können maximal 1.024 Domäneneinträge angeben.

    > *Prisma Access verfügt über eine vordefinierte Regel, um die Domänen *.amazonaws.com, *.aws.amazon.com, *.googleapis.com und *.google.internal mithilfe des Cloud-Standardservers aufzulösen. Wenn Sie möchten, dass Ihre internen DNS-Server eine spezifischere Domäne auflösen (z. B. *.s3.amazonaws.com anstatt *.amazonaws.com), geben Sie die URL in die **Domänenliste** ein. Prisma Access wertet die Domänennamen aus und geht dabei vom längsten zum kürzesten und anschließend in der Liste von oben nach unten vor.*
  - Wenn Sie über einen **benutzerdefinierten DNS-Server** verfügen, der auf Ihre internen Domänen zugreifen kann, geben Sie die IP-Adressen des primären und des sekundären

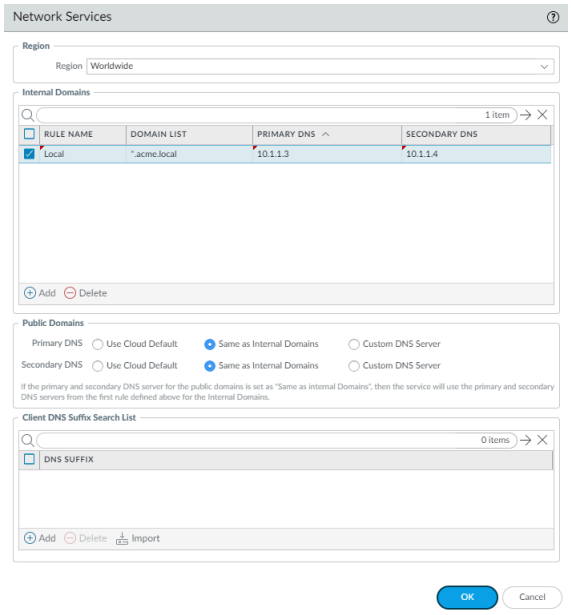
 ©2025 Palo Alto Networks, Inc.

DNS-Servers an (**Primärer DNS** und **Sekundärer DNS**) oder wählen Sie **Cloud-Standard verwenden** aus, um den Standard-DNS-Server von Prisma Access zu verwenden.

- Geben Sie die DNS-Einstellungen für **Öffentliche Domänen** an.
  - **Cloud-Standard verwenden** – Verwenden Sie den Standard-DNS-Server von Prisma Access.
  - **Wie interne Domänen** – Verwenden Sie denselben Server, den Sie zum Auflösen interner Domänen verwenden. Wenn Sie diese Option aktivieren, entspricht der DNS-Server, der zur Auflösung öffentlicher Domänen verwendet wird, dem Server, der für die erste Regel im Abschnitt **Interne Domänen** konfiguriert ist.
  - **Benutzerdefinierter DNS-Server** – Wenn Sie über einen DNS-Server verfügen, der auf Ihre öffentlichen (externen) Domänen zugreifen kann, geben Sie in dieses Feld die Adresse des primären DNS-Servers ein.

  (Optional) Sie können ein **DNS-Suffix hinzufügen**, um das Suffix anzugeben, das der Client lokal verwenden soll, wenn ein nicht qualifizierter Hostname eingegeben wird, den er nicht auflösen kann, z. B. acme.local. Geben Sie vor dem Domänensuffix (z. B. acme.com) kein Platzhalterzeichen (*) ein. Sie können mehrere Suffixe hinzufügen.
- Wenn Sie möchten, dass Prisma Access als Proxy für DNS-Anfragen fungiert, konfigurieren Sie Werte für UDP-Abfragen (das **Intervall** in Sek.), um die Abfrage nach einer bestimmten Anzahl von Sekunden zu wiederholen, sowie die Anzahl der durchzuführenden Wiederhol-**Versuche**.

  Weitere Informationen dazu, wie Prisma Access DNS-Anfragen im Proxy-Modus verarbeitet, finden Sie unter DNS-Auflösung für Bereitstellungen von „Mobile Benutzer – GlobalProtect“.

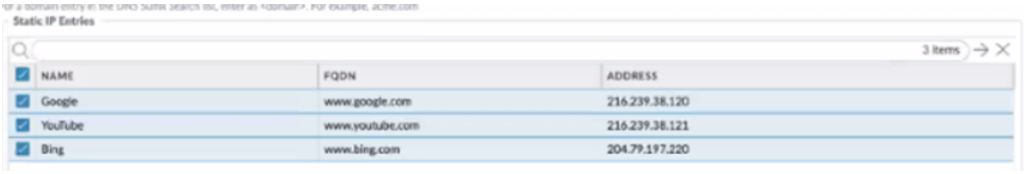



**STEP 11 |** (Optional) Verwenden Sie **Statische IP-Einträge**, um FQDNs auf bestimmte IP-Adressen aufzulösen.

Diese Funktionalität kann nützlich sein, wenn es in Ihrer Organisation Gast-Internetdienste gibt und Sie möchten, dass Ihre Gäste Suchmaschinen sicher verwenden, damit verhindert

 ©2025 Palo Alto Networks, Inc.

wird, dass sie nach potenziell unangemessenem oder anstößigem Material suchen, das gegen die Unternehmensrichtlinie verstoßen könnte. Geben Sie dazu einen eindeutigen **Namen** für die Regel für statische Einträge, einen **FQDN** und die IP-**Adresse** ein, an die die FQDN-Anfragen gerichtet werden soll.




**STEP 12 |** (Optional) Wenn Ihre Bereitstellung auf Windows Internet Name Service (WINS) basiert, können Sie WINS-Server angeben, um die NetBIOS-Name-zu-IP-Adresszuordnung aufzulösen, indem Sie **WINS-Konfiguration** auswählen, eine Region für den WINS-Server oder „Weltweit“ auswählen, um die WINS-Konfiguration weltweit anzuwenden, und dann eine **primäre WINS**- und optional eine **sekundäre WINS**-Serveradresse angeben.

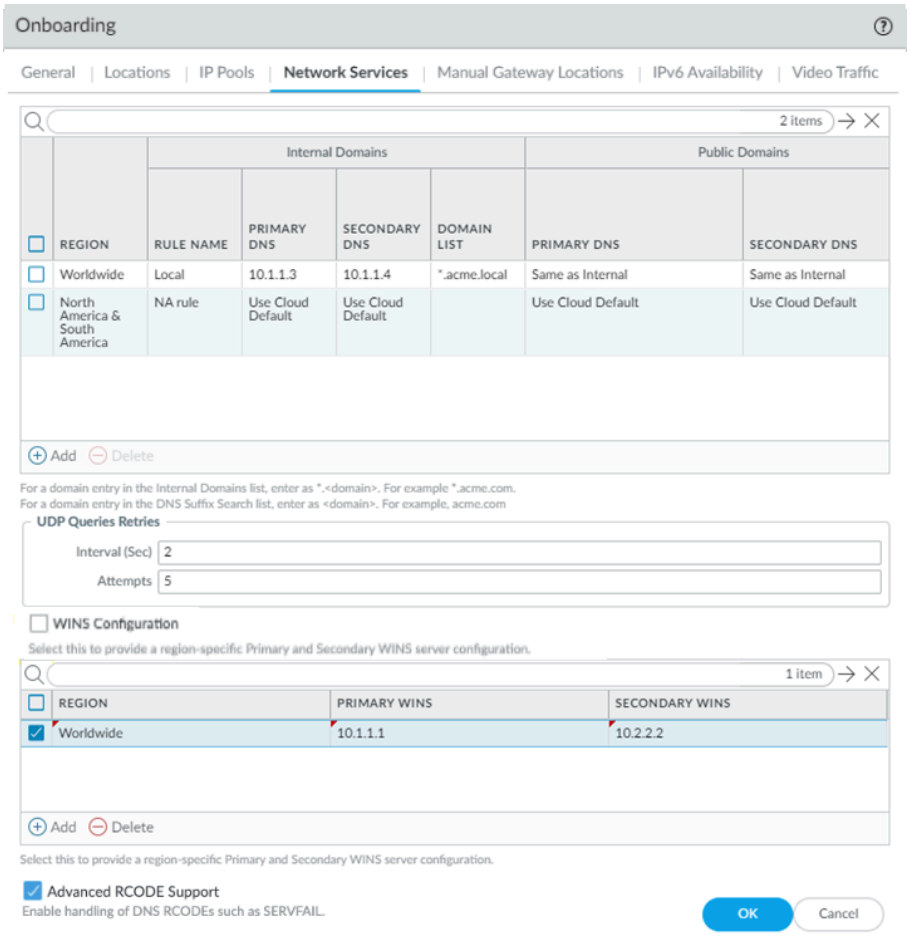
Nachdem Sie WINS aktiviert haben, kann Prisma Access die WINS-Konfiguration per Push über GlobalProtect auf die Endpunkte mobiler Benutzer übertragen.

**STEP 13 |** (Optional) Wählen Sie die erweiterte RCODE-Unterstützung aus, um ein Failover des primären DNS-Servers auf den sekundären DNS-Server zuzulassen, wenn ein DNS-Rückgabecode vom Typ RCODE 2 (SERVFAIL) oder RCODE 5 (REFUSED) empfangen wird.

Der DNS-Antwortcode SERVFAIL weist auf einen Kommunikationsfehler mit dem primären DNS-Server hin, und der DNS-Antwortcode REFUSED bedeutet, dass sich der primäre DNS-

 ©2025 Palo Alto Networks, Inc.

Server geweigert hat, die angeforderten Informationen bereitzustellen. In beiden Fällen wird für den Dienst ein Failover auf den sekundären DNS-Server durchgeführt.




 ©2025 Palo Alto Networks, Inc.

**STEP 14 |** (Optional) Wenn Sie Ihren mobilen Benutzern erlauben, Gateways manuell aus der GlobalProtect-App auszuwählen, wählen Sie die **manuellen Gatewaystandorte** aus, die die Benutzer in ihrer GlobalProtect-App anzeigen können.

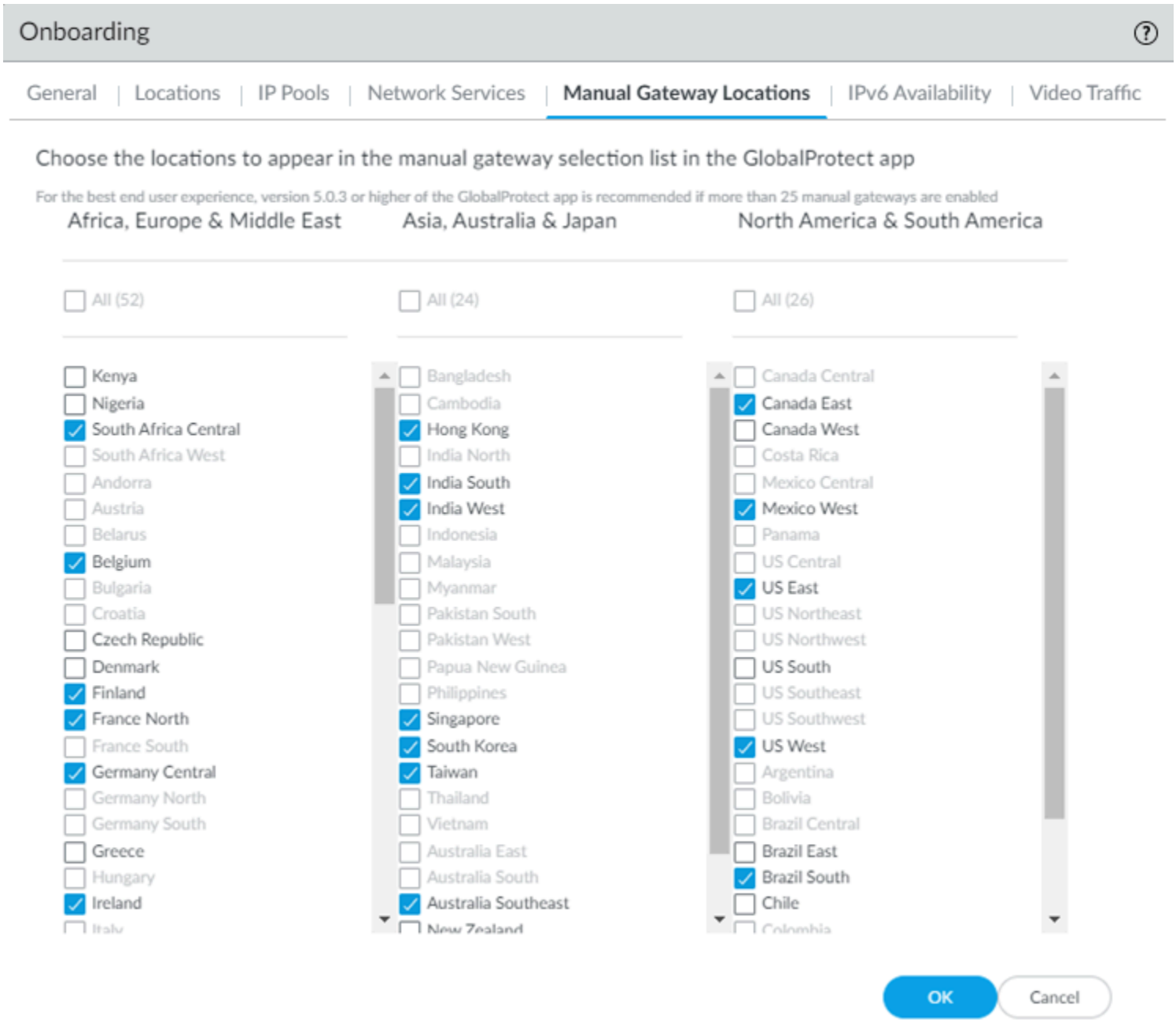
Die Auswahl einer Teilmenge integrierter Standorte verringert die Anzahl der verfügbaren Gateways, die mobile Benutzer in ihrer GlobalProtect-App zur Auswahl manueller Gateways anzeigen können.

Wenn Sie auf dieser Registerkarte keine manuellen Gateways auswählen, wählt Prisma Access standardmäßig die folgende Liste an Gateways aus.

- Australien (Südost)
- Belgien
- Brasilien (Süd)
- Kanada (Ost)
- Finnland
- Frankreich (Nord)
- Deutschland (Mitte)
- Hongkong
- Indien (West)
- Irland
- Israel
- Japan (Mitte)
- Niederlande (Mitte)
- Saudi Arabien
- Singapur
- Südafrika (Mitte)
- Südkorea
- Taiwan
- GB
- USA (Ost)
- USA (West)

Prisma Access ermöglicht Ihnen nur die Auswahl der von Ihnen eingebundenen Gateways. Wenn Sie beispielsweise bei der Auswahl von Standorten nicht **GB** auswählen, können Sie **GB** nicht als manuelles Gateway auswählen (der Standort wird abgeblendet angezeigt).

 ©2025 Palo Alto Networks, Inc.




*Wenn Sie einen Standort nach dem Onboarding löschen müssen und er als einer der **manuellen Gatewaystandorte** ausgewählt ist, deaktivieren Sie ihn hier und auf der Registerkarte **Standorte**.*

**STEP 15 |** Klicken Sie auf **OK**, um die Onboarding-Einstellungen zu speichern.

**STEP 16 |** Konfigurieren Sie Optionen für die **IPv6-Verfügbarkeit**.

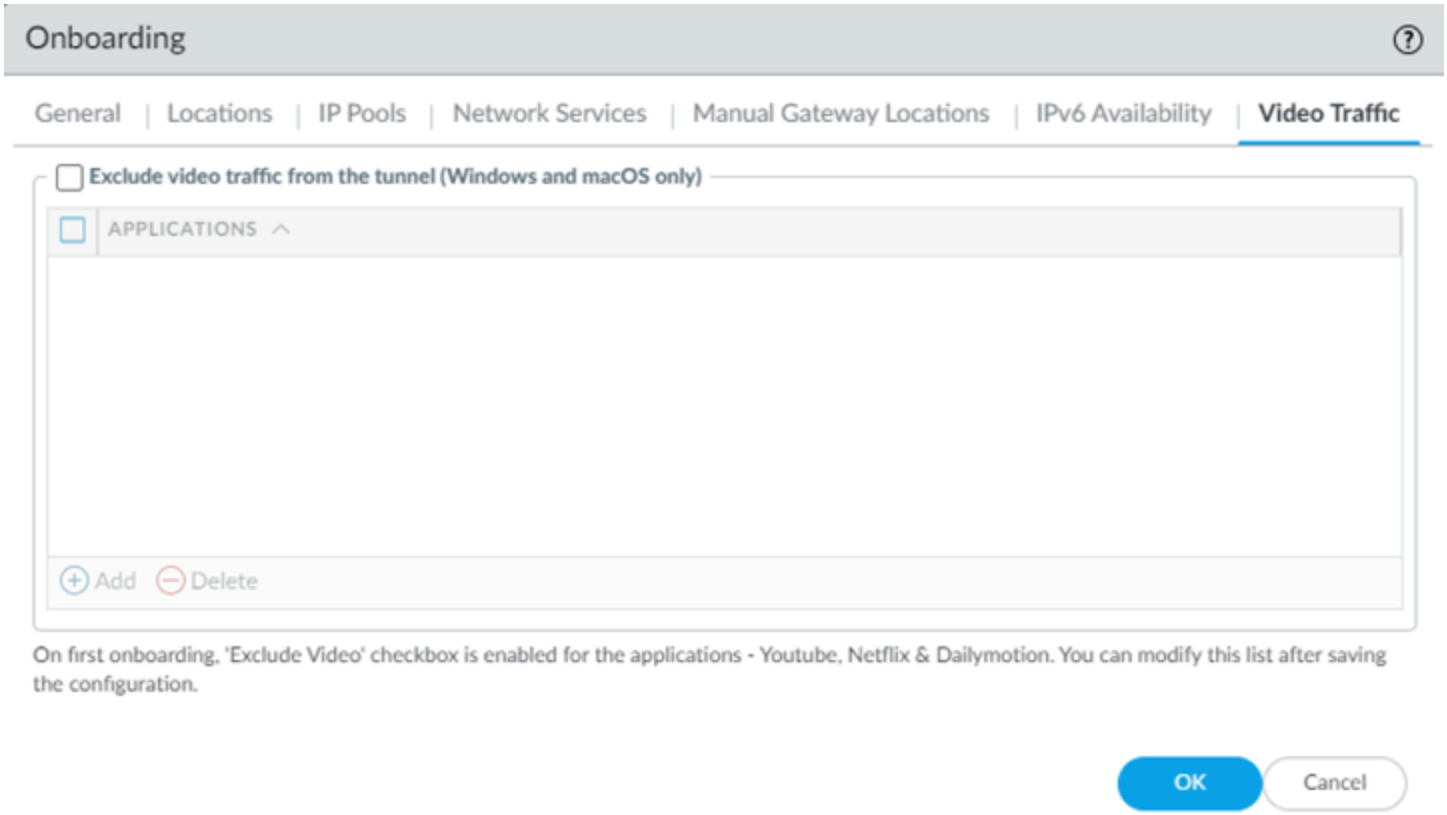
Wenn Sie IPv6-Netzwerke in Ihrer Bereitstellung des Typs Mobile Benutzer – GlobalProtect verwenden, können Sie Prisma Access so konfigurieren, dass IPv6-Adressen in Ihrer Vernetzung mobiler Benutzer verwendet werden. Des Weiteren müssen Sie die IPv6-

 ©2025 Palo Alto Networks, Inc.

Vernetzung weltweit in Ihrer Prisma Access-Infrastruktur aktivieren, bevor Sie die IPv6-Adressierung verwenden können.

**STEP 17 |** (Optional, nur Windows und macOS) Schließen Sie Videodatenverkehr vom GlobalProtect-Tunnel aus.

**Schließen Sie Videodatenverkehr vom Tunnel aus**. Anschließend müssen Sie Videostreaming-Anwendungen, die Sie vom GlobalProtect-Tunnel ausschließen möchten, **hinzufügen** oder **löschen**.




**STEP 18 |** Erstellen Sie Sicherheitsrichtlinienregeln, um den Datenverkehr für Ihre mobilen Benutzer abzusichern.

1. Wählen Sie die **Gerätegruppe** aus, in der Richtlinienregeln hinzugefügt werden sollen. Sie können die Gerätegruppe für mobile Benutzer (Mobile_User_Device_Group) oder die übergeordnete Gerätegruppe auswählen, die Sie beim Einrichten von Prisma Access für mobile Benutzer ausgewählt haben.
2. Erstellen Sie Sicherheitsrichtlinienregeln. Vergewissern Sie sich, dass keine Sicherheitsrichtlinienregeln definiert werden, mit denen Datenverkehr von einer Zone zu einer beliebigen anderen Zone zugelassen wird. Verwenden Sie in den Sicherheitsrichtlinienregeln die Zonen, die Sie in Ihrem Vorlagenstack definiert haben.

 ©2025 Palo Alto Networks, Inc.

**STEP 19 |** Konfigurieren Sie Protokolle so, dass sie Datenverkehr an Strata Logging Service weiterleiten.

Das Cloud Services-Plug-in fügt nach einer Neuinstallation oder beim Entfernen von Nicht-Prisma Access-Vorlagen aus einem Prisma Access-Vorlagenstack automatisch folgende Protokolleinstellungen (**Gerät** > **Protokolleinstellungen**) hinzu:

- Protokolleinstellungen für Systemprotokolle (**system-gpcs-default**), Benutzer-ID-Protokolle (**userid-gpcs-default**), HIP-Übereinstimmungsprotokolle (**hipmatch-gpcs-default**) und GlobalProtect-Protokolle (**gp-prismaaccess-default**) werden der Vorlage für mobile Benutzer (Mobile_User_Template) hinzugefügt.
- Protokolleinstellungen für Systemprotokolle (**system-gpcs-default**), Benutzer-ID-Protokolle (**userid-gpcs-default**) und GlobalProtect-Protokolle (**gp-prismaaccess-default**) werden der Vorlage für Remote-Netzwerke (Remote_Network_Template) hinzugefügt.
- Protokolleinstellungen für Systemprotokolle (**system-gpcs-default**) und GlobalProtect-Protokolle (**gp-prismaaccess-default**) werden der Vorlage für Dienstverbindungen (Service_Conn_Template) hinzugefügt.

Diese Protokolleinstellungskonfigurationen leiten automatisch System-, Benutzer-ID- und HIP-Übereinstimmungs-Protokolle an Strata Logging Service weiter.

**STEP 20 |** (Optional) Leiten Sie Protokolle für andere Protokolltypen an Strata Logging Service weiter.

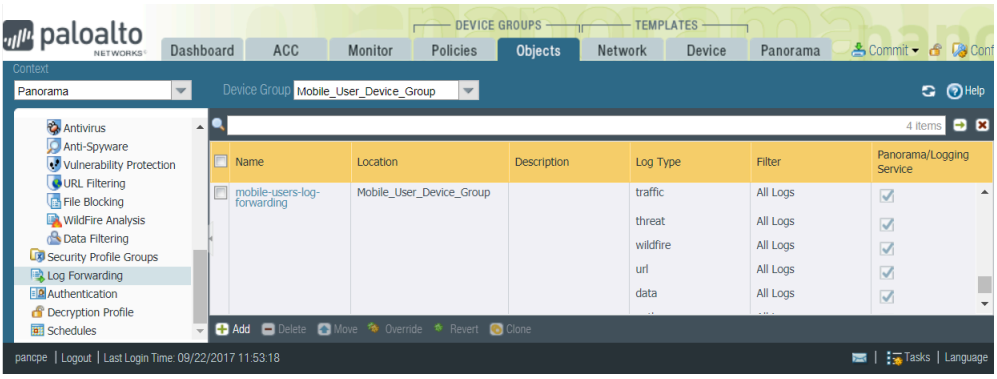
Dazu müssen Sie ein Protokollweiterleitungsprofil erstellen und jeder Richtlinienregel hinzufügen, für die Sie Protokolle weiterleiten möchten.

1. Wählen Sie die **Gerätegruppe** aus, in der Sie die Richtlinienregeln hinzugefügt haben.
2. Wählen Sie **Objekte** > **Protokollweiterleitung** aus, um ein Profil **hinzuzufügen**. Sie können in die Übereinstimmungsliste des Protokollweiterleitungsprofils jeden Protokolltyp **hinzufügen**, den Sie weiterleiten möchten.

   Im folgenden Beispiel wird die Weiterleitung von Datenverkehrs-, Threat Prevention-, WildFire-Übermittlungs-, URL-Filterungs-, Datenfilterungs- und Authentifizierungsprotokollen aktiviert.
3. Wählen Sie **Panorama/Strata-Protokollierungsdienst** als Weiterleitungsmethode aus. Wenn Sie Panorama auswählen, werden die Protokolle an Strata Logging Service weitergeleitet. Nun können Sie in Panorama die Protokolle überwachen und Berichte erstellen. Strata Logging Service bietet eine nahtlose Integration zum Speichern von Protokollen, ohne dass diese erneut an Panorama in der Unternehmenszentrale

 ©2025 Palo Alto Networks, Inc.

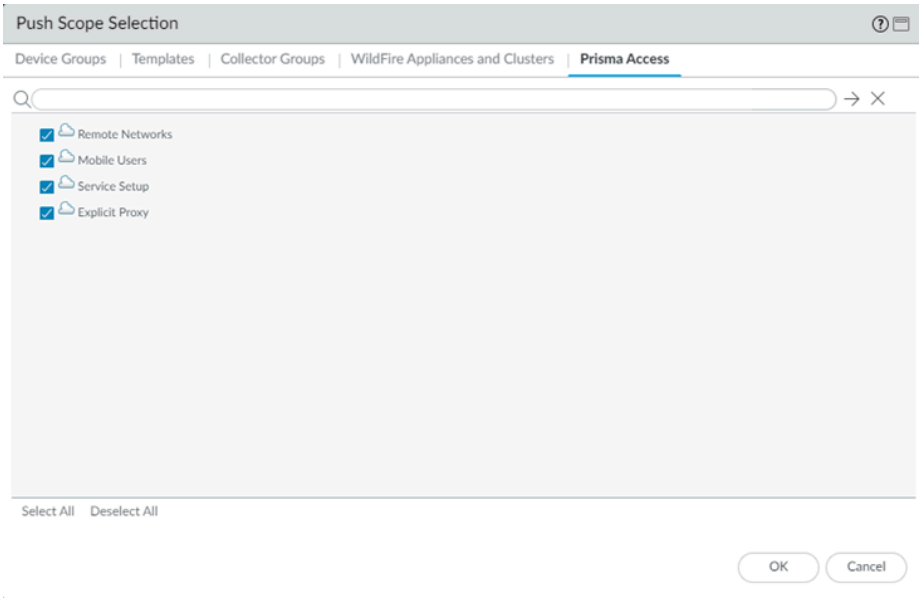
zurückgeleitet werden müssen. Panorama kann Abfragen im Strata Logging Service nach Bedarf durchführen.




4. Wählen Sie **Richtlinien** > **Sicherheit** aus und bearbeiten Sie die Richtlinienregel. Wählen Sie unter **Aktionen** das von Ihnen erstellte Protokollweiterleitungsprofil aus.

**STEP 21 |** Schreiben Sie alle Änderungen in Panorama fest und übertragen Sie die Konfigurationsänderungen per Push an Prisma Access.

1. Klicken Sie auf **Commit** > **Commit und Push**.
2. Wählen Sie **Auswahl bearbeiten** aus und vergewissern Sie sich, dass auf der Registerkarte **Prisma Access** die Optionen **Mobile Benutzer** und **Expliziter Proxy** im **Übertragungsumfang** ausgewählt sind. Klicken Sie anschließend auf **OK**.



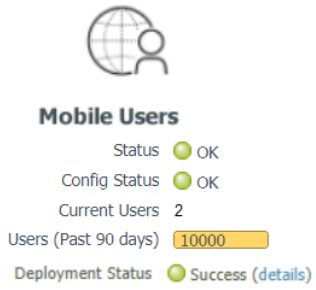

3. Vergewissern Sie sich, dass Sie auf der Registerkarte **Gerätegruppen** die Gerätegruppen **Expliziter Proxy** und **GlobalProtect** ausgewählt haben.
4. Klicken Sie auf **Commit und Push**.

 ©2025 Palo Alto Networks, Inc.

**STEP 22 |** Um zu überprüfen, ob Prisma Access für Benutzer bereitgestellt und aktiv ist, wählen Sie **Panorama** > **Cloud Services** > **Status** > **Status** aus.

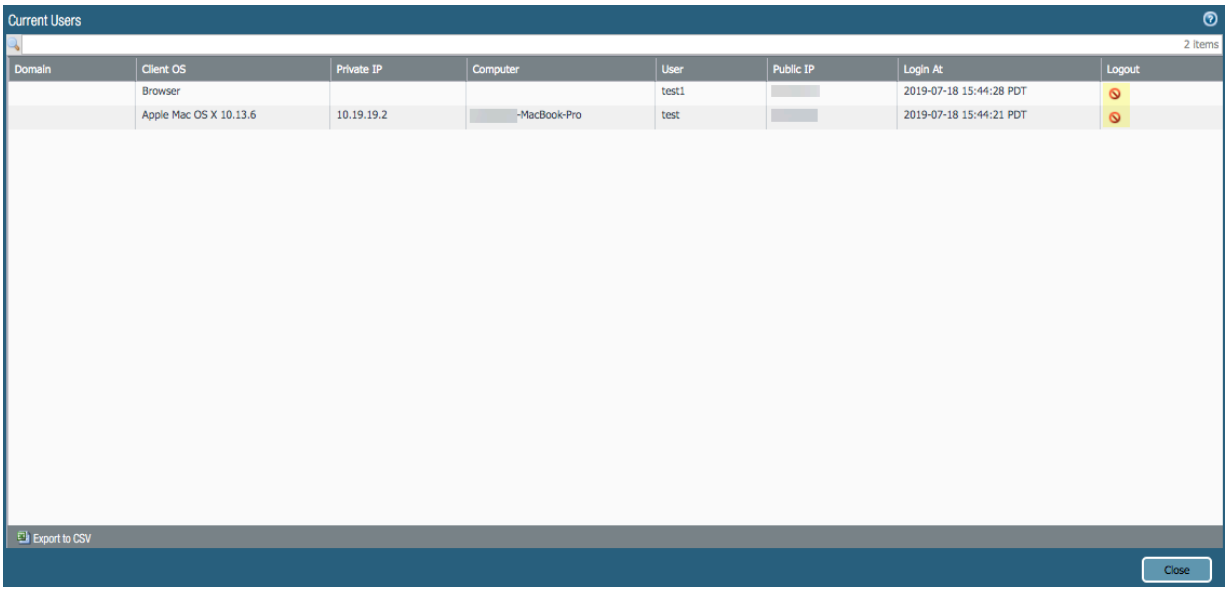
Nach Abschluss der Bereitstellung sollte für den **Status** und den **Konfigurationsstatus** mobiler Benutzer **OK** angezeigt werden.

Im Bereich **Bereitstellungsstatus** können Sie den Fortschritt der Onboarding- und Bereitstellungsjobs verfolgen, bevor sie abgeschlossen sind. Außerdem erhalten Sie in diesem Bereich weitere Informationen zum Status abgeschlossener Jobs.




Klicken Sie zum Anzeigen der Anzahl aktuell angemeldeter eindeutiger Benutzer oder zum Abmelden eines angemeldeten Benutzers auf die Hyperlink-Zahl neben **Aktuelle Benutzer**.

 ©2025 Palo Alto Networks, Inc.

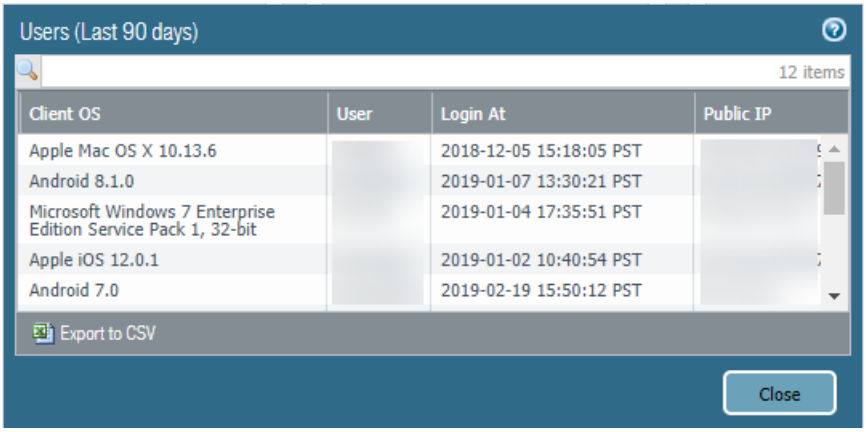



Klicken Sie auf die Zahl neben **Benutzer (letzte 90 Tage)**, um Verlaufsdaten zuvor angemeldeter Benutzer für einen Zeitraum von 90 Tagen anzuzeigen.

Wenn die Anzahl der Benutzer im Feld „Benutzer (letzte 90 Tage)“ 80 % der gesamten lizenzierten Anzahl erreicht, wird die Anzahl rot angezeigt.

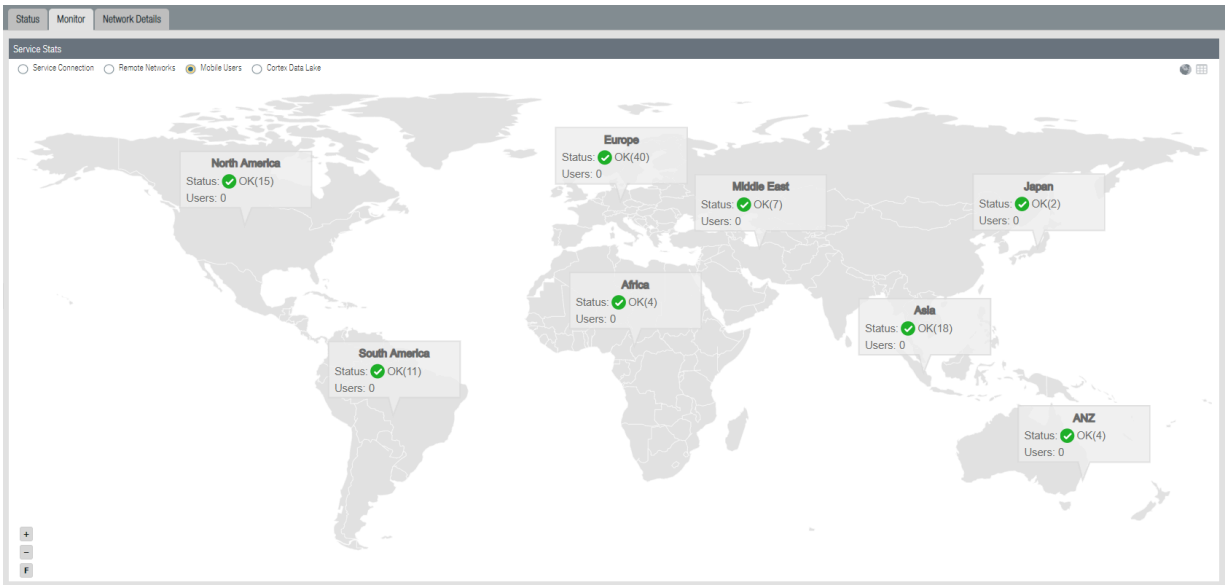
Um die Liste der Benutzer in eine CSV-Datei zu exportieren, wählen Sie **In CSV exportieren** aus. Beachten Sie, dass maximal 45.000 Benutzer in eine CSV-Datei exportiert werden können.

 ©2025 Palo Alto Networks, Inc.




Zum Anzeigen einer Karte mit den Standorten der Prisma Access-Portale und Gateways, die in den von Ihnen ausgewählten Regionen ausgeführt werden, wählen Sie **Überwachen** und anschließend **Mobile Benutzer** aus.

 ©2025 Palo Alto Networks, Inc.




Wählen Sie eine Region aus, um weiterführende Details zu dieser Region abzufragen.

- **Standort** – Der Ort, an dem Ihre Cloud-Dienst-Infrastruktur zum Schutz mobiler Benutzer in Ihrem Netzwerk bereitgestellt wird.

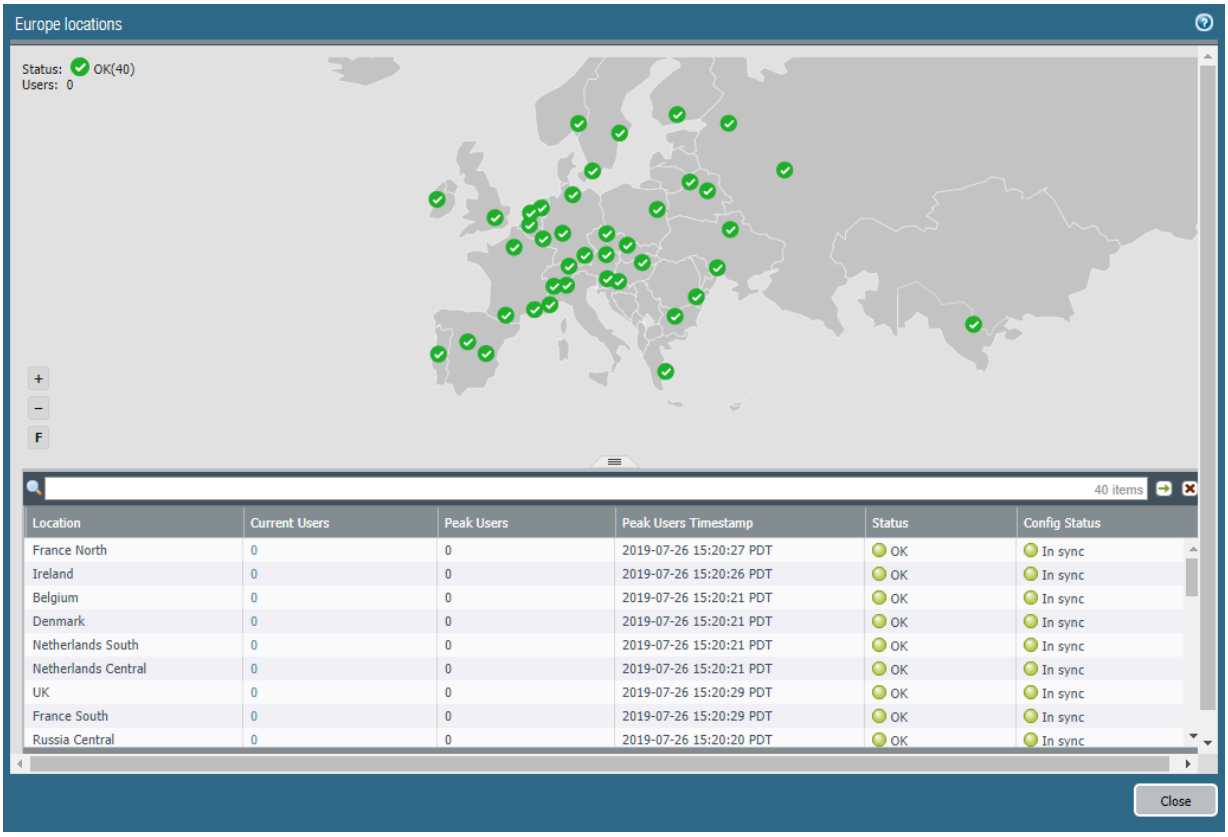
 ©2025 Palo Alto Networks, Inc.

- **Aktuelle Benutzer** – Die Anzahl der Benutzer, die durch den Dienst verbunden und gesichert sind.

  Wenn die aktuelle Anzahl mobiler Benutzer 80 % der gesamten lizenzierten Anzahl erreicht, wird diese Zahl rot angezeigt.
- **Höchstwert Benutzer** – Die maximale Anzahl gleichzeitiger Benutzer.
- **Timestamp Höchstwert Benutzer** – Der Timestamp, bei dem die Daten für „Höchstwert Benutzer“ zuletzt abgerufen wurden.
- **Status** – Der Betriebsstatus der Verbindung zwischen Prisma Access und Ihren mobilen Benutzern.
- **Konfigurationsstatus** – Der Status Ihrer letzten Konfigurationsübertragung an den Dienst. Wenn Sie lokal eine Änderung vorgenommen und die Konfiguration noch nicht in die Cloud übertragen haben, wird möglicherweise der Status **Nicht synchron** angezeigt. Bewegen Sie den Mauszeiger über die Statusanzeige, um detailliertere Informationen zu erhalten. Wenn

 ©2025 Palo Alto Networks, Inc.

Sie die Konfiguration festgeschrieben und per Push an Prisma Access übertragen haben, ändert sich der Konfigurationsstatus in **Synchron**.




**STEP 23 |** Wenn Sie für Ihren Portal-Hostnamen die Option **Unternehmensdomäne verwenden** ausgewählt haben, müssen Sie einen DNS-Eintrag auf Ihren internen DNS-Servern hinzufügen, um den von Ihnen definierten Portal-Hostnamen dem Portal-DNS-CNAME zuzuordnen, der auf der Registerkarte **Cloud Services** > **Konfiguration** > **Mobile Benutzer** > **Onboarding** > **Allgemein** angezeigt wird (z. B. `<portal_hostname>.gpcloudservice.com`).

 ©2025 Palo Alto Networks, Inc.

**STEP 24 |** Stellen Sie die Software der GlobalProtect-App für Ihre Endbenutzer bereit.

Sie können MacOS- oder Windows-Benutzer direkt an die Prisma Access-Portaladresse leiten, wo sie die GlobalProtect-App aus dem Portal herunterladen können.

*Prisma Access verwaltet die Version der GlobalProtect-App auf dem Portal und Sie können die aktive Version aus den Versionen auswählen, die Prisma Access hostet. Zudem können Sie steuern, ob Benutzer sie herunterladen können.*

Alternativ können Sie die Software der GlobalProtect-App auf einem Webserver für Ihre MacOS- und Windows-Benutzer hosten. Prisma Access ist mit allen GlobalProtect-App-Versionen kompatibel, die nicht mit einem End-of-Life-Datum aufgeführt sind.

Benutzer mobiler Apps können die mobile GlobalProtect-App aus dem entsprechenden App-Store für ihre Betriebssysteme herunterladen und installieren.

## GlobalProtect — Tunneleinstellungen anpassen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

Passen Sie die Einstellungen für den VPN-Tunnel an, den die GlobalProtect-App für die Verbindung mit Prisma Access einrichtet. Die Tunneleinstellungen umfassen Split-Tunneling-Optionen, mit denen Sie definieren können, welchen Datenverkehr die App an Prisma Access sendet und was stattdessen lokal geroutet werden kann (z. B. bandbreitenintensive Anwendungen, die für die geschäftliche Nutzung nicht erforderlich sind).

Die von Ihnen definierten **Übereinstimmungskriterien** für Tunneleinstellungen informieren Prisma Access darüber, welche Benutzer, Geräte oder Systeme die Einstellungen erhalten sollen. Sie können beispielsweise angeben, dass eine Tunneleinstellungsregel für alle Instanzen der GlobalProtect-App in einer bestimmten Region gilt. In Prisma Access (Managed by Panorama) können Sie Split-Tunnel-Einstellungen basierend auf Zugriffsroute sowie Domäne und Anwendung konfigurieren.

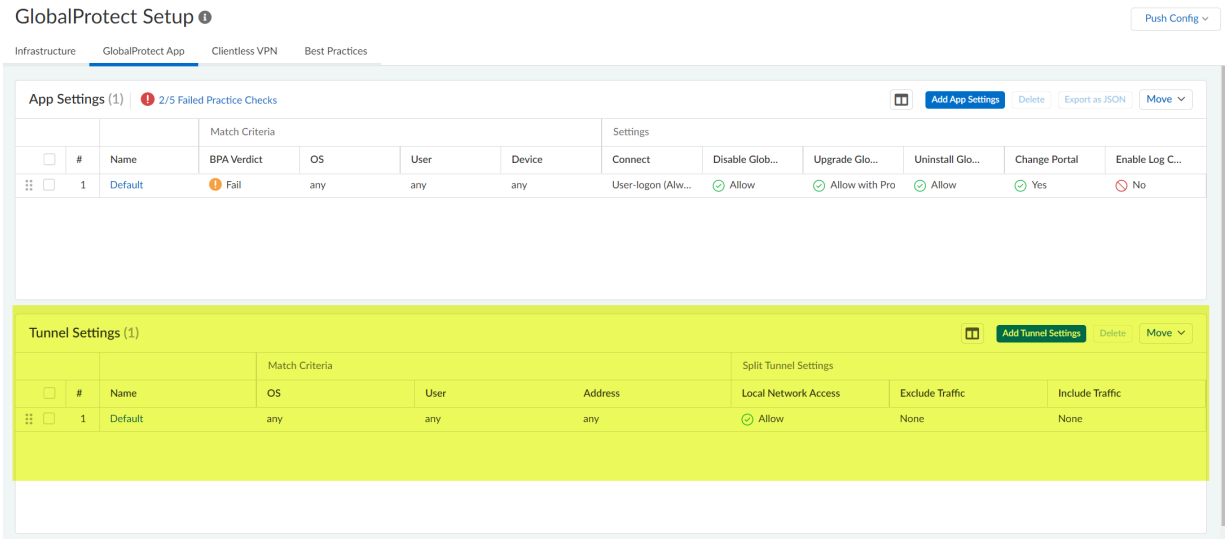
- Strata Cloud Manager
- Panorama

### GlobalProtect — Tunneleinstellungen anpassen (Strata Cloud Manager)

 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** Klicken Sie auf **Verwalten > Diensteinrichtung > Mobile Benutzer > GlobalProtect-Einrichtung > GlobalProtect-App > Tunneleinstellungen hinzufügen**.

*Wenn Sie Strata Cloud Manager verwenden, klicken Sie auf **Workflow > Einrichtung Prisma Access > Mobile Benutzer> GlobalProtect-Einrichtung > GlobalProtect-App > Tunneleinstellungen hinzufügen**.*




**STEP 2 |** Geben Sie einen Namen und die **Übereinstimmungskriterien** ein, um die Benutzer, Geräte oder Systeme anzugeben, die die Einstellungen erhalten sollen. Sie können beispielsweise angeben, dass eine Tunneleinstellungsregel für alle Instanzen der GlobalProtect-App in einer bestimmten Region gilt.

**STEP 3 |** Aktivieren Sie **Authentifizierungsüberschreibung** für Prisma Access, um sichere, verschlüsselte Cookies für die Benutzerauthentifizierung zu generieren und zu akzeptieren. Mit dieser Einstellung muss der Benutzer nur einmal während des angegebenen Zeitraums Anmeldeinformationen angeben.

- **Cookie zur Authentifizierungsüberschreibung generieren** – Ermöglicht Prisma Access, verschlüsselte, endpunktspezifische Cookies zu generieren und Authentifizierungscookies an den Endpunkt auszugeben.
- **Cookie für Authentifizierungsüberschreibung akzeptieren** – Ermöglicht Prisma Access, Benutzer mit einem gültigen, verschlüsselten Cookie zu authentifizieren. Wenn die App ein gültiges Cookie präsentiert, überprüft Prisma Access, dass das Cookie ursprünglich

 ©2025 Palo Alto Networks, Inc.

von Prisma Access verschlüsselt wurde, entschlüsselt das Cookie und authentifiziert den Benutzer.

*Die GlobalProtect-App muss den Benutzernamen des Benutzers, der die Verbindung herstellt, kennen, um die zugehörigen Authentifizierungscookies vom Endpunkt des Benutzers abzugleichen und abzurufen. Nachdem die App die Cookies abgerufen hat, sendet sie diese zur Benutzerauthentifizierung an Prisma Access.*

**STEP 4 |** Aktivieren Sie **Split-Tunneling**, um festzulegen, welchen Datenverkehr die GlobalProtect-App über den VPN-Tunnel zu Prisma Access zulässt oder einschränkt. Split-Tunneling spart Bandbreite, indem Datenverkehr von Prisma Access ausgeschlossen wird, wenn er nicht geschäftskritisch ist oder keine Produktivität ermöglicht.

- **Zugriff auf das lokale Netzwerk** – Gewähren Sie Windows- und Mac-Benutzern Zugriff auf lokale Ressourcen, ohne dass diese vorher eine Verbindung mit Prisma Access herstellen müssen.

  **Datenverkehr ausschließen** – Geben Sie Datenverkehr an, der je nach Anwendung, Domäne und Route (z. B. einer IP-Adresse) von Prisma Access ausgeschlossen werden soll.

  **Datenverkehrseinschluss anpassen** – Standardmäßig leitet die GlobalProtect-App den gesamten Datenverkehr an Prisma Access weiter. Dies gilt nicht für Datenverkehr, der in der Ausschlussliste aufgeführt ist. Geben Sie Datenverkehr an, den die GlobalProtect-App immer an Prisma Access weiterleiten soll, auch wenn er Kriterien der Ausschlussliste erfüllt.

**STEP 5 |** **Videostreaming-Datenverkehr ausschließen**, um Videostreaming-Datenverkehr aus den aufgeführten Anwendungen nicht an Prisma Access zu senden. Indem Sie Videostreaming-Datenverkehr mit geringerem Risiko (z. B. YouTube und Netflix) aus dem VPN-Tunnel ausschließen, können Sie den Bandbreitenverbrauch senken. Die Videostreaming-Ausschlüsse werden auf den gesamten Datenverkehr angewendet, den die GlobalProtect-App an Prisma Access sendet, nicht nur auf die Übereinstimmungskriterien, die Sie für diese Regel definiert haben.

**STEP 6 |** Speichern Sie die Einstellungen. Wiederholen Sie die obigen Schritte, um weitere Tunneleinstellungen hinzuzufügen.

**STEP 7 |** (Optional) **Ändern** Sie die Reihenfolge der Prioritäten, in der die VPN-Tunneleinstellung beim Herstellen einer Verbindung mit Prisma Access verwendet wird.

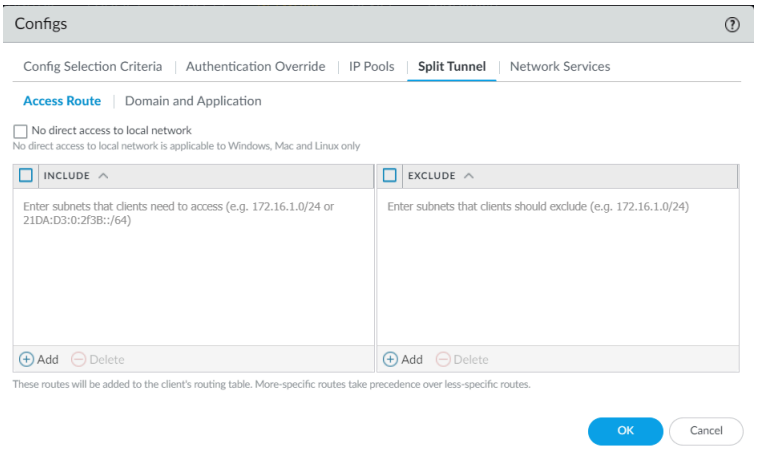
## GlobalProtect — Tunneleinstellungen anpassen (Panorama)

Sie können Split-Tunnel-Einstellungen basierend auf Zugriffsroute oder Domäne und Anwendung konfigurieren.

- Konfigurieren Sie Split-Tunnel-Einstellungen basierend auf der Zugriffsroute.
  1. Klicken Sie auf **Panorama > Netzwerk > GlobalProtect > Gateways** und wählen Sie das anzupassende Gateway aus.
  2. Klicken Sie auf **Agent > Clienteinstellungen** und wählen Sie die Konfiguration aus.
  3. Klicken Sie auf **Split-Tunnel > Zugriffsroute**. Die Split-Tunnel-Einstellungen werden dem virtuellen Netzwerkadapter auf dem Endpunkt zugewiesen, wenn die GlobalProtect-App

 ©2025 Palo Alto Networks, Inc.

einen Tunnel mit Prisma Access einrichtet. Sie können einen bestimmten IP-Subnetz-Datenverkehr über den VPN-Tunnel ein- oder ausschließen.




4. Aktivieren Sie die Option **Kein direkter Zugriff auf lokale Netzwerke**, um Benutzer daran zu hindern, Datenverkehr direkt an Proxys oder lokale Ressourcen zu senden, während sie mit GlobalProtect verbunden sind.

   *Aktivieren Sie die Einstellung **Kein direkter Zugriff auf das lokale Netzwerk**, um Risiken in nicht vertrauenswürdigen Netzwerken wie z. B. WLAN-Zugangspunkten mit bösartigem Verhalten zu reduzieren.*

5. Wählen Sie **Einschließen** und **Hinzufügen** aus, um die Zielsubnetze oder das Adressobjekt (vom Typ IP-Netzmaske) hinzuzufügen, um nur bestimmten Datenverkehr für Ihr LAN an GlobalProtect weiterzuleiten. Sie können IPv6- oder IPv4-Subnetze einschließen. Um alle Zielsubnetze oder Adressobjekte einzubinden, müssen Sie 0.0.0.0/0 und ::/0 als Zugriffsrouten **einschließen**.
6. Wählen Sie **Ausschließen Hinzufügen** aus, um die Zielsubnetze oder das Adressobjekt (des Typs „IP-Netzmaske“) hinzuzufügen, die bzw. das die App ausschließen soll. Ausgeschlossene Routen müssen spezifischer sein als die eingeschlossenen Routen. Andernfalls könnten Sie mehr Datenverkehr als beabsichtigt ausschließen. Sie können IPv6- oder IPv4-Subnetze ausschließen.

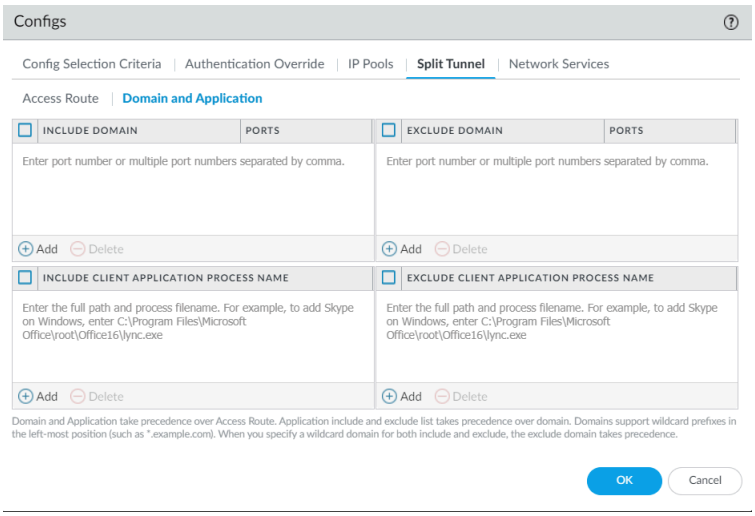
   *Zugriffsrouten für Endpunkte mit Android auf Chromebooks können nicht ausgeschlossen werden. Auf Chromebooks werden nur IPv4-Routen unterstützt.*

7. Speichern Sie die Tunneleinstellungen.

 ©2025 Palo Alto Networks, Inc.

- Konfigurieren Sie Split-Tunnel-Einstellungen basierend auf Domäne und Anwendung.
  1. Klicken Sie auf **Panorama > Netzwerk > GlobalProtect > Gateways** und wählen Sie das anzupassende Gateway aus.
  2. Klicken Sie auf **Agent > Clienteinstellungen** und wählen Sie die Konfiguration aus.
  3. Klicken Sie auf die Registerkarte **Split-Tunnel > Domäne und Anwendung**, um die Split-Tunnel-Einstellungen auf der Grundlage der Zieldomäne zu konfigurieren.

     *Bei Verwendung des Endpunktsicherheitsprodukts eines Drittanbieters wie Sophos auf macOS-Endpunkten können einige Inkompatibilitätsprobleme auftreten.*




     - (Optional) Wählen Sie **Domäne einschließen** und **Hinzufügen** aus, um die SaaS-Anwendungen oder Anwendungen in öffentlichen Clouds hinzuzufügen, die Sie über die VPN-Verbindung mit der Zieldomäne und dem Zielport an GlobalProtect weiterleiten möchten. Sie können der Liste bis zu 200 Einträge hinzufügen. Fügen Sie beispielsweise *.gmail.com hinzu, damit der gesamte Gmail-Datenverkehr durch den VPN-Tunnel geleitet werden kann.
     - (Optional) Wählen Sie **Domäne ausschließen** und **Hinzufügen** aus, um die SaaS-Anwendungen oder Anwendungen in öffentlichen Clouds hinzuzufügen, die Sie mithilfe der Zieldomäne und des Ports vom VPN-Tunnel ausschließen möchten. Sie können der Liste bis zu 200 Einträge hinzufügen. Fügen Sie beispielsweise *.target.com hinzu, um den gesamten Zieldatenverkehr aus dem VPN-Tunnel auszuschließen.
  4. Konfigurieren Sie Split-Tunnel-Einstellungen basierend auf der Anwendung.

     *Auf macOS-Endpunkten kann Safari-Datenverkehr nicht zur anwendungsbasierten Split-Tunnel-Regel hinzugefügt werden.*

     *Sie können mithilfe von Umgebungsvariablen einen Split-Tunnel basierend auf der Anwendung auf Windows- und macOS-Endpunkten konfigurieren.*

     - (Optional) Wählen Sie **Clientanwendungsprozessname einschließen** und **Hinzufügen** aus, um die SaaS-Anwendungen oder Anwendungen in öffentlichen Clouds hinzuzufügen, die

 ©2025 Palo Alto Networks, Inc.

Sie über die VPN-Verbindung mithilfe des Anwendungsprozessnamens an GlobalProtect weiterleiten möchten. Sie können der Liste bis zu 200 Einträge hinzufügen.

- (Optional) Wählen Sie **Clientanwendungsprozessname ausschließen** und **Hinzufügen** aus, um die SaaS-Anwendungen oder Anwendungen in öffentlichen Clouds hinzuzufügen, die Sie mithilfe des Anwendungsprozessnamens aus dem VPN-Tunnel ausschließen möchten. Sie können der Liste bis zu 200 Einträge hinzufügen.

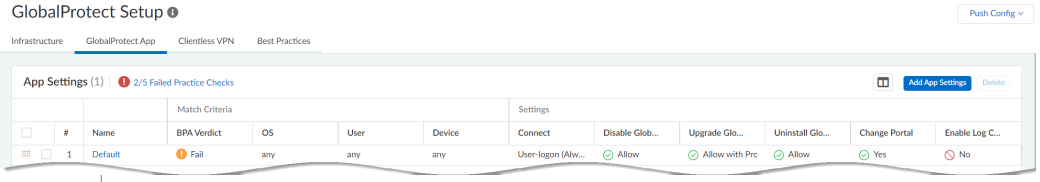
5. Speichern Sie die Tunneleinstellungen.

# GlobalProtect – Anpassen der App-Einstellungen

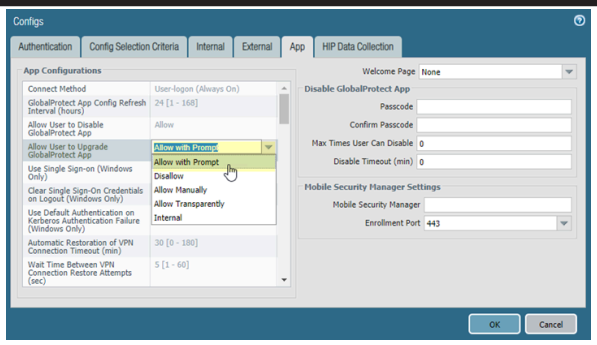
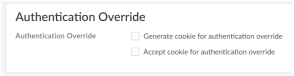
| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ☐ Prisma Access-Lizenz |

Passen Sie an, wie Ihre Endbenutzer mit der GlobalProtect-App interagieren.

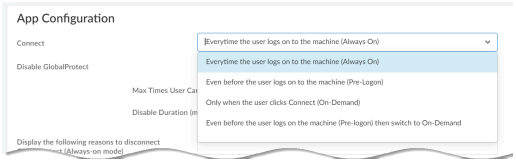
Es gibt einige Einstellungen, die Sie global anpassen können. Diese **globalen App-Einstellungen** gelten für die GlobalProtect-App auf allen Geräten. Andere Einstellungen der GlobalProtect-App werden standardmäßig festgelegt. Sie können diese Optionen anschließend anpassen und sie basierend auf **Übereinstimmungskriterien** auf bestimmte Benutzer und Geräte ausrichten. Die Übereinstimmungskriterien, die Sie für App-Einstellungen definieren, geben Prisma Access Informationen dazu, welche Benutzer, Geräte oder Systeme die Einstellungen erhalten sollen. Sie können beispielsweise angeben, dass eine Regel nur für Geräte gilt, deren Seriennummern mit Active Directory-Einträgen übereinstimmen.

| GlobalProtect-App-Einstellungen | |
|---|---|
| **Hier können Sie die App-Einstellungen prüfen und anpassen (Beispiele für Management finden Sie weiter unten) —>** | Prisma Access (Managed by Strata Cloud Manager)<br><br>Panorama Managed Prisma Access |

 ©2025 Palo Alto Networks, Inc.

| GlobalProtect-App-Einstellungen | |
|---|---|
| |  |
| **Authentifizierungsüberschreibung** | Ermöglichen Sie Prisma Access, sichere, verschlüsselte Cookies für die Benutzerauthentifizierung zu generieren und zu akzeptieren. Wenn Sie diese Option aktivieren, muss der Benutzer nur einmal während des angegebenen Zeitraums Anmeldeinformationen angeben.<br><br>• **Cookie für Authentifizierungsüberschreibung generieren** – Ermöglicht Prisma Access, verschlüsselte endpunktspezifische Cookies zu generieren und Authentifizierungscookies an den Endpunkt auszugeben.<br>• **Cookie für Authentifizierungsüberschreibung akzeptieren** – Ermöglicht Prisma Access, Benutzer mit einem gültigen, verschlüsselten Cookie zu authentifizieren. Wenn die App ein gültiges Cookie vorlegt, überprüft Prisma Access, ob das Cookie ursprünglich von Prisma Access verschlüsselt wurde, entschlüsselt das Cookie und authentifiziert dann den Benutzer.<br>*Die GlobalProtect-App muss den Benutzernamen des Benutzers, der die Verbindung herstellt, kennen, um die zugehörigen Authentifizierungscookies vom Endpunkt des Benutzers abzugleichen und abzurufen. Nachdem die App die Cookies abgerufen hat, sendet sie diese zur Benutzerauthentifizierung an Prisma Access.*<br>• **Cookie-Lebensdauer** – Gibt die Stunden, Tage oder Wochen an, für die das Cookie gültig ist (Standard sind 24 Stunden). Der Bereich für Stunden liegt zwischen 1 und 72, der für Wochen zwischen 1 und 52 und der für Tage zwischen 1 und 365. Nach Ablauf des Cookies muss der Benutzer seine Anmeldeinformationen erneut eingeben. Anschließend verschlüsselt Prisma Access ein neues Cookie, das an die App gesendet wird. Dieser Wert |

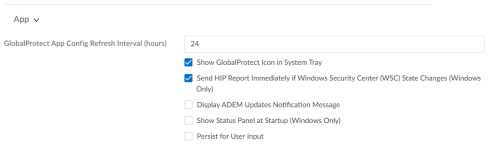
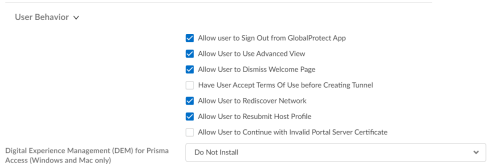
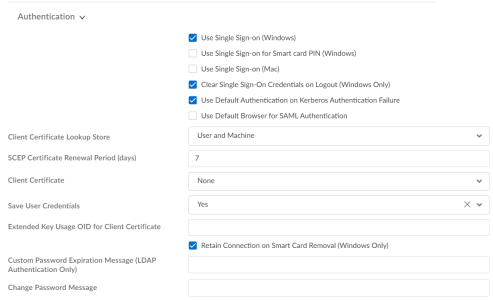
 ©2025 Palo Alto Networks, Inc.

| GlobalProtect-App-Einstellungen | |
|---|---|
| | kann mit der von Ihnen konfigurierten Cookie-Lebensdauer identisch sein oder sich davon unterscheiden.<br>• **Zertifikat zum Ver-/Entschlüsseln von Cookies** – Wählt das RSA-Zertifikat zum Verschlüsseln und Entschlüsseln von Cookies aus. |
| **Verbindungseinstellungen** | Geben Sie die Methode an, mit der die GlobalProtect-App eine **Verbindung** mit Prisma Access herstellt.<br><br>• **Benutzeranmeldung (immer aktiviert)** – Die GlobalProtect-App verbindet sich automatisch mit Prisma Access, sobald sich der Benutzer anmeldet. Bei Verwendung in Verbindung mit SSO (nur Windows-Endpunkte) ist die Anmeldung für den Endbenutzer transparent.<br>*Auf iOS-Endpunkten verhindert diese Einstellung, dass Anwendungen mit Einmalpasswort funktionieren, da die GlobalProtect-App durchsetzt, dass der gesamte Datenverkehr den Tunnel durchläuft.*<br>• **Voranmeldung (immer aktiviert)** – Die GlobalProtect-App authentifiziert den Benutzer und richtet einen VPN-Tunnel zu Prisma Access ein, bevor sich der Benutzer anmeldet. Für diese Option müssen Sie eine externe PKI-Lösung verwenden, um ein Maschinenzertifikat auf jedem Gerät, das diese Einstellungen empfängt, vorab bereitzustellen.<br>• **Bei Bedarf (vom Benutzer manuell initiierte Verbindung)** – Benutzer müssen die App manuell starten, um eine Verbindung mit GlobalProtect herzustellen.<br>• **Voranmeldung und dann bei Bedarf** – Ähnlich wie die Methode „Voranmeldung (immer aktiviert)“ (für die Content Release Version 590-3397 oder höher erforderlich ist) ermöglicht die GlobalProtect-App die Authentifizierung des Benutzers und die Einrichtung eines VPN-Tunnels für Prisma Access, bevor sich der Benutzer am Endpunkt anmeldet. Im Gegensatz zur Verbindungsmethode mit Voranmeldung müssen Benutzer nach der Anmeldung die App manuell starten, um eine Verbindung mit GlobalProtect herzustellen, wenn die Verbindung aus irgendeinem Grund beendet wird. Der Vorteil dieser Option ist, dass Sie Benutzern erlauben können, ein neues Passwort anzugeben, nachdem ihr |

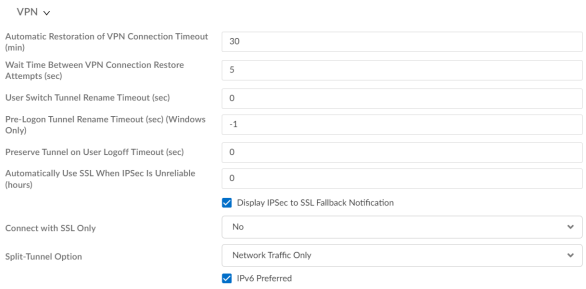
 ©2025 Palo Alto Networks, Inc.

| GlobalProtect-App-Einstellungen | |
|---|---|
| | Passwort abgelaufen ist oder sie ihr Passwort vergessen haben. Allerdings müssen sie dennoch die Verbindung manuell herstellen, nachdem sie sich angemeldet haben. |
| **GlobalProtect** | Entscheiden Sie, welche Einstellungen der GlobalProtect-App der Benutzer anpassen kann:<br>• **GlobalProtect deaktivieren** – Entscheiden Sie, ob Benutzer die GlobalProtect-App deaktivieren können. Benutzer, die die GlobalProtect-App deaktivieren, können sich erst dann wieder mit Prisma Access (und Ihren geschützten Unternehmensressourcen) verbinden, wenn sie die App wieder aktivieren.<br>• **GlobalProtect aktualisieren** – Legen Sie fest, wie App-Upgrades funktionieren sollen, z. B. ob Benutzer Aktualisierungen initiieren können.<br>Wenn Sie steuern möchten, wann Benutzer ein Upgrade durchführen können, haben Sie die Möglichkeit, das App-Upgrade auf Konfigurationsbasis anzupassen. Wenn Sie beispielsweise ein Release für eine kleine Gruppe von Benutzern testen möchten, bevor Sie es für Ihre gesamte Benutzerbasis bereitstellen, können Sie eine Konfiguration erstellen, die nur für Benutzer in Ihrer IT-Gruppe gilt, sodass diese Upgrades durchführen und testen können, während Upgrades in allen anderen Benutzer-/Gruppenkonfigurationen deaktiviert werden. Nachdem Sie die neue Version ausführlich getestet haben, können Sie die Agent-Konfigurationen für alle übrigen Benutzer ändern, um das Upgrade zu ermöglichen.<br>◦ **Mit Eingabeaufforderung zulassen** – Benutzer auffordern, ein Upgrade durchzuführen, wenn eine neue Version der App verfügbar ist.<br>◦ **Transparent zulassen** – Upgrades werden automatisch ohne Benutzerinteraktion durchgeführt.<br>◦ **Intern** – Upgrades werden automatisch ohne Benutzerinteraktion durchgeführt, wenn der Benutzer mit Prisma Access verbunden ist.<br>◦ **Nicht zulassen** – App-Upgrades werden verhindert.<br>◦ **Manuell zulassen** – Benutzer können App-Upgrades aus der GlobalProtect-App heraus starten.<br>• **GlobalProtect deinstallieren** – Mit dieser Einstellung können Sie zulassen oder verhindern, dass Benutzer die GlobalProtect-App deinstallieren, oder Sie können zulassen, dass sie die App deinstallieren, wenn sie ein von Ihnen erstelltes Passwort angeben. |

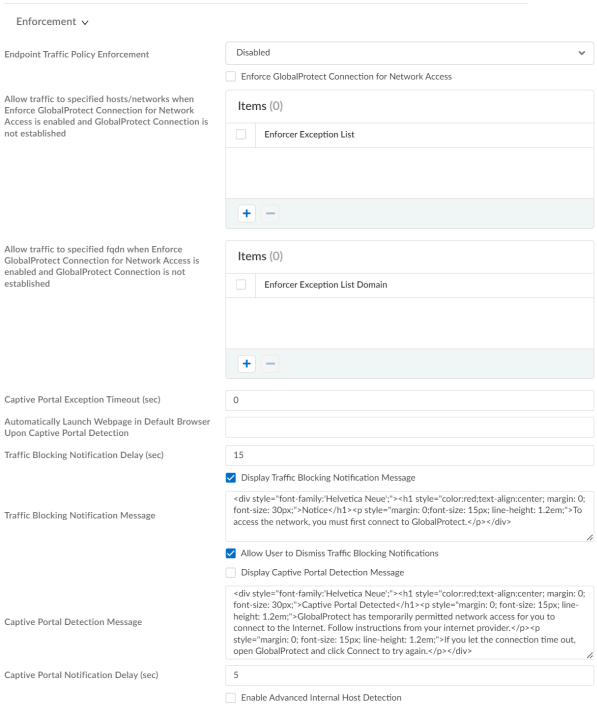
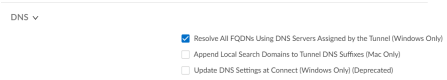
 ©2025 Palo Alto Networks, Inc.

| GlobalProtect-App-Einstellungen | |
|---|---|
| | • **Benutzer kann Portal ändern** – Lassen Sie zu, dass Benutzer das Portal ändern, über das die GlobalProtect-App eine Verbindung mit Prisma Access herstellt. |
| **App-Konfiguration – Erweiterte Optionen** | |
| **App-Einstellungen** | • HIP-Bericht sofort senden, wenn sich der Windows Security Center(WSC)-Status ändert (nur Windows) – Wählen Sie „Nein“ aus, um zu verhindern, dass die GlobalProtect-App HIP-Daten sendet, wenn sich der Status des Windows Security Center (WSC) ändert. Wählen Sie Ja (Standardeinstellung) aus, um HIP-Daten sofort zu senden, wenn sich der Status des WSC ändert.<br> |
| **Benutzerverhaltenseinstellungen** | Benutzerverhaltenseinstellungen umfassen:<br> |
| **Authentifizierungseinstellungen** | Authentifizierungseinstellungen umfassen:<br> |
| **VPN-Einstellungen** | Konfigurieren Sie VPN-Timeout und Tunneleinstellungen:<br>• **Benachrichtigung bei Fallback von IPSec auf SSL anzeigen** – Wählen Sie **Nein** aus, um Pop-up-Benachrichtigungen zu verhindern, wenn die GlobalProtect-App keine Verbindung zu einem IPSec-Tunnel herstellen kann und auf einen SSL-Tunnel zurückfällt. Wählen Sie **Ja** (Standardeinstellung) aus, um Pop-up-Benachrichtigungen zuzulassen, wenn sich die Verbindung ändert. |

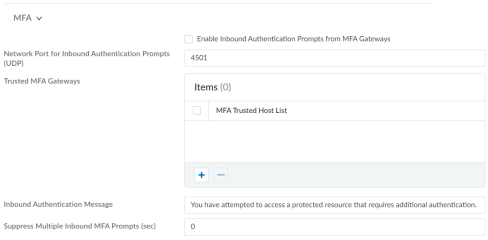
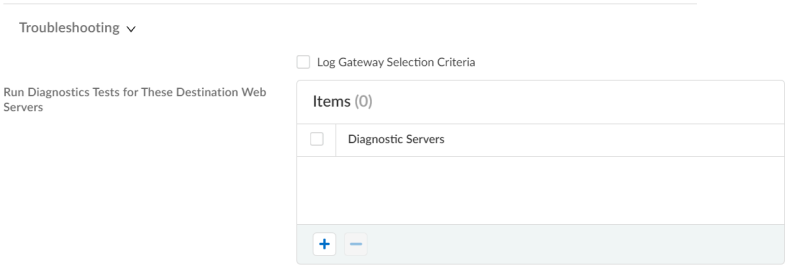
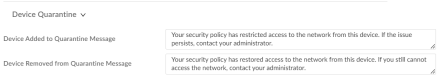
 ©2025 Palo Alto Networks, Inc.

| GlobalProtect-App-Einstellungen | |
|---|---|
| |  |
| **Durchsetzungseinstellungen** | Einstellungen für angegebenen Datenverkehr werden durchgesetzt:<br>• **Datenverkehr zu angegebenem FQDN zulassen, wenn „GlobalProtect-Verbindung für Netzwerkzugriff erzwingen“ aktiviert ist und die GlobalProtect-Verbindung nicht hergestellt ist**– Mehr erfahren.<br>• **Bei Authentifizierungs-(Captive-)Portal-Erkennung Webseite automatisch in Standardbrowser starten** – Um Ihre Standard-Webbrowser automatisch zu starten, damit Benutzer sich nahtlos am Authentifizierungsportal anmelden können, geben Sie den vollständig qualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) oder die IP-Adresse der Website ein, die Sie für den ersten Verbindungsversuch verwenden möchten, der beim Start des Standard-Webbrowsers Webdatenverkehr initiiert (maximal 256 Zeichen). Das Authentifizierungsportal fängt dann diesen Verbindungsversuch für die Website ab und leitet den Standard-Webbrowser auf die Anmeldeseite des Authentifizierungsportals um. Wenn dieses Feld leer ist (Standardeinstellung), startet Prisma Access beim Erkennen des Authentifizierungsportals den Standard-Webbrowser nicht automatisch.<br>• **Erweiterte interne Hosterkennung aktivieren** – Ermöglicht die erweiterte interne Hosterkennung, um eine zusätzliche Sicherheitsschicht während der internen Hosterkennung durch die GlobalProtect-App hinzuzufügen. Bei der erweiterten internen Hosterkennung validiert die App das Serverzertifikat der internen Gateways zusätzlich zum Durchführen eines Reverse-DNS-Lookups des internen Hosts, um festzustellen, ob sich die App innerhalb des Unternehmensnetzwerks befindet. Die Aktivierung der erweiterten internen Hosterkennung verhindert, dass bösartige Akteure während der internen Hosterkennung die Reverse-DNS-Serverantwort fälschen, und verhindert so den nicht autorisierten Zugriff auf die Endpunkte im Unternehmensnetzwerk. Wenn Sie die erweiterte |

 ©2025 Palo Alto Networks, Inc.

| GlobalProtect-App-Einstellungen | |
|---|---|
| | interne Hosterkennung nicht aktivieren, funktioniert die vorhandene interne Hosterkennung wie erwartet.<br> |
| **Einstellungen für das Verbindungsverhalten** | Einstellungen für das Verbindungsverhalten umfassen:<br><br>Weitere Informationen. |
| **DNS-Einstellungen** | DNS-Einstellungen umfassen:<br> |
| **Proxy-Einstellungen** | Geben Sie die **URL der Proxy Auto-Configuration(PAC)-Datei** an, die Sie zum Konfigurieren von Proxy-Einstellungen an den Endpunkt per Push übertragen möchten. Die maximale Länge der URL beträgt 256 Zeichen. Für „URL der Proxy Auto-Configuration(PAC)-Datei“ werden folgende Methoden unterstützt:<br>• Proxy Auto-Config (PAC) Standard (z. B. http://pac.<hostname or IP>/proxy.pac).<br>• Web Proxy Auto-Discovery(WPAD)-Protokoll Standard (z. B. http://wpad.<hostname or IP>/wpad.dat). |

 ©2025 Palo Alto Networks, Inc.

| GlobalProtect-App-Einstellungen | |
|---|---|
| |  |
| **MFA-Einstellungen** | MFA-Einstellungen umfassen:<br> |
| **Fehlerbehebungseinstellungen** | Fehlerbehebungseinstellungen umfassen:<br> |
| **Einstellungen für die Gerätequarantäne** | Einstellungen für die Gerätequarantäne umfassen:<br> |
| **Interne Hosterkennung** | Wenn Ihre mobilen Benutzer keine Verbindung mit Prisma Access herstellen müssen, wenn sie sich im internen Netzwerk befinden, aktivieren Sie die interne Hosterkennung, damit die GlobalProtect-App feststellen kann, ob sie sich in einem internen oder externen Netzwerk befindet.<br>• Geben Sie die IP-Adresse (IPv4 oder IPv6) eines Hosts ein, der nur vom internen Netzwerk aufgelöst werden kann.<br>• Geben Sie den DNS-Hostnamen ein, der in die von Ihnen eingegebene IP-Adresse aufgelöst wird.<br>Wenn ein mobiler Benutzer eine Verbindung mit Prisma Access herstellt, versucht die GlobalProtect-App, ein Reverse-DNS-Lookup für die angegebene Adresse durchzuführen. Wenn die Suche fehlschlägt, stellt die GlobalProtect-App |

 ©2025 Palo Alto Networks, Inc.

| GlobalProtect-App-Einstellungen | |
|---|---|
| | fest, dass sie sich im externen Netzwerk befindet, und initiiert dann eine Verbindung zu Prisma Access. |
| **Interne Hosterkennung aktivieren** | Wenn Sie möchten, dass die GlobalProtect-App die Netzwerkerkennung wiederholt, wenn ein internes Gateway und eine interne Hosterkennung ohne externes Gateway konfiguriert sind und die interne Hosterkennung fehlschlägt, legen Sie den Parameter **Intelligente interne Hosterkennung aktivieren** auf „Ja“ fest. |
| **Gateways** | Standardmäßig sind alle Gateways in Ihren Prisma Access-Standorten für Benutzer verfügbar. Wenn zusätzliche GlobalProtect-Gateways (intern oder extern) vorhanden sind, mit denen sich Ihre Benutzer verbinden können sollen, haben Sie hier die Möglichkeit, diese Gateways hinzuzufügen. |
| **HIP-Datenerfassung** | Definieren Sie benutzerdefinierte Host Information Profile(HIP)-Daten, die die App erfassen oder von der Erfassung ausschließen soll. Wenn diese Option aktiviert ist, erfasst die App Daten von Geräten mit Windows-, Mac- oder Linux-Betriebssystemen.<br><br>Mithilfe einer benutzerdefinierten Prüfung können Sie beispielsweise feststellen, ob eine bestimmte Anwendung auf einem Endpunkt installiert ist oder ausgeführt wird. Die Daten, die laut Ihrer Definition in einer benutzerdefinierten Überprüfung gesammelt werden sollen, werden in die Raw-Host-Informationen aufgenommen, die die GlobalProtect-App sammelt und dann an Prisma Access übermittelt, wenn die App eine Verbindung herstellt.<br><br>Erstellen Sie zum Überwachen der erfassten Daten mit benutzerdefinierten Prüfungen ein HIP-Objekt. Anschließend können Sie das HIP-Objekt einem HIP-Profil hinzufügen, um die gesammelten Daten zum Abgleich mit dem Endpunktverkehr und zur Durchsetzung von Sicherheitsregeln zu verwenden.<br><br>Gehen Sie zu **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Objekte** > **HIP** und **HIP-Objekte** oder **HIP-Profile**. Wählen Sie den Konfigurationsumfang **Prisma Access** > **Container für mobile Benutzer** > **GlobalProtect** aus. |
| **Timeout-Einstellungen** | • Wählen Sie auf der Seite „GlobalProtect-Einrichtung“ das Zahnradsymbol im Bereich „Globale App-Einstellungen“ aus.<br>• Ändern Sie die maximale **Anmeldungslebensdauer** für eine einzelne Gateway-Anmeldungssitzung (Standardeinstellung ist 30 Tage). Während der Lebensdauer bleibt der |

 ©2025 Palo Alto Networks, Inc.

| GlobalProtect-App-Einstellungen | |
|---|---|
| | Benutzer angemeldet, solange das Gateway innerhalb des Zeitraums für die **Inaktivitätsabmeldung** eine HIP-Überprüfung vom Endpunkt empfängt. Nach Ablauf dieser Zeit endet die Anmeldesitzung automatisch.<br>• Legen Sie fest, mit welcher Vorlaufzeit Benutzer darüber informiert werden, dass ihre App-Sitzungen aufgrund des Ablaufs der Anmeldungslebensdauer ablaufen. Der Standardwert ist 30 Minuten. Der zulässige Bereich liegt zwischen 0 und 60 Minuten.<br>• Passen Sie die Timeout-Benachrichtigungsmeldung an.<br>• Ändern Sie den Zeitraum für die **Inaktivitätsabmeldung**, um festzulegen, nach welcher Zeit inaktive Benutzer von GlobalProtect abgemeldet werden. Sie können eine Sicherheitsrichtlinie erzwingen, um den Datenverkehr von Endpunkten zu überwachen, während Sie mit GlobalProtect verbunden sind, und um inaktive GlobalProtect-Sitzungen schnell abzumelden, indem Sie einen kürzeren Zeitraum für die Inaktivitätsabmeldung festlegen. Benutzer werden von GlobalProtect abgemeldet, wenn die GlobalProtect-App den Datenverkehr nicht durch den VPN-Tunnel geleitet hat oder wenn das Gateway innerhalb des konfigurierten Zeitraums keine HIP-Überprüfung vom Endpunkt empfängt.<br>Der Standardwert ist 180 Minuten. Der zulässige Bereich liegt zwischen 5 und 43.200 Minuten.<br>• Legen Sie fest, mit welcher Vorlaufzeit Benutzer darüber informiert werden, dass ihre App-Sitzungen aufgrund von Inaktivität ablaufen. Der Standardwert ist 30 Minuten. Der zulässige Bereich liegt zwischen 0 und 60 Minuten.<br>• Passen Sie die Inaktivitätsbenachrichtigungsmeldung an.<br>• Geben Sie an, ob Endbenutzer benachrichtigt werden sollen, wenn sie von ihrem Administrator abgemeldet werden, und legen Sie die anzuzeigende Meldung fest.<br>• Klicken Sie auf **Speichern**. |
| **Durchsetzung der Quell-IP-Adresse für Authentifizierungscookies** | Konfigurieren Sie die Nutzungseinschränkungen für VPN-Verbindungseinstellungs- und -Authentifizierungscookies, um den Sicherheitsstatus zu verbessern.<br>• Wählen Sie auf der Seite „GlobalProtect-Einrichtung“ das Zahnradsymbol im Bereich „Globale App-Einstellungen“ aus. |

 ©2025 Palo Alto Networks, Inc.

| GlobalProtect-App-Einstellungen | |
|---|---|
| | • Konfigurieren Sie die automatische Wiederherstellung von SSL-VPN-Tunneln.<br><br>Wenn die automatische Wiederherstellung von VPN-Verbindungen im GlobalProtect-Portal aktiviert ist, können Sie sie für dieses Gateway deaktivieren, indem Sie **Automatische Wiederherstellung von SSL-VPN deaktivieren** auswählen.<br>• Konfigurieren Sie die Durchsetzung von Quell-IP-Adressen für Authentifizierungscookies.<br><br>Sie können das GlobalProtect-Portal oder -Gateway so konfigurieren, dass Cookies von Endpunkten nur akzeptiert werden, wenn die IP-Adresse des Endpunkts mit den ursprünglichen Quell-IP-Adressen übereinstimmt, für die das Cookie ausgestellt wurde, oder wenn die IP-Adresse des Endpunkts mit einem bestimmten Netzwerk-IP-Adressbereich übereinstimmt. Sie können den IP-Adressbereich des Netzwerks mit einer CIDR-Subnetzmaske definieren, z. B. /24 oder /32. Wenn beispielsweise ein Authentifizierungscookie ursprünglich an einen Endpunkt mit einer öffentlichen Quell-IP-Adresse von 201.109.11.10 ausgegeben und die Subnetzmaske des Netzwerk-IP-Adressbereichs auf /24 festgelegt wurde, ist das Authentifizierungscookie anschließend für Endpunkte mit öffentlichen Quell-IP-Adressen innerhalb des Netzwerk-IP-Adressbereichs 201.109.11.0/24 gültig.<br><br>Wählen Sie im Abschnitt „Nutzungseinschränkungen für Authentifizierungscookies“ die Option **Verwendung von Authentifizierungscookies (für die automatische Wiederherstellung des VPN-Tunnels oder die Authentifizierungsüberschreibung) beschränken** aus, und konfigurieren Sie dann eine der folgenden Bedingungen:<br><br>• Wenn Sie **Die ursprüngliche Quell-IP, für die das Authentifizierungscookie ausgegeben wurde** auswählen, ist das Authentifizierungscookie nur gültig, wenn die öffentliche Quell-IP-Adresse des Endpunkts, der das Cookie verwenden möchte, dieselbe öffentliche Quell-IP-Adresse des Endpunkts ist, auf die das Cookie ursprünglich ausgestellt wurde.<br>• Wenn Sie **Der ursprüngliche Quell-IP-Netzwerkbereich** auswählen, ist das Authentifizierungscookie nur gültig, wenn die öffentliche Quell-IP-Adresse des Endpunkts, der das Cookie verwenden möchte, innerhalb des vorgesehenen Netzwerk-IP-Adressbereichs liegt. Geben Sie eine Quell-IPv4-Netzmaske oder Quell-IPv6-Netzmaske ein, um die Subnetzmaske des |

 ©2025 Palo Alto Networks, Inc.

| GlobalProtect-App-Einstellungen | |
|---|---|
| | Netzwerk-IP-Adressbereichs zu definieren, für den das Authentifizierungscookie gültig ist (z. B. 32 oder 128). |

# Ticketanforderung zur Deaktivierung von GlobalProtect

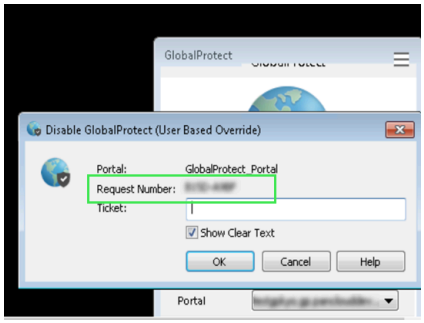
| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Anstatt Benutzern zu ermöglichen, GlobalProtect direkt zu deaktivieren, können Sie einem Benutzer erlauben, ein Ticket zu erstellen, um GlobalProtect zu deaktivieren. Der GlobalProtect-Administrator kann dann entscheiden, ob er jedem jeweiligen Benutzer die Deaktivierung von GlobalProtect erlaubt oder nicht.

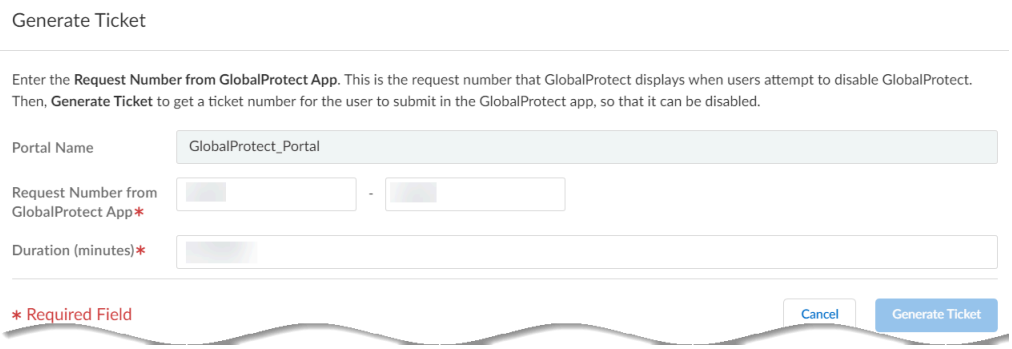
## Funktionsweise

Nachdem Sie diese Funktion eingerichtet haben, können Sie mit dem folgenden Workflow ein Ticket zur Deaktivierung von GlobalProtect anfordern:

- Ein Benutzer versucht, GlobalProtect in der GlobalProtect-App zu deaktivieren. GlobalProtect zeigt dem Benutzer eine Anforderungsnummer an.

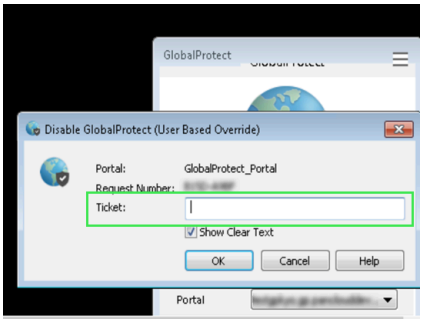



- Der Benutzer gibt die Anforderungsnummer an den GlobalProtect-Administrator weiter.
- Der GlobalProtect-Administrator meldet sich bei Prisma Access (Managed by Strata Cloud Manager) an und generiert mithilfe der Anforderungsnummer ein Ticket.




 ©2025 Palo Alto Networks, Inc.

- Der GlobalProtect-Administrator gibt die Ticketnummer an den Benutzer weiter. Der Benutzer gibt die Ticketnummer in die App ein, um GlobalProtect zu deaktivieren.




## Einrichten

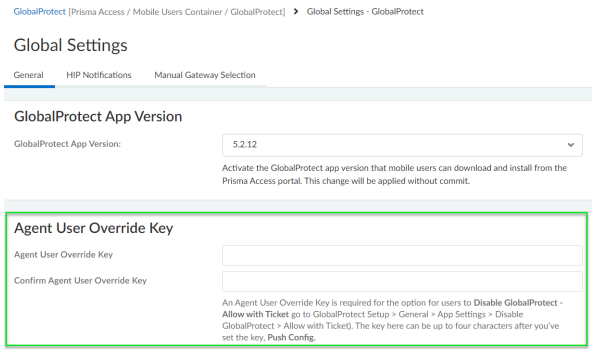
- Strata Cloud Manager
- Panorama

## Ticketanforderung zur Deaktivierung von GlobalProtect (Strata Cloud Manager)

**STEP 1 |** Schlüssel zum Überschreiben des Agenten festlegen

Bevor Sie die Option zum Anfordern eines Tickets für die Deaktivierung von GlobalProtect aktivieren können, müssen Sie zunächst einen Schlüssel zum Überschreiben des Agentenbenutzers festlegen.

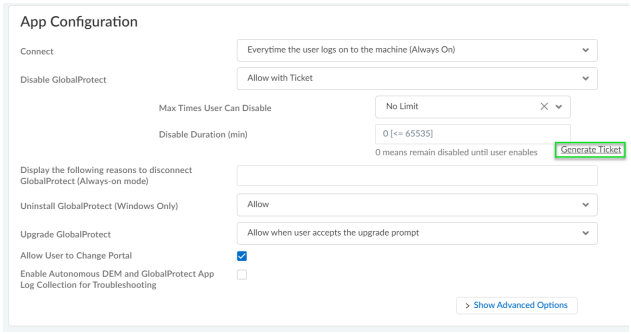
Wählen Sie **Workflows** > **Einrichtung Prisma Access** > **GlobalProtect** > **GlobalProtect-App** > **Globale App-Einstellungen** aus und geben Sie einen vierstelligen Schlüssel ein, um den **Schlüssel zum Überschreiben des Agenten** festzulegen.




 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Deaktivierung von GlobalProtect mit einem Ticket zulassen

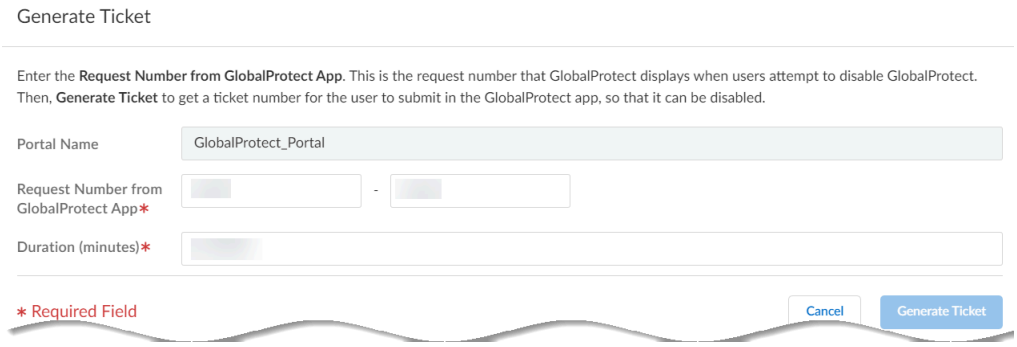
Wählen Sie **Workflows** > **Einrichtung Prisma Access** > **GlobalProtect** > **GlobalProtect-App** > **App-Einstellungen** > **App-Konfiguration** > **GlobalProtect deaktivieren** aus und setzen Sie die Option auf **Mit Ticket zulassen**.




**STEP 3 |** Ticket generieren

Nachdem Sie den **Schlüssel zum Überschreiben des Agenten** und die Option **Mit Ticket zulassen** festgelegt haben, können Sie das **Ticket generieren**.

Wenn ein Benutzer versucht, GlobalProtect in der App zu deaktivieren, wird in GlobalProtect eine Anforderungsnummer angezeigt. Übermitteln Sie diese Anforderungsnummer, um ein Ticket zu generieren, damit GlobalProtect für diesen Benutzer deaktiviert wird.




## Ticketanforderung zur Deaktivierung von GlobalProtect (Panorama)

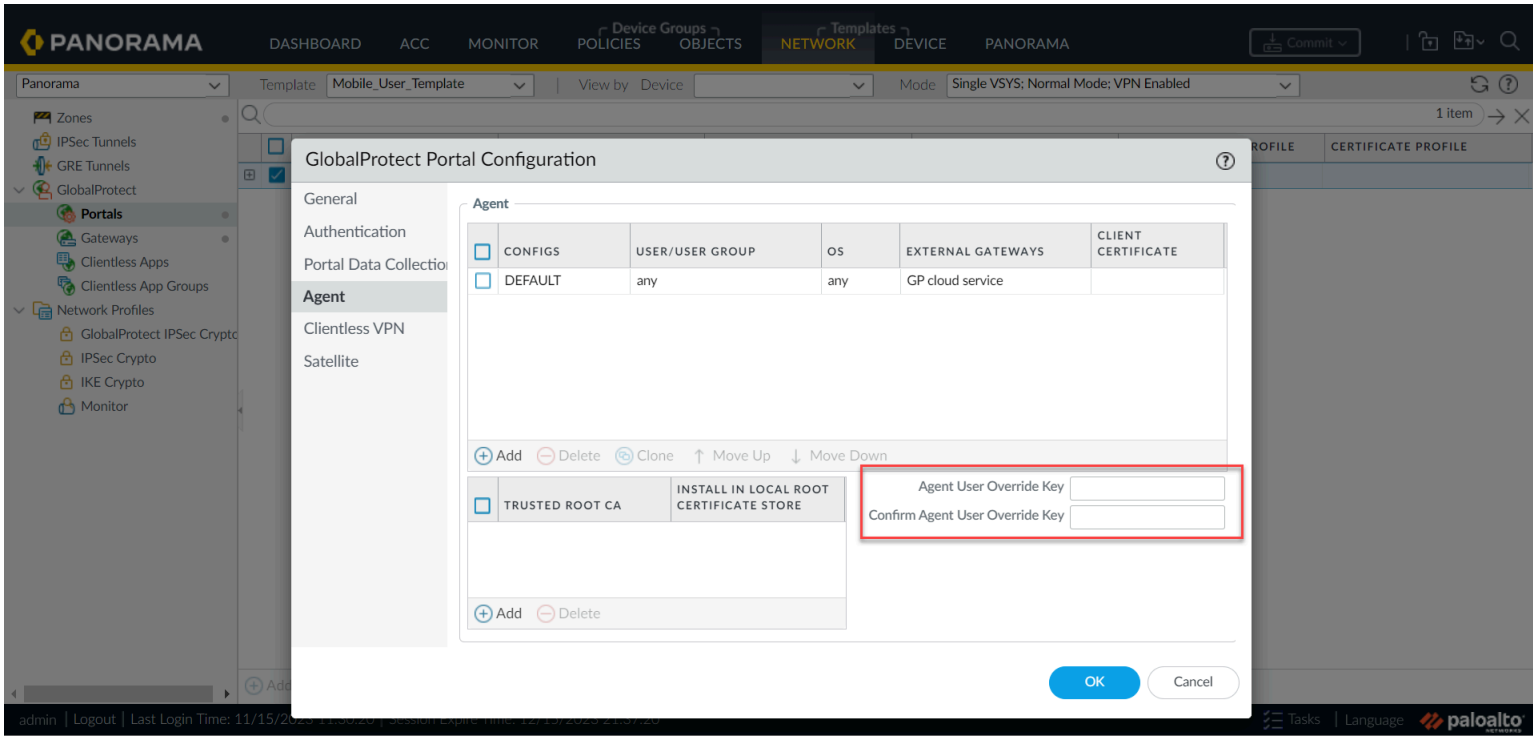
**STEP 1 |** Schlüssel zum Überschreiben des Agenten festlegen

Bevor Sie die Option zum Anfordern eines Tickets für die Deaktivierung von GlobalProtect aktivieren können, müssen Sie zunächst einen Schlüssel zum Überschreiben des Agentenbenutzers festlegen.

Gehen Sie zu **Netzwerk** > **GlobalProtect** > **Portale** und wählen Sie den Verbindungsnamen aus, für den Sie einen Überschreibungsschlüssel festlegen möchten. Wählen Sie **Agent** aus

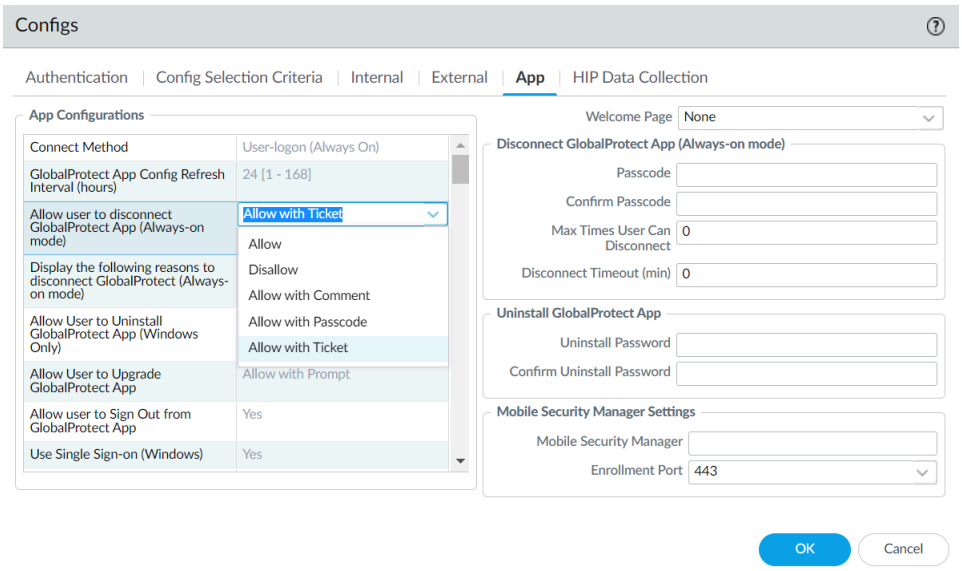
 ©2025 Palo Alto Networks, Inc.

und geben Sie dann einen Schlüssel ein, um den **Schlüssel zum Überschreiben des Agenten** festzulegen.




## STEP 2 | Deaktivierung von GlobalProtect mit einem Ticket zulassen

Wählen Sie unter **Netzwerk** > **GlobalProtect** > **Portale** den Namen der Verbindung aus, von der sich Benutzer abmelden können sollen. Wählen Sie **Agent** und eine **Konfiguration** aus und setzen Sie unter **App** > **App-Konfigurationen** > **Benutzer dürfen sich von der GlobalProtect-App abmelden (Modus „Immer aktiviert“)** die Option auf **Mit Ticket zulassen**.

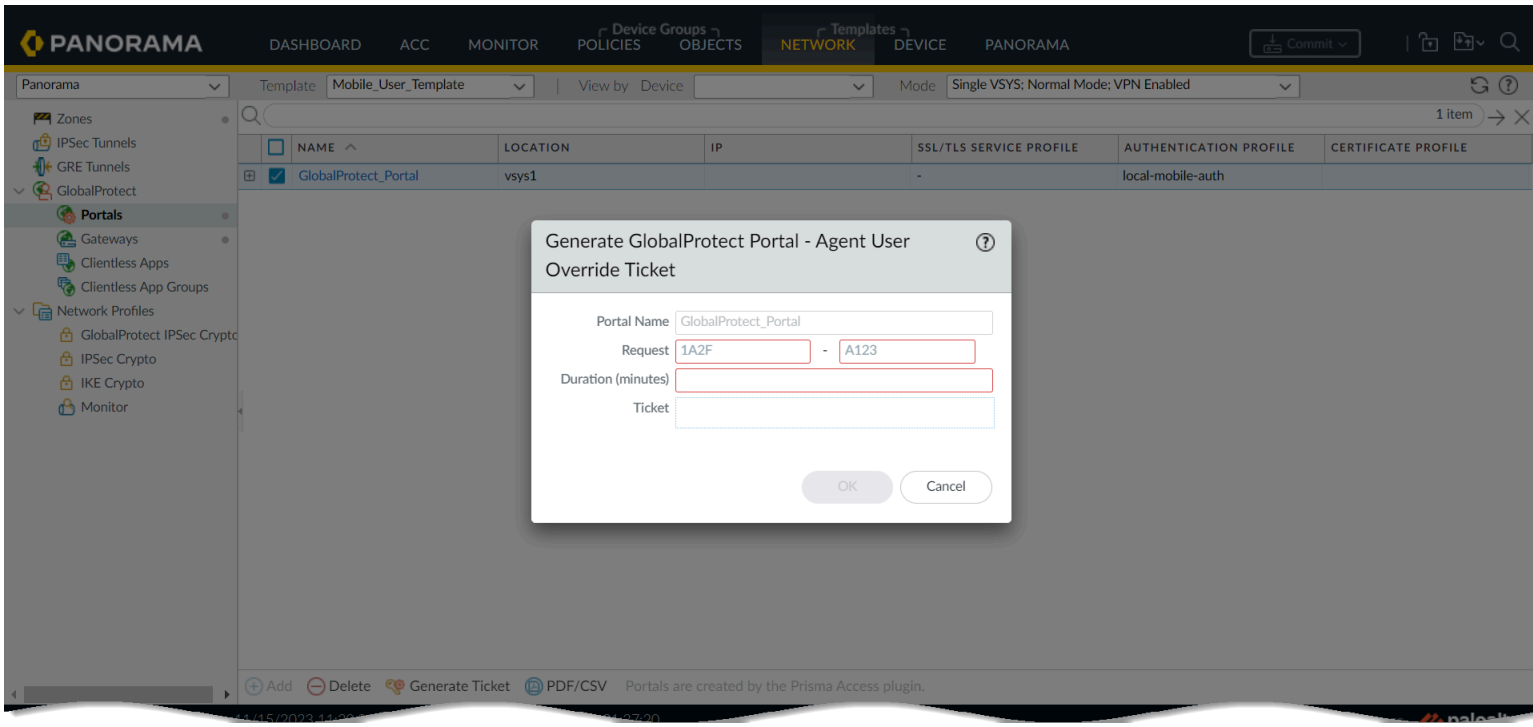



 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Ticket generieren

Nachdem Sie den **Schlüssel zum Überschreiben des Agenten** und die Option **Mit Ticket zulassen** festgelegt haben, können Sie das **Ticket generieren**.

Wenn ein Benutzer versucht, GlobalProtect in der App zu deaktivieren, wird in GlobalProtect eine Anforderungsnummer angezeigt. Übermitteln Sie diese Anforderungsnummer, um ein Ticket zu generieren, damit GlobalProtect für diesen Benutzer deaktiviert wird.




# GlobalProtect-Voranmeldung

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | ☐ Prisma Access-Lizenz<br>☐ Administratorzugang zum Endpunkt für die Installation des Maschinenzertifikats<br>☐ Auf dem Endpunkt bereitgestelltes vertrauenswürdiges PKI-Zertifikat |

Die Voranmeldung ist eine Verbindungsmethode, die einen VPN-Tunnel einrichtet, bevor sich ein Benutzer anmeldet. Der Zweck der Voranmeldung besteht darin, anstelle des Benutzers den Endpunkt zu authentifizieren und die Ausführung von Domänenskripten oder anderen Aufgaben zu ermöglichen, sobald der Endpunkt eingeschaltet wird. Maschinenzertifikate ermöglichen es dem Endpunkt, einen VPN-Tunnel zum GlobalProtect-Gateway herzustellen. Eine gängige Praxis für IT-Administratoren besteht darin, das Maschinenzertifikat zu installieren, während der Endpunkt für den Benutzer vorbereitet wird. Ein VPN-Tunnel für die Voranmeldung verwendet einen generischen Benutzernamen für die Voranmeldung, da sich der Benutzer nicht angemeldet hat. Um Endpunkten den Zugriff auf Ressourcen zu ermöglichen, müssen

 ©2025 Palo Alto Networks, Inc.

Sie Sicherheitsrichtlinienregeln erstellen, die mit dem Benutzer für die Voranmeldung übereinstimmen. Diese Richtlinienregeln sollten ausschließlich den Zugriff auf die grundlegenden Dienste zum Starten des Systems ermöglichen, z. B. DHCP, DNS, spezifische Active Directory-Dienste, Antivirenprogramme oder andere Aktualisierungsdienste. Nachdem sich der Benutzer am Gateway authentifiziert hat, weist die GlobalProtect-App diesem Benutzer den VPN-Tunnel zu. Die IP-Adresszuordnung in Prisma Access erfolgt nicht mehr zum Endpunkt für die Voranmeldung, sondern zum authentifizierten Benutzer.

Das für die Voranmeldungsauthentifizierung verwendete Zertifikat befindet sich im persönlichen Zertifikatspeicher des Endpunkts. Verwenden Sie eine vertrauenswürdige Zertifizierungsstelle eines Drittanbieters, eine selbstsignierte Zertifizierungsstelle oder eine interne PKI-Zertifizierungsstelle, um ein Maschinenzertifikat auszustellen. Sie müssen ein Maschinenzertifikat als Authentifizierungsmethode konfigurieren, um einen Tunnel von einem Endpunkt aus einzurichten, bevor Sie sich bei Prisma Access anmelden, und anschließend ein Zertifikatprofil erstellen, das das CA-Zertifikat für die Voranmeldung enthält.

- Strata Cloud Manager
- Panorama

## GlobalProtect-Voranmeldung (Strata Cloud Manager)

### CA-Stammzertifikat eines Drittanbieters importieren

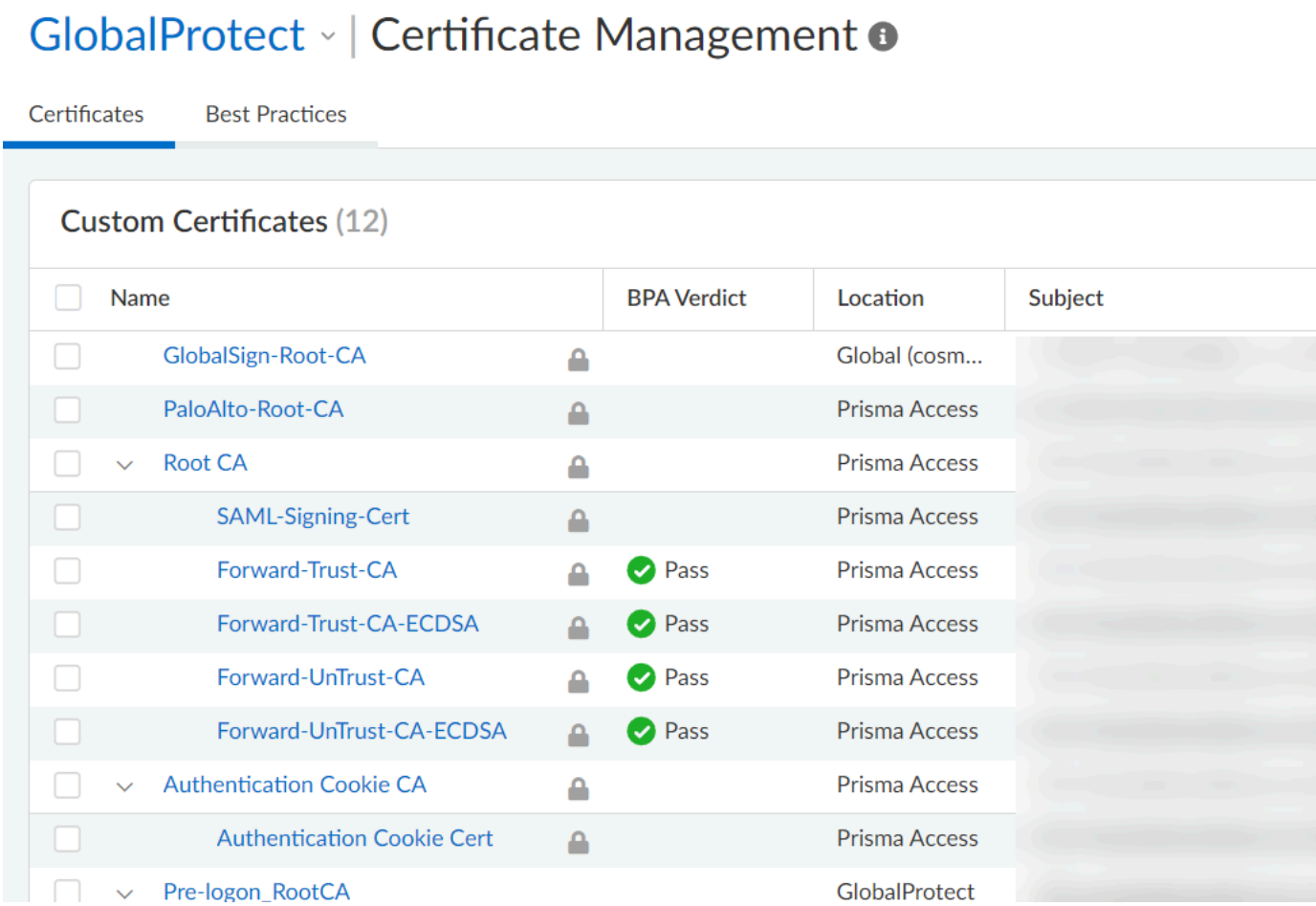
Verwenden Sie ein Maschinenzertifikat als Authentifizierungsmethode, um einen Tunnel von einem Endpunkt aus einzurichten, bevor Sie sich bei Prisma Access anmelden.

**STEP 1 |** Wählen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Objekte** > **Zertifikatverwaltung** aus. Wählen Sie den Konfigurationsumfang von **Prisma Access** aus.

Vergewissern Sie sich, dass Sie das Zertifikat für mobile Benutzer von GlobalProtect importieren.

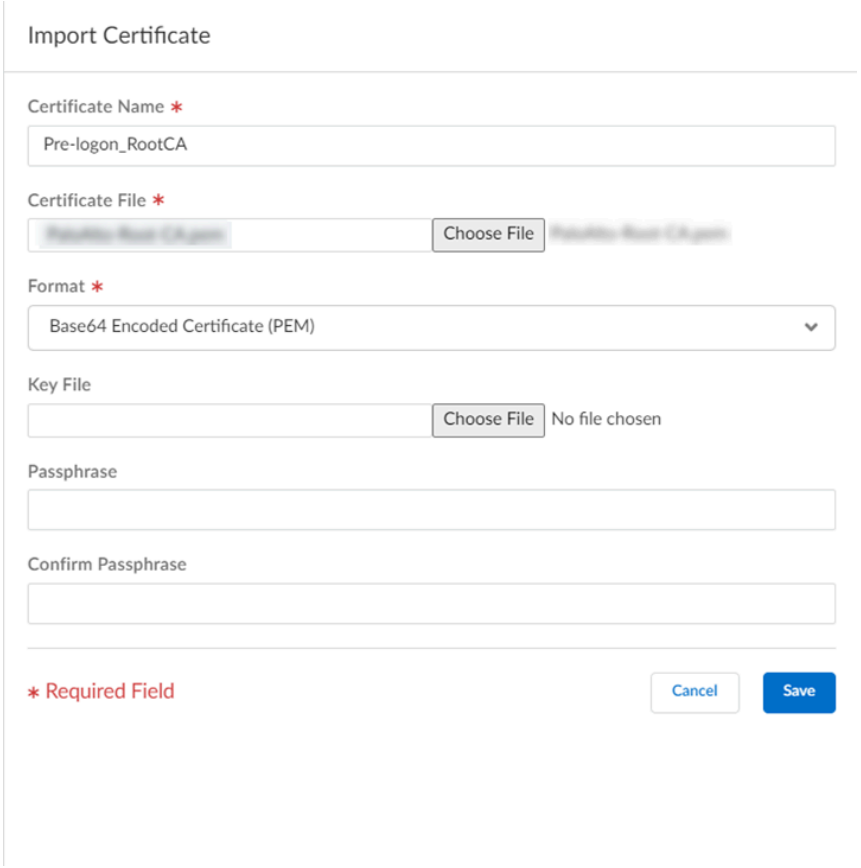
 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** **Importieren** Sie ein benutzerdefiniertes Zertifikat.




 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Geben Sie Werte ein und **Speichern** Sie die Zertifikateinstellungen.




### Erstellen Sie ein Zertifikatprofil für die Voranmeldung

Erstellen Sie ein Zertifikatprofil und schließen Sie die Zertifizierungsstelle für selbstsignierte Stammzertifikate ein. Diese Zertifizierungsstelle validiert das Maschinenzertifikat durch den mobilen GlobalProtect-Benutzer bei der Voranmeldung.

**STEP 1 |** Wählen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Objekte** > **Zertifikatverwaltung** aus. Wählen Sie den Konfigurationsumfang von **Prisma Access** aus.

**STEP 2 |** **Fügen Sie das Profil hinzu**.

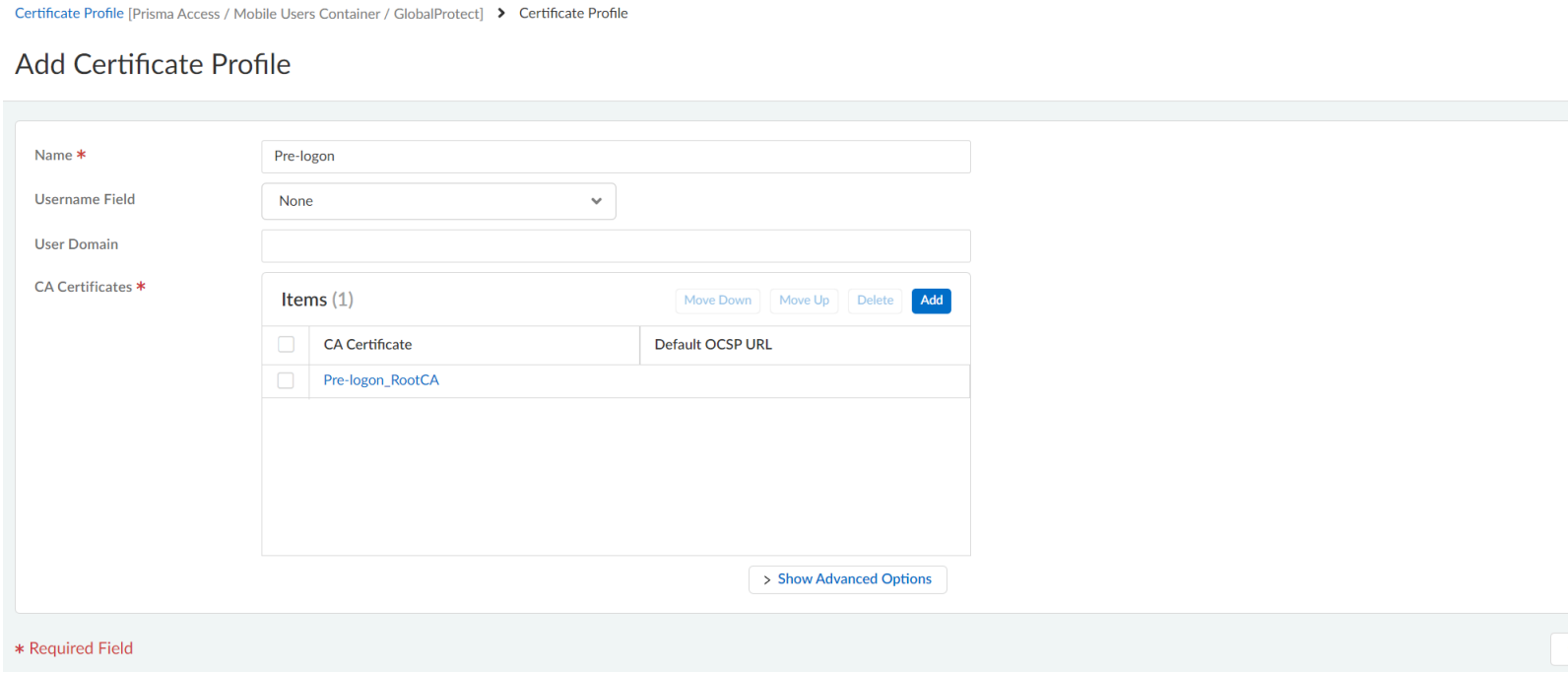
 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Geben Sie Werte ein.

1. Vergewissern Sie sich, dass das Feld **Benutzername** auf **Keine** gesetzt ist, um zu verhindern, dass das Zertifikat einem Benutzer zugeordnet wird.

   *Das Feld **Benutzername** darf nicht auf **Keine** gesetzt sein, wenn Sie Ihr Zertifikat mit einer beliebigen Authentifizierungsmethode **ODER** mit einem Clientzertifikat authentifizieren, wie unter 2 beschrieben.*

2. Sie müssen das CA-Stammzertifikat für die Voranmeldung **hinzufügen**, das Sie im Schritt 1 importiert haben.
3. **Speichern** Sie die Einstellungen des Zertifikatprofils.




### Konfigurieren Sie das GlobalProtect-Portal für die Voranmeldung

Konfigurieren Sie das GlobalProtect-Portal so, dass Verbindungen mit einem Maschinenzertifikat authentifiziert werden.

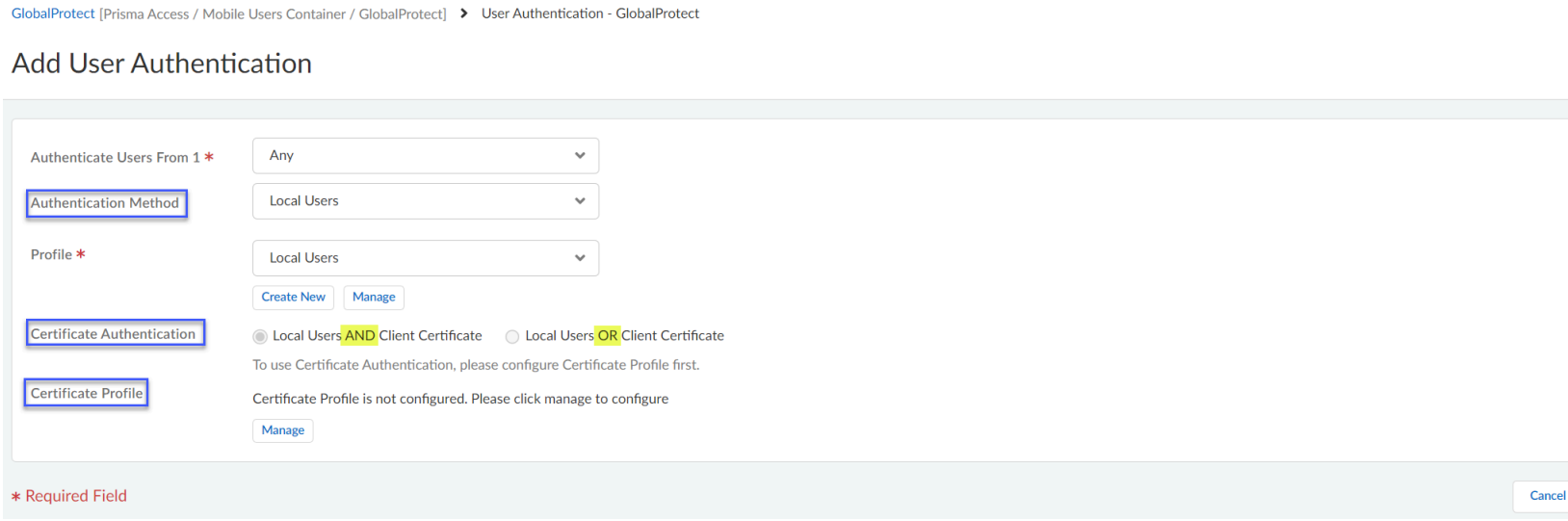
**STEP 1 |** Wählen Sie **Workflows** > **Prisma AccessEinrichtung** > **GlobalProtect** > **Infrastruktur** aus.

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Bearbeiten Sie die Konfigurationseinstellungen für die Benutzerauthentifizierung.

Wählen Sie eine von GlobalProtect unterstützte Authentifizierungsmethode, das von Ihnen erstellte Voranmeldungszertifikatprofil und die Zertifikatauthentifizierung aus.

*Wählen Sie eine beliebige Zertifikatauthentifizierung aus, die von GlobalProtect unterstützt wird.*

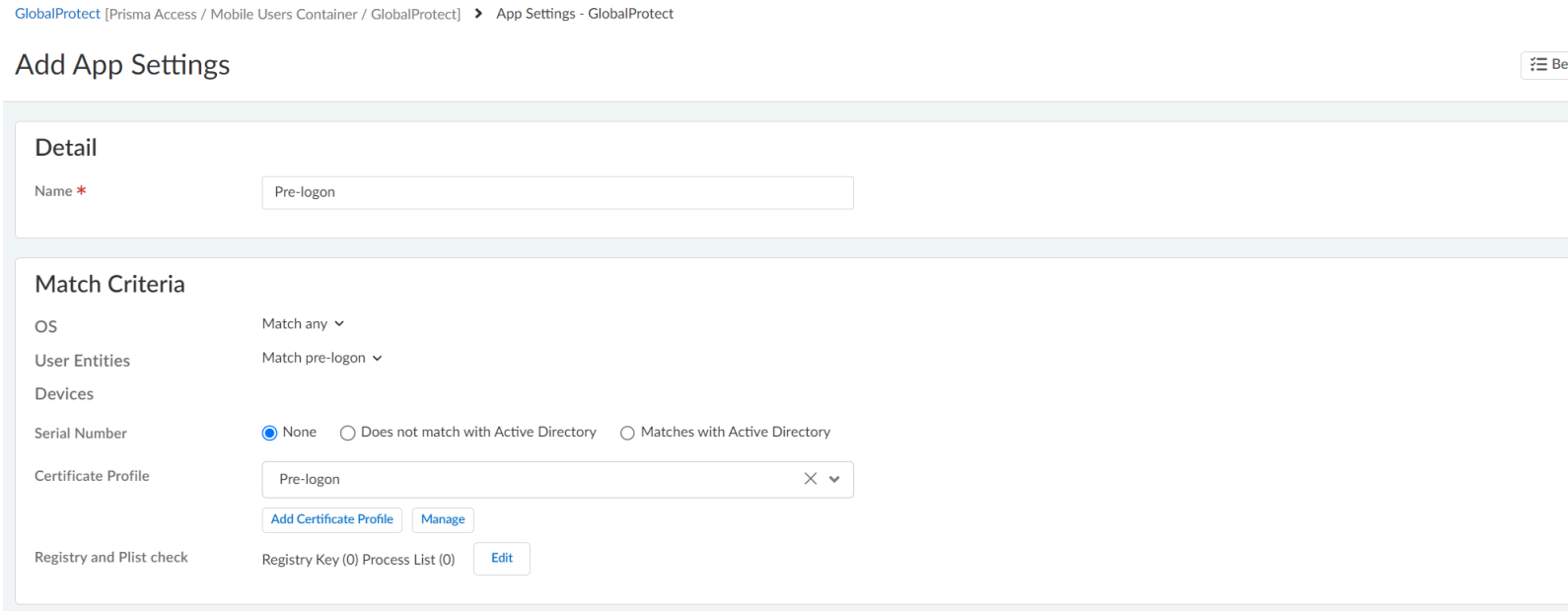



 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Konfigurieren Sie die Einstellungen der GlobalProtect-App so, dass sie den Kriterien der Voranmeldung entsprechen.

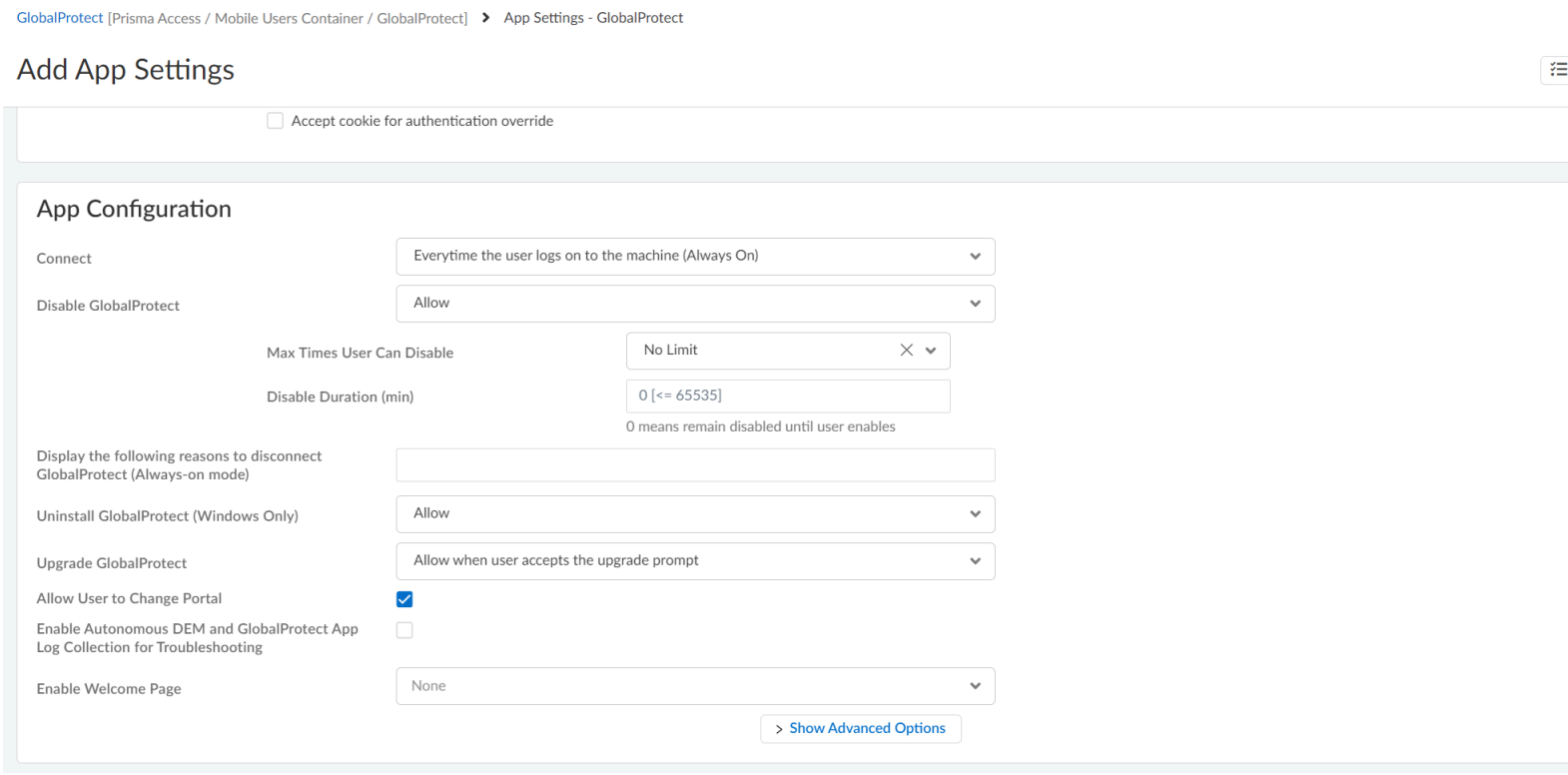
1. Navigieren Sie zur Registerkarte **GlobalProtect-App**.
2. **Fügen Sie App-Einstellungen hinzu.**

   *Achten Sie bei der Eingabe von Werten darauf, dass die Benutzerentitäten **für die Voranmeldung** mit dem Zertifikatprofil für die Voranmeldung übereinstimmen.*




- Wählen Sie eine Verbindungsmethode für die Voranmeldung aus.

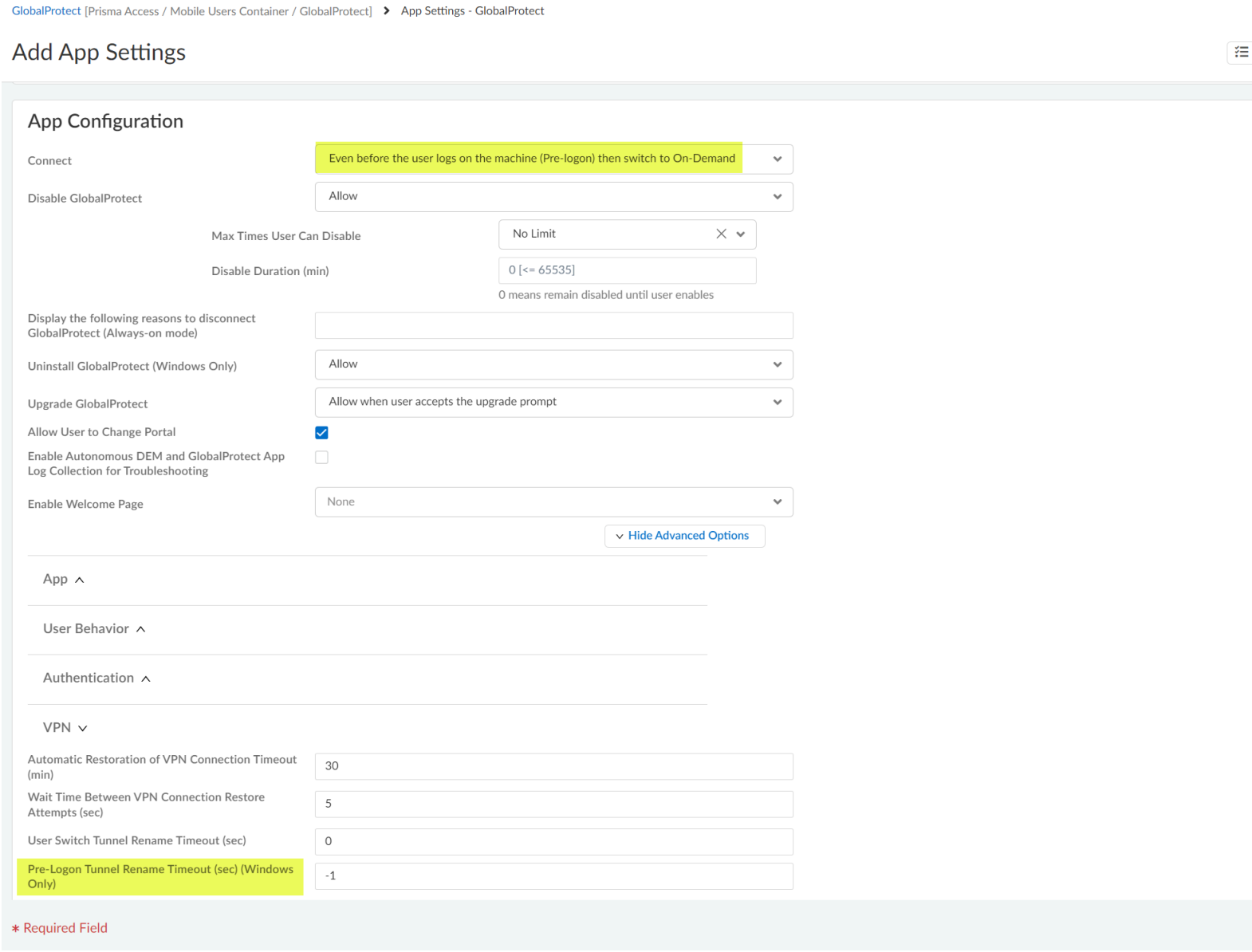
 ©2025 Palo Alto Networks, Inc.




- Wenn Sie **Noch bevor sich der Benutzer am Computer anmeldet (Vor der Anmeldung)** auswählen und dann auf „On-Demand“ umschalten, setzen Sie den Wert

 ©2025 Palo Alto Networks, Inc.

von **Timeout für Voranmeldungstunnel-Umbenennung** auf –1. Sehen Sie sich die erweiterten VPN-Optionen an, um dieses Feld zu bearbeiten.




3. Verschieben Sie die App-Einstellung für die Voranmeldung über andere App-Einstellungen.
4. Bearbeiten Sie alle anderen App-Einstellungen für authentifizierte Benutzer.

   Aktualisieren Sie die Verbindungsmethode und das Zertifikatprofil.

**STEP 4 |** Übertragen Sie die Änderungen per Push an Prisma Access.

### Maschinenzertifikat installieren – Windows

Installieren Sie das Maschinenzertifikat auf dem Endpunkt, der für die Authentifizierung verwendet wird.

**STEP 1 |** Exportieren Sie das selbstsignierte CA-Stammzertifikat aus Ihrer PKI im Format **Binär codiertes Zertifikat (DER)**.

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Übertragen Sie die Zertifikatdateien auf einen Windows-Computer.

**STEP 3 |** Installieren Sie das CA-Stammzertifikat für die Voranmeldung im Ordner **Trusted Root Certification Authorities** (Vertrauenswürdige Stammzertifizierungsstellen) auf Ihrem lokalen Computer.

**STEP 4 |** Installieren Sie das Maschinenzertifikat für die Voranmeldung im lokalen Computerspeicher.

**STEP 5 |** Fahren Sie mit der Installation fort, geben Sie die Passphrase ein, wenn Sie dazu aufgefordert werden, und schließen Sie die Installation ab.

**STEP 6 |** Stellen Sie eine Verbindung zum GlobalProtect-Portal her und löschen Sie alle Cookies vom Host.

**STEP 7 |** (Optional) Melden Sie sich von Ihrem Computer ab und sehen Sie sich die GlobalProtect-Protokolle an, um die Verbindung für die Voranmeldung zu überprüfen.

## GlobalProtect-Voranmeldung (Panorama)

### Zertifikat und Profil für die Voranmeldung konfigurieren

Konfigurieren Sie ein Maschinenzertifikat als Authentifizierungsmethode, um einen Tunnel von einem Endpunkt aus einzurichten, bevor Sie sich bei Prisma Access anmelden, und erstellen Sie dann ein Zertifikatprofil, das das CA-Zertifikat für die Voranmeldung enthält.

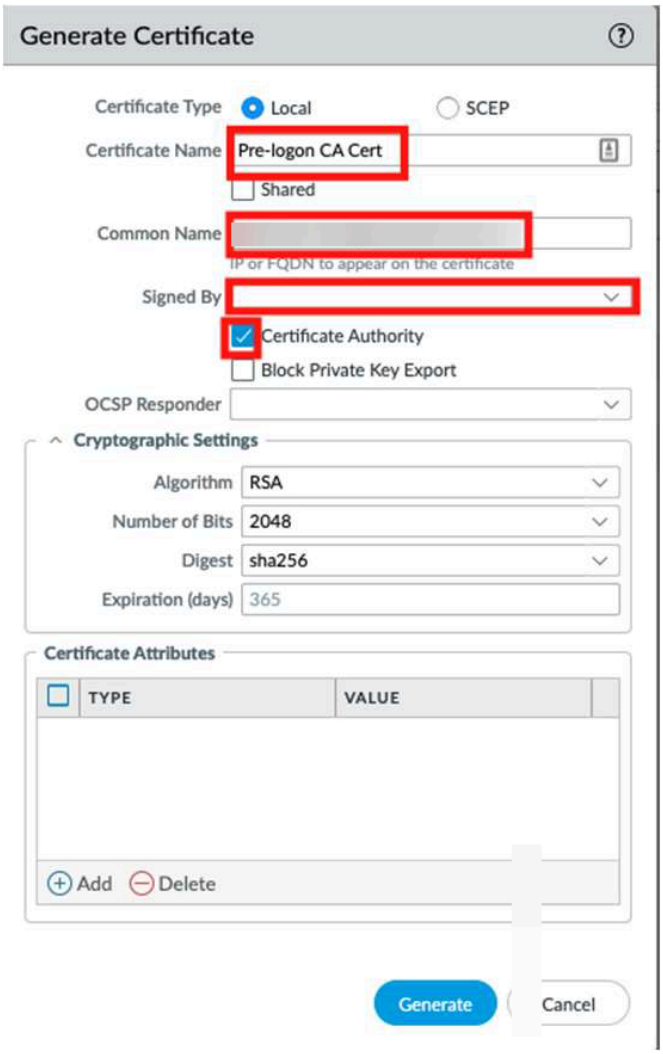
 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** Konfigurieren Sie eine selbstsignierte CA, und verwenden Sie sie, um ein Maschinenzertifikat in der Vorlage „Mobiler Benutzer“ zu generieren. Gehen Sie zu **Gerät** > **Zertifikatverwaltung** > **Zertifikate**.

Vergewissern Sie sich in der Vorlage für mobile Benutzer (**Mobile_User_Template**) befinden und der **Standort** auf **Freigegeben** gesetzt ist.

1. Geben Sie einen Namen für das Zertifikat ein, z. B. **CA-Zertifikat für die Voranmeldung**.
2. Geben Sie einen **allgemeinen Namen** ein.

   Der allgemeine Name (Common Name, CN) ist der Domänenname, wie z. B. www.yourdomainname.com, den Sie mit Ihrem Zertifikat schützen möchten.
3. Lassen Sie das Feld **Signiert von** leer, und aktivieren Sie das Kontrollkästchen **Zertifizierungsstelle**.
4. **Generieren** Sie das Zertifikat für die Verwendung in Verbindungen für die Voranmeldung.

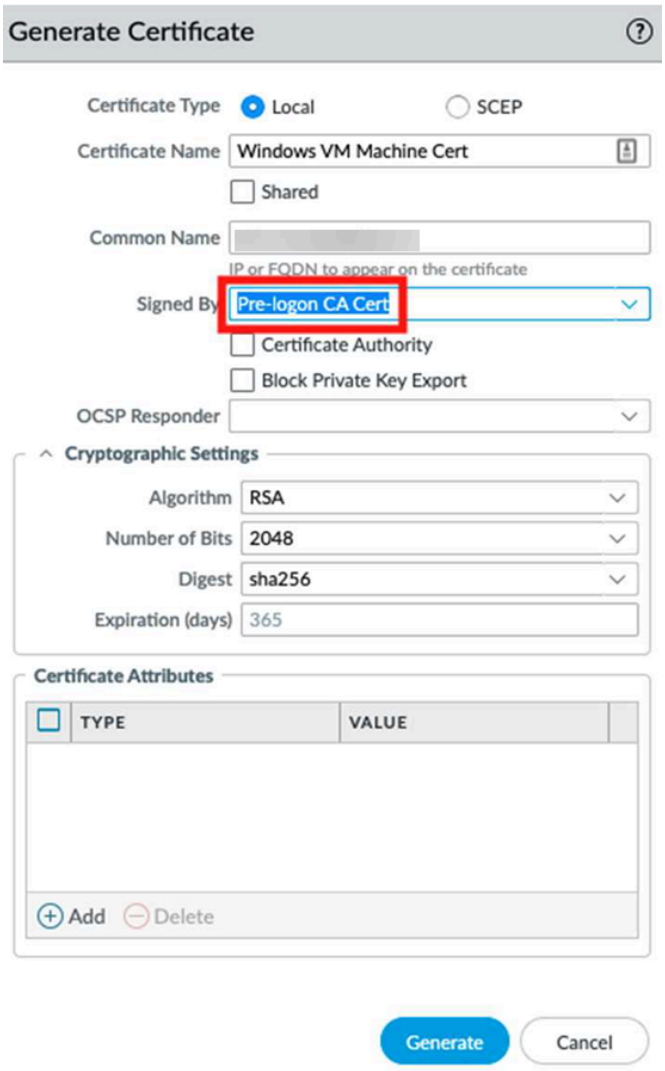



 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Nachdem Sie die selbstsignierte CA konfiguriert haben, generieren Sie das Maschinenzertifikat.

1. Geben Sie einen **Zertifikatnamen** und einen **allgemeinen Namen** ein.
2. Wählen Sie im Drop-down-Menü **Signiert von** das **CA-Zertifikat für die Voranmeldung** aus, das Sie in Schritt 1 erstellt haben.
3. **Generieren** Sie das **Windows VM-Maschinenzertifikat**, das Sie später auf einem Windows-Computer installieren.

   Dieses Zertifikat ist ein untergeordnetes Zertifikat der CA für die Voranmeldung.

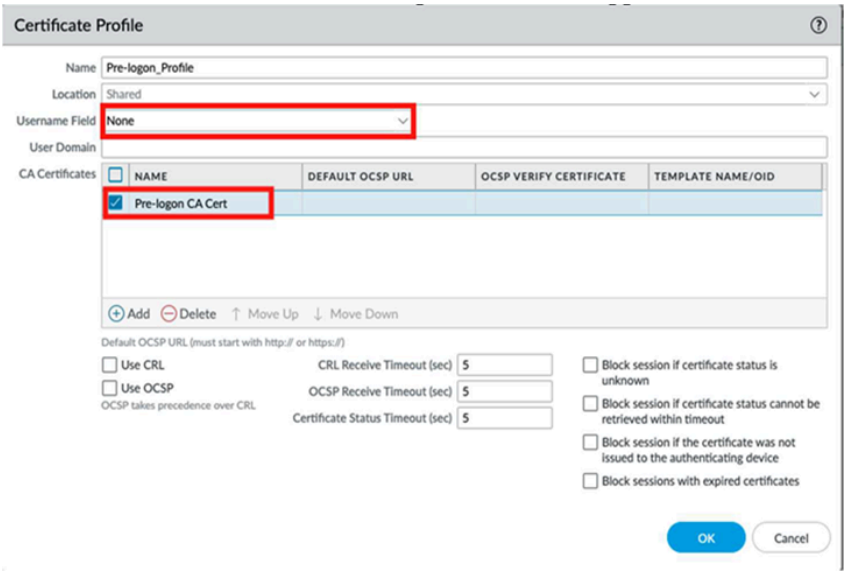



**STEP 3 |** Um ein Zertifikatprofil zu erstellen, das das CA-Zertifikat für die Voranmeldung enthält, gehen Sie zu **Gerät** > **Zertifikatverwaltung** > **Zertifikatprofil**.

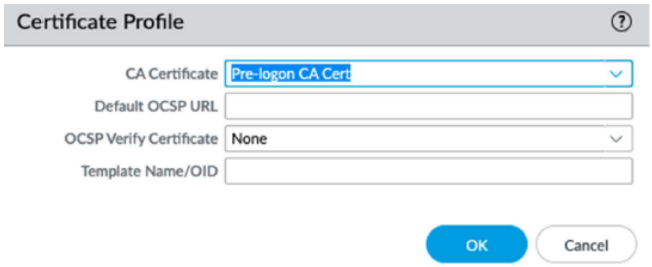
Verwenden Sie diese Zertifizierungsstelle (CA), um das Maschinenzertifikat zu validieren, das vom GlobalProtect-Client während der Initialisierung des Tunnels für die Voranmeldung präsentiert wurde.

 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** Erstellen Sie das Profil und geben Sie einen Namen für das Profil ein. Stellen Sie sicher, dass das Feld **Benutzername** auf **Keine** gesetzt ist, um die Zuordnung des Zertifikats zu einem Benutzer zu verhindern.




**STEP 5 |** Wählen Sie unter **CA-Zertifikate** die Option **Hinzufügen** und im Drop-down-Menü die Option **CA-Zertifikat für die Voranmeldung** aus.




**STEP 6 |** Wählen Sie **OK** und anschließend erneut **OK** aus.

### Konfigurieren Sie das GlobalProtect-Portal für die Voranmeldung

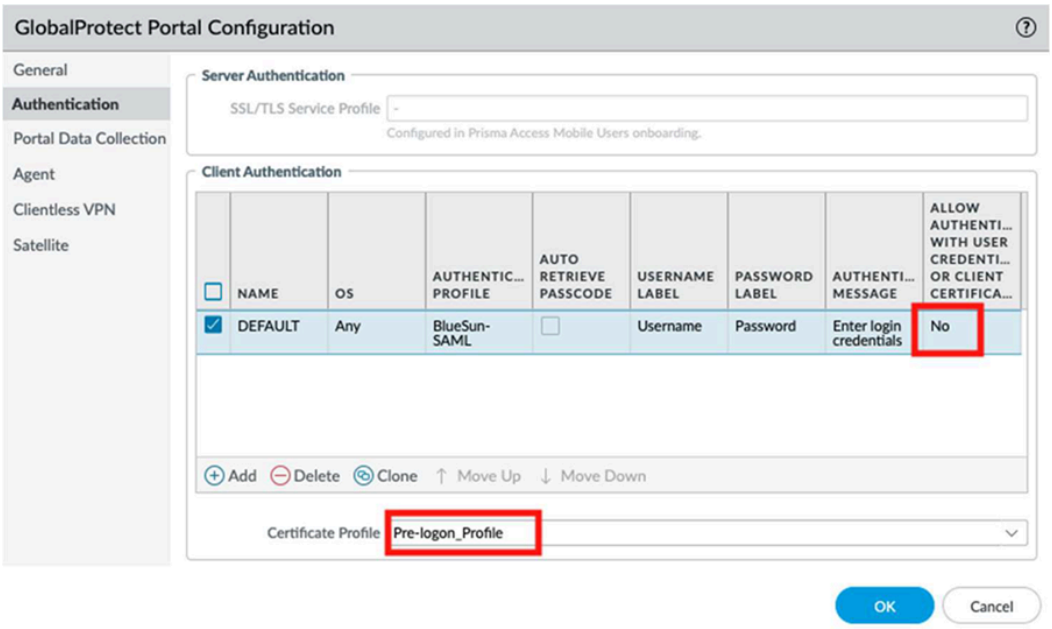
Konfigurieren Sie das GlobalProtect-Portal so, dass Verbindungen mit einem Maschinenzertifikat authentifiziert werden.

**STEP 1 |** Gehen Sie zu **Netzwerk** > **GlobalProtect** > **Portale** > **GlobalProtect_Portal** > **Authentifizierung**.

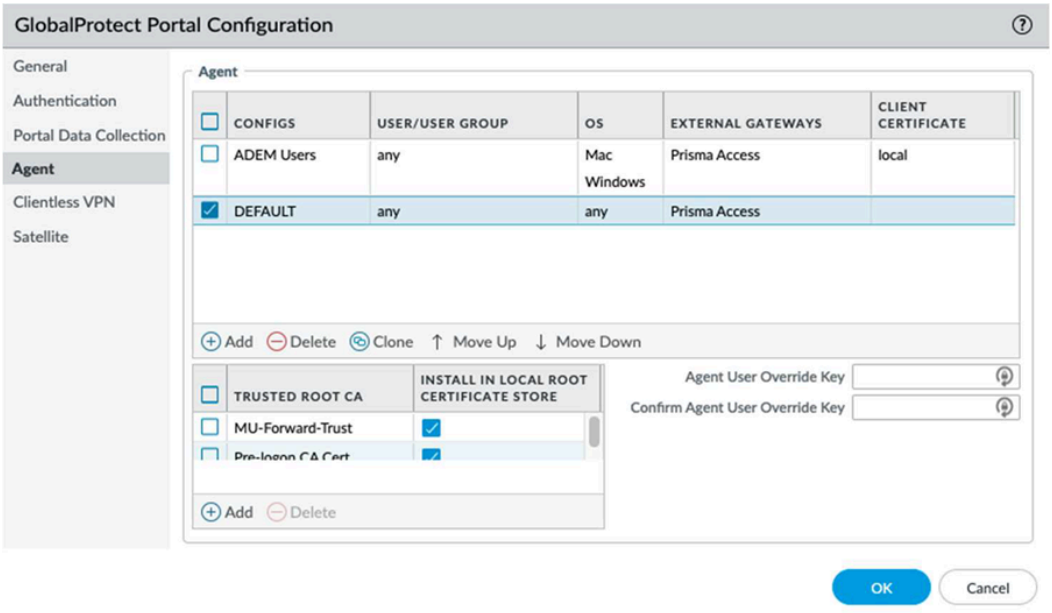
**STEP 2 |** Wählen Sie unter **Authentifizierung mit Benutzeranmeldeinformationen ODER Clientzertifikat zulassen** die Option **Nein** aus, um nur die zertifikatbasierte Authentifizierung zu erzwingen.

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Wählen Sie im **Zertifikatprofil** das erstellte Profil für die Voranmeldung (**Pre-logon_Profile**) aus, und klicken Sie auf **OK**.



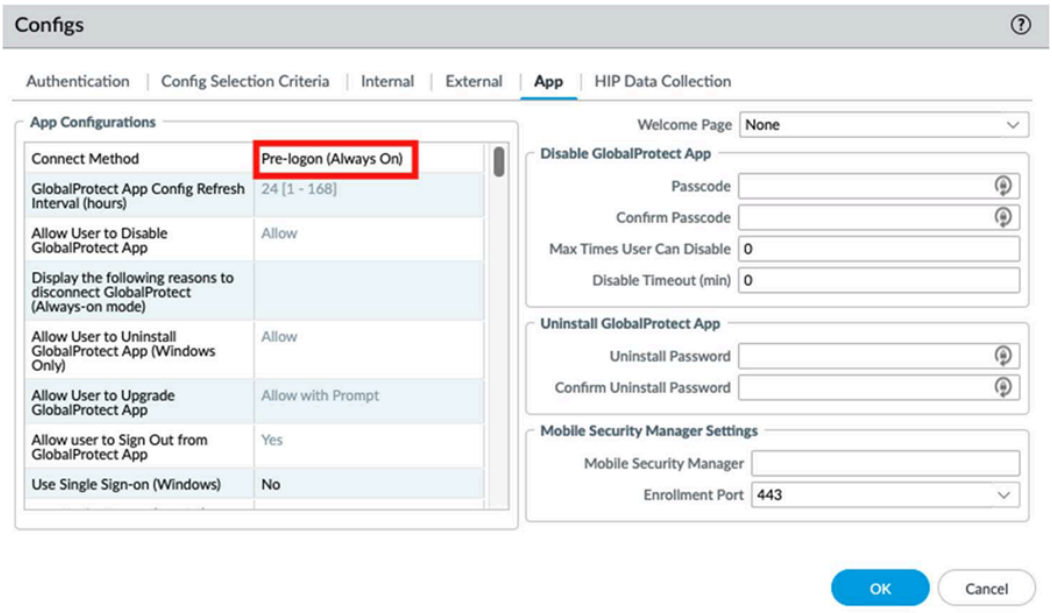

**STEP 4 |** Wählen Sie **Agent** aus und öffnen Sie die Agent-Konfiguration für authentifizierte Benutzer.




**STEP 5 |** Wählen Sie die Registerkarte **App** aus.

 ©2025 Palo Alto Networks, Inc.

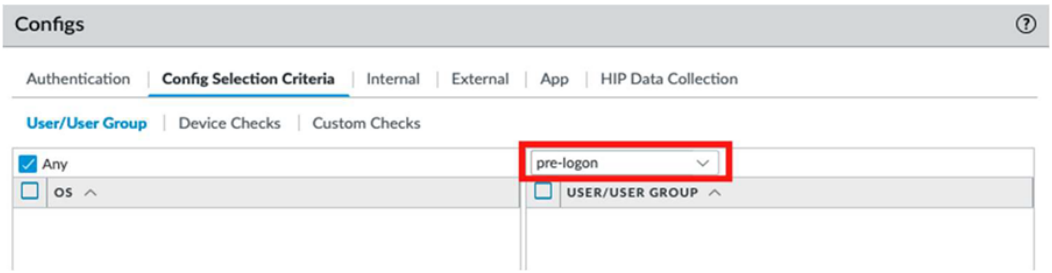
**STEP 6 |** Wählen Sie **Voranmeldung (immer aktiviert)** und anschließend **OK** aus, um zum Bereich „Agent“ zurückzukehren.




**STEP 7 |** **Klonen** Sie im Bereich „Agent“ die Standardkonfiguration. Ändern Sie den Konfigurationsnamen in **Voranmeldung**, damit er der Verbindungsmethode für die Maschinenzertifikatauthentifizierung entspricht.

**STEP 8 |** Wählen Sie die neu geklonte Agent-Konfiguration aus.

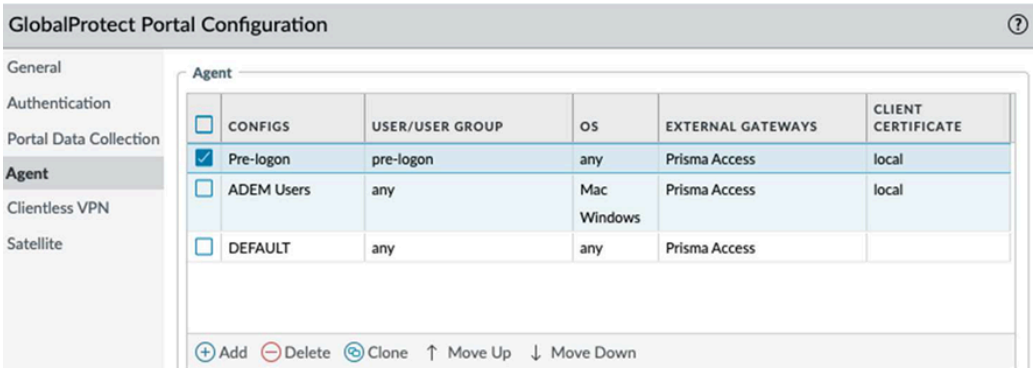
**STEP 9 |** Wählen Sie **Auswahlkriterien für die Konfiguration** aus. Wählen Sie unter der Konfiguration **Benutzer/Benutzergruppe** die Option **Voranmeldung** aus dem Drop-down-Menü oberhalb des Konfigurationsfelds **Benutzer/Benutzergruppe** aus und vergewissern Sie sich, dass die Konfiguration auf **Beliebig** festgelegt ist.




**STEP 10 |** Konfigurieren Sie die App-Einstellungen nach Bedarf und wählen Sie **OK** aus. Stellen Sie sicher, dass Sie sowohl für die Voranmeldungs- als auch für die aktuelle Konfiguration eine Verbindungsmethode für die Voranmeldung auswählen.


©2025 Palo Alto Networks, Inc.

**STEP 11 |** Verschieben Sie die Agent-Konfiguration für die Voranmeldung an den Anfang der **CONFIGS**-Liste, um sicherzustellen, dass zuerst ein Abgleich mit der Voranmeldungsbedingung durchgeführt wird.




**STEP 12 |** Klicken Sie auf **OK**, um die Portalkonfiguration zu speichern.

### Konfigurieren der Prisma Access GlobalProtect-Gateways

Konfigurieren Sie die GlobalProtect-Gateways in von Panorama verwaltetem Prisma Access.

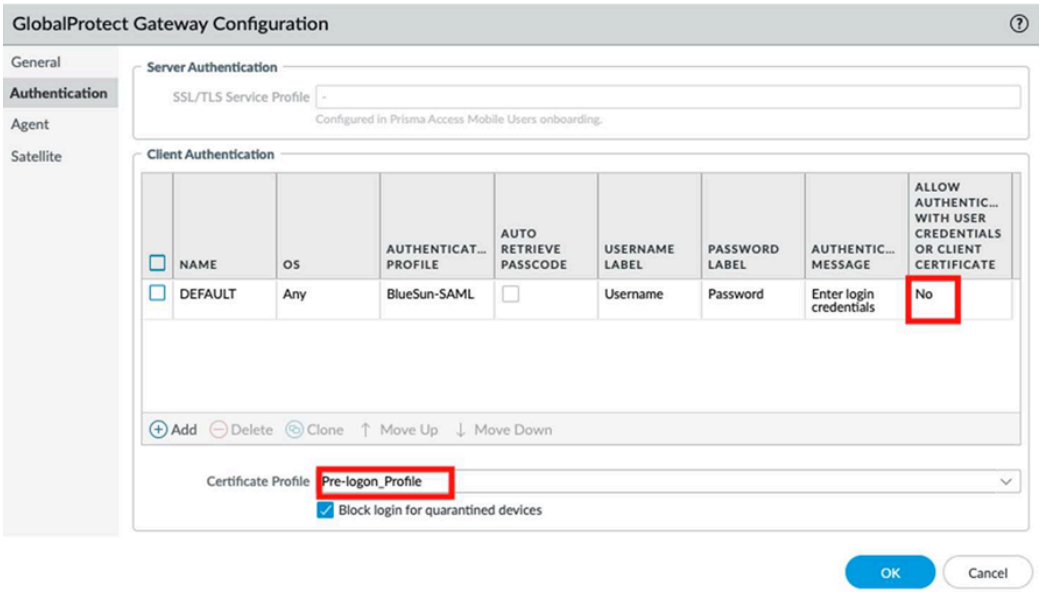
*Mit dieser Konfiguration wird nur die zertifikatbasierte Authentifizierung erzwungen.*

**STEP 1 |** Wechseln Sie zu **Netzwerk** > **GlobalProtect** > **Gateways** > **GlobalProtect_External_Gateway** > **Authentifizierung**.

**STEP 2 |** Wählen Sie die Authentifizierungsmethode **Standard** aus.

Wenn Sie bereits eine Clientauthentifizierung (z. B. SAML) konfiguriert haben, wählen Sie diese anstelle von **Standard** aus.

**STEP 3 |** Wählen Sie unter **Authentifizierung mit Benutzeranmeldeinformationen ODER Clientzertifikat zulassen** die Option **Nein** aus. Wählen Sie dann **OK** aus, um die Konfiguration zu speichern.



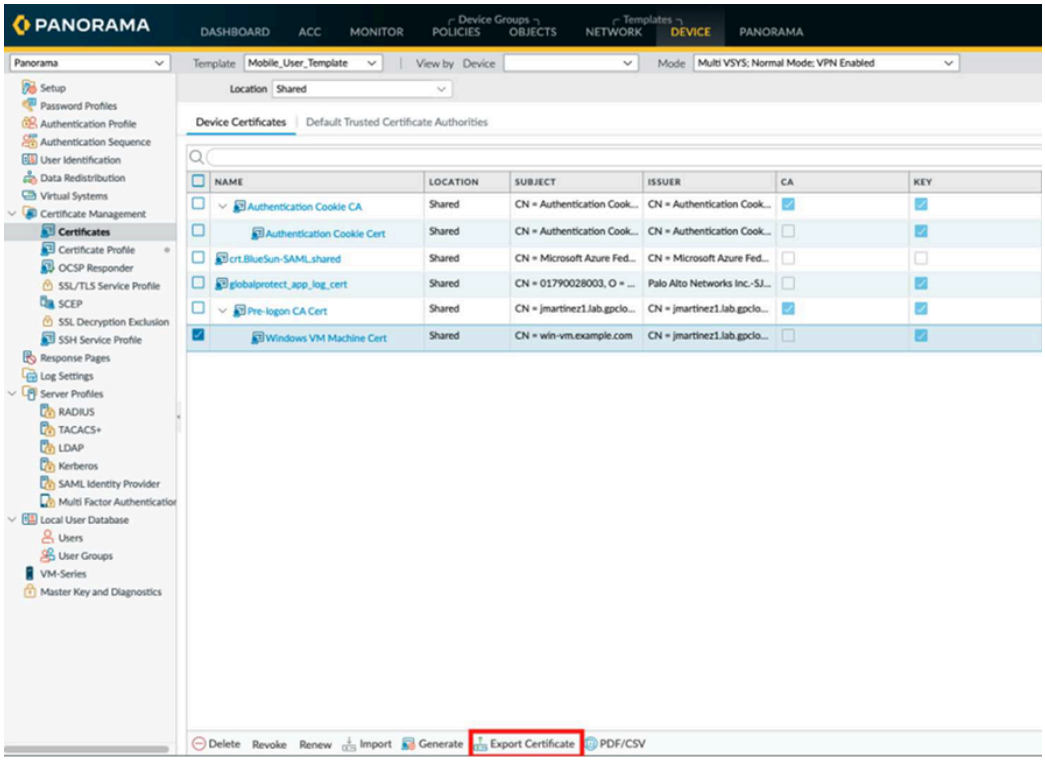

 ©2025 Palo Alto Networks, Inc.

### Maschinenzertifikat installieren – Windows

Installieren Sie das Maschinenzertifikat an den Endpunkten der mobilen Benutzer, die zur Authentifizierung verwendet werden.

**STEP 1 |** Gehen Sie zu **Gerät** > **Zertifikatverwaltung** > **Zertifikate**.

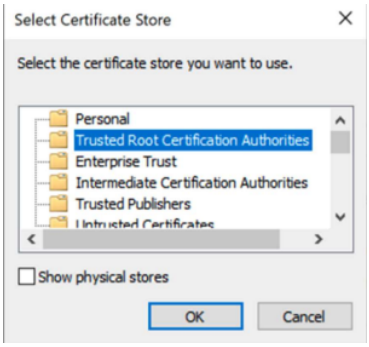
**STEP 2 |** Vergewissern Sie sich, dass Sie noch immer mit Mobile_User_Template arbeiten. Wählen Sie das **Windows VM-Maschinenzertifikat** aus, das Sie zuvor erstellt haben, und wählen Sie **Zertifikat exportieren** aus, um es als PKCS12-Datei mit einer Passphrase herunterzuladen.




**STEP 3 |** Exportieren Sie das CA-Zertifikat für die Voranmeldung als base64-codiertes Zertifikat.

**STEP 4 |** Übertragen Sie die Zertifikatdateien auf einen Windows-Computer.

**STEP 5 |** Installieren Sie das CA-Stammzertifikat für die Voranmeldung im Ordner **Trusted Root Certification Authorities** (Vertrauenswürdige Stammzertifizierungsstellen) auf Ihrem lokalen Computer.




 ©2025 Palo Alto Networks, Inc.

**STEP 6 |** Installieren Sie das Maschinenzertifikat für die Voranmeldung im lokalen Computerspeicher. Vervollständigen Sie die Berechtigungen und wählen Sie **Weiter** aus, um mit der Installation fortzufahren.

**STEP 7 |** Prüfen Sie den Dateinamen für das Zertifikat und wählen Sie **Weiter** aus.

**STEP 8 |** Geben Sie das Passwort ein, das Sie beim Zertifikatexport aus Panorama verwendet haben, und wählen Sie **Weiter** aus.

**STEP 9 |** Wählen Sie im Dialogfeld **Zertifikatspeicher** die Option **Alle Zertifikate im folgenden Speicher ablegen** und anschließend **Durchsuchen** aus.

**STEP 10 |** Wählen Sie den **Persönlichen Ordner** aus, in dem Sie das Maschinenzertifikat installieren möchten, und wählen Sie **OK** aus.

**STEP 11 |** Wählen Sie **Weiter** aus, um mit der Installation fortzufahren.

**STEP 12 |** Stellen Sie eine Verbindung zum GlobalProtect-Portal her und löschen Sie alle Cookies vom Host.

**STEP 13 |** (Optional) Melden Sie sich von Ihrem Computer ab und sehen Sie sich die GlobalProtect-Protokolle an, um die Verbindung für die Voranmeldung zu überprüfen.

## GlobalProtect – Clientloses VPN

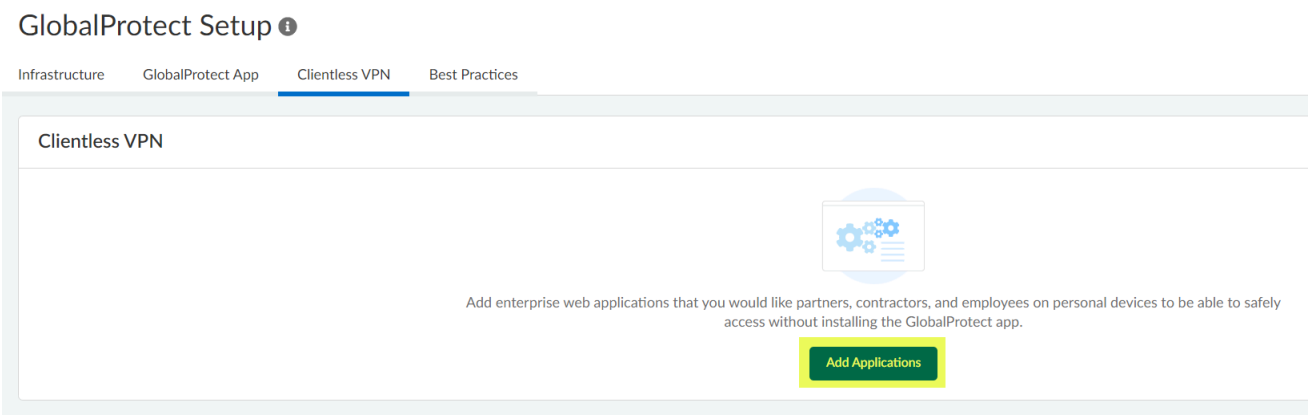
| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Clientloses VPN ermöglicht den sicheren Remote-Zugriff auf Unternehmensanwendungen über SSL-fähige Webbrowser. Mit clientlosem VPN müssen Endbenutzer die GlobalProtect App-Software nicht auf ihren Endpunkten installieren. Dies ist nützlich, wenn Sie Partnern oder Auftragnehmern den Zugriff auf Anwendungen ermöglichen und nicht verwaltete Assets, einschließlich persönlicher Endpunkte, sicher aktivieren müssen.

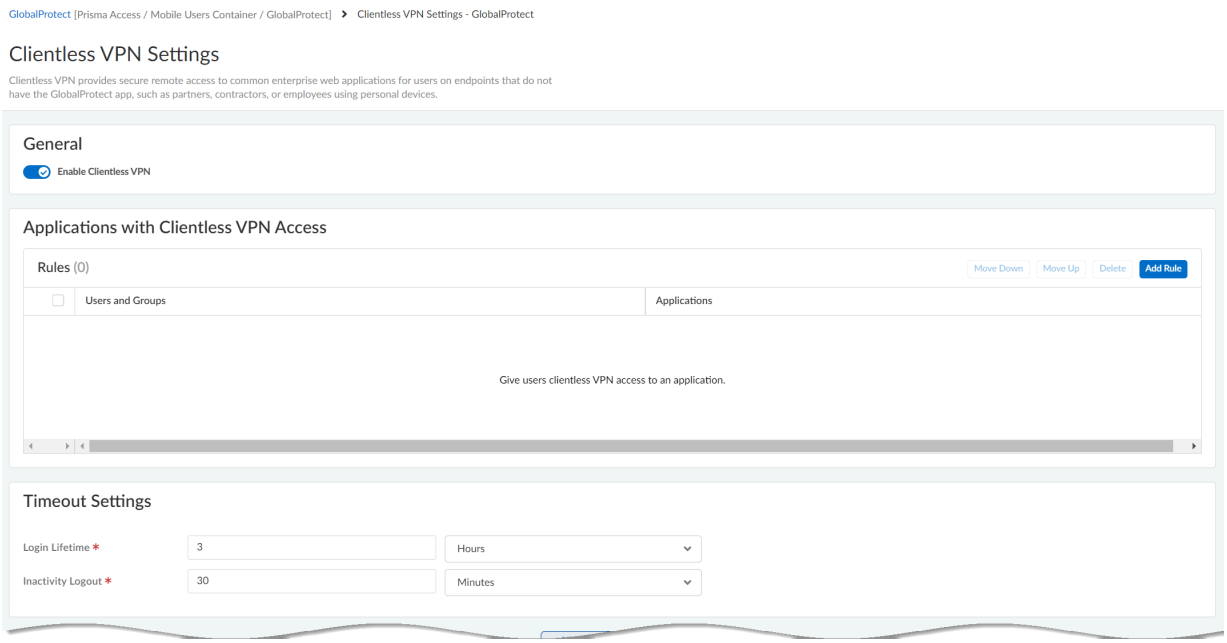
Führen Sie die folgenden Schritte aus, um das clientlose VPN für Prisma Access einzurichten:

 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** Wählen Sie **Einstellungen** > **Prisma Access-Einrichtung** > **GlobalProtect** > **GlobalProtect-Einrichtung** > **Clientloses VPN** und **Anwendungen hinzufügen** aus.




**STEP 2 |** **Clientloses VPN aktivieren.**




**STEP 3 |** Regeln für clientloses VPN hinzufügen.

Geben Sie die Benutzer und Anwendungen an, die clientloses VPN verwenden können.

 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** Wenn Benutzer die Anwendungen über einen Proxyserver erreichen müssen, dann wählen Sie **Proxy hinzufügen** aus.

Es wird nur die einfache Authentifizierung gegenüber dem Proxy unterstützt (Benutzername und Passwort). Sie können mehrere Konfigurationen für Proxyserver hinzufügen, und zwar eine für jede Domänengruppe. Im Folgenden ist eine Auswahl der hinzuzufügenden Einstellungen aufgeführt:

- **Domänen** – Fügen Sie die vom Proxyserver bedienten Domänen hinzu. Sie können ein Platzhalterzeichen (*) am Anfang des Domänennamens verwenden, um mehrere Domänen anzugeben.
- **Proxy aktivieren** – Weisen Sie einen Proxyserver zu, der den Zugriff auf die Domänen ermöglicht.
- **Server** – Geben Sie die IP-Adresse oder den Hostnamen des Proxyservers an.
- **Port** – Geben Sie einen Port für die Kommunikation mit dem Proxyserver an.
- **Benutzer und Passwort** – Geben Sie die Benutzer- und Passwortanmeldeinformationen an, die für die Anmeldung am Proxyserver erforderlich sind. Geben Sie das Passwort zur Überprüfung erneut an.

**STEP 5 |** Ändern Sie die standardmäßigen **Verschlüsselungseinstellungen**, um die Authentifizierungs- und Verschlüsselungsalgorithmen für SSL-Sitzungen zwischen Prisma Access und Anwendungen mit clientlosem VPN anzugeben.

**STEP 6 |** Fügen Sie Domänen zu **Domänen-Ausschlussliste neu schreiben** hinzu.

Das clientlose VPN fungiert als Reverse Proxy und dient zum Ändern von Webseiten, die von den veröffentlichten Webanwendungen zurückgegeben werden. Es schreibt alle URLs um und präsentiert Remote-Benutzern eine neu geschriebene Seite, sodass die Anfragen beim Zugriff auf eine dieser URLs über das GlobalProtect-Portal ausgeführt werden. In einigen Fällen kann die Anwendung über Seiten verfügen, auf die nicht über das Portal zugegriffen werden muss (dies kann zum Beispiel der Fall sein, wenn die Anwendung einen Aktienticker von yahoo.finance.com enthält). Sie können diese Seiten ausschließen. Die Domänen, die Sie zu **Domänen-Ausschlussliste neu schreiben** hinzufügen, sind von den Rewrite-Regeln ausgeschlossen und können nicht neu geschrieben werden. Pfade werden in Domänennamen nicht unterstützt. Das Platzhalterzeichen (*) für Domänennamen kann nur am Anfang des Namens erscheinen (z. B. *.etrade.com).

# GlobalProtect für mobile Benutzer überwachen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

## Prisma Access (Managed by Strata Cloud Manager)

Prisma Access (Managed by Strata Cloud Manager)-Benutzer können die Funktion **Überwachen** > **Benutzer** verwenden. Wählen Sie die verbundene Methode **GlobalProtect** oder **Expliziter**

 ©2025 Palo Alto Networks, Inc.

**Proxy** aus. Die Seite **Mobile Benutzer** bezieht sich eigens auf die von Ihnen verwendete Verbindungsmethode.

## Prisma Access (Managed by Panorama)

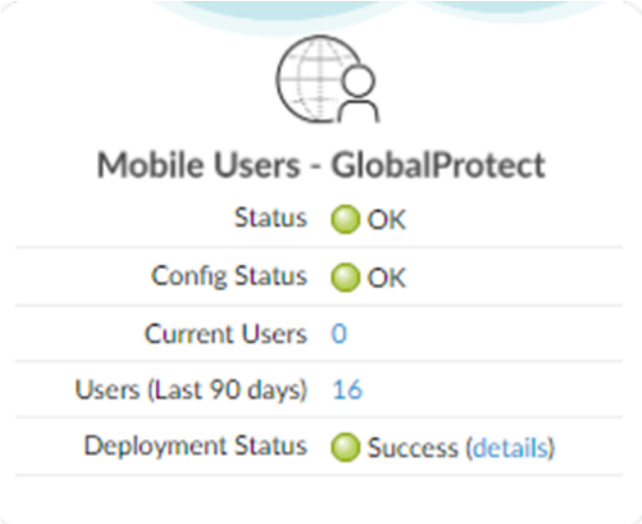
Es gibt mehrere Stellen in Panorama, an denen Sie die Liste der angemeldeten Benutzer anzeigen können. Sie können eindeutige Benutzer, den Standort, an dem die Benutzer angemeldet sind, und Tabellen mit zusätzlichen Informationen anzeigen. Es ist auch wichtig zu verstehen, wie Prisma Access die Anzahl der Benutzer an jedem Standort in einer Bereitstellung des Typs „Mobile Benutzer –GlobalProtect“ ermittelt.

Eine detaillierte Ansicht der Benutzer finden Sie an mehreren Stellen:

- Zum Anzeigen einer Gesamtansicht der Benutzer und zum Öffnen einer Tabelle, in der Sie angemeldete Benutzer anzeigen und abmelden können, wählen Sie **Panorama** > **Cloud Services** > **Status** > **Status** aus.
- Zum Anzeigen einer grafischen Ansicht der Benutzer in einer Kartenansicht und um Benutzer nach Region und Standort anzuzeigen, wählen Sie **Panorama** > **Cloud Services** > **Status** > **Dienststatistiken** > **Mobile Benutzer – GlobalProtect** aus.
- Erfahren Sie außerdem mehr darüber, wie Prisma Access mobile Benutzer zählt.

### GlobalProtect für mobile Benutzer über die Registerkarte „Status“ anzeigen

Um die Gesamtzahl der eindeutigen Benutzer anzuzeigen, die derzeit an allen Standorten angemeldet sind, wählen Sie**Panorama** > **Cloud Services** > **Status** > **Status** > **Mobile Benutzer – GlobalProtect** aus.




Wenn Sie weitere Details zu den aktuell angemeldeten Benutzern anzeigen möchten, klicken Sie auf die Hyperlink-Zahl neben **Aktuelle Benutzer**, um die Tabelle **Aktuelle Benutzer** anzuzeigen.

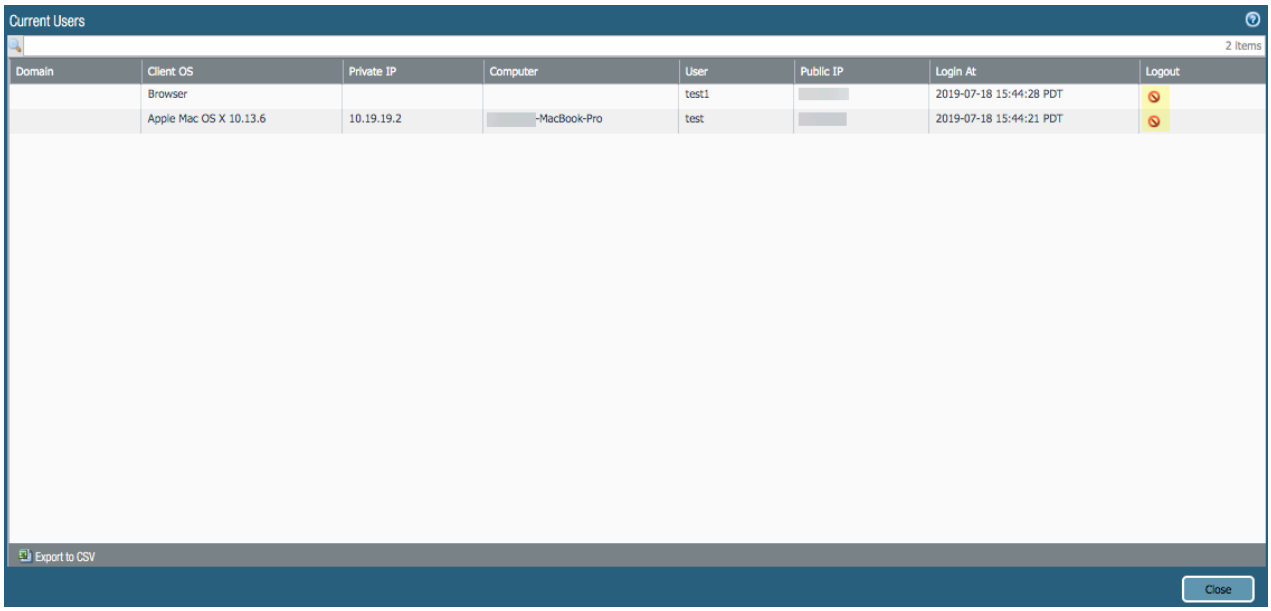
*Die Gesamtzahl der Benutzer, die auf der Statusseite angezeigt wird, kann sich von der Zahl, die in der Popup-Tabelle angezeigt wird, unterscheiden.* Die Zahl, die in der Tabelle angezeigt wird, *ist möglicherweise größer.*

Sie können aktive Benutzer aus der Tabelle **Aktuelle Benutzer** abmelden. Wählen Sie dazu den Benutzer aus und klicken Sie auf **Abmeldung**. Beachten Sie, dass Sie den Bildschirm

 ©2025 Palo Alto Networks, Inc.

möglicherweise schließen und erneut öffnen müssen, damit Prisma Access den abgemeldeten Benutzer von der Seite **Aktuelle Benutzer** entfernt.

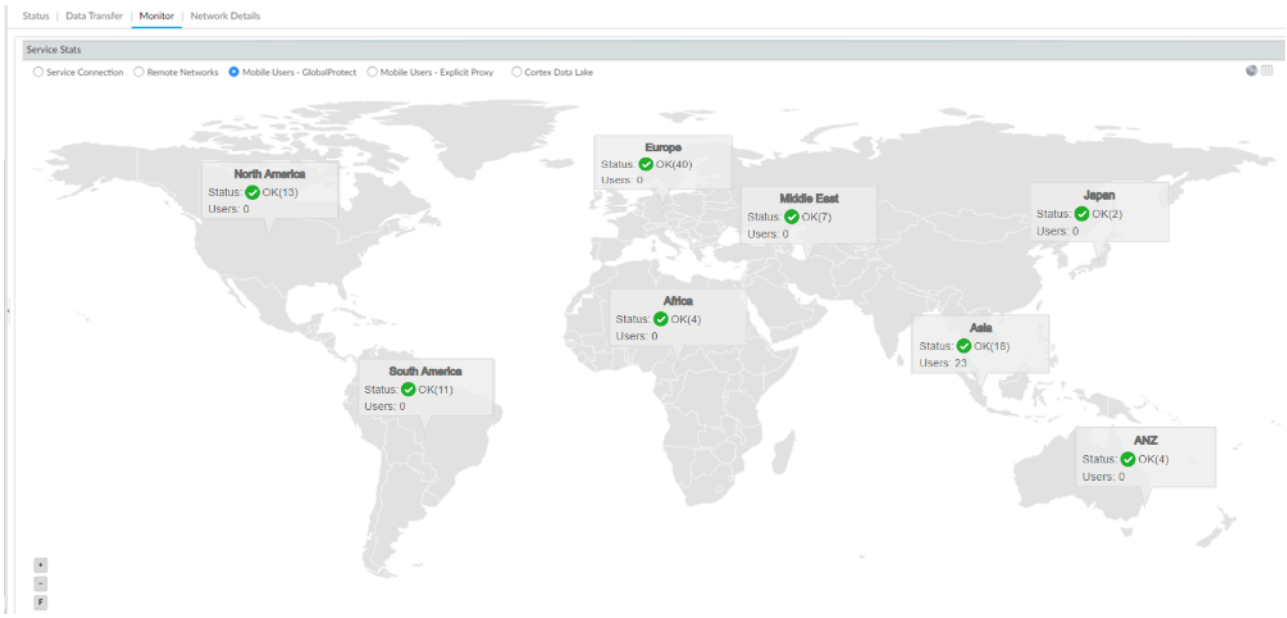
Im folgenden Bildschirm werden Benutzer angezeigt, die sich mit der GlobalProtect-App und mit clientlosem VPN angemeldet haben. Auf dem Bildschirm werden Name, öffentliche IP-Adresse und der Zeitpunkt der letzten Anmeldung des Benutzers angezeigt. Wenn der Benutzer mit der GlobalProtect-App angemeldet ist, werden auch sein Clientbetriebssystem, seine private IP-Adresse und sein Computername angezeigt.




### GlobalProtect für mobile Benutzer über die Registerkarte „Überwachen“ anzeigen

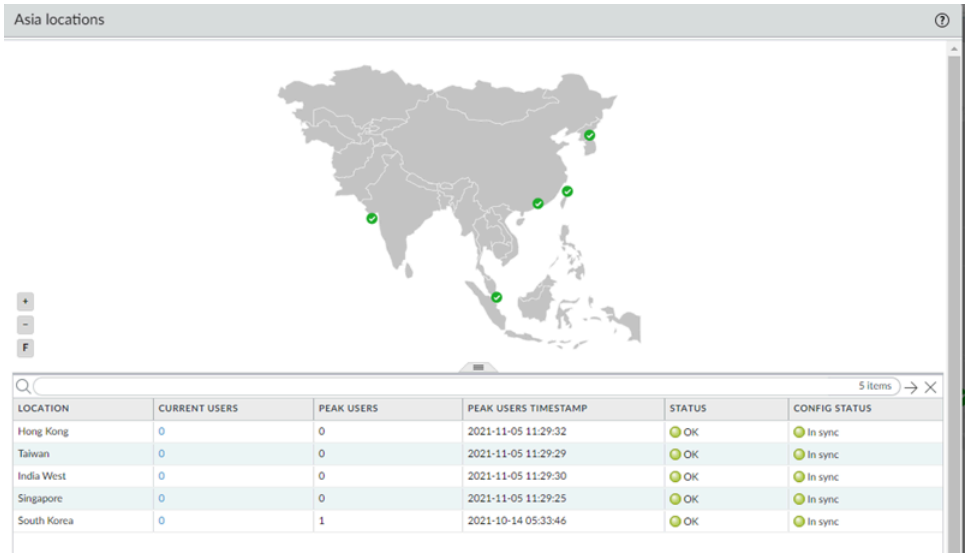
Zum Anzeigen der Anzahl der eindeutigen Benutzer, die pro Region angemeldet sind, wählen Sie **Panorama** > **Cloud Services** > **Status** > **Dienststatistiken** > **Mobile Benutzer – GlobalProtect** aus.

 ©2025 Palo Alto Networks, Inc.




Klicken Sie auf die Region, um Details zu Standorten in einer Region anzuzeigen.

*Die Anzahl der Benutzer, die auf der Seite mit der globalen Kartenansicht angezeigt wird, kann sich von der Anzahl, die in der Tabelle pro Region angezeigt wird, unterscheiden.* Die Anzahl, die in der Tabelle angezeigt wird, *ist möglicherweise größer.*




### Wie Prisma Access mobile Benutzer von GlobalProtect zählt

Die Gesamtzahl der Benutzer, die in den Statusbereichen angezeigt wird, kann von der Zahl abweichen, die in den zugehörigen Tabellen angezeigt wird. Im folgenden Abschnitt werden die Unterschiede beschrieben.

- Registerkarte **Status** ( **Panorama** > **Cloud Services** > **Status** > **Status**) – Die Anzahl der Benutzer, die auf der Hauptseite im Bereich **Mobile Benutzer – GlobalProtect** angezeigt wird, unterscheidet sich möglicherweise von der Anzahl, die in der Tabelle angezeigt wird, wenn Sie auf den Hyperlink **Aktuelle Benutzer** klicken. Die im Bereich **Mobile Benutzer – GlobalProtect** angezeigte Zahl entspricht der Anzahl eindeutiger Benutzer. Die Benutzerliste in der Tabelle

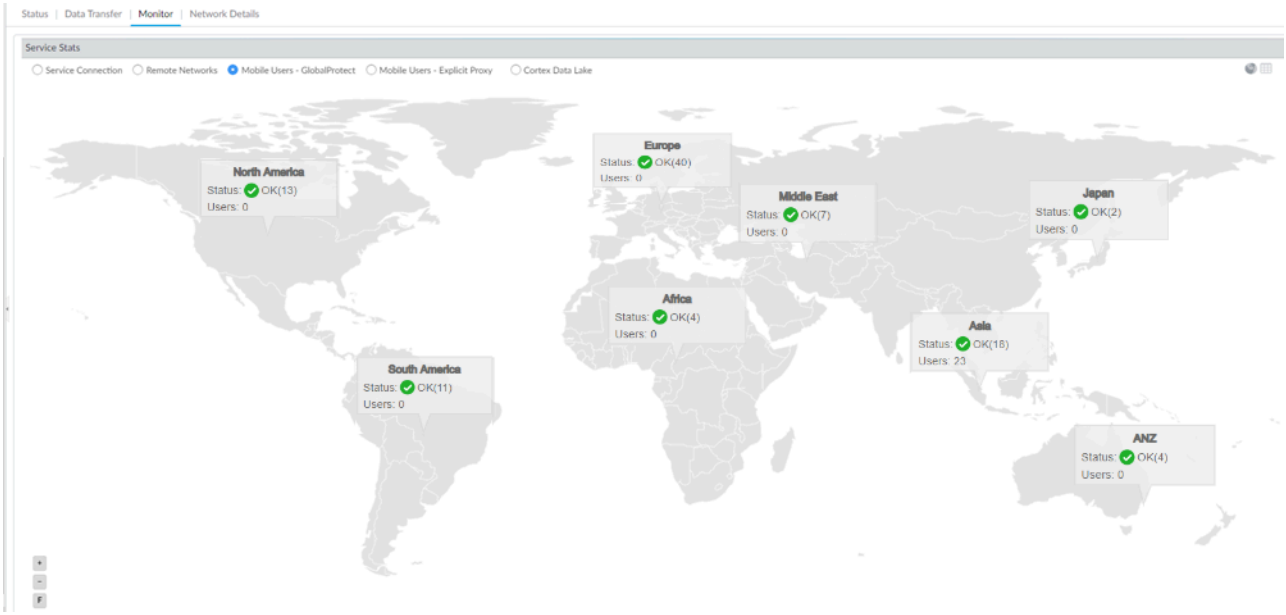
 ©2025 Palo Alto Networks, Inc.

**Aktuelle Benutzer** enthält eine Zählung aller Benutzer pro Anmeldung oder Verbindung. Wenn ein einzelner Benutzer bei mehr als einem Gateway angemeldet ist oder mit mehreren Geräten verbunden ist, kann die Zahl in der Tabelle größer sein.

Beispielsweise kann ein Benutzer **Benutzer1** bei zwei Gateways am Standort **Großbritannien** angemeldet sein. Dieser Zustand kann eintreten, weil Gateways von Prisma Access automatisch hinzugefügt werden, wenn sich eine große Anzahl von Benutzern am selben Standort anmeldet. In diesem Fall zählt Prisma Access **Benutzer1** einmal im Bereich **Mobile Benutzer – GlobalProtect**, aber zweimal in der Tabelle **Aktuelle Benutzer**.

- Registerkarte **Überwachen** ( **Panorama** > **Cloud Services** > **Status** > **, Dienststatistiken** > **Mobile Benutzer – GlobalProtect**) – Die Anzahl der **Benutzer**, die Sie auf der globalen Karte sehen, kann von der Anzahl abweichen, die in der Tabelle angezeigt wird, wenn Sie eine Region auswählen. Ein Benutzer, der bei mehr als einem Gateway angemeldet ist oder mit mehreren Geräten verbunden ist, wird möglicherweise mehrmals in der Tabelle angezeigt.

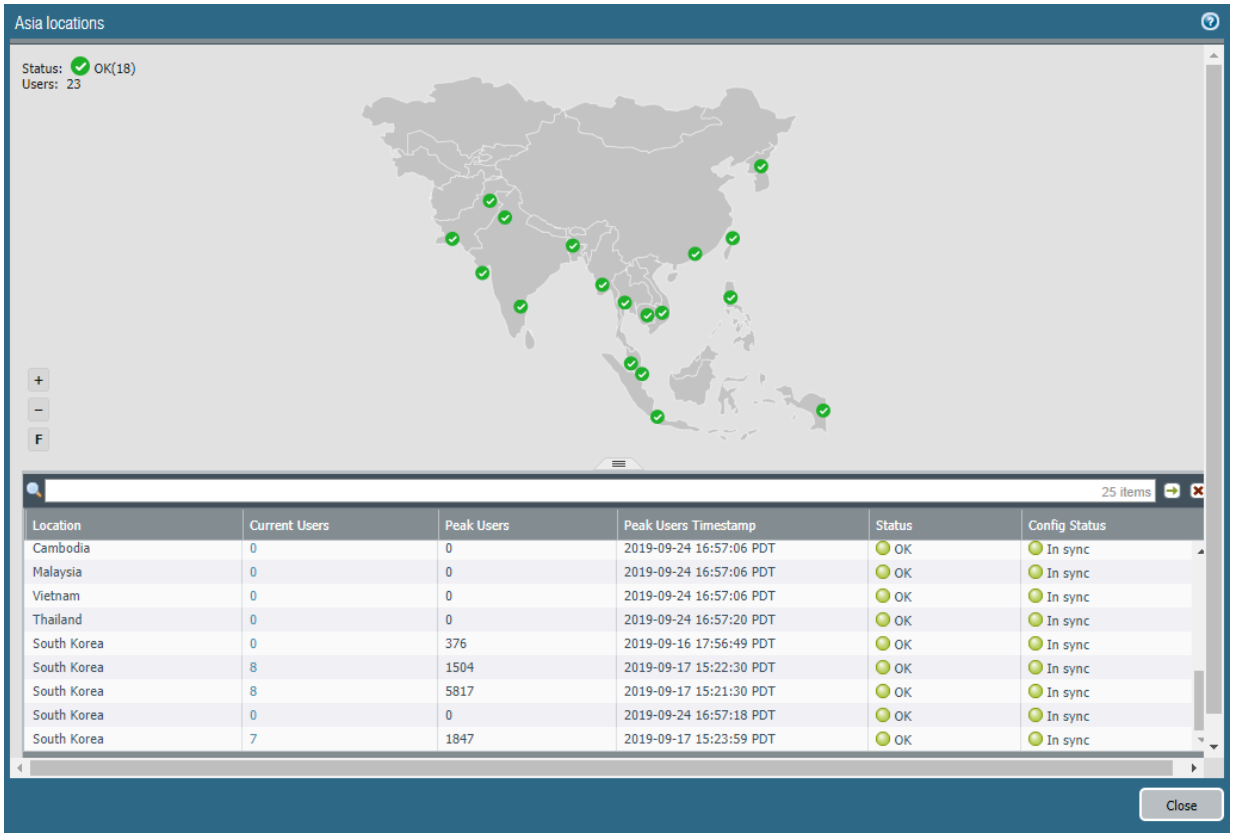
  Die folgenden Screenshots zeigen ein Beispiel. Wie auf der Weltkarte zu sehen, sind in der Region **Asien** 23 eindeutige Benutzer angemeldet.




Wenn Sie die Region **Asien** auswählen, zeigt Prisma Access oben links auf der Regionsseite die Anzahl der eindeutigen Benutzer (23) an. Allerdings sind am Standort **Südkorea** zwei Benutzer über mehrere Geräte verbunden (beispielsweise über ein Smartphone und einen Computer). Da

 ©2025 Palo Alto Networks, Inc.

die Benutzer über zwei getrennte Anschlüsse verfügen, werden sie von Prisma Access zweimal in der Tabelle gezählt, was in der Tabelle zu einer Gesamtzahl von 25 führt.




 ©2025 Palo Alto Networks, Inc.

# IP-Adresspools für eine GlobalProtect-Bereitstellung für mobile Benutzer

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

Stellen Sie sicher, dass Sie einen IP-Adresspool angegeben haben, der für die mobilen Benutzer in Ihrer Organisation ausreichend ist. Sie müssen unbedingt daran denken, dass jeder eindeutige Benutzer mehrere Geräte verwenden kann, mit denen er sich gleichzeitig mit Prisma Access verbinden kann. Dabei benötigt jedes verbundene Gerät eine eindeutige IP-Adresse aus dem Pool. Die Adressen in diesem Pool dürfen sich nicht mit anderen Adresspools überschneiden, die Sie intern verwenden, oder mit dem IP-Subnetz, das Sie beim Aktivieren der Dienstinfrastruktur zuweisen.

Es wird empfohlen, dass die Anzahl der IP-Adressen im Pool das Zweifache der Anzahl der mobilen Benutzergeräte beträgt, die eine Verbindung zu Prisma Access herstellen. Wenn Ihre Organisation über eine Bring Your Own Device(BYOD)-Richtlinie verfügt oder ein einzelner Benutzer mehrere Benutzerkonten hat, stellen Sie sicher, dass Sie diese zusätzlichen Geräte und Konten bei der Zuweisung Ihrer IP-Pools berücksichtigen. Wenn Ihr Poolspeicherplatz begrenzt ist, können Sie einen kleineren Adresspool angeben. Wenn Ihr IP-Adresspool jedoch seine Grenze erreicht, können keine weiteren mobilen Benutzergeräte Verbindungen herstellen.

Die Benutzeroberfläche prüft, ob Sie gültige IP-Subnetze eingeben (wenn Sie beispielsweise einen Pool mit einem Subnetz von weniger als /23 eingeben, werden Sie aufgefordert, diesen zu ändern). Es wird jedoch nicht überprüft, ob Sie ausreichend IP-Adressen für Ihre Bereitstellung zugewiesen haben.

*Diese Validierung ist nicht verfügbar, wenn Sie Standorte mithilfe der CLI konfigurieren. Wenn Sie alle Standorte mithilfe der CLI bereitstellen, empfehlen wir Ihnen, eine /18-Adresse im weltweiten Pool für mobile Benutzer hinzuzufügen.*

Prisma Access überprüft Ihre Konfiguration, um sicherzustellen, dass Sie den folgenden Mindestpool für IP-Adressen angegeben haben:

- Ein Minimum von /23 (512 IP-Adressen) ist für einen weltweiten oder regionalen Adresspool erforderlich.
- Wenn ein vorhandener Standort in einen Compute-Standort konvertiert wird, benötigt dieser Standort nach der Konvertierung mindestens ein /23-Subnetz.
- Wenn Sie in einer Region keine Prisma Access-Gateways einbinden, ist für diese Region kein IP-Adresspool erforderlich. Wenn Sie beispielsweise Gateways in den Standorten „USA (Ost)“, „USA (Nordwest)“ und „USA (Nordost)“ angeben, müssen Sie nur einen IP-Adresspool für die Region „Nordamerika und Südamerika“ angeben. Wenn Sie hingegen Standorte mit mobilen Benutzern in Europa aktivieren, ohne einen weltweiten Adresspool oder einen IP-Adresspool in Afrika, Europa und dem Nahen Osten anzugeben, schlägt Ihre Bereitstellung fehl.

 ©2025 Palo Alto Networks, Inc.

- Mobile Benutzer von GlobalProtect verwenden zuerst die IP-Adressen in der Standortgruppe, dann die schauplatzspezifischen IP-Adressen und dann die weltweiten IP-Adressen. Wenn Sie beispielsweise einen Pool für eine Standortgruppe und „Weltweit“ angeben und dann die verfügbaren IP-Adressen im Pool der Standortgruppe aufgebraucht sind, verwendet Prisma Access für diese Standortgruppe IP-Adressen aus dem Pool **Weltweit**.

  Wenn Sie mehr als einen Block von IP-Adresspools angeben, verwendet Prisma Access die Pools in der Reihenfolge, in der Sie sie bei der Einrichtung mobiler Benutzer eingegeben haben.

## Statische IP-Adressenzuweisung für Bereitstellungen von „Mobile Benutzer – GlobalProtect“

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | • Prisma Access-Version 5.2.1<br>• PAN-OS-Dataplane-Version 11.2.4<br>umfasst Unterstützung für Activity Insights, Benutzergruppen und Standortgruppen<br>• GlobalProtect-Version 6.1.4<br>*Dies ist ein Release mit begrenzter Verfügbarkeit. Um diese Funktionalität zu aktivieren, wenden Sie sich nach Aktivierung des Mandanten an Ihren Palo Alto Networks-Kundenberater.* |

Einige Legacy-Netzwerke verwenden auf IP-Adressen basierende Autorisierung, um den Zugriff der Benutzer auf interne oder externe Ressourcen einzuschränken. Eine Prisma Access-Bereitstellung des Typs „Mobile Benutzer – GlobalProtect“ weist Benutzern eine IP-Adresse aus dem IP-Adresspool für mobile Benutzer zu, den Sie während des Onboardings zuweisen. Diese Zuordnung von Benutzern zu IP-Adressen kann sich bei nachfolgenden Anmeldungen ändern. Um die Zuordnung von Benutzern zu IP-Adressen beizubehalten, können Sie in Prisma Access Benutzern statische IP-Adressen zuweisen.

*Diese Funktionalität ist nur für neue Prisma Access-Bereitstellungen verfügbar.*

Zum Erstellen eines IP-Pool-Profils verwenden Sie eines oder mehrere dieser Kriterien:

- **Schauplatz** – Weisen Sie IP-Adressen basierend auf dem Schauplatz zu, in dem sich Ihre Benutzer befinden. Sie können beispielsweise ein /30-Subnetz für einen bestimmten Schauplatz erstellen. Diese IP-Adressen sind für diesen Schauplatz statisch. Sie können den Zugriff auf Ressourcen basierend auf dem Schauplatz anwenden, indem Sie Sicherheitsrichtlinienregeln mithilfe der IP-Adressen erstellen, die Sie für diesen Schauplatz angeben.
- **Benutzer** – Weisen Sie IP-Adressen basierend auf einer Benutzer-ID zu, indem Sie eine /30- oder /32-Adresse im IP-Adresspool für mobile Benutzer konfigurieren und anhand

 ©2025 Palo Alto Networks, Inc.

von Übereinstimmungskriterien diesen Benutzer mit einer IP-Adresse verknüpfen. Auf diese Weise können Sie eine statische IP-Adresse zuweisen, die Prisma Access für einen bestimmten Benutzer beibehält, sodass Sie Ihre aktuellen, auf IP-Adressen basierenden Sicherheitsrichtlinienregeln beibehalten können, um den Zugriff eines Benutzers auf Ressourcen zu steuern.

- **Benutzergruppe** – Weisen Sie IP-Adressen basierend auf der Benutzergruppe zu. Der Benutzer erhält die IP-Adresse aus dem definierten IP-Pool-Subnetz, wenn er Teil der konfigurierten Benutzergruppe ist.
- **Standortgruppe** – Weisen Sie IP-Adressen basierend auf der im IP-Pool-Profil definierten Standortgruppe zu.

Verwenden Sie bei der Zuweisung statischer IP-Adressen die folgenden Richtlinien:

- Wenn Sie mehrere IP-Pools angeben, wertet Prisma Access die Regeln von oben nach unten aus und weist IP-Adressen basierend auf der ersten Übereinstimmung in der Liste der Regeln zu.
- Integrieren Sie Ihre Prisma Access-Bereitstellung in die Cloud Identity Engine, wenn Sie die Benutzer-ID oder die Benutzergruppe als Kriterien für den Abgleich von IP-Pools verwenden möchten.
- Pro Mandant werden folgende Höchstzuweisungen unterstützt:
  - 20.000 Benutzer
  - 5.000 Benutzergruppen mit 50.000 Benutzern pro Benutzergruppe
  - 10.000 IP-Adresspool-Profile
  - 10.000 IP-Adresspools
- Geben Sie eine Präfixlänge zwischen /23 und /32 ein.
- Für jedes **Client-IP-Pool**-Profil für mobile Benutzer gilt Folgendes:
  - Es werden bis zu 10 IP-Präfixe unterstützt.
  - Es werden bis zu 256 Benutzer unterstützt.
- Bei der statischen IP-Adressierung wird eine **Leasingzeit** und eine **Karenzzeit** verwendet, um festzulegen, wie lange Prisma Access eine Zuordnung von Benutzern zu IP-Adressen beibehält.
  - Die **Leasingzeit** gibt an, wie lange die Zuordnung zwischen Benutzer und IP-Adresse nach der Zuweisung gültig ist.

    Die Standard-Leasingzeit beträgt 86.400 Sekunden (24 Stunden).

    Die Mindest-Leasingzeit beträgt 3.600 Sekunden (1 Stunde).

    Die maximale Leasingzeit beträgt 7.776.000 Sekunden (90 Tage).
  - Die **Karenzzeit** gibt an, wie lange Prisma Access nach Ablauf einer Leasingzeit die Zuordnung zwischen Benutzer und IP-Adresse beibehält, bevor die IP-Adresse einem anderen Benutzer zugewiesen wird.

    Die Standard-Karenzzeit beträgt 14.400 Sekunden (4 Stunden).

    Die Mindest-Karenzzeit beträgt 60 Sekunden.

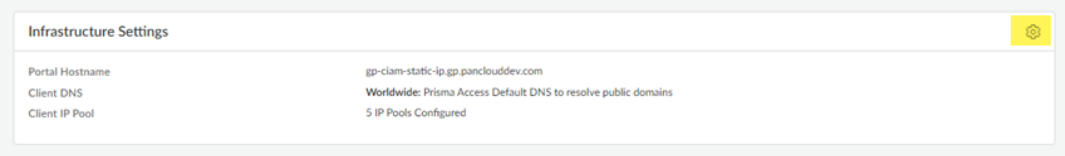
    Die maximale Karenzzeit beträgt 7.776.000 Sekunden (90 Tage).

 ©2025 Palo Alto Networks, Inc.

### Statische IP-Adresszuweisung konfigurieren

Gehen Sie wie folgt vor, um eine statische IP-Adresszuweisung in einer Bereitstellung zu konfigurieren.

**STEP 1 |** Gehen Sie zu **Workflows** > **Einrichtung Prisma Access** > **GlobalProtect** und klicken Sie auf das Zahnrad, um die **Infrastruktureinstellungen** hervorzuheben.




**STEP 2 |** Klicken Sie im Bereich „Client-IP-Pool“ auf die Schaltfläche **IP-Pool hinzufügen**, um einen IP-Pool für die statischen IP-Adressen hinzuzufügen.

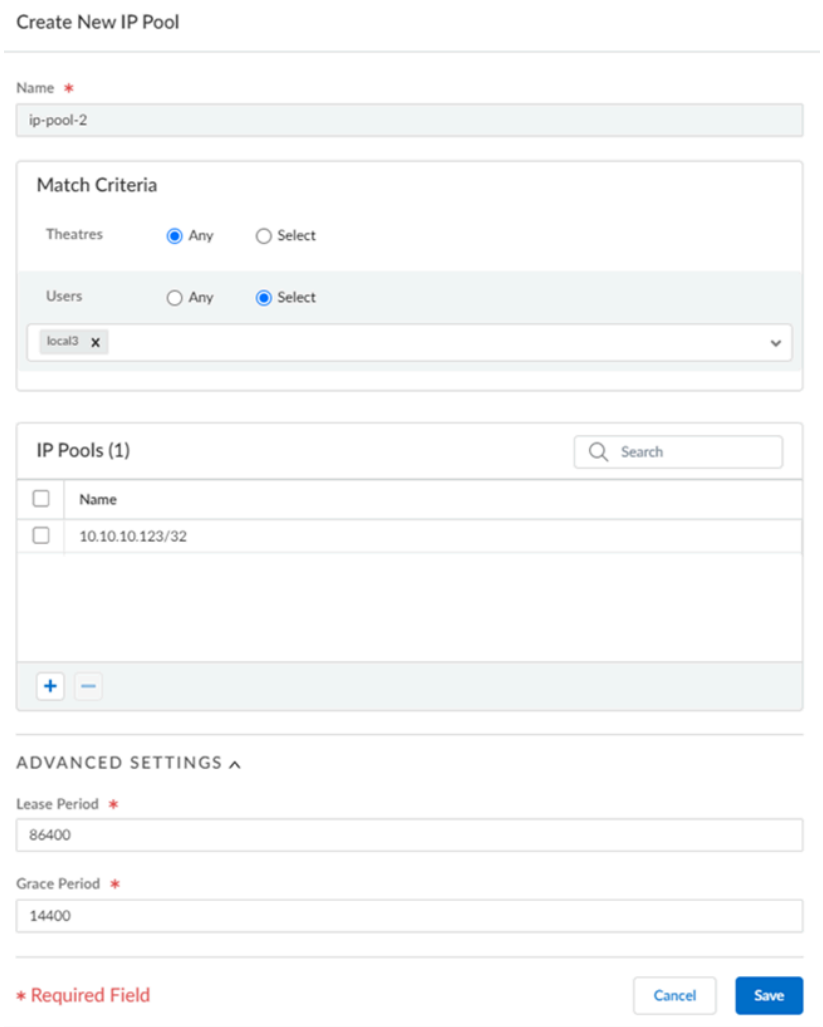
 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Weisen Sie einem Schauplatz, einer Prisma Access-Standortgruppe oder einem Benutzer eine statische IP-Adresse zu.

1. Geben Sie dem IP-Adresspool einen eindeutigen **Namen**.
2. **Wählen** Sie mindestens einen **Schauplatz** aus, in dem die Verwendung des Pools zugelassen werden soll, oder wählen Sie **Beliebige** aus, damit der Pool in allen Schauplätzen verwendet werden kann.
3. **Wählen** Sie eine oder mehrere der **Prisma Access-Standortgruppen** aus, um die Verwendung des Pools in dieser Standortgruppe zu ermöglichen, oder wählen Sie **Beliebige** aus, um die Verwendung des Pools in allen Standortgruppen zu ermöglichen.
4. **Wählen** Sie einen Benutzer oder eine Benutzergruppe aus, oder wählen Sie **Beliebige** aus, um die Verwendung des Pools für einen Benutzer oder eine Benutzergruppe zu ermöglichen.
   - Um einem IP-Adresspool einen oder mehrere Benutzer zuzuweisen, wählen Sie den Benutzer auf der Registerkarte **Benutzer** aus.
   - Um einem IP-Adresspool eine oder mehrere Benutzergruppen zuzuweisen, wählen Sie den Benutzer auf der Registerkarte **Benutzergruppen** aus.
5. Geben Sie im Bereich **IP-Pools** einen IP-Adresspool ein.

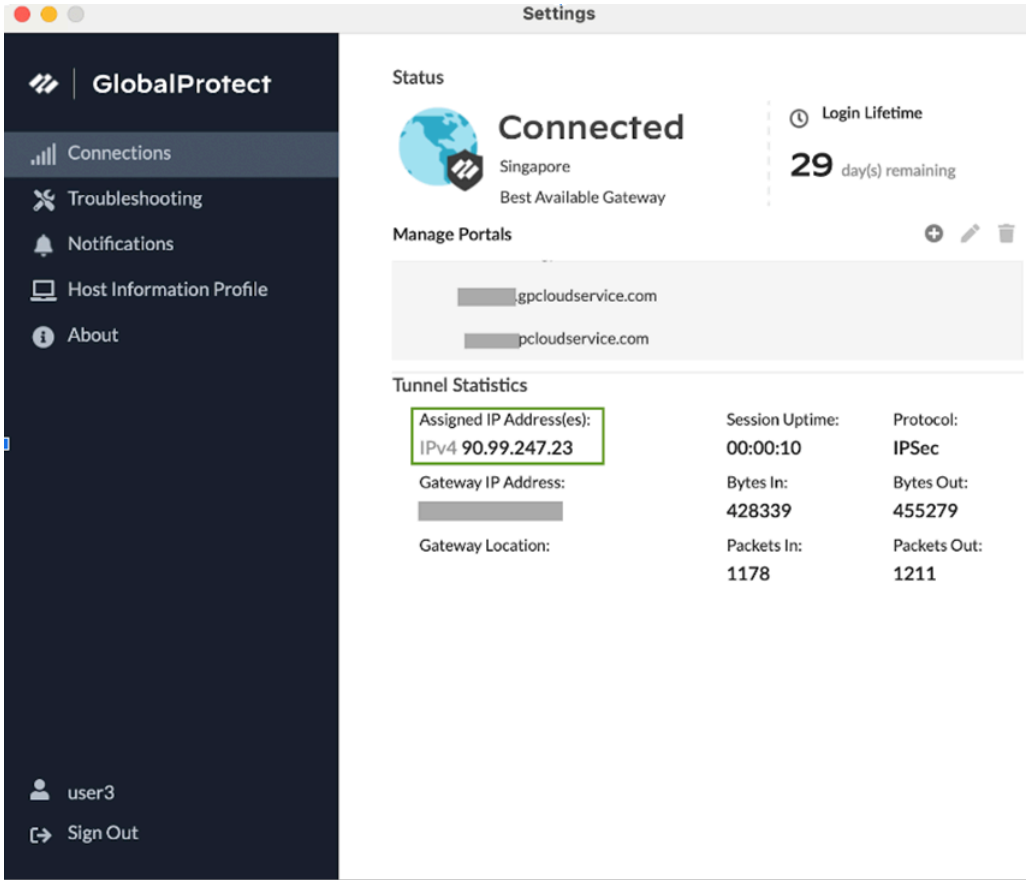
   *Um einen Benutzer auf eine einzige IP-Adresse zu beschränken, geben Sie eine /30- oder /32-IP-Adresse an. Prisma Access weist den Benutzer dieser Adresse zu. Da /32 nur eine IP-Adresse bereitstellen würde, empfehlen wir ein minimales Subnetz von /30 und die Beschränkung des Benutzers auf dieses Subnetz.*
6. (Optional) Geben Sie eine **Leasingzeit** und eine **Karenzzeit** für die Zuordnung von Benutzern zu IP-Adressen ein.
7. **Speichern** Sie Ihre Änderungen.

 ©2025 Palo Alto Networks, Inc.




 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** Überprüfen Sie Ihre Änderungen, indem Sie auf dem Client-Computer unter **GlobalProtect** > **Einstellungen** die **Tunnelstatistik** ansehen und die **zugewiesene(n) IP-Adresse(n)** überprüfen.




# Wie die GlobalProtect-App Prisma Access-Standorte für mobile Benutzer auswählt

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

Wenn sich ein mobiler Benutzer mit einem Prisma Access-Standort verbindet, ermittelt die App anhand des folgenden Auswahlverfahrens, mit welchem Standort sie sich verbindet.

*Sie aktivieren die Standorte mobiler Benutzer, an denen Prisma Access beim Onboarding mobiler Benutzer vorhanden sein soll. Wenn Sie den Standort während des Onboardings nicht auswählen, verwendet Prisma Access ihn nicht in Ihrer Bereitstellung.*

- Wenn der mobile Benutzer eine Verbindung in einem Land herstellt, das über einen Prisma Access-Standort verfügt, wird der Benutzer mit dem Standort in diesem Land verbunden.

 ©2025 Palo Alto Networks, Inc.

- Wenn der mobile Benutzer aus irgendeinem Grund keine Verbindung zu einem Standort im Land herstellen kann, wählt Prisma Access einen der folgenden mobilen Benutzerstandorte aus, um den Benutzer basierend auf der Region zu verbinden.
  - **Asien, Australien und Japan**: Hongkong, Japan (zentral) oder Japan (Süd)
  - **Afrika, Europa und Naher Osten**: Niederlande (Mitte)
  - **Nordamerika und Südamerika** USA (Nordwest)

  Palo Alto Networks empfiehlt, dass Sie mindestens einen dieser Standorte in ihrer jeweiligen Region beim Onboarding mobiler Benutzer aktivieren, um Redundanz bereitzustellen. Wenn mobile Benutzer vorhanden sind, die sich mit Prisma Access aus einem Land verbinden, das keinen Prisma Access-Standort hat, müssen Sie mindestens einen der Fallback-Standorte in der vorherigen Liste aktivieren.

  Die Standorte Hongkong, Japan (zentral), Japan (Süd), Niederlande (zentral) und USA (Nordwest) können Clientverbindungen von überall akzeptieren und werden als *globale Fallback-Standorte* bezeichnet. Zusätzlich zu diesen Standorten können Sie einen oder mehrere der folgenden Standorte aktivieren, die ebenfalls die Funktion globaler Fallback-Standorte übernehmen:
  - Bahrain
  - Frankreich (Nord)
  - Irland
  - Südafrika (West)
  - Südkorea
- Palo Alto Networks empfiehlt, Standorte an mehr als einem Compute-Standort zu Redundanzzwecken zu aktivieren.
- Wenn Sie lokale Gateways mit Prisma Access-Standorten verwenden, können Sie in Prisma Access Prioritäten angeben, damit mobile Benutzer entweder eine Verbindung mit einem bestimmten lokalen GlobalProtect-Gateway oder einem Prisma Access-Standort herstellen können. Weitere Informationen finden Sie unter Prioritäten für Prisma Access und lokale Gateways verwalten.
- Wenn mobile Benutzer eine Verbindung herstellen, verwendet die GlobalProtect-App im automatischen Gateway-Auswahlprozess nicht die folgenden Prisma Access-Standorte, selbst wenn Sie die Prisma Access-Standorte beim Onboarding im Plug-in ausgewählt haben. Mobile Benutzer können jedoch weiterhin manuell einen dieser Standorte auswählen und als bevorzugten Standort (Gateway) festlegen, solange Sie ihnen beim Onboarding mobiler Benutzer erlauben, diese Standorte manuell auszuwählen:
  - Australien: Australien (Ost)
  - Brasilien: Brasilien (Ost) und Brasilien (zentral)
  - Frankreich Frankreich (Süd)
  - Deutschland: Deutschland (Nord) und Deutschland (Süd)
  - Indien: Indien (Süd)
  - Mexiko: Mexiko (West)
  - Niederlande: Niederlande (Süd)

 ©2025 Palo Alto Networks, Inc.

- Pakistan: Pakistan (West)
- Russland: Russland (Nordwest)
- Spanien: Spanien (Ost)

*Möglicherweise müssen Sie Ihre **Verbindungsmethode** in **On-Demand** ändern, damit der mobile Benutzer manuell eine Verbindung zu einem Gateway herstellen kann.*

# Zulassungslisten mobiler GlobalProtect-Benutzer erstellen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz<br>❑ Minimum Required Prisma Access Version: 3.0 Bevorzugt |

Erfahren Sie, wie die Ausgangs-IP-Zulassungslisten für die vorhandenen mobilen Benutzer aktiviert werden.

Damit Sie die öffentlichen (Ausgangs-)IP-Adressen für Ihre GlobalProtect-Bereitstellung für mobile Benutzer zu allen Zulassungslisten Ihrer SaaS-Anwendungen hinzufügen können, die Sie in Ihrer Organisation verwenden, stellt Prisma Access die IP-Adressen zur Verfügung. Sie können überprüfen, ob Sie sie zu den Zulassungslisten hinzugefügt haben, bevor Sie sie in Ihrer Umgebung einsetzen. Wenn Sie Zulassungslisten für Ausgangs-IP-Adressen für vorhandene Prisma Access-Bereitstellungen aktivieren, migriert Prisma Access alle bereits zugewiesenen Ausgangs-IP-Adressen für Ihre Standorte in die Zulassungslisten für Ausgangs-IP-Adressen. Aktivieren Sie für neue Prisma Access-Bereitstellungen die Zulassungsliste für Ausgangs-IP-Adressen beim Onboarding der mobilen GlobalProtect-Benutzer.

Nachdem Sie die Ausgangs-IP-Adressen zu den Zulassungslisten Ihrer Organisation hinzugefügt haben, kehren Sie zur Prisma Access-Benutzeroberfläche zurück, bestätigen die GlobalProtect-Ausgangs-IP-Adressen als zulässig und führen die Aktion **Push** aus, um Ihre Änderungen zu übertragen. Prisma Access gibt diese Ausgangs-IP-Adressen dann frei und fügt sie Ihrer Bereitstellung hinzu. Wenn Prisma Access nach der Erstkonfiguration infolge eines Autoskalierungsereignisses weitere IP-Adressen hinzufügt, bestätigen Sie, dass die neuen Ausgangs-IP-Adressen hinzugefügt wurden, bevor Prisma Access sie Ihrer Bereitstellung hinzufügt.

Sobald die IP-Adressen aktiviert wurden, werden in der Tabelle für die IP-Zulassungslisten Informationen zu den IP-Adressen angezeigt, die bestätigt wurden oder noch zu bestätigen sind. Des Weiteren wird auch ihr Bereitstellungsstatus aufgelistet.

- Strata Cloud Manager
- Panorama

## Zulassungslisten mobiler GlobalProtect-Benutzer erstellen (Strata Cloud Manager)

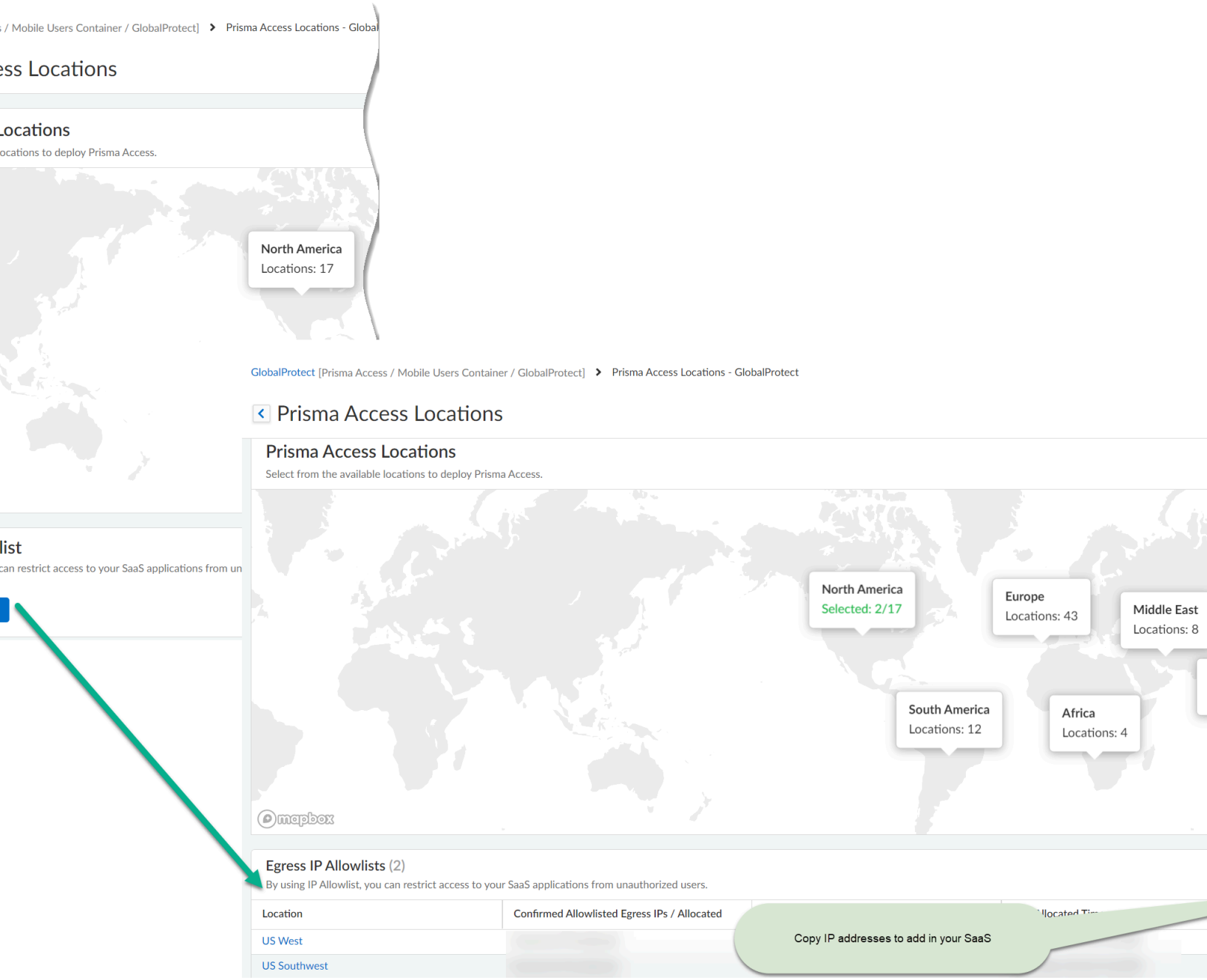
Aktivieren Sie Prisma Access, um die Ausgangs-IP-Adressen für den Prisma Access-Datenverkehr anzuzeigen. Verwenden Sie diese IP-Adressen in den IP-Zulassungslisten für Ihre SaaS-Anwendungen, in denen Sie die Nutzung auf autorisierte Benutzer oder Quellen beschränken.

 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** Wählen Sie **Workflows** > **Prisma Access-Einrichtung** > **GlobalProtect** > **Infrastruktur** aus und bearbeiten Sie die Einstellungen für die **Prisma Access-Standorte**.

**STEP 2 |** Zeigen Sie die IP-Adressen für Prisma Access-Standorte an.

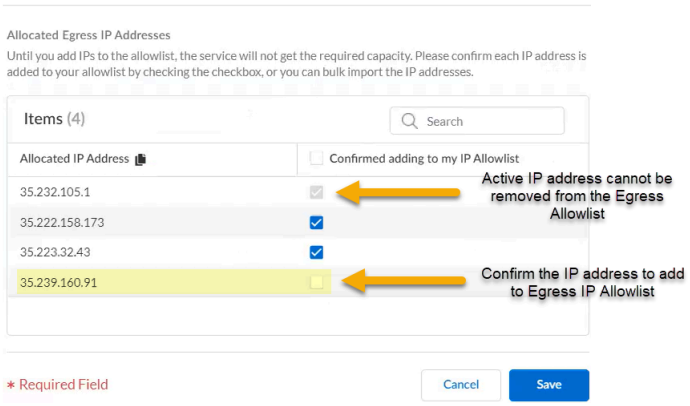
1. **Aktivieren** Sie die Ausgangs-IP-Zulassungsliste, um die IP-Adressen für eingebundene Prisma Access-Standorte anzuzeigen.
2. Kopieren Sie die zugewiesenen IP-Adressen und fügen Sie sie den Zulassungslisten Ihrer SaaS-Anwendungen hinzu.
3. Wählen Sie **Migrieren** aus, um die IP-Adressen zu bestätigen, die den eingebundenen Standorten in Prisma Access zugewiesen wurden.




 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Rufen Sie die IP-Adressen für neue eingebundene Standorte oder während eines Ereignisses mit automatischer Skalierung ab.

1. Wählen Sie den **Standort**namen aus, um die dem Standort zugewiesenen neuen Ausgangs-IP-Adressen zu suchen.
2. Wählen Sie **Erweiterung meiner IP-Zulassungsliste bestätigt** aus, um diese IP-Adressen zu den Zulassungslisten für Ihre SaaS-Anwendungen hinzuzufügen, bevor Sie sie in Prisma Access bestätigen.




Wenn Sie über IPv6-Adressen verfügen, wählen Sie **Erweiterung meiner IPv6-Zulassungsliste bestätigt** aus.




**STEP 4 |** Übertragen Sie Ihre Änderungen mit einer Push-Aktion an Prisma Access.

### Status zugewiesener Ausgangs-IP-Adressen

Die Statusspalte in den Ausgangs-IP-Zulassungslisten gibt an, ob alle zugewiesenen IP-Adressen für die Standorte für Ihre Bereitstellung bereitgestellt werden. Lesen Sie weiter, um mehr über jeden Status zu erfahren.

- **Bereitgestellt** – Sie haben die Ausgangs-IP-Adressen zu den Zulassungslisten Ihrer SaaS-Anwendungen hinzugefügt, die IP-Adressen in Prisma Access bestätigt und Ihre Änderungen mit einer Push-Aktion übertragen, um sie vollständig bereitzustellen.

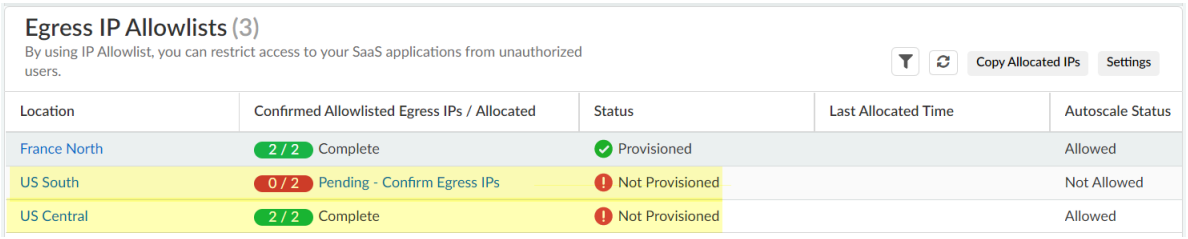
- **Teilweise bereitgestellt** – Sie haben den ersten Satz von Ausgangs-IP-Adressen hinzugefügt, diese in Prisma Access bestätigt und Ihre Änderungen mit einer Push-Aktion übertragen. Prisma Access hat jedoch einen weiteren Satz von IP-Adressen als Teil eines Autoskalierungsereignisses hinzugefügt und diese IP-Adressen sind in Prisma Access nicht bestätigt.

- **Nicht bereitgestellt** – Prisma Access hat IP-Adressen für den Standort zugewiesen und Sie haben die Ausgangs-IP-Adressen zu den Zulassungslisten Ihrer SaaS-Anwendungen hinzugefügt und in Prisma Access bestätigt, diesen Standort jedoch noch nicht eingebunden.

 ©2025 Palo Alto Networks, Inc.

- **Kann nicht bereitgestellt werden** – Sie haben diesen Standort eingebunden, jedoch in Prisma Access noch nicht bestätigt und Ihre Änderungen noch nicht mit einer Push-Aktion übertragen.

In der Tabelle mit den Ausgangs-IP-Zulassungslisten wird auch die Anzahl der IP-Adressen angegeben, die in Prisma Access bereits bestätigt wurden und noch bestätigt werden müssen. Beispielsweise bedeutet 1/2, dass 1 von 2 IP-Adressen, die für den Standort vergeben wurden, in Prisma Access bereits bestätigt wurde.




## Zulassungslisten mobiler GlobalProtect-Benutzer erstellen (Panorama)

Damit Sie die öffentlichen (Ausgangs-)IP-Adressen für Ihre Bereitstellung für mobile GlobalProtect-Benutzer zu allen Zulassungslisten Ihrer SaaS-Anwendungen hinzufügen können, die Sie in Ihrer Organisation verwenden, stellt Prisma Access die IP-Adressen zur Verfügung und ermöglicht es Ihnen, zu überprüfen, ob Sie sie zu Ihrer Zulassungsliste hinzugefügt haben, bevor Sie sie in Ihrer Umgebung verwenden.

Diese Methode der Vergabe von Ausgangs-IP-Adressen hat folgende Vorteile:

- Es wird sichergestellt, dass Prisma Access nur IP-Adressen bereitstellt, die Sie in Ihre Zulassungsliste aufgenommen haben.
- Es wird verhindert, dass mobile Benutzer versuchen, über eine IP-Adresse eine Verbindung zu Prisma Access herzustellen, die für das Netzwerk Ihres Unternehmens blockiert wurde. Prisma Access gibt IP-Adressen erst dann für Ihre Bereitstellung frei, wenn sie von Ihnen in die Zulassungsliste aufgenommen wurden.
- Es wird die Möglichkeit geboten, Ihre aktuellen Ausgangs-IP-Adressen abzurufen, ohne die API zu verwenden.

Prisma Access vergibt Ausgangs-IP-Adressen in folgenden Situationen:

- Beim Onboarding Ihrer Standorte während der Einbindung mobiler Benutzer.

  Prisma Access weist jedem Standort, der eingebunden wird, zwei Gateway-IP-Adressen zu.

  *Wenn Sie einen Standort einbinden und an anderen Standorten am selben Compute-Standort ein Autoskalierungsereignis auftritt, weist Prisma Access möglicherweise mehr als zwei IP-Adressen für den neuen Standort zu. Vergewissern Sie sich in diesem Fall, dass alle diese IP-Adressen zu Ihren Zulassungslisten hinzugefügt wurden, und bestätigen Sie, dass für alle Adressen die Angabe* ***Zu meiner Zulassungsliste hinzugefügt*** *festgelegt wurde.*

 ©2025 Palo Alto Networks, Inc.

- Während eines großen Skalierungsereignisses.

  Übersteigt die Anzahl der mobilen Benutzer die Kapazität der beiden vorab zugewiesenen IP-Adressen, weist Prisma Access einen weiteren Satz aus zwei IP-Adressen zu.

  Autoskalierungsereignisse betreffen alle eingebundenen Standorte an einem Compute-Standort. Wenn ein Autoskalierungsereignis für einen Standort auftritt und Sie noch nicht bestätigt haben, dass die Adressen zu Ihren Zulassungslisten hinzugefügt wurden, wird an allen Standorten an diesem Compute-Standort der **Autoskalierungsstatus Nicht zulässig** angezeigt.

  *Der **Autoskalierungsstatus** zeigt den Status der Autoskalierung in Prisma Access an.*

  - ***Zulässig** – Sie haben IP-Adressen zu den Zulassungslisten hinzugefügt. Wenn sich eine große Anzahl mobiler Benutzer an einem einzigen Standort anmeldet und ein Autoskalierungsereignis auslöst, verwendet Prisma Access die in der Zulassungsliste enthaltenen IP-Adressen für das Autoskalierungsereignis.*
  - ***Nicht zulässig** – Sie haben nicht alle IP-Adressen in der Prisma Access-Benutzeroberfläche als zu Ihren Zulassungslisten hinzugefügt angegeben oder Sie haben Ihre Änderungen nicht mit Commit und Push festgeschrieben und übertragen, nachdem Sie sie als hinzugefügt markiert haben. Wenn Prisma Access ein Autoskalierungsereignis auslöst, stellt Prisma Access keine weiteren IP-Adressen zur Verfügung, um mehr Kapazität für den Standort hinzuzufügen.*

    *Jedes Mal, wenn Sie einen Standort hinzufügen oder wenn Prisma Access IP-Adressen als Ergebnis eines Autoskalierungsereignisses hinzufügt, müssen Sie die Seite aktualisieren, die die Tabelle **Ausgangs-IP-Zulassungsliste** enthält. Geben Sie **Zu meiner Zulassungsliste hinzugefügt** an, um anzugeben, dass die IP-Adressen zu den Zulassungslisten Ihrer Organisation hinzugefügt wurden, und führen Sie dann die Aktion **Commit und Push** aus, um Ihre Änderungen festzuschreiben und zu übertragen.*

  *Um über alle IP-Adressen auf dem Laufenden zu bleiben, die Prisma Access infolge eines Autoskalierungsereignisses hinzufügt, können Sie eine URL einrichten, über die Prisma Access Sie über Änderungen der IP-Adressen informiert.*

Sie müssen diese Funktionalität nicht aktivieren; Sie entscheiden, ob Prisma Access die IP-Adressen freigeben soll oder nicht, bis Sie bestätigt haben, dass sie in der Benutzeroberfläche als zulässig aufgeführt sind.

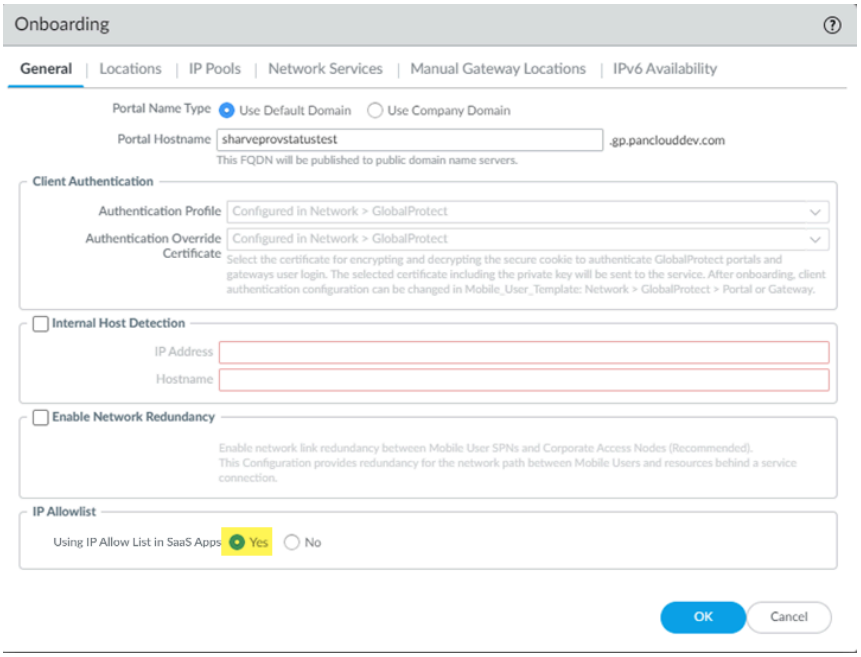
Um zu verhindern, dass Prisma Access öffentliche (Ausgangs-)GlobalProtect-IP-Adressen für Ihre Bereitstellung zur Verfügung stellt, bevor Sie sie zu Ihren Zulassungslisten hinzugefügt haben, geben Sie beim GlobalProtect-Onboarding mobiler Benutzer für die Einstellung **IP-Zulassungsliste in SaaS-Apps verwenden Ja** an. Bestätigen Sie, dass Sie sie in der Prisma Access-Benutzeroberfläche hinzugefügt haben, indem Sie die folgende Aufgabe ausführen.

**STEP 1 |** Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Mobile Benutzer – GlobalProtect** aus.

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Wählen Sie unter **Hostname** Ihren Hostnamen und dann **Konfigurieren** aus, um ihn (für eine bestehende Bereitstellung) zu konfigurieren. Alternativ hierzu können Sie mit **Konfigurieren** Ihre Bereitstellung auch zum ersten Mal (für eine neue Bereitstellung) konfigurieren.

**STEP 3 |** Geben Sie für **IP-Zulassungsliste in SaaS-Apps verwenden** die Einstellung **Ja** an.



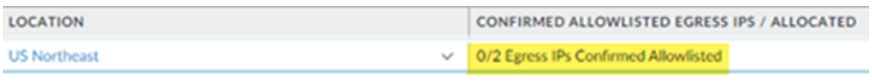

**STEP 4 |** Setzen Sie Ihr Prisma Access-Onboarding fort und wählen Sie dabei auch die Standorte aus, die in Ihrer GlobalProtect-Bereitstellung für mobile Benutzer verwendet werden sollen. Führen Sie die Aktion **Commit und Push** aus, um Ihre Änderungen festzuschreiben und zu übertragen.

Es kann bis zu einer Minute dauern, bis die Änderungen in der Benutzeroberfläche angezeigt werden. Wenn Sie die **Ausgangs-IP-Zulassungsliste** anzeigen, bevor Sie Ihre Änderungen festgeschrieben und übertragen haben, wird als Status **0/0 Ausgangs-IPs in Zulassungsliste bestätigt** angezeigt, da Prisma Access Ihrer Bereitstellung keine Ausgangs-IP-Adressen zugewiesen hat.

**STEP 5 |** Prüfen Sie die Tabelle **Ausgangs-IP-Zulassungsliste** und notieren Sie die Ausgangs-IP-Adressen, die zu Ihren Zulassungslisten hinzugefügt werden müssen.

Sie können die Ausgangs-IP-Adressen im Feld **Bestätigte Ausgangs-IPs in Zulassungsliste/ Zugewiesen** in der Tabelle **Ausgangs-IP-Zulassungsliste** anzeigen. Die erste Zahl gibt an, ob bestätigt wurde, dass die IP-Adresse zu Ihren Zulassungslisten hinzugefügt wurde.

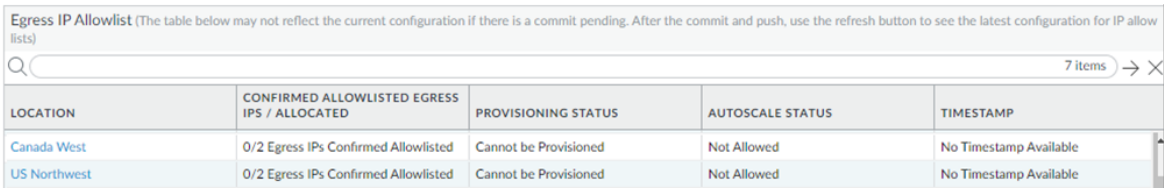
Das folgende Beispiel zeigt die IP-Adressen für den Standort US Northeast. Die Beschreibung `0/2 Ausgangs-IPs in Zulassungsliste bestätigt` zeigt an, dass 0 der beiden Ausgangs-IP-Adressen als zu den Zulassungslisten hinzugefügt markiert wurden und Sie diese hinzufügen müssen.



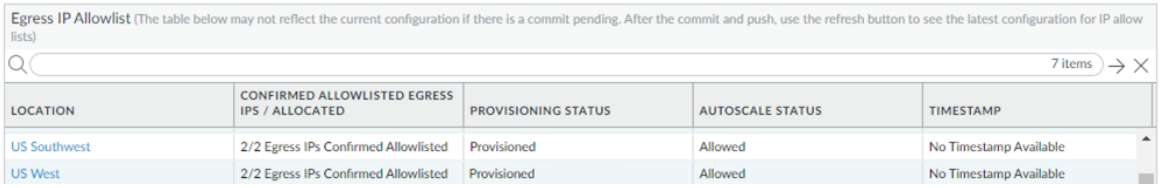

Wenn Sie über eine neue Prisma Access-Bereitstellung verfügen oder Standorte hinzugefügt haben oder wenn ein Autoskalierungsereignis aufgetreten ist, wird in der Tabelle angezeigt,

 ©2025 Palo Alto Networks, Inc.

dass keine der Ausgangs-IP-Adressen zur Zulassungsliste Ihrer Organisation hinzugefügt wurde.

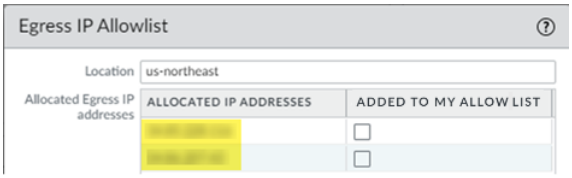



Wenn Sie über eine vorhandene Prisma Access-Bereitstellung verfügen, zeigt die Tabelle den **Bereitstellungsstatus Bereitgestellt** und den **Autoskalierungsstatus Zulässig** an. Dies bedeutet, dass Prisma Access die Ausgangs-IP-Adressen als hinzugefügt markiert hat.




Prisma Access vergibt für jeden neu hinzugefügten Standort zwei Adressen. Wenn an einem bestehenden Standort zuvor ein Autoskalierungsereignis aufgetreten ist, als sich eine große Anzahl mobiler Benutzer gleichzeitig an einem einzelnen Standort angemeldet hat, weist Prisma Access zusätzliche Ausgangs-IP-Adressen in einem Vielfachen von zwei zu und ein bestehender Standort könnte dann vier oder mehr Adressen aufweisen.

**STEP 6 |** Suchen Sie die neuen Ausgangs-IP-Adressen, die zu den Zulassungslisten Ihrer Organisation hinzugefügt werden müssen, indem Sie den Namen für Ihren **Standort** in der Tabelle auswählen.

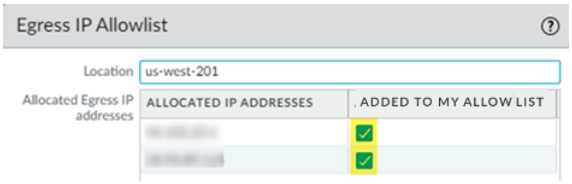



**STEP 7 |** Fügen Sie diese Ausgangs-IP-Adressen zu den Zulassungslisten Ihrer Organisation hinzu.

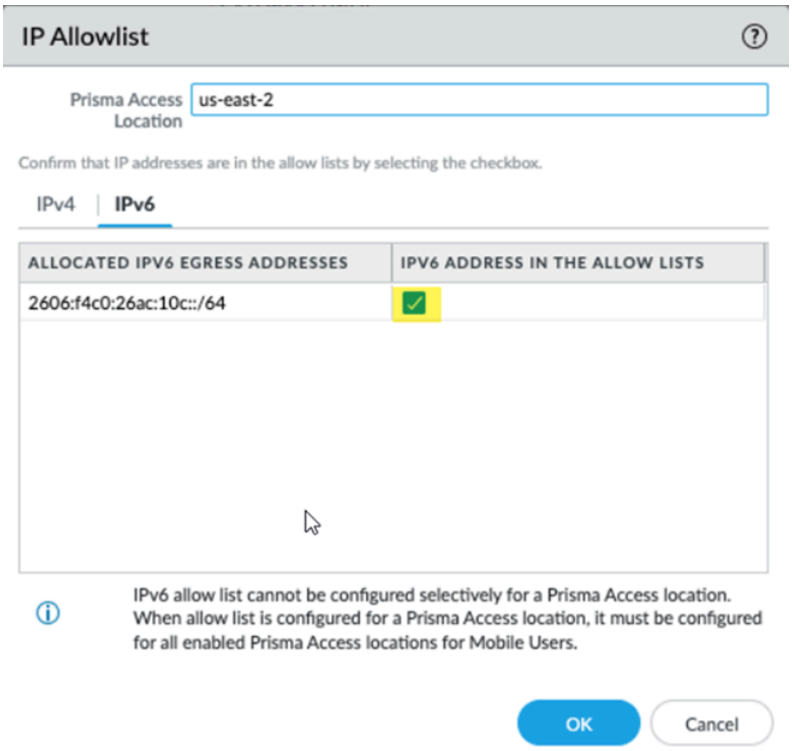
**STEP 8 |** Nachdem Sie die Ausgangs-IP-Adresse in die Zulassungsliste aufgenommen haben, kehren Sie zum Ausgangs-IP-Bereich zurück und geben Sie dort an, dass Sie die Adresse zu

 ©2025 Palo Alto Networks, Inc.

Ihren Zulassungslisten hinzugefügt haben. Wählen Sie hierzu **Zu meiner Zulassungsliste hinzugefügt** aus.



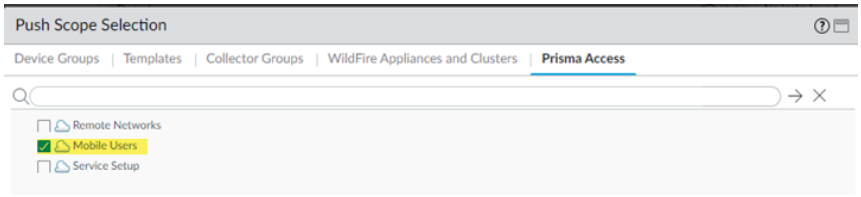

Wenn Sie über IPv6-Adressen verfügen, wählen Sie **IPv6-Adresse in den Zulassungslisten** aus.




 ©2025 Palo Alto Networks, Inc.

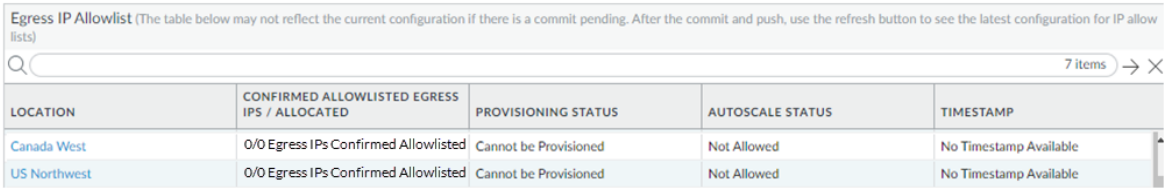
**STEP 9 |** Führen Sie die Aktion „Commit und Push“ aus, um Ihre Änderungen festzuschreiben und zu übertragen und sie so in Prisma Access zu aktivieren.

1. Wählen Sie im Übertragungsumfang **Commit** > **Commit und Push** und dann **Auswahl bearbeiten** aus.
2. Wählen Sie **Prisma Access** aus und stellen Sie sicher, dass **Mobile Benutzer** ausgewählt ist.




3. Klicken Sie auf **OK**, um Ihre Änderungen im Übertragungsumfang zu speichern.
4. Führen Sie die Aktion **Commit** und **Push** aus, um Ihre Änderungen festzuschreiben und zu übertragen.

Wenn Sie die Tabelle **Ausgangs-IP-Zulassungsliste** anzeigen, bevor Sie Ihre Änderungen mit Commit und Push festschreiben und übertragen, wird in der Spalte „Bestätigt“ der Status **0/0 Ausgangs-IPs in Zulassungsliste bestätigt** angezeigt, da Prisma Access Ihrer Bereitstellung keine IP-Adressen zuweisen kann, bevor Sie die Änderungen mit der Aktion **Commit und Push** festschreiben und übertragen.



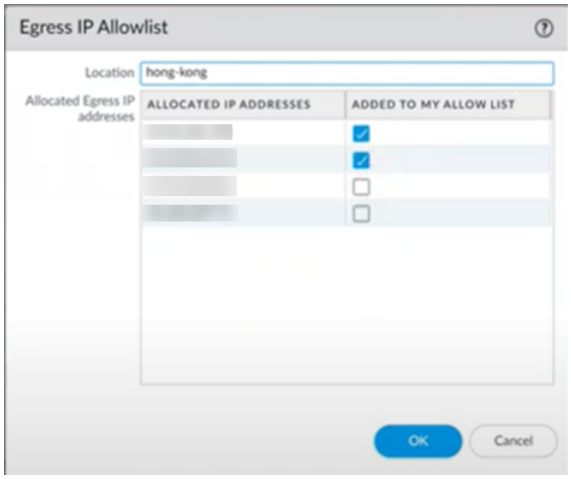

Die Tabelle **Ausgangs-IP-Zulassungsliste** enthält die folgenden zusätzlichen Felder:

| Feld | Beschreibung |
|---|---|
| **Standort** | Der eingebundene Standort für mobile Benutzer. |
| **Bestätigte Ausgangs-IPs in der Zulassungsliste/Zugewiesen** | Die Anzahl der bestätigten Ausgangs-IP-Adressen in der Zulassungsliste und die Anzahl der zugewiesenen Ausgangs-IP-Adressen. |
| **Bereitstellungsstatus** | Der Zulassungslistenstatus der Ausgangs-IP-Adressen.<br>• **Bereitgestellt** – Sie haben die Ausgangs-IP-Adressen zu den Zulassungslisten Ihrer Organisation hinzugefügt, haben sie in der Prisma Access-Benutzeroberfläche als hinzugefügt bestätigt, indem Sie **Zu meiner Zulassungsliste hinzugefügt** aktiviert haben, und Sie haben Ihre Änderungen mit „Commit |

 ©2025 Palo Alto Networks, Inc.

| Feld | Beschreibung |
| --- | --- |
| | und Push“ festgeschrieben und übertragen, um sie vollständig bereitzustellen.<br>• **Nicht bereitgestellt** – Prisma Access hat IP-Adressen für den Standort zugewiesen und Sie haben die Ausgangs-IP-Adressen zu den Zulassungslisten Ihrer Organisation hinzugefügt und in der Prisma Access-Benutzeroberfläche als hinzugefügt bestätigt, aber Sie haben diesen Standort noch nicht eingebunden.<br>• **Kann nicht bereitgestellt werden** – Sie haben diesen Standort eingebunden, aber noch nicht **Zu meiner Zulassungsliste hinzugefügt** aktiviert und Ihre Änderungen noch nicht festgeschrieben und übertragen.<br>Erst nachdem Sie in Prisma Access angegeben haben, dass Sie diese Ausgangs-IPs zu den Zulassungslisten Ihrer Organisation hinzugefügt haben und Ihre Änderungen mit der Aktion **Commit und Push** festgeschrieben und übertragen haben, stellt Prisma Access diese IP-Adressen für Ihre Bereitstellung bereit.<br>• **Teilweise verfügbar** – Sie haben den ersten Satz von Ausgangs-IP-Adressen hinzugefügt, sie in der Prisma Access-Benutzeroberfläche als hinzugefügt bestätigt und Ihre Änderungen festgeschrieben und übertragen. Prisma Access hat jedoch einen weiteren Satz von IP-Adressen als Teil eines Autoskalierungsereignisses hinzugefügt und diese IP-Adressen wurden in der Prisma Access-Benutzeroberfläche noch nicht als zu Ihren Zulassungslisten hinzugefügt angegeben.<br>Der folgende Screenshot zeigt ein Beispiel für eine Bereitstellung, die als **Teilweise verfügbar** markiert wäre. Zwei IP-Adressen wurden als **Zu meiner Zulassungsliste hinzugefügt** markiert; Prisma Access hat jedoch zwei weitere IP-Adressen zu diesem Standort hinzugefügt und diese Standorte |

 ©2025 Palo Alto Networks, Inc.

| Feld | Beschreibung |
| --- | --- |
| | wurden in der Benutzeroberfläche nicht hinzugefügt.<br> |
| **Autoskalierungsstatus** | Zeigt den Status der Autoskalierung in Prisma Access.<br>• **Zulässig** – Sie haben IP-Adressen zu den Zulassungslisten hinzugefügt. Wenn sich eine große Anzahl mobiler Benutzer an einem einzigen Standort anmeldet und ein Autoskalierungsereignis auslöst, verwendet Prisma Access die in der Zulassungsliste enthaltenen IP-Adressen für das Autoskalierungsereignis.<br>• **Nicht zulässig** – Sie haben nicht alle IP-Adressen in der Prisma Access-Benutzeroberfläche als zu Ihren Zulassungslisten hinzugefügt angegeben oder Sie haben Ihre Änderungen nicht festgeschrieben und übertragen, nachdem Sie sie als hinzugefügt markiert haben. Wenn Prisma Access ein Autoskalierungsereignis auslöst, stellt Prisma Access keine weiteren IP-Adressen zur Verfügung, um mehr Kapazität für den Standort hinzuzufügen.<br>Jedes Mal, wenn Sie einen Standort hinzufügen oder wenn Prisma Access IP-Adressen als Ergebnis eines Autoskalierungsereignisses hinzufügt, müssen Sie die Seite aktualisieren, die die Tabelle **Ausgangs-IP-Zulassungsliste** enthält. Geben Sie **Zu meiner Zulassungsliste hinzugefügt** an, um anzugeben, dass die IP-Adressen zu den Zulassungslisten Ihrer |

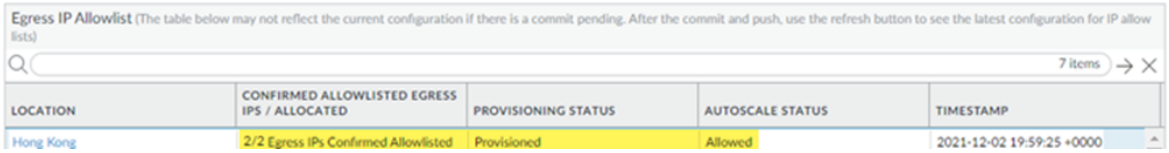
 ©2025 Palo Alto Networks, Inc.

| Feld | Beschreibung |
|---|---|
| | Organisation hinzugefügt wurden, und führen Sie dann die Aktion **Commit und Push** aus, um Ihre Änderungen festzuschreiben und zu übertragen.<br><br>*Um über alle IP-Adressen informiert zu sein, die Prisma Access infolge eines Autoskalierungsereignisses hinzufügt, sollten Sie eine URL einrichten, über die Prisma Access Sie über Änderungen der IP-Adressen informiert.* |
| **Timestamp** | Der letzte bekannte Zeitpunkt in Coordinated Universal Time (UTC), zu dem eine IP für diese Region zugewiesen wurde. |

Nach Ausführung der Aktion **Commit und Push** wird in der Spalte „Bestätigt“ der Status **0/2 Ausgangs-IPs in Zulassungsliste bestätigt** angezeigt, da Sie noch nicht bestätigt haben, dass die IP-Adressen in der Prisma Access-Benutzeroberfläche als in die Zulassungsliste aufgenommen markiert wurden.

Wenn Sie ein Onboarding für einen Standort für mobile Benutzer durchführen, stellt Ihnen Prisma Access zwei Ausgangs-IP-Adressen zur Verfügung, und zwar eine aktive IP-Adresse und eine Adresse, die Sie im Falle eines Autoskalierungsereignisses verwenden können. Im Folgenden finden Sie Beispiele dafür, wie Prisma Access Ausgangs-IP-Adressen nach einem Autoskalierungsereignis zuweist und bereitstellt.

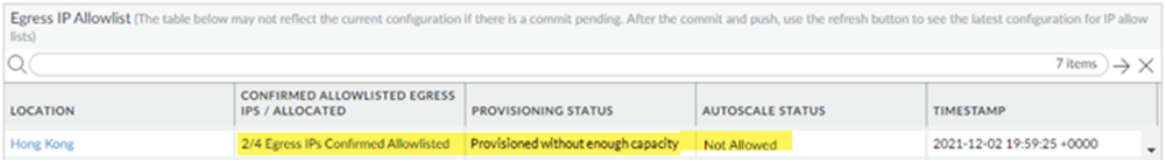
**Autoskalierungsereignis** – Wenn sich eine große Anzahl mobiler Benutzer gleichzeitig an einem Standort für mobile Benutzer anmeldet, kann dieses Ereignis dazu führen, dass Prisma Access einen zusätzlichen Satz von zwei Ausgangs-IP-Adressen zuweist, um die große Anzahl von Benutzern zu unterstützen. Nachdem Sie die ersten beiden Ausgangs-IP-Adressen in die Zulassungsliste aufgenommen haben, werden im Status vor einem Autoskalierungsereignis die beiden Ausgangs-IP-Adressen als zulässig angezeigt. Der bestätigte Status lautet **2/2 Ausgangs-IPs in der Zulassungsliste bestätigt**, der Bereitstellungsstatus **Bereitgestellt** und der Autoskalierungsstatus lautet **Zulässig**. Dies wird im folgenden Screenshot am Standort in Hongkong angezeigt.



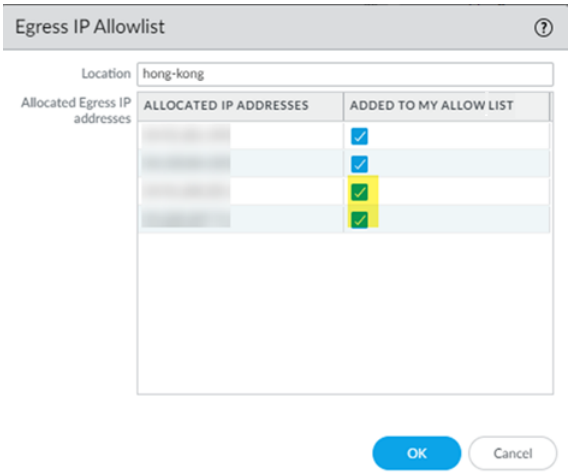

Meldet sich eine große Anzahl mobiler Benutzer gleichzeitig am Standort Hongkong an, aktiviert Prisma Access die Backup-Ausgangs-IP-Adresse. Es werden zwei weitere IP-Adressen

 ©2025 Palo Alto Networks, Inc.

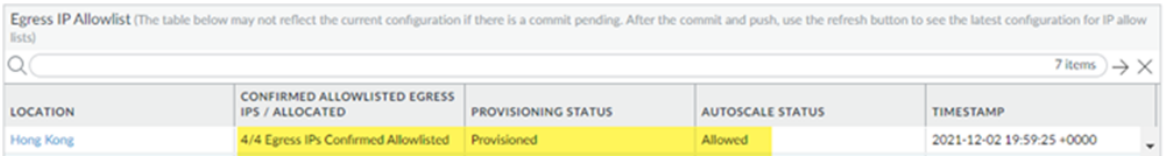
zugewiesen, von denen eine IP-Adresse aktiviert wird. Wenn ein Autoskalierungsereignis auftritt, wurden die Ausgangs-IP-Adressen zugewiesen, aber nicht bereitgestellt. Der bestätigte Status lautet **2/4 Ausgangs-IPs in der Zulassungsliste bestätigt** und der Bereitstellungsstatus **Bereitgestellt ohne ausreichende Kapazität**. Darüber hinaus lautet der Autoskalierungsstatus **Nicht zulässig**, was bedeutet, dass Prisma Access die zusätzliche Ausgangs-IP-Adresse für Ihre Bereitstellung nicht bereitstellt, wenn ein Autoskalierungsereignis auftritt.




Nachdem Sie die neuen Ausgangs-IP-Adressen zu Ihren Zulassungslisten hinzugefügt haben, wählen Sie den Standortnamen aus. Wählen Sie dann für die beiden hinzugefügten IP-Adressen **Zu meiner Zulassungsliste hinzugefügt** aus und führen Sie die Aktion **Commit und Push** aus, um die Änderungen festzuschreiben und zu übertragen.




Nach Abschluss dieser Arbeitsschritte wird für den Standort Hongkong angezeigt, dass alle vier Ausgangs-IP-Adressen bestätigt und bereitgestellt wurden und dass die Autoskalierung aktiv ist.




# GlobalProtect-App-Upgrades

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | • Prisma Access-Lizenz |

 ©2025 Palo Alto Networks, Inc.

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama) | |

Prisma Access hostet die GlobalProtect-App-Version, die macOS- und Windows-Benutzer in Ihrer Organisation über das Prisma Access-Portal herunterladen können. Prisma Access bietet mehrere Versionen der GlobalProtect-App an und Sie können wählen, ob Sie eine dieser Versionen zur aktiven Version machen möchten. Sie können auch den Zugriff mobiler Benutzer auf die GlobalProtect-App verwalten oder mehrstufige Upgrades durchführen.

- Aktive GlobalProtect-App-Version für Prisma Access auswählen
- Benutzern das Upgrade der GlobalProtect-App erlauben
- Updates für GlobalProtect-Apps staffeln

## Aktive GlobalProtect-App-Version für Prisma Access auswählen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

Prisma Access verwaltet die GlobalProtect-App-Version für Windows- und macOS-Benutzer in Ihrer Organisation. Zwar werden von Prisma Access mehrere GlobalProtect-App-Versionen gehostet, doch es ist nur eine der gehosteten Versionen aktiv. Wenn sich mobile Benutzer beim Prisma Access-Portal anmelden, steht den mobilen Benutzern die aktive Version zum Herunterladen und Installieren auf ihren Windows- und macOS-Geräten zur Verfügung.

In einer Mehrmandantenbereitstellung können Sie mehrere GlobalProtect-Versionen auswählen. Die von Ihnen angewandten Einstellungen für die GlobalProtect-App-Version gelten pro Mandant und nicht global. Sie steuern die App-Version für einzelne Mandanten.

Für einige Funktionen, wie z. B. die IP-Optimierung, müssen Benutzer ausreichend aktualisierte Versionen von GlobalProtect verwenden. Lesen Sie weiter, um zu erfahren, wie Sie die aktive GlobalProtect-App-Version in Prisma Access auswählen.

- Strata Cloud Manager
- Panorama

### Aktive GlobalProtect-App-Version für Prisma Access (Managed by Strata Cloud Manager) auswählen

Sie können die derzeit aktive Version durch eine andere gehostete Version auf der Seite „Diensteinrichtung“ ersetzen, indem Sie wie folgt vorgehen.

**STEP 1 |** Wählen Sie **Workflows** > **Einrichtung Prisma Access** > **Mobile Benutzer** aus und suchen Sie dann den Bereich **GlobalProtect-Verbindung**.

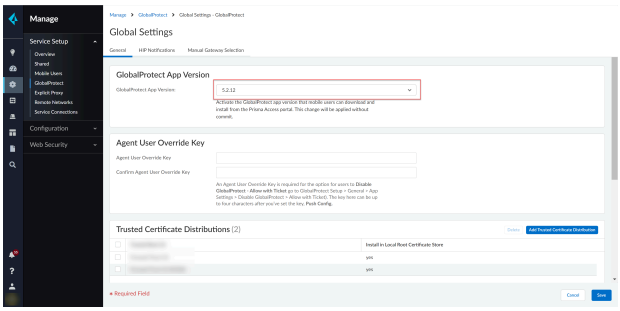
**STEP 2 |** Wählen Sie **GlobalProtect-Einrichtung** oder **Aktivieren** > **GlobalProtect-Einrichtung** aus, wenn GlobalProtect noch nicht aktiviert ist.

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Wählen Sie die Registerkarte **GlobalProtect-App** aus, und bearbeiten Sie dann die **Globalen App-Einstellungen**.

**STEP 4 |** Wählen Sie auf der Registerkarte **Allgemein** der Seite **Globale Einstellungen** die **GlobalProtect-App-Version** aus, die mobile Benutzer vom Prisma Access-Portal herunterladen und installieren können sollen.

Die aktive Version wird in der Dropdown-Liste angezeigt.




### Aktive GlobalProtect-App-Version für Prisma Access (Managed by Panorama) auswählen

Wenn Ihre derzeit aktive Version das Ende ihrer Lebensdauer erreicht hat, werden Sie von Prisma Access benachrichtigt und aufgefordert, eine unterstützte Version zu aktivieren.

Sie können die derzeit aktive Version durch eine andere gehostete Version auf der Seite „Diensteinrichtung“ ersetzen, indem Sie wie folgt vorgehen.

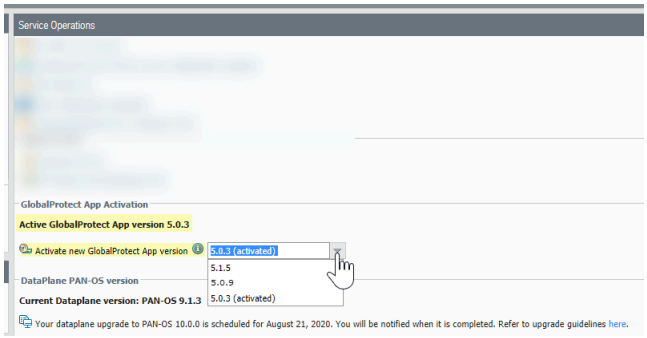
*Wenn Sie Prisma Access in einer FedRAMP-Umgebung verwenden, müssen Sie die FIPS-zertifizierte Version von GlobalProtect verwenden, also Version 5.1.4. Wenn Sie eine andere GlobalProtect-Standardversion als 5.1.4 festlegen, können Sie Version 5.1.4 in der Panorama-Benutzeroberfläche nicht auswählen und müssen einen Supportfall beim technischen Support von Palo Alto Networks einleiten, um die Version wieder hinzuzufügen.*

**STEP 1 |** Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Diensteinrichtung** aus.

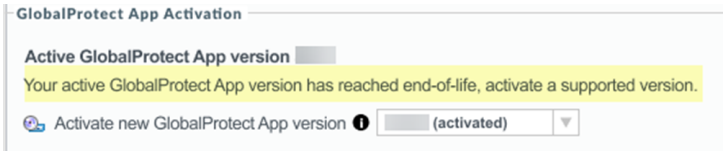
 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Wählen Sie **Neue GlobalProtect-App-Version aktivieren** aus.

Die aktive Version wird in der Dropdown-Liste angezeigt.

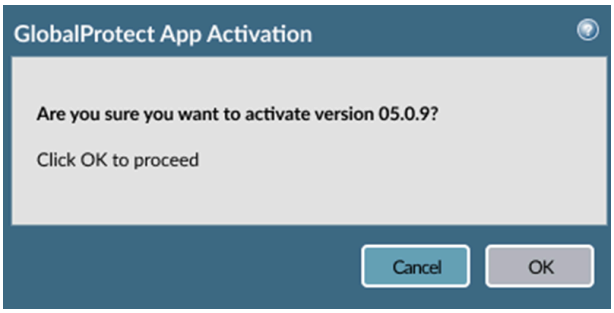



*Wenn Ihre aktuelle GlobalProtect-Version das Ende ihrer Lebensdauer (EoL) erreicht hat, wird in diesem Bereich auf der Seite „Diensteinrichtung“ eine Meldung angezeigt. Wenn Sie diese Meldung erhalten, aktualisieren Sie Ihre GlobalProtect-App-Version, indem Sie mit dem nächsten Schritt fortfahren.*

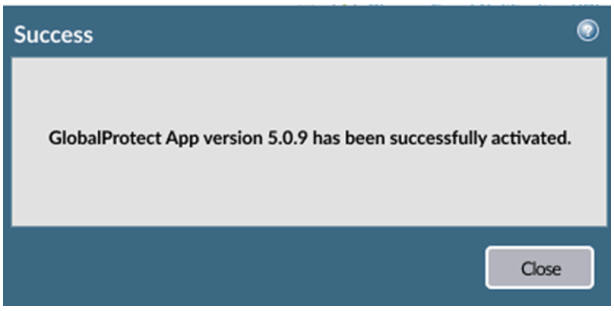



**STEP 3 |** Wählen Sie die Version aus, auf die Sie aktualisieren möchten, und klicken Sie auf **OK**.

Es wird ein Fenster angezeigt, um Ihre Wahl zu bestätigen.




Nachdem die App aktiviert wurde, wird eine Erfolgsmeldung angezeigt.




**STEP 4 |** Überprüfen Sie auf der Seite „Systemstatus“ die **aktive GlobalProtect-App-Version**.

 ©2025 Palo Alto Networks, Inc.

## Benutzern das Upgrade der GlobalProtect-App erlauben

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

Erfahren Sie, wie der Zugriff mobiler Benutzer auf die GlobalProtect-App-Version für Prisma Access-GlobalProtect-Bereitstellungen gesteuert wird.

- Strata Cloud Manager
- Panorama

### Benutzern das Upgrade der GlobalProtect-App erlauben (Strata Cloud Manager)

Sie können den Zugriff mobiler Benutzer auf die aktive GlobalProtect-App-Version verwalten, die von Prisma Access gehostet wird. Hierzu müssen Sie in Prisma Access (Managed by Strata Cloud Manager) die Einstellung **Upgrade für GlobalProtect ausführen** konfigurieren. Führen Sie für Prisma Access (Managed by Strata Cloud Manager) die folgenden Schritte aus.

**STEP 1 |** Wählen Sie **Workflows** > **Prisma Access-Einrichtung** > **Mobile Benutzer** aus und suchen Sie dann die Anzeige **GlobalProtect-Verbindung**.

**STEP 2 |** Wählen Sie **GlobalProtect-Einrichtung** oder **Aktivieren** > **GlobalProtect-Einrichtung** aus, wenn GlobalProtect noch nicht aktiviert wurde.

**STEP 3 |** Wählen Sie die Registerkarte **GlobalProtect-App** und dann **App-Einstellungen hinzufügen** aus.

**STEP 4 |** Wählen Sie im Bereich **App-Konfiguration** unter **GlobalProtect-App aktualisieren** eine Option aus, um anzugeben, ob mobile Benutzer für ihre GlobalProtect-App-Version ein Upgrade auf die aktive Version durchführen können, die auf Prisma Access gehostet wird, und ob sie (wenn dies möglich ist) auswählen können, wann das Upgrade ausgeführt werden soll:

- **Zulassen, wenn Benutzer die Upgrade-Eingabeaufforderung akzeptiert** (Standardeinstellung) – Die Benutzer erhalten eine Eingabeaufforderung, wenn eine neue Version aktiviert wird. Die Benutzer können dann ein Upgrade ihrer Software zu einem von ihnen gewählten Zeitpunkt durchführen.
- **Nicht zulassen** – Verhindert, dass Benutzer ein Upgrade ihrer App-Software durchführen können.
- **Manuell zulassen** – Erlaubt Benutzern, manuell nach Upgrades zu suchen und diese einzuleiten, indem sie in der GlobalProtect-App **Version prüfen** auswählen.
- **Transparent zulassen** – Ermöglicht ein automatisches Upgrade der App-Software, sobald eine neue Version im Portal verfügbar ist.
- **Zulassen, wenn der Benutzer sich im Unternehmensnetzwerk befindet** – Ermöglicht das automatische Upgrade der App-Software, sobald eine neue Version im Portal zur Verfügung gestellt wird. Es wird dabei jedoch gewartet, bis der Endpunkt intern mit dem

 ©2025 Palo Alto Networks, Inc.

Unternehmensnetzwerk verbunden ist. Dies verhindert Verzögerungen durch Upgrades über Verbindungen mit geringer Bandbreite.

#### Benutzern das Upgrade der GlobalProtect-App erlauben (Panorama)

Sie können den Zugriff mobiler Benutzer auf die aktive GlobalProtect-App-Version verwalten, die von Prisma Access gehostet wird. Hierzu müssen Sie in Prisma Access (Managed by Strata Cloud Manager) die Einstellung **Upgrade für GlobalProtect ausführen** konfigurieren. Führen Sie für Prisma Access (Managed by Panorama) die folgenden Schritte aus.

**STEP 1 |** Wählen Sie **Netzwerk** > **GlobalProtect** > **Portale** aus.

**STEP 2 |** Wählen Sie die Vorlage **Mobile_User_Template** im Dropdown-Menü **Vorlage** aus.

**STEP 3 |** Wählen Sie **GlobalProtect_Portal** aus, um die Prisma Access-Portalkonfiguration zu bearbeiten.

**STEP 4 |** Wählen Sie die Registerkarte **Agent** und dann die App-Konfiguration aus.

**STEP 5 |** Wählen Sie die Registerkarte **App** aus.

**STEP 6 |** Wählen Sie im Bereich **App-Konfigurationen** unter **Benutzer das Upgrade der GlobalProtect-App erlauben** eine Option aus, um anzugeben, ob mobile Benutzer ein Upgrade für ihre GlobalProtect-App-Version auf die aktive Version durchführen können, die auf Prisma Access gehostet wird, und ob sie (wenn möglich) auswählen können, wann das Upgrade durchgeführt wird:

- **Mit Eingabeaufforderung zulassen** (Standardeinstellung) – Benutzer erhalten eine Eingabeaufforderung, wenn eine neue Version aktiviert wird. Die Benutzer können dann ein Upgrade ihrer Software zu einem von ihnen gewählten Zeitpunkt durchführen.
- **Nicht zulassen** – Verhindert, dass Benutzer ein Upgrade ihrer App-Software durchführen können.
- **Manuell zulassen** – Erlaubt Benutzern, manuell nach Upgrades zu suchen und diese einzuleiten, indem sie in der GlobalProtect-App **Version prüfen** auswählen.
- **Transparent zulassen** – Ermöglicht ein automatisches Upgrade der App-Software, sobald eine neue Version im Portal verfügbar ist.
- **Intern** – Ermöglicht ein automatisches Upgrade der App-Software, sobald eine neue Version im Portal zur Verfügung gestellt wird. Dabei wird jedoch gewartet, bis der Endpunkt intern mit dem Unternehmensnetzwerk verbunden ist. Dies verhindert Verzögerungen durch Upgrades über Verbindungen mit geringer Bandbreite.

## Updates für GlobalProtect-Apps staffeln

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

Wenn Sie eine große Organisation verwalten, sollten Sie mobile Benutzer schrittweise auf die neueste Version der GlobalProtect-App aktualisieren. Sie können z. B. eine kleinere Gruppe

 ©2025 Palo Alto Networks, Inc.

anweisen, ihre GlobalProtect-App zu aktualisieren, bevor das Update für alle in Ihrer Organisation bereitgestellt wird. Gehen Sie dazu wie folgt vor:

**STEP 1 |** Falls noch nicht geschehen, erstellen Sie eine Benutzergruppe für die erste Gruppe an Benutzern, für die Sie mit dem Rollout des GlobalProtect-App-Updates beginnen möchten.

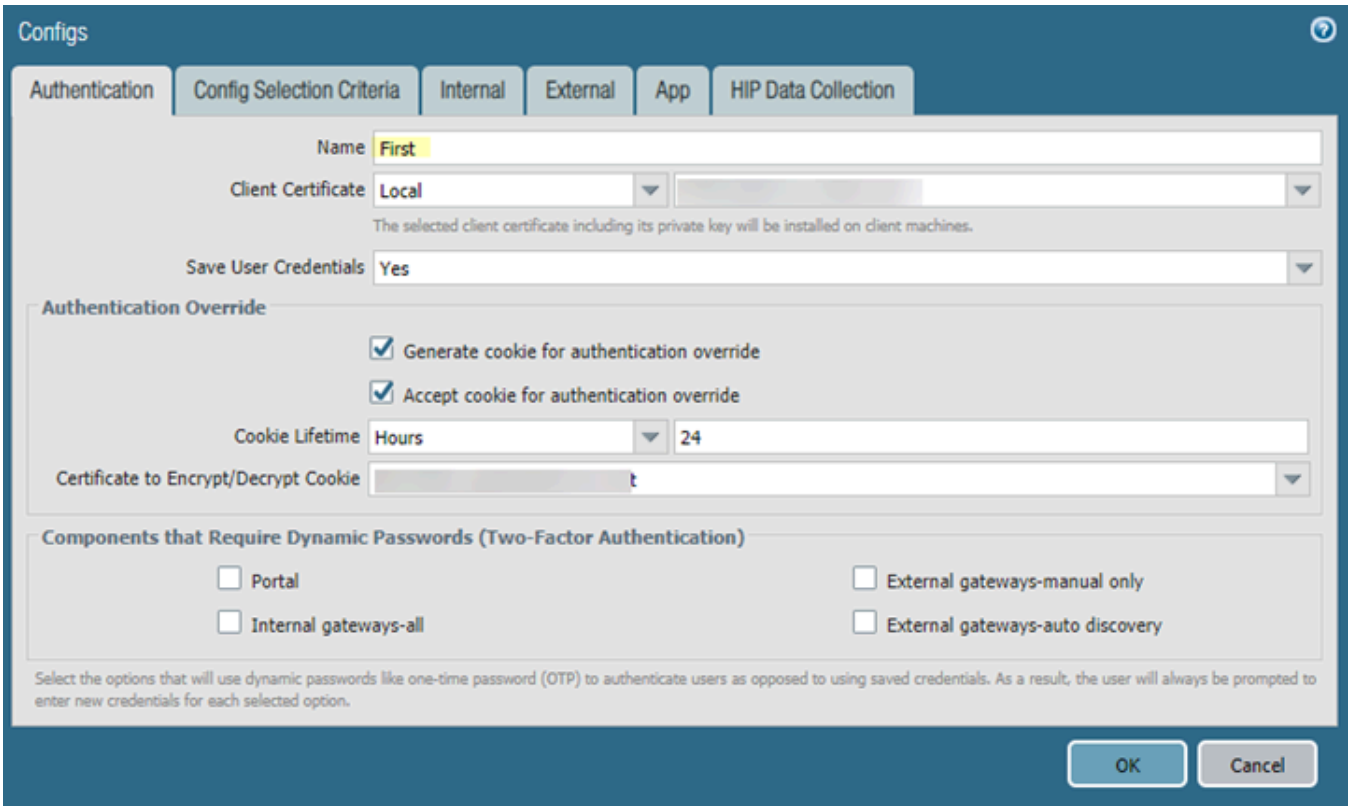
Sie können die Benutzer-ID verwenden, um Benutzer Gruppen zuzuordnen, oder **Gerät** > **Lokale Benutzerdatenbank** > **Benutzergruppen** auswählen, um eine Gruppe manuell zu erstellen.

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Erstellen Sie eine neue GlobalProtect-Agent-Konfiguration zur Verwendung für die erste Gruppe von Benutzern.

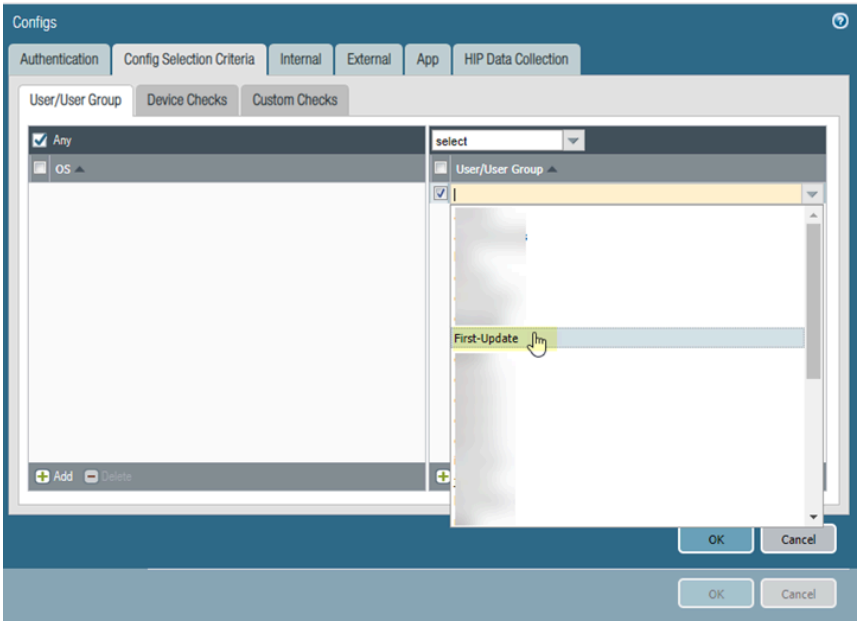
1. Wählen Sie in Panorama **Netzwerk** > **GlobalProtect** > **Portale** aus.
2. Wählen Sie die Vorlage **Mobile_User_Template** im Dropdown-Menü **Vorlage** aus.
3. Wählen Sie **GlobalProtect_Portal** aus, um die Prisma Access-Portalkonfiguration zu bearbeiten.
4. Wählen Sie die Registerkarte **Agent** aus.
5. Wählen Sie die Konfiguration **STANDARD** aus und **klonen** Sie sie.

   Sie können auch eine neue Konfiguration **hinzufügen**. Allerdings werden beim Klonen der vorhandenen Konfiguration die erforderlichen Informationen für die neue Konfiguration kopiert.
6. Geben Sie einen **Namen** für die Konfiguration an.



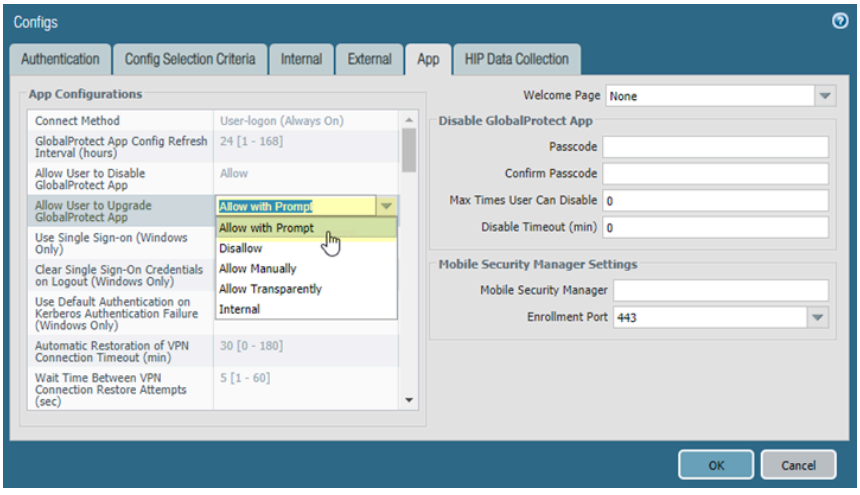

7. Wählen Sie die Registerkarte **Auswahlkriterien für die Konfiguration** aus.
8. Wählen Sie im Bereich **Benutzer/Benutzergruppe** den Benutzer aus, den Sie in Schritt 1 erstellt haben.

 ©2025 Palo Alto Networks, Inc.




9. Wählen Sie die Registerkarte **App** aus.
10. Ändern Sie **Benutzern das Upgrade der GlobalProtect-App erlauben** entweder in **Mit Eingabeaufforderung zulassen** oder in **Transparent zulassen**.

    **Mit Eingabeaufforderung zulassen** informiert Benutzer, wenn eine neue Version aktiviert wird, und ermöglicht es ihnen, ein Upgrade ihrer Software zu einem für sie passenden Zeitpunkt durchzuführen. **Transparent zulassen** aktualisiert die App-Software automatisch, sobald eine neue Version im Portal verfügbar ist.



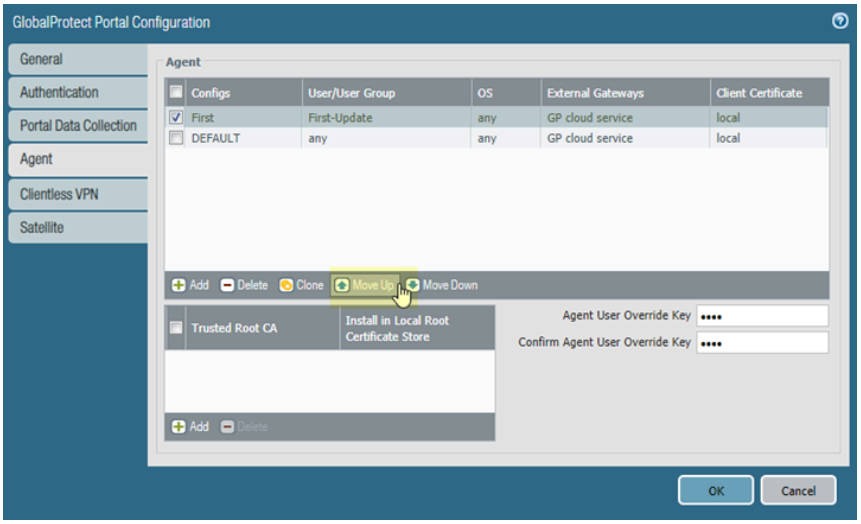

11. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

**STEP 3 |** Wählen Sie **Nach oben verschieben** aus, um Ihre Konfiguration über die Standardkonfiguration zu verschieben.

Wenn eine App eine Verbindung herstellt, vergleicht das Portal die Quellinformationen im Paket mit den von Ihnen definierten Agent-Konfigurationen. Wie bei der Auswertung von Sicherheitsregeln sucht das Portal nach einer Übereinstimmung, beginnend am Anfang der

 ©2025 Palo Alto Networks, Inc.

Liste. Wird eine Übereinstimmung erkannt, wird die entsprechende Konfiguration an die App übermittelt.




**STEP 4 |** Wiederholen Sie diese Schritte für die Konfiguration **STANDARD**, ändern Sie jedoch **Benutzern das Upgrade der GlobalProtect-App erlauben** in **Nicht zulassen** um zu verhindern, dass Benutzer auf die neueste GlobalProtect-App-Software aktualisieren.

**STEP 5 |** Wenn Sie möchten, dass auch die übrigen Benutzer ihre Apps aktualisieren, ändern Sie **Benutzern das Upgrade der GlobalProtect-App erlauben** in der Konfiguration **STANDARD** in eine Auswahl, die dies ermöglicht (entweder **Mit Eingabeaufforderung zulassen** oder **Transparent zulassen**).

## Prisma Access mit lokalen GlobalProtect-Gateways integrieren

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama)<br>• Prisma Access (Managed by Strata Cloud Manager) | • Prisma Access-Lizenz |

Prisma Access ermöglicht Ihnen, die Sicherheitsplattform von Palo Alto Networks auf Ihre Remote-Netzwerkstandorte und Ihre mobilen Benutzer auszuweiten, ohne dass Sie Ihre eigene globale Sicherheitsinfrastruktur aufbauen und Ihre Betriebskapazität erweitern müssen. In Fällen, in denen Sie GlobalProtect-Gateways bereits in Regionen bereitgestellt haben, in denen Sie schon eine entsprechende Infrastruktur zur Verwaltung aufgebaut haben, können Sie diese Investition nutzen, indem Sie Prisma Access so konfigurieren, dass mobile Benutzer bei Bedarf an Ihre vorhandenen externen Gateways weitergeleitet werden.

Sie können Prioritäten für Prisma Access und lokale Gateways verwalten, die Ihnen die Angabe von Prioritäten für lokale und Prisma Access-Gateways ermöglichen. Administratoren können keine mobilen Benutzer für die Verbindung mit einem bestimmten Prisma Access Gateway angeben. Sie können jedoch mobilen Benutzern erlauben, bestimmte Prisma Access-Gateways mithilfe der GlobalProtect-App manuell auszuwählen.

 ©2025 Palo Alto Networks, Inc.

*Sie können Ihr eigenes Portal nicht mit Prisma Access verwenden. Sie können das Portal nur verwenden, wenn Ihr Prisma Access für mobile Benutzer bereitgestellt wurde.*

- Strata Cloud Manager
- Panorama

## Prisma Access in lokale GlobalProtect-Gateways integrieren (Prisma Access (Managed by Strata Cloud Manager))

**STEP 1 |** Fügen Sie Ihr lokales Gateway der Liste der Gateways in der Agent-Konfiguration hinzu.

1. Gehen Sie zu **Workflows** > **Einrichtung Prisma Access** > **GlobalProtect** und wählen Sie die Registerkarte **GlobalProtect App** aus.
2. **Fügen Sie App-Einstellungen hinzu**.
3. **Fügen Sie ein externes Gateway hinzu.**

   *Wenn Sie eine neue Agent-Konfiguration hinzufügen und die Prisma Access-Gateways der Liste der externen Gateways in dieser Konfiguration hinzufügen möchten, müssen Sie den **Namen** auf **GP Cloud Service** und die **Adresse** auf **gpcloudservice.com** festlegen. Sie müssen diese Werte genau wie dargestellt eingeben und können keinen dieser Werte für Nicht-Prisma Access-Gateways.*
4. Geben Sie den **Namen** des Gateways ein und geben Sie entweder den **FQDN** oder die **IP**-Adresse des Gateways in das Feld **Adresse** ein. Dieser Wert muss exakt mit dem Common Name (CN) im Gateway-Zertifikat übereinstimmen.
5. (Optional) Wenn mobile Benutzer sich nur dann mit dem Gateway verbinden sollen, wenn sie sich in der entsprechenden Region befinden, müssen Sie die **Quellregion hinzufügen**, auf die das Gateway beschränkt werden soll. Wenn beispielsweise ein

 ©2025 Palo Alto Networks, Inc.

Gateway in Frankreich vorliegt, würden Sie FR (Frankreich) auswählen. Wenn ein Gateway in Schweden vorliegt, würden Sie SE (Schweden) auswählen.

Dies hat unter anderem den Vorteil, dass Benutzer dann auf ein Gateway zugreifen können, das den Zugriff auf Internetressourcen in ihrer eigenen Sprache ermöglicht.

6. (Optional) Geben Sie Prioritäten in Ihrer Gateway-Konfiguration an.

   Sie können für das lokale Gateway eine höhere Priorität oder eine niedrigere Priorität festlegen.

   - Um für das lokale Gateway eine niedrigere Priorität als das Prisma Access-Standard-Gateway festzulegen, setzen Sie die **Priorität** auf **Hoch** oder **Mittel**.

     Wenn Sie weitere Gateways hinzufügen und für jedes Gateway andere Prioritäten festlegen möchten, können Sie die **Priorität** auf **Hoch**, **Mittel**, **Niedrig** oder **Niedrigst** festlegen.
   - Um das lokale Gateway auf eine höhere Priorität als die Standardpriorität festzulegen, setzen Sie die **Priorität** auf **Höchste**.

     Wenn Sie das lokale Gateway auf eine höhere Priorität festlegen möchten, müssen Sie auch das **Prisma Access**-Standard-Gateway bearbeiten und eine **Priorität** festlegen, die niedriger als **Höchste** ist.

7. Wählen Sie **Manuell** aus.

   Wenn Sie dieses Kontrollkästchen aktivieren, können GlobalProtect-Benutzer dieses externe Gateway manuell in ihrer GlobalProtect-App auswählen.

**STEP 2 |** **Save (Speichern)** Sie Ihre Änderungen.

**STEP 3 |** Wählen Sie **Konfiguration übertragen** aus.

## Prisma Access mit lokalen GlobalProtect-Gateways integrieren (Prisma Access (Managed by Panorama))

Um eine dieser hybriden Prisma Access-Bereitstellungen zu konfigurieren, müssen Sie die GlobalProtect_Portal-Konfiguration in der Vorlage für mobile Benutzer (Mobile_User_Template) bearbeiten, um Ihre lokalen Gateways den entsprechenden Regionen hinzuzufügen.

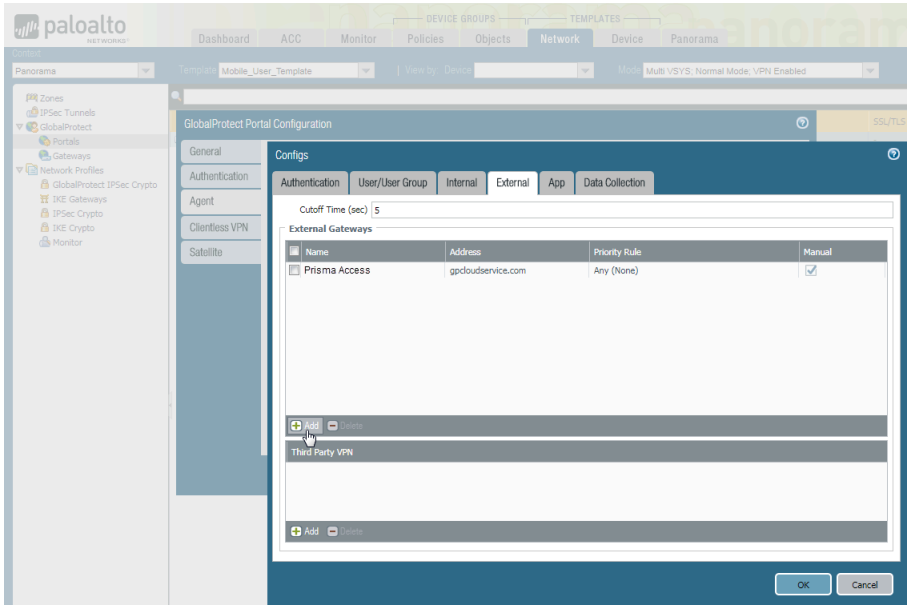
**STEP 1 |** Bearbeiten Sie die Prisma Access-Portalkonfiguration.

1. Um ein vorhandenes Gateway zur Liste der verfügbaren Gateways hinzuzufügen, wählen Sie **Netzwerk** > **GlobalProtect** > **Portale** aus.
2. Wählen Sie **Mobile_User_Template** aus dem Drop-down-Menü **Vorlage** aus.
3. Wählen Sie **GlobalProtect_Portal** aus, um die Prisma Access-Portalkonfiguration zu bearbeiten.

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Fügen Sie Ihr lokales Gateway der Liste der Gateways in der Agent-Konfiguration hinzu.

1. Wählen Sie die Registerkarte **Agent** und die Agent-Konfiguration **DEFAULT** (Standard) aus. Alternativ können Sie eine neue Agent-Konfiguration **hinzufügen**.
2. Wählen Sie die Registerkarte **Extern** aus, um Ihr lokales Gateway **hinzuzufügen**.




*Wenn Sie eine neue Agent-Konfiguration hinzufügen und die Prisma Access-Gateways der Liste der externen Gateways in dieser Konfiguration hinzufügen möchten, müssen Sie den **Namen** auf **GP Cloud Service** und die **Adresse** auf **gpcloudservice.com** festlegen. Geben Sie diese Werte genau wie angegeben ein. Sie können keinen dieser Werte für Nicht-Prisma Access Gateways verwenden.*

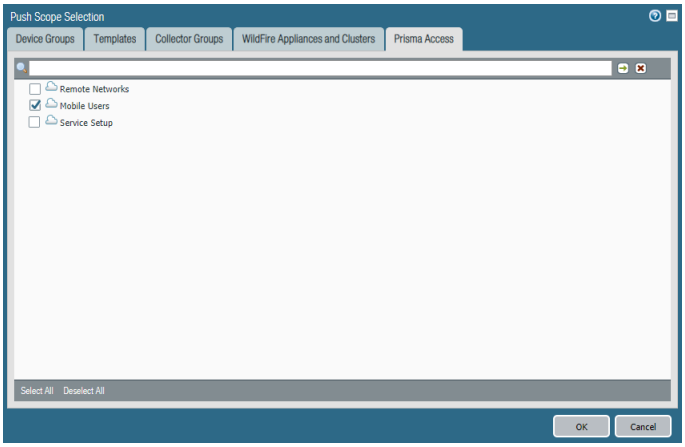
3. Geben Sie den **Namen** des Gateways ein und legen Sie entweder den **FQDN** oder die **IP**-Adresse des Gateways im Feld **Adresse** fest. Dieser Wert muss exakt mit dem allgemeinen Namen (Common Name, CN) im Gateway-Zertifikat übereinstimmen.
4. (Optional) Wenn mobile Benutzer sich nur dann mit dem Gateway verbinden sollen, wenn sie sich in der entsprechenden Region befinden, müssen Sie die **Quellregion hinzufügen**, auf die das Gateway beschränkt werden soll. Wenn beispielsweise ein Gateway in Frankreich vorliegt, würden Sie FR (Frankreich) auswählen. Wenn ein Gateway in Schweden vorliegt, würden Sie SE (Schweden) auswählen.

   Dies hat unter anderem den Vorteil, dass Benutzer dann auf ein Gateway zugreifen können, das den Zugriff auf Internetressourcen in ihrer eigenen Sprache ermöglicht.
5. (Optional) Legen Sie die Priorität des Gateways fest.
6. Konfigurieren Sie weitere Agent-Einstellungen, um die Agent-Konfiguration abzuschließen.
7. Klicken Sie auf **OK**, um die Portalkonfiguration zu speichern.

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Übertragen Sie alle Änderungen an Panorama und übertragen Sie die Konfigurationsänderungen per Push an Prisma Access.

1. Klicken Sie auf **Commit** > **Commit in Panorama**.
2. Klicken Sie auf **Commit** > **An Geräte übertragen**, und klicken Sie auf **Auswahl bearbeiten**.
3. Vergewissern Sie sich, dass auf der Registerkarte **Prisma Access Prisma Access für Benutzer** ausgewählt ist, und klicken Sie dann auf **OK**.




4. Klicken Sie auf **Push**.

## Priorität für Prisma Access und lokale Gateways festlegen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

Sie können ein lokales Gateway auswählen, das Ihren mobilen Benutzern physisch am nächsten liegt, und Benutzern erlauben, sich mit einem anderen Gateway (entweder lokal oder in der Cloud) zu verbinden, um einen sicheren Zugriff für mobile Benutzer zu gewährleisten, wenn sie den Standort wechseln. Sie können für Gateways, die sich im selben Land oder Sprachgebiet wie Ihre mobilen Benutzer befinden, auch Prioritäten festlegen.

Wenn Benutzer eine Verbindung zu einem bestimmten Prisma Access-Gateway herstellen müssen, können Sie mobilen Benutzern erlauben, bestimmte Prisma Access-Gateways manuell auszuwählen. Mobile Benutzer wählen eines der Prisma Access-Gateways mit der GlobalProtect-App aus, die auf ihrem Endpunkt installiert ist.

Gehen Sie wie folgt vor, um Gateway-Prioritäten in Prisma Access zu konfigurieren.

- Gleiche Gateway-Prioritäten für lokale und Prisma Access-Gateways festlegen
- Höhere Gateway-Priorität für ein lokales Gateway festlegen
- Höhere Prioritäten für mehrere lokale Gateways festlegen
- Prioritäten für Prisma Access- und lokale Gateways konfigurieren

 ©2025 Palo Alto Networks, Inc.

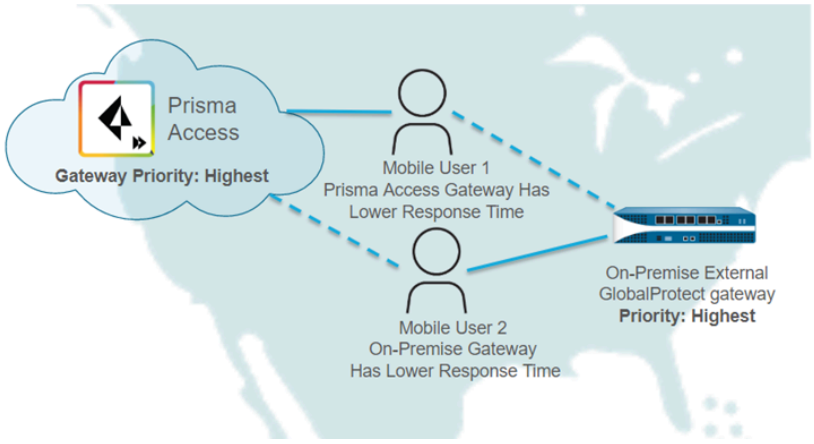
### Gleiche Gateway-Prioritäten für lokale und Prisma Access-Gateways festlegen

Damit Ihre mobilen Mitarbeiter unabhängig vom Standort sicheren Zugriff haben, können Sie für die lokalen GlobalProtect-Gateways und die Prisma Access-Gateways gleiche Prioritäten festlegen. Die GlobalProtect-App verwendet Gateway-Priorität in einer Konfiguration mit mehreren Gateways, um das bevorzugte Gateway zu ermitteln.

Sie können diese Konfiguration verwenden, wenn sich Ihre mobilen Benutzer meist näher an einem lokalen Gateway befinden. Wenn Benutzer den Standort wechseln, wählt die GlobalProtect-App ein anderes Gateway (entweder ein lokales oder ein Prisma Access-Gateway) basierend auf der höchsten Priorität und der niedrigsten Reaktionszeit aus.

In der folgenden Abbildung ist ein Konfigurationsbeispiel mit zwei mobilen Benutzern in Nordamerika dargestellt. Legen Sie die Gateway-Priorität sowohl für die Prisma Access-Gateways als auch für die lokalen Gateways auf **Höchste** fest.

In diesem Beispiel bestimmt die GlobalProtect-App von Benutzer 1, dass das Prisma Access-Gateway eine geringere Reaktionszeit als das lokale Gateway hat, und die GlobalProtect-App von Benutzer 2 bestimmt, dass das lokale Gateway eine geringere Reaktionszeit hat. Da alle Gateways die gleiche Priorität haben, verbindet sich Benutzer 1 mit dem Prisma Access-Gateway und Benutzer 2 mit dem lokalen Gateway aufgrund der geringeren Reaktionszeit.




### Höhere Gateway-Priorität für ein lokales Gateway festlegen

Wenn Sie mobile Benutzer anweisen möchten, ein lokales Gateway anstelle der Prisma Access-Gateways zu verwenden, geben Sie die lokalen Gateways mit einer Quellregion und einer höheren Priorität als das Prisma Access-Gateway an.

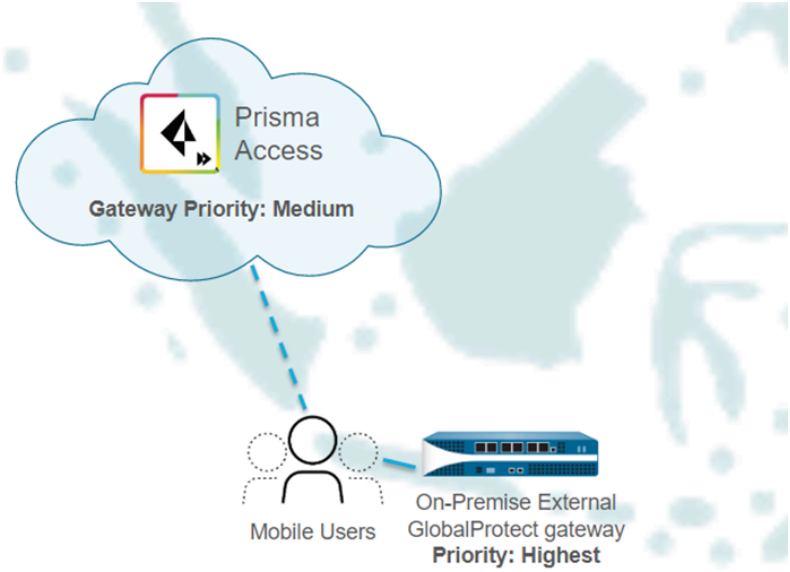
In der folgenden Abbildung ist ein Konfigurationsbeispiel für mobile Benutzer in Indonesien dargestellt. Um zu vermeiden, dass mobile Benutzer mit dem nächstgelegenen Prisma Access-Gateway in Singapur verbunden werden, legen Sie für das lokale Gateway in Indonesien die Gateway-Priorität **Höchste** und für die Prisma Access-Gateways die Priorität **Mittel** fest.

In diesem Beispiel wird auch die Quellregion „Indonesien“ für das lokale Gateway angegeben. Wir empfehlen die Angabe einer Quellregion aus folgenden Gründen:

- Durch die Angabe einer Quellregion für ein lokales Gateway können Benutzer in einer Region auf dieses Gateway zugreifen, während verhindert wird, dass sich Benutzer außerhalb dieser Region mit diesem Gateway verbinden. In diesem Beispiel können sich nur mobile Benutzer in Indonesien mit dem lokalen Gateway mit der Quellregion „Indonesien“ verbinden. Die höhere Priorität bedeutet, dass das lokale Gateway Vorrang vor den Prisma Access-Gateways hat.

 ©2025 Palo Alto Networks, Inc.

- Wenn Sie eine **beliebige** Quellregion für das lokale Gateway in Indonesien festlegen, würde jeder mobile Benutzer in Ihrer Organisation das lokale Gateway in Indonesien bevorzugen, da es eine höhere Priorität hat und weltweit zugänglich ist. Diese Konfiguration bedeutet, dass sich mobile Benutzer möglicherweise nie mit den Prisma Access-Gateways verbinden.




### Höhere Prioritäten für mehrere lokale Gateways festlegen

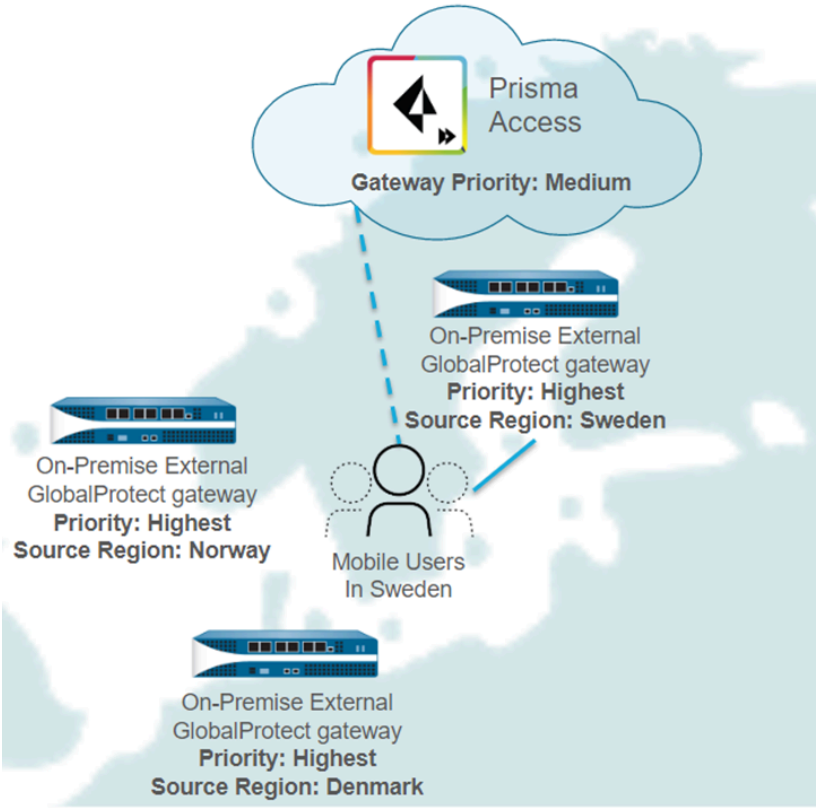
Um sicherzustellen, dass der Datenverkehr ins Internet innerhalb sprachspezifischer Regionen bleibt, können Sie mehrere Gateways in mehreren Quellregionen konfigurieren. Legen Sie dabei für die lokalen Gateways die Priorität **Höchste** und für die Prisma Access-Gateways die Priorität **Mittel** fest.

In der folgenden Abbildung ist ein Konfigurationsbeispiel für mobile Benutzer in Skandinavien dargestellt. Wenn mobile Benutzer mit dieser Konfiguration auf Internet-Websites zugreifen, verwenden die Websites den Zeichencodierungssatz für die jeweiligen Sprachen.

In diesem Beispiel konfigurieren Sie lokale Gateways mit Quellregionen in Dänemark, Norwegen und Schweden. Sie setzen die Priorität dieser Gateways auf **Höchste** und die Priorität der Prisma Access-Gateways auf **Mittel**. Durch die Angabe einer Quellregion für die lokalen Gateways können Benutzer in diesen Regionen auf diese Gateways zugreifen, während verhindert wird, dass sich Benutzer außerhalb dieser Regionen mit diesen Gateways verbinden.

In diesem Beispiel wählt die GlobalProtect-App für mobile Benutzer in Schweden aufgrund der Quellregion und der höheren Gateway-Priorität das lokale Gateway in Schweden aus.

 ©2025 Palo Alto Networks, Inc.




### Prioritäten für Prisma Access- und lokale Gateways konfigurieren

Verwenden Sie diesen Workflow, um Prioritäten für eine Bereitstellung zu konfigurieren, die lokale Gateways mit Prisma Access verwendet.

**STEP 1 |** Melden Sie sich bei Prisma Access an.

**STEP 2 |** Wählen Sie in der Vorlage **Mobile_User_Template** die Optionen **Netzwerk** > **GlobalProtect** > **Portale** aus.

**STEP 3 |** Klicken Sie im Feld **Name** auf den Portalnamen.

**STEP 4 |** Klicken Sie auf die Registerkarte **Agent**.

**STEP 5 |** Klicken Sie auf den Namen des zu konfigurierenden Agenten.

Der Standardagent hat den Namen **STANDARD**.

**STEP 6 |** Klicken Sie auf die Registerkarte **Extern**.

 ©2025 Palo Alto Networks, Inc.

**STEP 7 |** Legen Sie die Priorität der Prisma Access-Gateways fest.

1. Klicken Sie auf **GP-Cloud-Dienst**.
2. Legen Sie die Priorität für Ihre bevorzugte Konfiguration fest.
   - Wenn Sie gleiche Gateway-Prioritäten für lokale und Prisma Access-Gateways festlegen möchten, ändern Sie die Priorität von **Keine** in **Höchste**.
   - Zum Festlegen einer höheren Gateway-Priorität für ein lokales Gateway oder zum Festlegen höherer Prioritäten für mehrere lokale Gateways ändern Sie die Priorität von **Keine** in **Mittel**.
3. Stellen Sie sicher, dass das Kontrollkästchen **Manuell** aktiviert ist.

   Aktivieren Sie das Kontrollkästchen **Manuell**, um sicherzustellen, dass mobile Benutzer bei Bedarf ein bestimmtes Prisma Access-Gateway auswählen können.

   *Fügen Sie keine Quellregion für die Prisma Access-Gateways hinzu. Keine der von Ihnen angegebenen Regionen wird auf die Konfiguration angewendet.*
4. Klicken Sie auf **OK**.

**STEP 8 |** Sie können Ihrer Konfiguration eine oder mehrere lokale externe Gateways **hinzufügen**.

1. Geben Sie einen aussagekräftigen **Namen** für das Gateway ein.

   Der eingegebene Name muss mit dem Namen übereinstimmen, den Sie bei der Konfiguration des Gateways definiert haben. Er sollte aussagekräftig genug sein, damit Benutzer wissen, an welchem Standort sich das Gateway befindet, mit dem sie sich verbinden.
2. Geben Sie in das Feld „Adresse“ den FQDN oder die IP-Adresse der Schnittstelle ein, an der das Gateway konfiguriert ist.

   Sie können eine IPv4-Adresse konfigurieren. Die von Ihnen angegebene Adresse muss exakt mit dem allgemeinen Namen (Common Name, CN) im Gateway-Serverzertifikat übereinstimmen.
3. Fügen Sie eine oder mehrere **Quellregionen** für das lokale Gateway hinzu, oder wählen Sie **Beliebige** aus, um das Gateway für alle Regionen verfügbar zu machen.

   *Wenn Sie die Priorität lokaler externer Gateways höher als die von Prisma Access-Gateways festlegen, empfehlen wir, Quellregionen für die externen Gateways anzugeben. Wenn Sie **Beliebige** für die Region angeben, wählt die GlobalProtect-App aufgrund der höheren Priorität für die lokalen Gateways möglicherweise niemals Prisma Access-Gateways anstelle von lokalen Gateways aus.*
4. Aktivieren Sie das Kontrollkästchen **Manuell**, damit Benutzer manuell zum Gateway wechseln können.
5. Setzen Sie die **Priorität** des lokalen Gateways auf **Höchste** (Standardeinstellung).
6. Klicken Sie auf **OK**.

 ©2025 Palo Alto Networks, Inc.

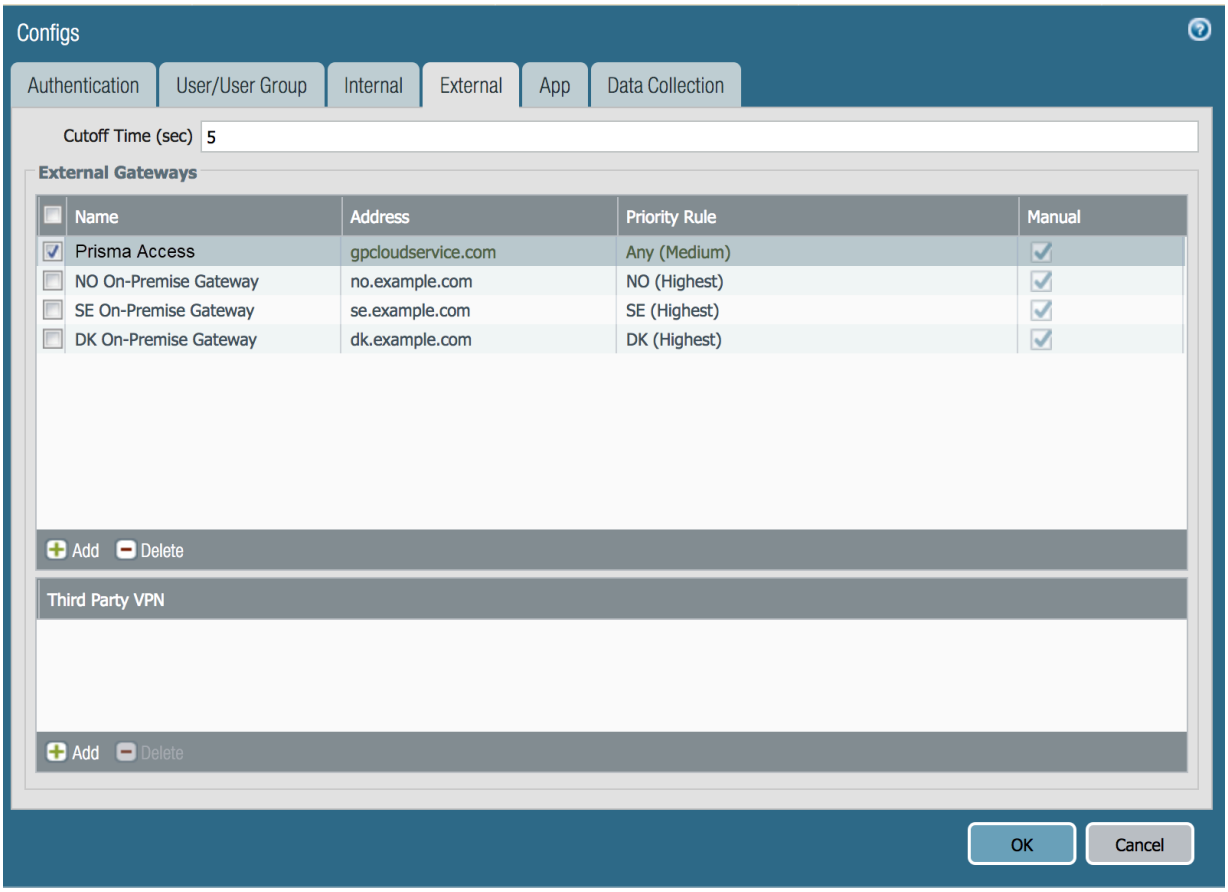
**STEP 9 |** (Optional) Legen Sie die Priorität für zusätzliche Gateways fest, indem Sie Schritt 8 wiederholen.

*Achten Sie darauf, die richtigen Quellregionen anzugeben.*

In der folgenden Abbildung ist eine Beispielkonfiguration mit mehreren Gateways mit Quellregionen in Norwegen, Schweden und Dänemark dargestellt. Beachten Sie, dass das

 ©2025 Palo Alto Networks, Inc.

Kontrollkästchen **Manuell** aktiviert ist. Dies weist darauf hin, dass ein mobiler Benutzer ein beliebiges dieser Gateways manuell auswählen kann.




 ©2025 Palo Alto Networks, Inc.

# Mobile Benutzer: Expliziter Proxy

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

Prisma Access von Palo Alto Networks ist eine Security Service Edge(SSE)-Lösung, die branchenführende Cloud-SWG-Funktionalität bietet, darunter erweiterte URL-Filterung, SSL-Entschlüsselung, SaaS-Anwendungssteuerung und fortschrittliche Bedrohungsabwehr. Prisma Access operationalisiert Sicherheitsbereitstellungen der nächsten Generation mit einer flächendeckenden und immer verfügbaren cloudnativen Infrastruktur, die vollständig von Palo Alto Networks verwaltet wird. Mobile Benutzer und Remote-Standorte können im Rahmen der Unternehmensrichtlinien sicher auf das Internet und SaaS-Anwendungen zugreifen. Prisma Access bietet flexible Konnektivitätsoptionen: „PAC-Dateien“, „Agent“, „Agentenlos“ und „Site-to-Site-IPSEC“, um sicherzustellen, dass ältere oder alternative Cloud-Proxy-Architekturen mit minimalen Netzwerkänderungen auf Prisma Access verschoben werden können.

**Expliziter Proxy**

Prisma Access bietet eine umfassende Secure Web Gateway(SWG)-Funktion für die Cloud, einschließlich einer Verbindungsmethode mit explizitem Proxy, die auf der Cloud basiert. Wenn das bestehende Netzwerk Ihres Unternehmens bereits explizite Proxys verwendet und PAC-Dateien auf Ihren Clientendpunkten bereitstellt, können Sie problemlos von älteren proxybasierten SWG-Lösungen zu Prisma Access migrieren, um den ausgehenden Internetdatenverkehr mobiler Benutzer zu schützen. Sie können auch einen expliziten Proxy verwenden, wenn Sie einen Proxy für Compliancezwecke verwenden müssen. Expliziter Proxy verwendet die Lizenz für mobile Benutzer.

Wenn Sie mehrere PAC-Dateien verwenden, um zu definieren, wie Sie Webdatenverkehr für verschiedene Benutzer oder Systeme leiten, bietet Ihnen Prisma Access die Möglichkeit, diese PAC-Dateien mit Weiterleitungsprofilen zu verknüpfen, sodass Sie mehrere PAC-Dateien gleichzeitig verwenden können. Anstatt eine PAC-Datei zu erstellen, können Sie darüber hinaus mithilfe von Weiterleitungsprofilen einfache Weiterleitungsregeln konfigurieren, um die Richtung Ihres Webdatenverkehrs zu definieren.


- Unterstützte Standorte
- Expliziter Proxy mit der GlobalProtect-App
  - GlobalProtect im Proxy-Modus
  - GlobalProtect im Tunnel- und Proxy-Modus
- Expliziter Proxy mit PAC-Dateien
  - Einrichtung mit SAML
  - Einrichtung mit Kerberos


 ©2025 Palo Alto Networks, Inc.

- Weiterleitungsprofile
  - Unterstützung mehrerer PAC-Dateien
  - Weiterleitungsregeln
  - Weiterleitungsprofile mit GlobalProtect

**Prisma Access-Funktionen für expliziten Proxy**

| Merkmal | Beschreibung |
|---|---|
| App-ID | Klassifiziert kontinuierlich alle Anwendungen unabhängig von Port, TLS/SSL-Verschlüsselung oder Technik, die ein Angreifer verwendet, um sich der Erkennung zu entziehen. Im Gegensatz zu älteren Lösungen, die von den Layern 3 und 4 als ersten Kontrollebenen abhängen, bevor die Anwendungsklassifizierung angewendet wird, wendet Prisma Access die App-ID zusammen mit anderen Layer-7-Steuerelementen an, wie z. B. die Benutzer-ID. |
| Benutzer-ID | Lasst sich in eine Vielzahl von Benutzeridentitätsrepositorys integrieren, sodass Ihre Richtlinien Ihren Benutzern und Gruppen unabhängig von deren Standort folgen. |
| SSL-Entschlüsselung | Prüft und wendet die Richtlinie auf TLS/SSL-verschlüsselten Datenverkehr an. Für Datenschutz und regulatorische Compliance können Sie die Entschlüsselung flexibel basierend auf URL, Quelle, Ziel, Benutzer, Benutzergruppe und Port aktivieren oder deaktivieren. |
| KI/ML-basierte Erkennung | Bietet eine signaturlose Inline-Angriffserkennung und Zero-Day-Exploit-Prävention. Prisma Access passt sich an und bietet im Vergleich zu geplanten Updates sofortigen Echtzeitschutz. Damit werden bis zu 95 % der unbekannten Bedrohungen sofort verhindert, mit einer Signaturzustellung von weniger als 10 Sekunden, was zu einer Reduzierung der infizierten Systeme um 99,5 % führt. |
| DNS Security | Wendet Echtzeitschutz und Inline Machine Learning an, um C2-Rückrufe und andere Angriffe, die DNS verwenden, zu unterbrechen. Erweiterte DNS-Sicherheit ist nativ in Prisma Access integriert und bietet automatisierten Schutz, wodurch Angreifer daran gehindert werden, Sicherheitsmaßnahmen zu umgehen. Zudem sind weder unabhängige Tools noch Änderungen am DNS-Routing erforderlich. |
| Erweiterte URL-Filterung | Herausragender Schutz vor webbasierten Bedrohungen wie Phishing, Malware und C2, der leistungsstarken Datenbankschutz mit einer ML-basierten Websicherheits-Engine kombiniert, die neue bösartige URLs in Echtzeit kategorisiert und blockiert. Der branchenführende Phishing-Schutz bekämpft die häufigsten Ursachen von Sicherheitsverletzungen und ermöglicht es Ihnen, die Kontrolle über Ihren Webdatenverkehr durch fein abgestimmte Kontrollen und Richtlinieneinstellungen zurückzugewinnen, die |

 ©2025 Palo Alto Networks, Inc.

| Merkmal | Beschreibung |
|---|---|
| | Sicherheitsmaßnahmen basierend auf Benutzern, Risikobewertungen und Inhaltskategorien automatisieren. |
| Fortschrittliche Bedrohungsabwehr | Stoppen Sie Zero-Day-Bedrohungen, bekannte Exploits, Malware, Spyware und bösartige Command-and-Control(C2)-Funktionen mit branchenführender Threat Prevention. Steigern Sie im Vergleich zu herkömmlichen Einbruchschutzsystemen die Verhinderung unbekannter Injektionsangriffe um 60 % und die Verhinderung von stark ausweichendem C2-Verkehr um 48 %. |
| Advanced WildFire | Sorgen Sie für die Sicherheit von Dateien, indem Sie bekannte, unbekannte und stark ausweichende Malware mit der branchenweit größten Engine zur Abwehr von Bedrohungsdaten und Malware 60-mal schneller verhindern. |
| NG-CASB* | Gewinnen Sie proaktive SaaS-Transparenz, Schutz vor Fehlkonfigurationen und Echtzeitdatenschutz für erstklassige SaaS-Sicherheit. |
| Data Loss Prevention (DLP)* | Umfasst eine Reihe von Tools und Prozessen, mit denen Sie vertrauliche Informationen vor unbefugtem Zugriff, Missbrauch, Extraktion oder Weitergabe schützen können. Mit DLP in Prisma Access können Sie Datensicherheitsrichtlinien durchsetzen und den Verlust sensibler Daten von mobilen Benutzern und Remote-Netzwerken verhindern. |
| Unterstützung von Remote-Browser-Isolation | Wird über CloudBlades in RBI-Clouds von Drittanbietern integriert, indem vorhandene NGFW-URL-Kategorisierung und URL-Umschreibungsfunktionen genutzt werden, um ausgewählten oder den gesamten internetgebundenen Datenverkehr an die RBI-Cloud weiterzuleiten. Diese Funktion bietet eine nahtlose Benutzererfahrung, da bestimmter Datenverkehr (unbekannte oder Hochrisikokategorien) zur zusätzlichen Inspektion an RBI weitergeleitet wird, während der verbleibende Datenverkehr von Prisma Access geprüft werden und direkt ins Internet gelangen kann. |
| Berichterstattung | Umfasst standardmäßig einen detaillierten, anpassbaren SaaS-Anwendungsnutzungsbericht, der Einblick in den gesamten SaaS-Datenverkehr – sanktioniert und nicht sanktioniert – in Ihrem Netzwerk bietet. Sie können auch benutzerdefinierte Berichte basierend auf Ihren Bedürfnissen erstellen und diese einfach planen, herunterladen und mit anderen in Ihrer Organisation teilen. |
| Benutzerauthentifizierung | Unterstützt alle vorhandenen PAN-OS-Authentifizierungsmethoden, einschließlich Kerberos, RADIUS, SAML, LDAP, Clientzertifikate und einer lokalen Benutzerdatenbank. Kerberos und SAML werden nur mit PAC unterstützt. |

 ©2025 Palo Alto Networks, Inc.

| Merkmal | Beschreibung |
|---|---|
| Site-to-Site-IPsec-VPN | Unterstützt Site-to-Site-Tunnel über IPv4 und IKEv1/IKEv2, um Kompatibilität zu gewährleisten. Für mehrere Verbindungsstandorte kann das ECMP-Routing zusätzliche Redundanz und Kosteneffizienz bieten, indem Sitzungen über verfügbare Internetverbindungen ausgeglichen werden. |
| Protokollierung | Zeigt die Protokollierung von Datenverkehr, Anwendungen, Benutzern, Bedrohungen, URLs und Datenfiltern an, um die Organisation von Daten über den cloudbasierten Strata-Protokollierungsdienst zu erleichtern. |
| Weiterleitungsprofile | Ermöglicht die Verwendung mehrerer PAC-Dateien für verschiedene Benutzergruppen oder Systeme. Unterstützt auch die Erstellung von Weiterleitungsregeln zur Definition der Richtung des Webdatenverkehrs, um eine einfachere Alternative zum Erstellen und Pflegen einer PAC-Datei bereitzustellen. |

*Erfordert eine Add-on-Lizenz.

Eine detaillierte Beschreibung der Produkteigenschaften und -funktionen entnehmen Sie bitte dem Prisma Access-Datenblatt.

# Konfigurationsrichtlinien für den expliziten Proxy

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

### Systemanforderungen und unterstützte Funktionen

Dies sind die Systemanforderungen und unterstützten Funktionen für die verschiedenen Verbindungsmethoden, die Sie mit dem expliziten Proxy verwenden können.

| | SAML ohne Agent | Kerberos ohne Agent | Proxy-Modus für Agent (erfordert GP 6.2 oder höher) | Proxy-Modus für Remote-Netzwerke |
|---|---|---|---|---|
| **Anwendungen und OS-Unterstützung** | | | | |
| **Datenverkehrstyp** | Nur Internet- und öffentlicher | Nur Internet- und öffentlicher | Nur Internet- und öffentlicher | Nur Internet- und öffentlicher |

 ©2025 Palo Alto Networks, Inc.

| | | | | |
|---|---|---|---|---|
| | SaaS-Datenverkehr | SaaS-Datenverkehr | SaaS-Datenverkehr | SaaS-Datenverkehr |
| **Unterstütztes Protokoll** | Proxyfähiges HTTP oder HTTPS | Proxyfähiges HTTP oder HTTPS | Proxyfähiges HTTP oder HTTPS | Proxyfähiges HTTP oder HTTPS |
| **Transportkanal nach Prisma Access** | HTTP-Verbindung | HTTP-Verbindung | HTTP-Verbindung innerhalb von TLS | HTTP-Verbindung innerhalb von IPSec vom Zweig zum Sicherheitsverarbeitungsknote (SPN) des Remote-Netzwerks |
| **Unterstützte Umgebungen** | Windows, Mac, Linux, ChromeOS, VDI | Windows, Mac, Linux,<br>ChromeOS, VDI | Windows und Mac | Windows, Mac, Linux,<br>ChromeOS, VDI |
| **App-Unterstützung** | Proxyfähige HTTP(s)-Apps | Jede App, die eine PAC-Datei oder System-Proxy-Einstellung berücksichtigt und Kerberos unterstützt | Proxyfähige HTTP(s)-Apps | Proxyfähige HTTP(s)-Apps |
| **Browser-Unterstützung** | Chrome#, Edge, Firefox ab Version 115 | Chrome#, Edge, Firefox ab Version 115 | Chrome#, Edge, Firefox ab Version 115* | Chrome#, Edge, Firefox ab Version 115 |
| **O365-Unterstützung†** | Browser- und Client-Apps | Browser- und Client-Apps | Browser- und Client-Apps | Browser- und Client-Apps |
| **Identität** | | | | |
| **Benutzer-ID‡** | Entschlüsselter und Nicht-HTTP-CORS-Datenverkehr | Gesamter unterstützter Datenverkehr | Gesamter unterstützter Datenverkehr | Je nachdem, ob Sie SAML oder Kerberos verwenden: entschlüsselter/ Nicht-CORS X-Authenticated-User-Datenverkehr |

 ©2025 Palo Alto Networks, Inc.

| | | | | |
|---|---|---|---|---|
| **Unterstützte Authentifizierungen** | SAML (beliebige IDPs von SAML 2.0 oder über CIE) | Kerberos | Alle von GlobalProtect unterstützten Authentifizierungen | SAML, Kerberos, X-Authenticated-User-basiert |
| **Authentifizierungen überspringen** | Nach Domäne und Quell-IP | Nach Domäne und Quell-IP | Nach Domäne | Nach Domäne und Quell-IP |
| **Benutzergruppenverzeichnis** | Alle CIE-unterstützten Verzeichnisse | Alle CIE-unterstützten Verzeichnisse | Alle CIE-unterstützten Verzeichnisse | Alle CIE-unterstützten Verzeichnisse |
| **Lizenz** | Mobiler Benutzer-Einheit pro Benutzer | Mobiler Benutzer-Einheit pro Benutzer | Mobiler Benutzer-Einheit pro Benutzer | Mobiler Benutzer-Einheit pro Benutzer oder Headless-Gerät und NET-Einheiten für Bandbreite für Remote-Netzwerke |
| **Verwaltung** | | | | |
| **Multitenant Panorama** | Unterstützt auf ersten Mandanten | Unterstützt auf ersten Mandanten | Unterstützt auf ersten Mandanten | Unterstützt auf ersten Mandanten |
| **Multitenant Cloud Management** | Unterstützt | Unterstützt | Unterstützt | Unterstützt |
| **Sicherheitsdienste** | | | | |
| **SaaS Inline** | Unterstützt | Unterstützt | Unterstützt | Unterstützt |
| **DLP** | Unterstützt | Unterstützt | Unterstützt | Unterstützt |
| **DNS Security§** | Unterstützt | Unterstützt | Unterstützt | Unterstützt |
| **Erweiterte URL-Filterung** | Unterstützt | Unterstützt | Unterstützt | Unterstützt |
| **Advanced WildFire** | Unterstützt | Unterstützt | Unterstützt | Unterstützt |
| **Fortschrittliche Bedrohungsabwehr** | Unterstützt | Unterstützt | Unterstützt | Unterstützt |

 ©2025 Palo Alto Networks, Inc.

| | | | | |
|---|---|---|---|---|
| Remote-Browser-Isolation | Unterstützt | Unterstützt | Unterstützt | Unterstützt |
| **Private IP-Sichtbarkeit und Durchsetzung** | Nicht unterstützt | Nicht unterstützt | Unterstützt für bekannte Standorte oder Zweigstellen | Unterstützt |
| **Ausgangs-NAT** | Unterstützt | Unterstützt | Unterstützt | Unterstützt |
| **Privater App-Zugriff** | Nicht unterstützt | Nicht unterstützt | Unterstützt über Dienstverbindungen | Nicht unterstützt |
| **Gesamter TCP-Datenverkehr** | Nicht unterstützt | Nicht unterstützt | Unterstützt (mit GlobalProtect Version 6.3.1) | Nicht unterstützt |
| **ZTNA-Connector** | Nicht unterstützt | Nicht unterstützt | Unterstützt | Nicht unterstützt |
| **Colo Connect** | Nicht unterstützt | Nicht unterstützt | Unterstützt | Nicht unterstützt |
| **Dienstverbindungen** | Unterstützt | Unterstützt | Unterstützt | Unterstützt |
| **HIP-Unterstützung (Tunnel- und Proxy-Modus)** | Nicht unterstützt | Nicht unterstützt | Unterstützt | Nicht unterstützt |

# Folgen Sie für den Chrome-Browser den unten aufgeführten Anweisungen, um TLS 1.3 Kyber zu deaktivieren, wenn die Entschlüsselung aktiviert ist:

1. Öffnen Sie den Chrome-Browser.
2. Fügen Sie `chrome://flags/#enable-tls13-kyber` in der Adressleiste hinzu und deaktivieren Sie es.
3. Klicken Sie auf **Neu starten**.

* Für den Proxy-Modus für Agent benötigt Firefox eine manuelle Richtlinienregel, die über die Mobilgeräteverwaltung übertragen wird und den System-Proxy anweist.

† Der explizite Proxy unterstützt nur HTTP-Datenverkehr, nicht UDP. Mit SAML bietet der explizite Proxy keine Benutzer-ID für Client-App-Flüsse. Für Agent-Proxys müssen Sie eine PAC-Datei verwenden, um Client-App-Authentifizierungsflüsse an den Cloud-Proxy zu senden.

‡ Für das Umgehen der Authentifizierung ist keine Benutzer-ID verfügbar.

§ Sie können DNS-Sicherheitsprofile nicht auf Flüsse des expliziten Proxys anwenden. Blockieren Sie stattdessen Domänen.

**Überlegungen zum App-Support**

 ©2025 Palo Alto Networks, Inc.

1. Der explizite Proxy unterstützt keine Apps, die IP-Affinität benötigen. Die App muss Datenverkehr unterstützen, der von mehreren IPs für eine bestimmte Benutzersitzung kommt.
2. Der explizite Proxy stuft entschlüsselte HTTP/2-Flüsse auf HTTP/1 herunter.
3. Der explizite Proxy ruft keine lokalen externen dynamischen Listen ab.
4. Nur SAML ohne Agent:
    1. Konfigurieren Sie eine SSL-Entschlüsselungsrichtlinie, um eine Umgehung der Authentifizierung nach Domäne für agentenlosen PAC-basierten expliziten Proxy mit SAML-Authentifizierung zu ermöglichen.

        *Entschlüsselung ist erforderlich, damit Prisma Access das von Prisma Access eingerichtete Authentifizierungsstatus-Cookie auf dem Browser des mobilen Benutzers lesen kann. Wenn die Entschlüsselung nicht erzwungen wird, kann der explizite Proxy als offener Proxy missbraucht werden, den Angreifer als Weiterleitungsdienst für Denial-of-Service-Angriffe nutzen können.*
    2. In Datenverkehrsprotokollen zeigt der explizite Proxy unverschlüsselte und HTTP-CORS-Datenverkehrsprotokolle mobiler Benutzer als SWG-authentifizierte Benutzer an.
    3. Beachten Sie die folgenden Browseranforderungen und Nutzungsrichtlinien:
        - Wenn Sie den expliziten Proxy verwenden, deaktivieren Sie nicht Cookies in Ihrem Browser. Andernfalls können Sie keine Webseiten durchsuchen.
        - Wenn Sie den expliziten Proxy mit Microsoft Edge verwenden, stellen Sie sicher, dass Sie **Einstellungen** > **Datenschutz, Suche und Dienste** > **Verhindern der Nachverfolgung** auf **Einfach** setzen.

**Konnektivitätsanforderungen**

Wenn mobile Benutzer eine Verbindung von Remote-Standorten oder Zentralen oder Rechenzentrumsstandorten mit einem expliziten Proxy herstellen, muss der Endpunkt des mobilen Benutzers in der Lage sein, den IdP, den ACS-FQDN, die URL des expliziten Proxys und die URL der PAC-Datei, die von Prisma Access gehostet wird, zu erreichen und dorthin weiterzuleiten.

**Anforderungen und Richtlinien für die PAC-Datei** – Befolgen Sie die Richtlinien für PAC-Dateien, wenn Sie die PAC-Datei für die Verwendung mit explizitem Proxy einrichten.

**Richtlinien zur Proxy-Verkettung** – Wenn Sie Proxy-Verkettung von einem Drittanbieter-Proxy zum expliziten Proxy verwenden, geben Sie die **URL des expliziten Proxys** im Drittanbieter-Proxy an, um Datenverkehr an den expliziten Proxy weiterzuleiten

**Lokale Unterstützung** – Der explizite Proxy ist eine cloudbasierte Proxy-Lösung und kein lokales Produkt. Konfigurieren Sie einen PAN-OS-Web-Proxy für eine lokale Proxy-Lösung.

## GlobalProtect im Proxy-Modus

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama)<br>• Prisma Access (Managed by Strata Cloud Manager) | • Prisma Access Version 5.2<br>• GlobalProtect-App Version 6.2 für Windows oder macOS<br>• Inhaltsversion 8700-7994 |

 ©2025 Palo Alto Networks, Inc.

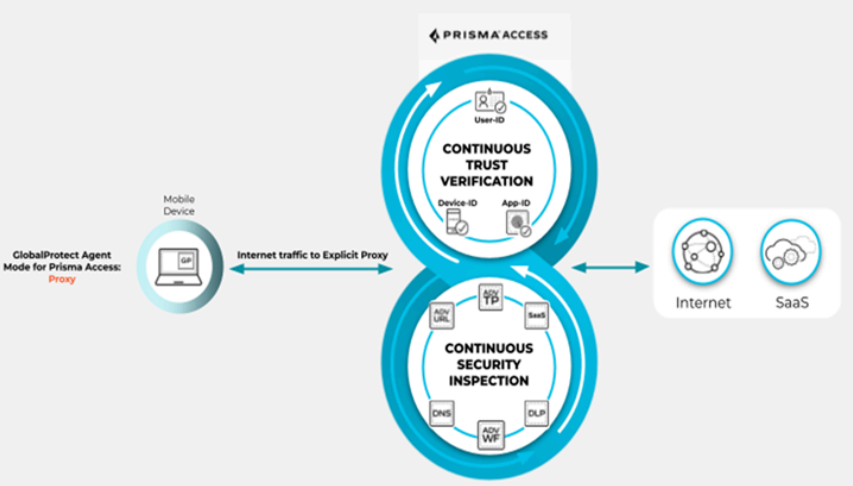
| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| Wenn Sie diese Funktion in Ihrer Prisma Access-Umgebung nutzen möchten, dann wenden Sie sich an Ihr Account-Team, um weiterführende Informationen zu erhalten. | • Prisma Access Mobile-Benutzer-Lizenz |

Im Modus **Proxy** bietet die GlobalProtect-App permanente Internetsicherheit. In diesem Modus leitet die GlobalProtect-App den Datenverkehr auf Basis der Weiterleitungsregeln und der entsprechenden Logik aus der PAC-Datei an Prisma Access weiter. Das Hosting findet in Prisma Access oder in Ihrer Umgebung statt. Dies ist nützlich, wenn Sie über eine vorhandene (ältere) Proxy-Architektur verfügen oder Ihre Proxy-Architektur aus Gründen bestehender Regelungen oder aus Compliance-Gründen beibehalten müssen.

Die agentenbasierte Proxy-Funktion erleichtert die Koexistenz und Interoperabilität der GlobalProtect-App mit VPNs von Drittanbietern. So können Sie den Internetverkehr Ihrer mobilen Benutzer über die GlobalProtect-App zum expliziten Proxy sichern und das VPN von Drittanbietern Ihrer Wahl verwenden, um den Zugriff auf private Anwendungen zu sichern.

*Sie benötigen Strata Cloud Manager und den GlobalProtect-Agenten der Version 6.3.0 für den GlobalProtect-Proxy-Kanal zur Unterstützung aller IPv4-TCP-Verbindungen einschließlich des nicht Proxy-fähigen Datenverkehrs. Um eine nahtlose Funktionalität sicherzustellen, muss das auf den Endpunkten konfigurierte DNS (Domain Name System) in der Lage sein, den vollständig qualifizierten Domänennamen (FQDN) des Ziels aufzulösen.*

In diesem Szenario sendet die GlobalProtect-App den Internetverkehr basierend auf den von Ihnen definierten PAC-Dateiregeln an Prisma Access, während die Endpunktrouten auf Ihre privaten Anwendungen über ein VPN eines Drittanbieters mithilfe eines IPSec/TLS-Tunnels zugreifen.



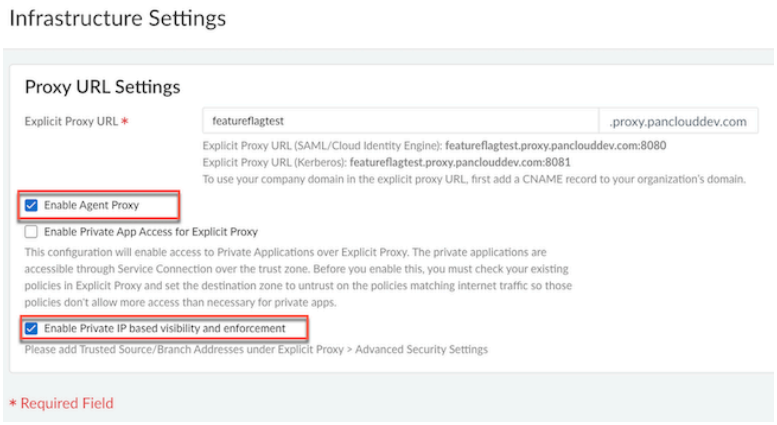

- Strata Cloud Manager
- Panorama

## GlobalProtect im Proxy-Modus (Strata Cloud Manager)

 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** Aktivieren Sie die agentenbasierte Proxy-Funktionalität für mobile Benutzer auf Prisma Access.

1. Aktivieren Sie expliziten Proxy.
   1. Wählen Sie **Workflows** > **Prisma Access-Einrichtung** > **Mobile Benutzer** aus und klicken Sie dann auf **Einrichtung expliziter Proxy**.
   2. Klicken Sie im Bereich „Infrastruktureinstellungen“ auf **Proxy-Einstellungen einrichten** und geben Sie eine **URL des expliziten Proxy** an.
2. Sie müssen den **Agent-Proxy aktivieren** und optional **Sichtbarkeit und Durchsetzung basierend auf privaten IP-Adressen aktivieren** und dann auf **Speichern** klicken.



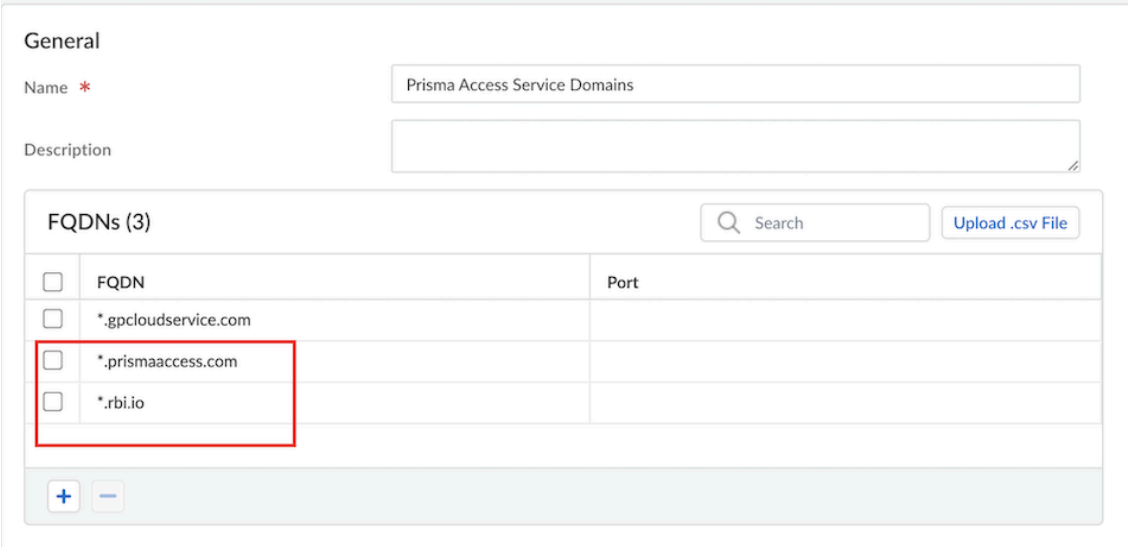

3. Wählen Sie die Prisma Access-Standorte aus, an denen mobile Benutzer unterstützt werden sollen.

   Wenn Sie die Anzahl der Standorte begrenzen möchten, wählen Sie zur Optimierung der Benutzererfahrung die Standorte mit der kürzesten Entfernung zu Ihren Endbenutzern aus. Wenn ein Standort in dem Land, in dem sich Ihre mobilen Benutzer befinden, nicht

 ©2025 Palo Alto Networks, Inc.

verfügbar ist, wählen Sie den Standort mit der kürzesten Entfernung zu Ihren mobilen Benutzern aus.

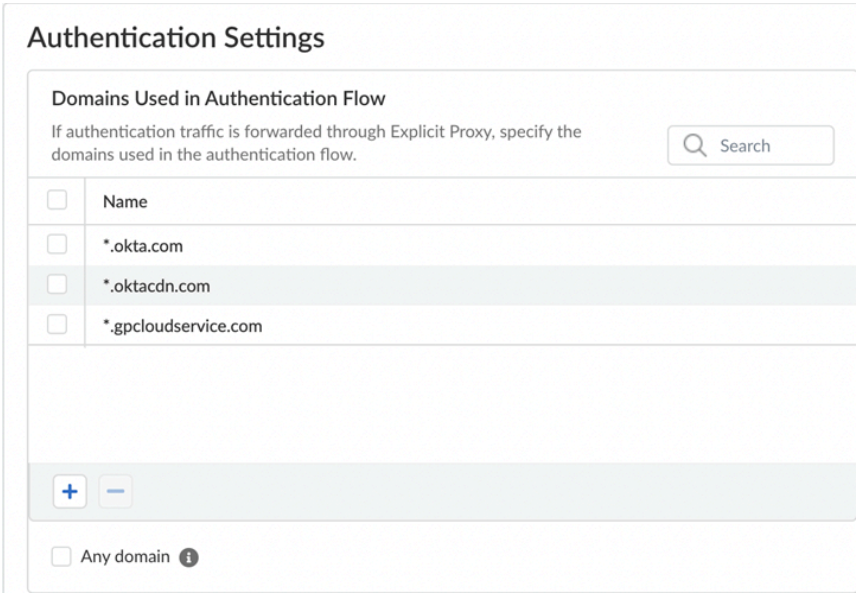
4. Erstellen Sie ein Weiterleitungsprofil, um den Datenverkehr zu definieren, den Sie über expliziten Proxy senden möchten. Umgehen Sie bei der Konfiguration des Weiterleitungsprofils die Domänen *.prismaaccess.com und *.gpcloudservice.com.




5. Verbinden Sie das Weiterleitungsprofil mit Ihrer GlobalProtect-App-Konfiguration.
6. Wählen Sie **Workflows** > **Einrichtung** > **Expliziter Proxy** > **Erweiterte Sicherheitseinstellungen** > **Authentifizierungseinstellungen** aus und fügen Sie die Domänen hinzu, die Sie umgehen müssen.

   Alle Anfragen an den Proxy werden authentifiziert. Wenn Sie jedoch IdP-Abläufe über den Proxy weiterleiten, müssen Sie diese umgehen, damit die Authentifizierung erfolgreich ist.

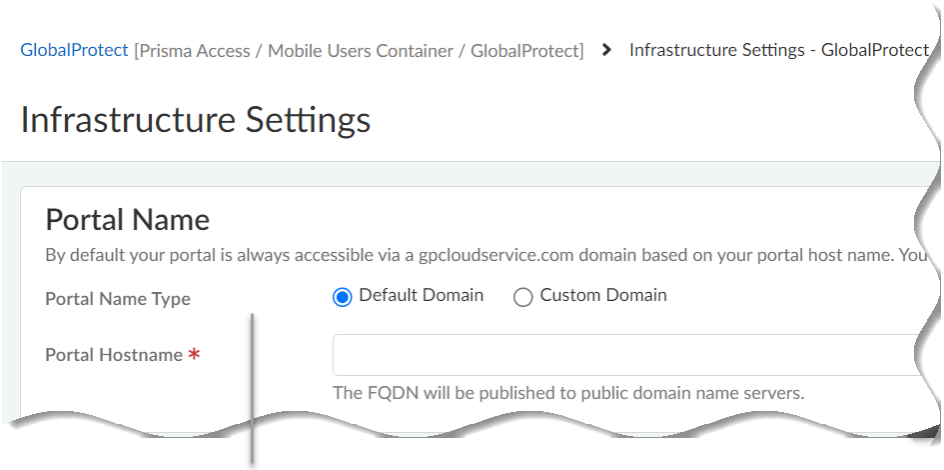
   In diesem Beispiel werden das GlobalProtect-Portal und Okta umgangen. Doch Sie sollten die Domänen an die von Ihnen verwendeten IdPs anpassen.




 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Richten Sie das GlobalProtect-Portal sowie die Authentifizierung ein und konfigurieren Sie den Proxy-Modus für die GlobalProtect-App.

1. Wählen Sie **Workflows** > **Prisma Access-Einrichtung** > **GlobalProtect** > **Infrastruktur** > **Infrastruktureinstellungen** aus und geben Sie einen Wert für **Portalname** ein.




GlobalProtect Infrastructure Settings

   - **Standarddomäne** – Wenn Sie diese Option auswählen, wird als Portal-Hostname der Standarddomänenname `.gpcloudservice.com` verwendet. Geben Sie in diesem Fall einfach einen Wert für **Portal-Hostname** ein, der an den Standarddomänennamen angefügt wird. Prisma Access for Users erstellt automatisch die erforderlichen Zertifikate und veröffentlicht den Hostnamen auf den öffentlichen DNS-Servern.
   - **Benutzerdefinierte Domäne** – Sie können die Portaladresse auch anpassen, wenn die Domäne im Portal-Hostnamen mit Ihrem Firmendomänennamen (z. B. myportal.mydomain.com) übereinstimmen soll.
2. Mobilen Benutzern die Authentifizierung bei Prisma Access ermöglichen.
3. Aktivieren Sie den GlobalProtect-Proxy-Modus für Prisma Access in den GlobalProtect-App-Einstellungen, um Internetverkehr an den agentenbasierten Proxy zu senden.

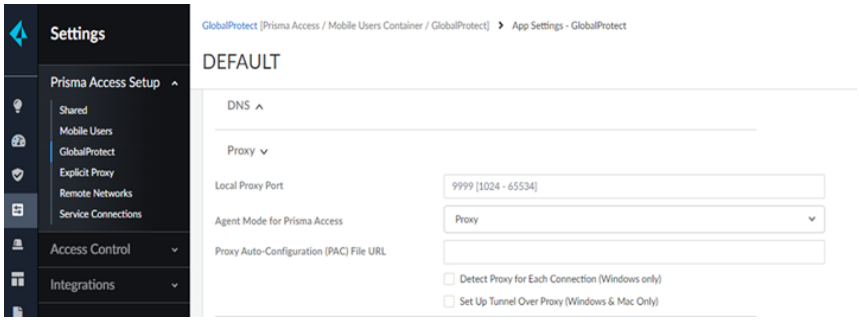
   *Die GlobalProtect-Verbindungsmethode gilt nicht im Proxy-Modus, da sie immer aktiviert ist.*

   - Wählen Sie **Workflows** > **Prisma Access-Einrichtung** > **GlobalProtect** aus.
   - Klicken Sie auf der Registerkarte **GlobalProtect-App** auf **Standard**, um die App-Einstellungen anzupassen. Alternativ hierzu können Sie auch auf **App-Einstellungen hinzufügen** klicken, um eine neue Konfiguration hinzuzufügen.
   - Klicken Sie auf **Erweiterte Optionen anzeigen** und auf den Abschnitt **App-Konfiguration**.
   - Legen Sie als **Agentenmodus für Prisma Access** die Einstellung **Proxy** fest, um die GlobalProtect-App anzuweisen, den Internetverkehr an den expliziten Proxy in Prisma Access zu senden.
   - (Optional) Konfigurieren Sie den lokalen Proxy-Port. Der Portbereich liegt zwischen 1024 und 65534 und der Standardport ist 9999. Wenn der Standardport nicht verfügbar ist, prüft GlobalProtect zehn andere Ports im Bereich von 9999 bis 10009

 ©2025 Palo Alto Networks, Inc.

und verwendet den verfügbaren Port. Sie können auch Ihre eigene Portnummer innerhalb des Bereichs auswählen.

- (Optional) Konfigurieren Sie die URL der Proxy Auto-Configuration-(PAC-)Datei, wenn Sie die neue PAC-URL für die Proxy-Einstellungen per Push an den Endpunkt übertragen möchten. Die PAC-URL wird per Push an den Endpunkt übertragen, sobald der Benutzer eine Verbindung herstellt. Wenn der Benutzer die Verbindung zur GlobalProtect-App trennt, werden die Endpunkt-Proxy-Konfigurationen automatisch deaktiviert und auf die vorherigen Einstellungen zurückgesetzt.
- (Optional) Aktivieren Sie Benutzer darf Netzwerk erneut erkennen, wenn der Benutzer das Portal auf neue Einstellungen überprüfen soll.
- (Optional) Konfigurieren Sie Konfigurationsaktualisierungsintervall für GlobalProtect-App (Stunden). Standardmäßig aktualisiert der GlobalProtect-Client die zwischengespeicherte Portalkonfiguration alle 24 Stunden. Sie können das Aktualisierungsintervall entsprechend Ihren Geschäftsanforderungen ändern.
- Deaktivieren Sie **Tunnel über Proxy einrichten (nur Windows und Mac)**.

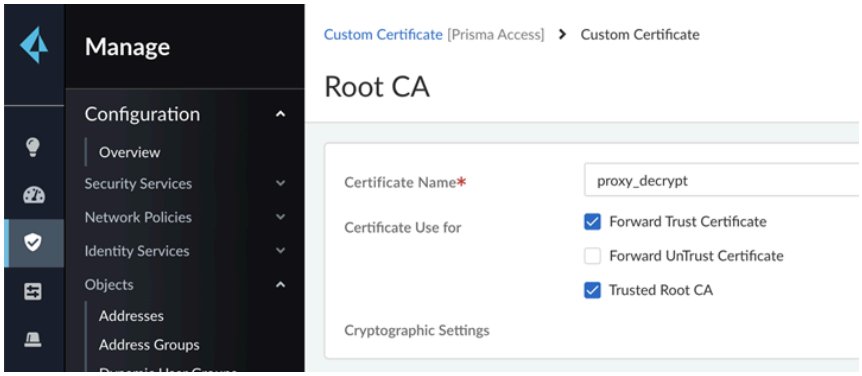



4. Aktivieren Sie für die Internetsicherheit die Option „Immer aktiviert“, indem Sie die folgenden Einstellungen auf der Seite **Workflows** > **Prisma Access-Einrichtung** > **GlobalProtect** > **GlobalProtect-App** > **App-Einstellungen hinzufügen** konfigurieren:
   1. Setzen Sie GlobalProtect deaktivieren auf **Nicht zulassen**, **Mit Passcode zulassen** oder auf **Mit Ticket zulassen**.
   2. Deaktivieren Sie die Option Zulassen, dass sich Benutzer von der GlobalProtect-App abmelden.

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Konfigurieren Sie die Entschlüsselung für Datenverkehr für expliziten Proxy.

- Wählen Sie **Verwalten** > **Konfiguration** > **NGFW und** > **Sicherheitsdienste** > **Entschlüsselung** aus.
- Wenn Sie die Entschlüsselung aktivieren, stellen Sie sicher, dass Sie das Entschlüsselungszertifikat als vertrauenswürdige Stammzertifizierungsstelle einrichten.




**STEP 4 |** Konfigurieren Sie die Sicherheitsrichtlinienregeln für den Datenverkehr über expliziten Proxy.

- Wählen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Sicherheitsdienste** > **Sicherheitsrichtlinie** aus.
- Befolgen Sie die Best Practices der Internet-Gateway-Sicherheitsrichtlinie.

**STEP 5 |** (Optional) Konfigurieren Sie die GlobalProtect-App in einem Netzwerk ohne Standardroute im Proxy-Modus.

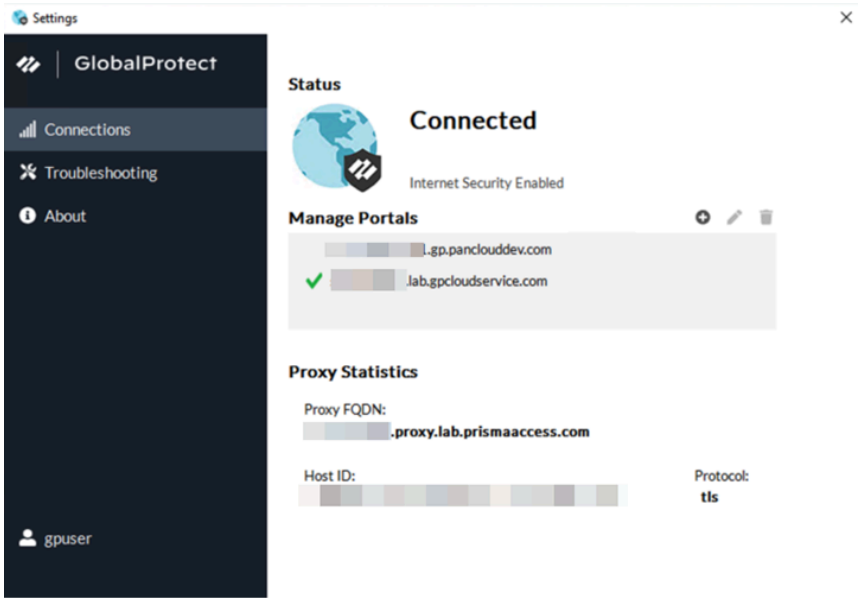
- (Optional) Hosten Sie eine PAC-Datei intern und fügen Sie den FQDN des expliziten Proxy für Prisma Access als Proxy in der PAC-Datei hinzu, oder hosten Sie die PAC-Datei in einem Weiterleitungsprofil und fügen Sie Routen in Ihrem Netzwerk für IP-Adressen des PAC-Dienstes hinzu.
- Leiten Sie in der PAC-Datei die IdP-URL und die URL des Prisma Access-Portals an expliziten Proxy weiter.
- Schließen Sie im expliziten Proxy die IdP- und Portal-URL aus den Authentifizierungseinstellungen aus. Fügen Sie die IdP- und Portal-URL zu der Domäne hinzu, die in den Authentifizierungsabläufen verwendet wird.
- Richten Sie Routen zum FQDN des expliziten Proxy oder dessen IP-Adressen auf Perimetergeräten ein, damit Benutzer über den expliziten Proxy auf das Internet zugreifen können.
- (Optional) Fügen Sie DNS-Einträge hinzu, um den FQDN des expliziten Proxy für Prisma Access in eine interne IP-Adresse aufzulösen, wenn Benutzer öffentliche Domänen im Zweignetzwerk nicht auflösen können. Fügen Sie außerdem dem FQDN des expliziten Proxy oder dessen IP-Adresse die NAT (Network Address Translation) der Zieleinheit hinzu.

**STEP 6 |** Klicken Sie auf **Speichern** und **Konfiguration übertragen** an **GlobalProtect** und **Expliziten Proxy**.

 ©2025 Palo Alto Networks, Inc.

**STEP 7 |** Überprüfen Sie die Agent-Proxy-Bereitstellung und beheben Sie dabei gefundene Fehler.

1. Überprüfen Sie unter **Einstellungen** auf der Registerkarte **Verbindungen** die Informationen zu Ihrer Netzwerkverbindung in der GlobalProtect-App.
   1. Öffnen Sie die GlobalProtect-App.
   2. Wählen Sie **Einstellungen** aus, um die Anzeige mit den GlobalProtect-Einstellungen zu öffnen, und wählen Sie dann **Verbindungen** aus.




2. Zeigen Sie die GlobalProtect-Protokolle an und erfassen Sie diese.

   Zeigen Sie das PanGPS-Protokoll an, um die Konfiguration des Proxy-Modus im GlobalProtect-Portal zu überprüfen.

   Sie können überprüfen, ob der Proxy-Modus konfiguriert ist, indem Sie im PanGPS-Protokoll nach dem folgenden Ereignis suchen:

   ```
   OnProxyAgentMode: Nur-Proxy-Modus
   ```

   Wenn Sie GlobalProtect-Protokolle in  anzeigen möchten, wählen Sie **Vorfälle und Benachrichtigungen** > **Protokoll-Viewer** aus und:

   - **GlobalProtect** für Authentifizierungsprotokolle
   - **Verkehr** und **Entschlüsselung** für Benutzerzugriffsprotokolle

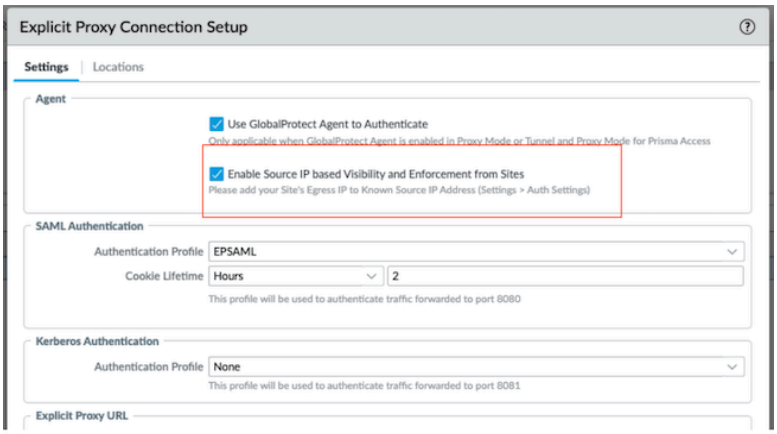
## GlobalProtect im Proxy-Modus (Panorama)

*Wenn Sie einePrisma Access (Managed by Panorama)-Bereitstellung mit nur einem Mandanten in eine Bereitstellung mit mehreren Mandanten konvertieren, unterstützt nur der erste (d. h. der von Ihnen migrierte) Mandant diese Funktion. Außerdem müssen Sie für diesen ersten Mandanten Ihre Richtlinienregeln in der vordefinierten Gerätegruppe für expliziten Proxy (Explicit_Proxy_Device_Group) und nicht in einer benutzerdefinierten Gerätegruppe einrichten. Alle nachfolgenden Mandanten, die Sie für die Bereitstellung mit mehreren Mandanten nach dem ersten Mandanten erstellen, unterstützen diese Funktion nicht.*

 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** Aktivieren Sie die agentenbasierte Proxy-Funktionalität für mobile Benutzer.

1. Aktivieren Sie expliziten Proxy.
   1. Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Mobile Benutzer – Expliziter Proxy** aus.
   2. **Konfigurieren** Sie die Einrichtung des expliziten Proxy, um eine **URL des expliziten Proxy** anzugeben.
2. Wählen Sie **GlobalProtect-App zur Authentifizierung verwenden** aus, um die agentenbasierte Proxy-Funktionalität zu aktivieren. Optional kann außerdem **Quell-IP-basierte Sichtbarkeit und Durchsetzung über Websites aktivieren** ausgewählt werden.




3. Geben Sie die URL der **PAC-Datei** (PAC – Proxy Auto-Configuration) ein. Vergewissern Sie sich, dass in der PAC-Datei der Port 8080 eingegeben wurde.
   - Vergewissern Sie sich, dass in der PAC-Datei der Port 8080 eingegeben wurde.
   - Die Proxy-Anweisung in der PAC-Datei muss den Prisma Access-FQDN (Fully Qualified Domain Name) verwenden, den Sie oben konfiguriert haben.
   - Die PAC-Datei muss so konfiguriert sein, dass der Datenverkehr über das VPN von Drittanbietern umgangen wird.

   Beispiel für eine PAC-Datei:

```
function FindProxyForURL (url, host) { /* Bypass localhost
 and Private IPs * / var resolved_ ip = dnsResolve (host) ;
 if (isplainHostName (host) || shExpMatch (host,"* ,local")
 || isInNet (resolved_ip,"10.0.0.0", "255.0.0.0") ||
 isInNet (resolved ip,"172.16.0.0","255.240.0.0") ||
 isInNet (resolved_ip,"192.168.0.0","255.255.0.0") ||
 isInNet (resolved ip, "127.0.0.0", "255.255.255.0" ))
 return "DIRECT"; /* Bypass Non-HTTP * / if (url.substring
 (0,4) == "ftp: ") return "DIRECT”; /* Bypass VPN */ if
 (shExpMatch (host, "vpn. acme.com") || shExpMatch (host,
 "gateway. acme.com" )) return "DIRECT"; /* Bypass Private
 Apps */ if (shExpMatch (host,"internalapps. acme.com" ) )
 return "DIRECT"; /* Forward to  */ return "PROXY acme-
demo.proxy.prismaaccess.com: 8080";}
```

4. Wählen Sie den **Verbindungsnamen** für die Einrichtung des expliziten Proxy aus, die Sie konfiguriert haben.

 ©2025 Palo Alto Networks, Inc.

5. Wählen Sie die **Standorte** und Regionen aus, in denen Sie expliziten Proxy für mobile Benutzer bereitstellen möchten.

   Prisma Access fügt jedem von Ihnen ausgewählten Standort einen Proxy-Knoten hinzu. Expliziter Proxy unterstützt eine Teilmenge aller Prisma Access-Standorte. Wenn Sie die Anzahl der Standorte begrenzen möchten, wählen Sie zur Optimierung der Benutzererfahrung die Standorte mit der kürzesten Entfernung zu Ihren Endbenutzern aus. Wenn ein Standort in dem Land, in dem sich Ihre mobilen Benutzer befinden, nicht verfügbar ist, wählen Sie den Standort mit der kürzesten Entfernung zu Ihren mobilen Benutzern aus.

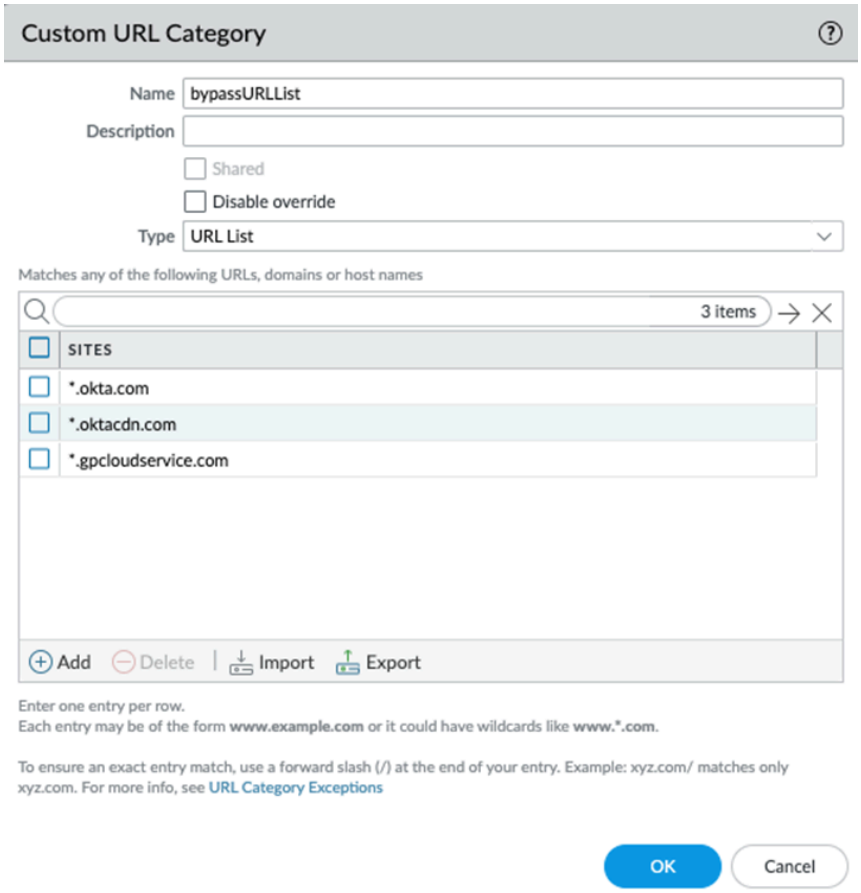
 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Identitätsanbieter (IdPs) umgehen.

Alle Anfragen an den Proxy werden authentifiziert. Wenn Sie jedoch IdP-Abläufe über den Proxy weiterleiten, müssen Sie diese umgehen, damit die Authentifizierung erfolgreich ausgeführt werden kann.

In diesem Beispiel werden das GlobalProtect-Portal und Okta umgangen. Diese Komponenten müssen jedoch an die jeweils verwendeten IdPs angepasst werden.

1. Wählen Sie die Gruppe **Explicit_Proxy_Device_Group** und dann die Optionen **Objekt** > **Benutzerdefinierte Objekte** > **URL-Kategorie** aus und erstellen Sie anschließend eine benutzerdefinierte URL-Kategorie.
2. Fügen Sie in der benutzerdefinierten URL-Kategorie alle FQDN-Domänen hinzu, die von der EP-Authentifizierung umgangen werden müssen.




3. Wählen Sie **Cloud Services** > **Konfiguration** > **Mobile Benutzer** > **Expliziter Proxy** > **Einstellungen** > **Authentifizierungseinstellungen** aus und fügen Sie die benutzerdefinierte URL-Kategorie hinzu.




 ©2025 Palo Alto Networks, Inc.

4. Führen Sie die Aktion „Commit und Push“ aus, um die Informationen festzuschreiben und an die Gruppe **Explicit_Proxy_Device_Group** zu übertragen.

**STEP 3 |** Konfigurieren Sie das GlobalProtect-Portal.

*Im Proxy-Modus ändert die von Ihnen festgelegte Verbindungsmethode das Verhalten der Proxy-Funktionalität nicht. Selbst wenn Sie eine On-Demand-Verbindungsmethode festlegen, wird der gesamte internetgebundene Datenverkehr weiterhin im Proxy-Modus verarbeitet, um eine immer aktivierte Internetsicherheit zu gewährleisten.*

1. Klicken Sie im Abschnitt für das Onboarding auf **Konfigurieren**.
2. Machen Sie auf der Registerkarte **Allgemein** die gewünschten Angaben für **Portal-Namenstyp**:

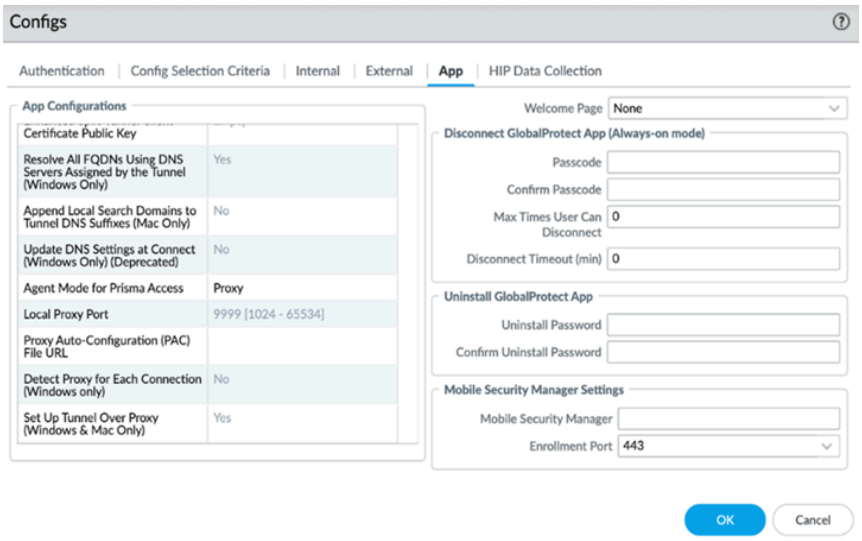
   **Standarddomäne verwenden –** Wenn Sie diese Option auswählen, verwendet Ihr Portal-Hostname den Standarddomänennamen: .gpcloudservice.com. In diesem Fall geben Sie einfach einen Portal-Hostnamen ein, der an den Standarddomänennamen angefügt wird. Prisma Access wird automatisch die erforderlichen Zertifikate erstellen und den Hostnamen auf öffentlichen DNS-Servern veröffentlichen.

   **Unternehmensdomäne verwenden –** Wählen Sie diese Option aus, wenn die Domäne im Portal-Hostnamen mit dem Domänennamen Ihres Unternehmens übereinstimmen soll (z. B. myportal.mydomain.com).
3. Wählen Sie ein **Authentifizierungsprofil** aus, das angibt, wie Prisma Access mobile Benutzer authentifizieren soll oder erstellen Sie ein neues Profil.
4. (Optional) Wählen Sie ein **Authentifizierungsüberschreibungszertifikat** aus, um die sicheren Cookies zu verschlüsseln, die mobile Benutzer zur Authentifizierung beim Portal und Gateway verwenden.

 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** Aktivieren Sie den Proxy-Modus für GlobalProtect.

1. Wählen Sie **Netzwerk** > **GlobalProtect-Portale** aus.
2. Wählen Sie die Portalkonfiguration aus, der Sie die Agentenkonfiguration hinzufügen möchten, und anschließend die Registerkarte **Agent**.
3. Wählen Sie auf der Registerkarte **Agent App** aus.
4. Legen Sie im Bereich App-Konfigurationen den **Agent-Modus für Prisma Access** auf **Proxy** fest, um den Internetverkehr an den agentenbasierten Proxy von GlobalProtect zu senden.




**STEP 5 |** Führen Sie die gewünschten optionalen Konfigurationsschritte aus.

1. (Optional) Konfigurieren Sie den lokalen Proxy-Port. Der Portbereich liegt zwischen 1024 und 65534 und der Standardport ist 9999. Wenn der Standardport nicht verfügbar ist, prüft GlobalProtect zehn andere Ports im Bereich von 9999 bis 10009 und verwendet den verfügbaren Port. Sie können auch Ihre eigene Portnummer innerhalb des Bereichs auswählen.
2. (Optional) Konfigurieren Sie die PAC-Autokonfigurationsdatei-URL, wenn Sie eine benutzerdefinierte PAC-URL für die Proxyeinstellungen per Push an den Endpunkt übertragen möchten. Die PAC-URL wird per Push an den Endpunkt übertragen, sobald der Benutzer eine Verbindung herstellt. Wenn der Benutzer die Verbindung zur GlobalProtect-App trennt, werden die Endpunkt-Proxy-Konfigurationen automatisch deaktiviert und auf die vorherigen Einstellungen zurückgesetzt.
3. (Optional) Aktivieren Sie Benutzer darf Netzwerk erneut erkennen, wenn der Benutzer das Portal auf neue Einstellungen überprüfen soll.
4. (Optional) Konfigurieren Sie Konfigurationsaktualisierungsintervall für GlobalProtect-App (Stunden). Standardmäßig aktualisiert der GlobalProtect-Client die zwischengespeicherte Portalkonfiguration alle 24 Stunden. Sie können das Aktualisierungsintervall entsprechend Ihren Geschäftsanforderungen ändern.


©2025 Palo Alto Networks, Inc.

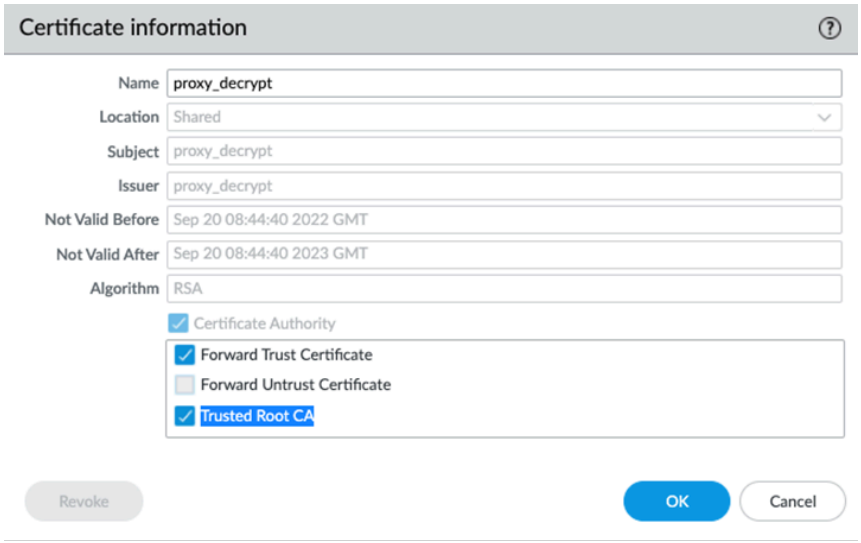
**STEP 6 |** Aktivieren Sie die Always-On-Internetsicherheit, indem Sie die folgenden Einstellungen konfigurieren:

1. Legen Sie für die Option Benutzern das Deaktivieren von GlobalProtect erlauben die Einstellung **Nicht zulassen**, **Mit Passcode zulassen** oder **Mit Ticket zulassen** fest.
2. Legen Sie für die Option Zulassen, dass sich Benutzer von der GlobalProtect-App abmelden die Einstellung **Nein** fest.

**STEP 7 |** (Optional) Konfigurieren Sie die Entschlüsselungsrichtlinie für Datenverkehr für expliziten Proxy.

Wenn Sie die Entschlüsselung aktivieren, stellen Sie sicher, dass das Entschlüsselungszertifikat auch als vertrauenswürdige Stammzertifizierungsstelle eingerichtet ist.

1. Wählen Sie **Gerät** > **Zertifikatverwaltung** > **Zertifikate** aus und erstellen Sie ein Zertifikat, das eine vertrauenswürdige Stammzertifizierungsstelle und ein Forward-Trust-Zertifikat ist.




2. Erstellen Sie eine Entschlüsselungsregel unter **Explicit_Proxy_Device Group** mit SSL-Forward-Proxy.

**STEP 8 |** Konfigurieren Sie die Sicherheitsrichtlinienregeln für den Datenverkehr über expliziten Proxy.

1. Wählen Sie **Richtlinien** > **Sicherheit** aus.
2. Legen Sie unter **Gerätegruppe** die Angabe **Explicit_Proxy_Device_Group** fest.
3. Befolgen Sie die Best Practices der Internet-Gateway-Sicherheitsrichtlinie.

**STEP 9 |** (Optional) Konfigurieren Sie die GlobalProtect-App im Proxy-Modus in einem Netzwerk ohne Standardroute.

- (Optional) Hosten Sie eine PAC-Datei intern und fügen Sie den FQDN des expliziten Proxy für Prisma Access als Proxy in der PAC-Datei hinzu, oder hosten Sie die PAC-Datei in einem Weiterleitungsprofil und fügen Sie Routen in Ihrem Netzwerk für IP-Adressen des PAC-Dienstes hinzu.
- Leiten Sie in der PAC-Datei die IdP-URL und die URL des Prisma Access-Portals an expliziten Proxy weiter.

 ©2025 Palo Alto Networks, Inc.

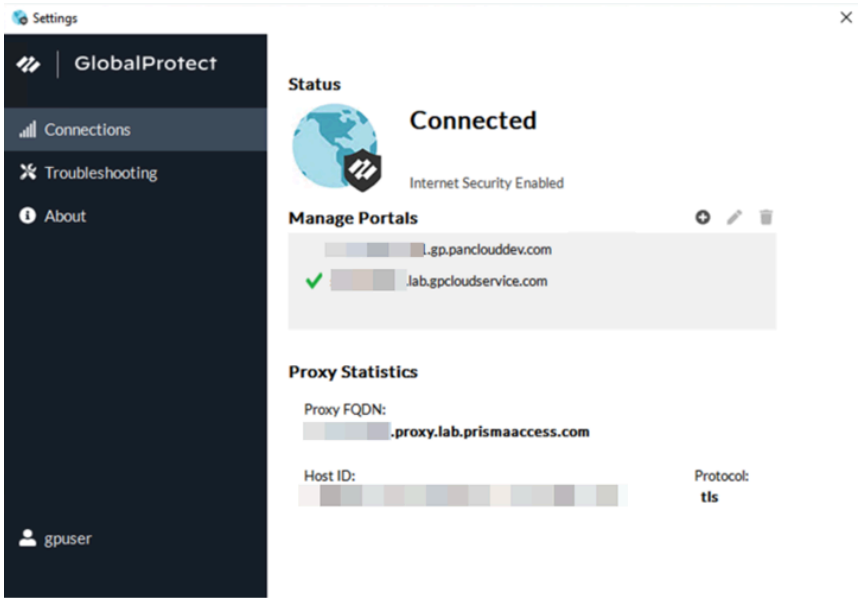
- Schließen Sie im expliziten Proxy die IdP- und Portal-URL aus den Authentifizierungseinstellungen aus. Fügen Sie der Domäne, die in den Authentifizierungsabläufen verwendet wird, die IdP- und Portal-URL hinzu.
- Richten Sie Routen zum FQDN des expliziten Proxy oder dessen IP-Adressen auf Perimetergeräten ein, damit Benutzer über den expliziten Proxy auf das Internet zugreifen können.
- (Optional) Fügen Sie DNS-Einträge hinzu, um den FQDN des expliziten Proxy für Prisma Access in eine interne IP-Adresse aufzulösen, wenn Benutzer öffentliche Domänen im Zweignetzwerk nicht auflösen können. Fügen Sie außerdem dem FQDN des expliziten Proxy oder dessen IP-Adresse die NAT (Network Address Translation) der Zieleinheit hinzu.

**STEP 10 |** Führen Sie die Aktion **Commit** aus, um Ihre Änderungen in Panorama festzuschreiben. Mit **Commit und Push** können Sie die Konfigurationsänderungen für die **Mobilen Benutzer** von Prisma Access und dem **Expliziten Proxy** festschreiben und übertragen.

 ©2025 Palo Alto Networks, Inc.

**STEP 11 |** Überprüfen Sie die Agent-Proxy-Bereitstellung und beheben Sie dabei gefundene Fehler.

1. Überprüfen Sie unter **Einstellungen** auf der Registerkarte **Verbindungen** die Informationen zu Ihrer Netzwerkverbindung in der GlobalProtect-App.
   1. Öffnen Sie die GlobalProtect-App.
   2. Wählen Sie **Einstellungen** aus, um die Anzeige mit den GlobalProtect-Einstellungen zu öffnen, und wählen Sie dann **Verbindungen** aus.




2. Zeigen Sie die GlobalProtect-Protokolle an und erfassen Sie diese.

   Zeigen Sie das PanGPS-Protokoll an, um die Konfiguration des Proxy-Modus im GlobalProtect-Portal zu überprüfen.

   Sie können überprüfen, ob der Proxy-Modus konfiguriert ist, indem Sie im PanGPS-Protokoll nach dem folgenden Ereignis suchen:

   ```
   OnProxyAgentMode: Nur-Proxy-Modus
   ```

   Um GlobalProtect-Protokolle in Panorama anzuzeigen, wählen Sie **Überwachen** > **Protokolle** und:

   - **GlobalProtect**, für Authentifizierungsprotokolle
   - **Datenverkehr** und **Entschlüsselung** für Benutzerzugriffsprotokolle

# GlobalProtect im Tunnel- und Proxy-Modus

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama)<br>• Prisma Access (Managed by Strata Cloud Manager)<br><br>Wenn Sie diese Funktion in Ihrer Prisma Access-Umgebung nutzen möchten, dann wenden Sie | • Prisma Access Version 5.2<br>• GlobalProtect-App Version 6.2 für Windows oder macOS<br>• Inhaltsversion 8700-7994<br>• Prisma Access Mobile-Benutzer-Lizenz |

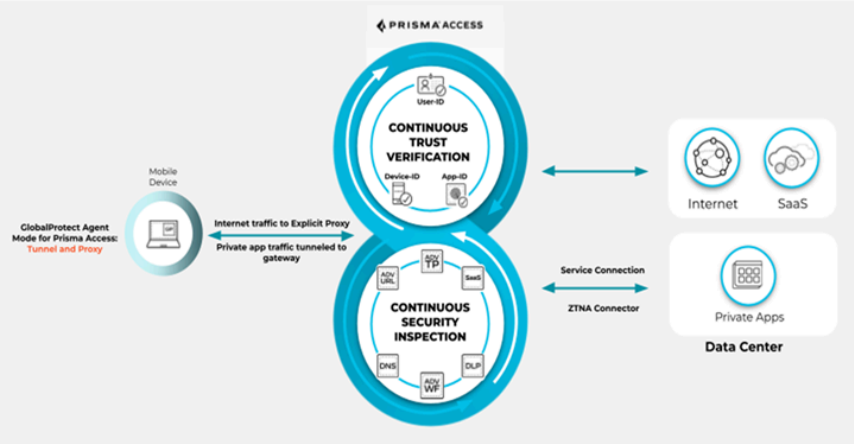
 ©2025 Palo Alto Networks, Inc.

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| sich an Ihr Account-Team, um weiterführende Informationen zu erhalten. | |

Im Modus **Tunnel und Proxy** sendet die GlobalProtect-App internetgebundenen Datenverkehr auf Basis der Regeln, die Sie in einer PAC-Datei definieren, an den expliziten Proxy. Für den verbleibenden Datenverkehr werden die Split-Tunneling-Regeln und die Logik verwendet, die in der PAC-Datei definiert wurden. Anhand dieser Daten wird ermittelt, welcher Datenverkehr durch den Tunnel gesendet werden muss und für welchen Datenverkehr der Tunnel umgangen werden kann. Wenn Sie keine Split-Tunnel-Regeln definiert haben, sendet die App den gesamten verbleibenden Datenverkehr durch den Tunnel.

*Wenn Sie die GlobalProtect-App im Modus „Tunnel und Proxy“ ausführen, wird die HIP-Funktionalität (HIP – Host Information Profile) nur für den Datenverkehr über einen GlobalProtect-Tunnel unterstützt.*

*Sie benötigen Strata Cloud Manager und GlobalProtect Agent Version 6.3.0 für den GlobalProtect-Proxy-Kanal, um alle IPv4-TCP-Verbindungen einschließlich des Datenverkehrs ohne Proxy-Erkennung zu unterstützen. Um eine nahtlose Funktionalität sicherzustellen, muss das auf den Endpunkten konfigurierte DNS (Domain Name System) in der Lage sein, den vollständig qualifizierten Domänennamen (FQDN) des Ziels aufzulösen.*



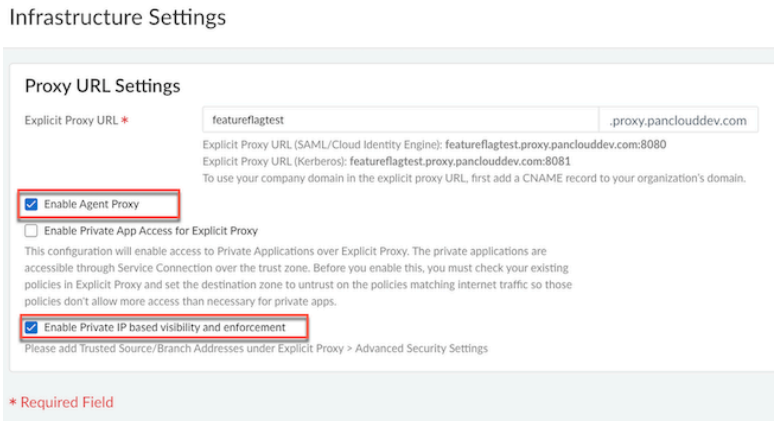

- Strata Cloud Manager
- Panorama

## GlobalProtect im Tunnel- und Proxy-Modus (Strata Cloud Manager)

 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** Aktivieren Sie die agentenbasierte Proxy-Funktionalität für mobile Benutzer in Prisma Access.

1. Aktivieren Sie expliziten Proxy.
   1. Wählen Sie **Workflows** > **Prisma Access Setup** > **Expliziter Proxy** aus.
   2. Klicken Sie im Bereich „Infrastruktureinstellungen“ auf **Proxy-Einstellungen einrichten** und geben Sie eine **URL des expliziten Proxy** an.
2. Sie müssen den **Agent-Proxy aktivieren** und optional **Sichtbarkeit und Durchsetzung basierend auf privaten IP-Adressen aktivieren** und dann auf **Speichern** klicken.



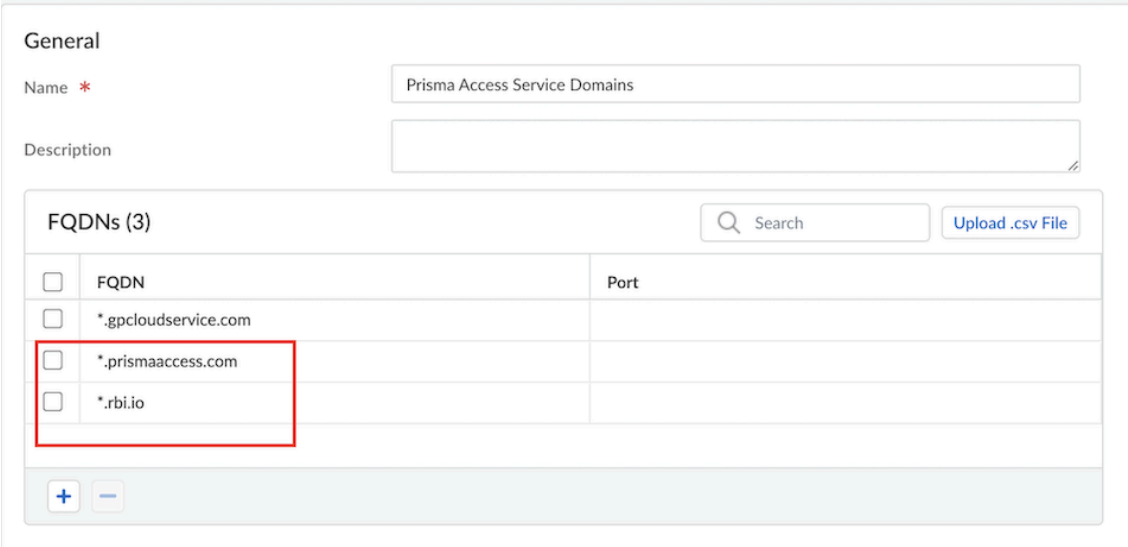

3. Wählen Sie die Prisma Access-Standorte aus, an denen mobile Benutzer unterstützt werden sollen.

   Wenn Sie die Anzahl der Standorte begrenzen möchten, wählen Sie zur Optimierung der Benutzererfahrung die Standorte mit der kürzesten Entfernung zu Ihren Endbenutzern aus. Wenn ein Standort in dem Land, in dem sich Ihre mobilen Benutzer befinden, nicht

 ©2025 Palo Alto Networks, Inc.

verfügbar ist, wählen Sie den Standort mit der kürzesten Entfernung zu Ihren Benutzern aus.

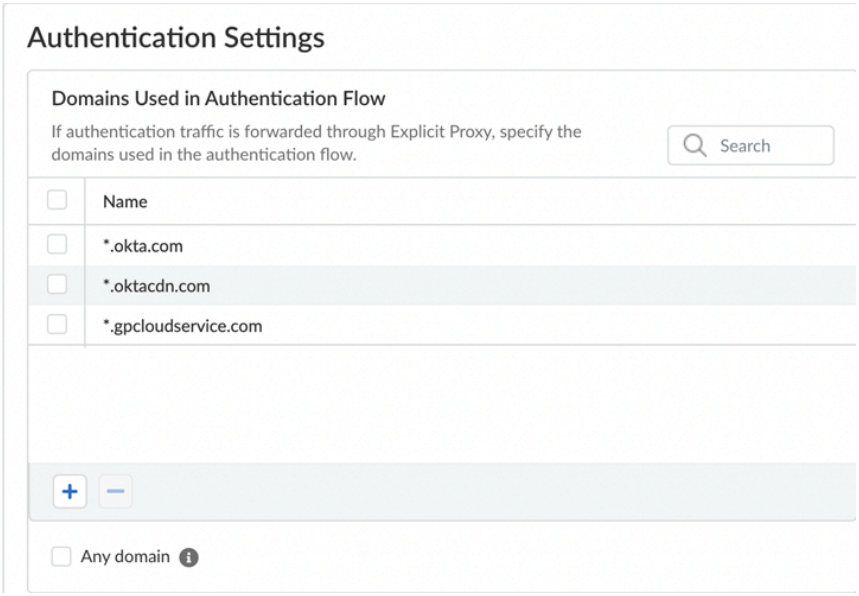
4. Erstellen Sie ein Weiterleitungsprofil, um den Datenverkehr zu definieren, den Sie über expliziten Proxy senden möchten. Umgehen Sie bei der Konfiguration des Weiterleitungsprofils die Domänen *.prismaaccess.com und *.gpcloudservice.com.




5. Verbinden Sie das Weiterleitungsprofil mit Ihrer GlobalProtect-App-Konfiguration.
6. Wählen Sie **Workflows** > **Einrichtung** > **Expliziter Proxy** > **Erweiterte Sicherheitseinstellungen** > **Authentifizierungseinstellungen** aus und fügen Sie die Domänen hinzu, die Sie umgehen müssen.

   Alle Anfragen an den Proxy werden authentifiziert. Wenn Sie jedoch IdP-Abläufe über den Proxy weiterleiten, müssen Sie diese umgehen, damit die Authentifizierung erfolgreich ist.

   In diesem Beispiel werden das GlobalProtect-Portal und Okta umgangen. Doch Sie sollten die Domänen an die von Ihnen verwendeten IdPs anpassen.

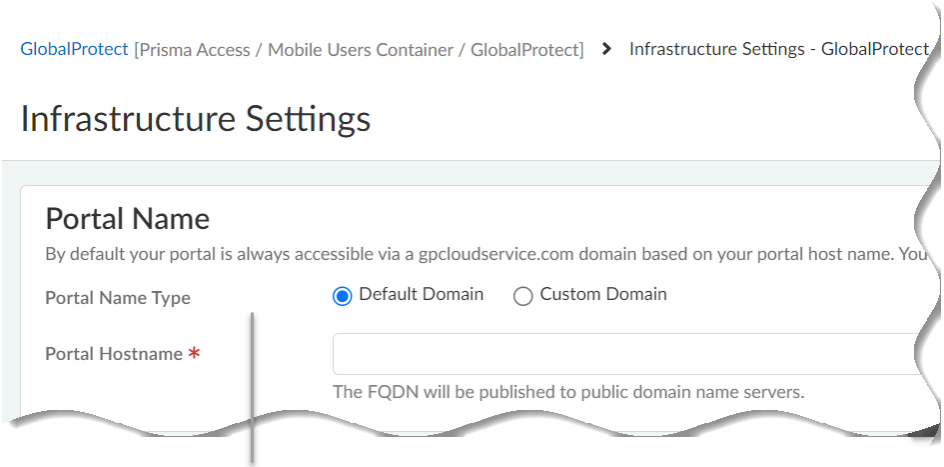



 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Konfigurieren Sie den Tunnel- und den Proxy-Modus für die GlobalProtect-App in Prisma Access.

*Im Tunnel- und im Proxy-Modus gilt die von Ihnen festgelegte Verbindungsmethode nur für den durch GlobalProtect getunnelten Datenverkehr. Bei der agentenbasierten Proxy-Funktionalität ist die Internetsicherheit immer aktiviert. Auch wenn Sie eine On-Demand-Verbindungsmethode festlegen, wird der gesamte internetgebundene Datenverkehr weiterhin über einen Proxy geleitet, bei dem die Internetsicherheit immer aktiviert ist. Dies gilt auch dann, wenn Benutzer die Verbindung zur GlobalProtect-App trennen.*

1. Wählen Sie **Workflows** > **Prisma Access-Einrichtung** > **GlobalProtect** > **Infrastruktur** > **Infrastruktureinstellungen** aus und geben Sie einen Wert für **Portalname** ein.




**GlobalProtect Infrastructure Settings**

- **Standarddomäne** – Wenn Sie diese Option auswählen, wird als Portal-Hostname der Standarddomänenname `.gpcloudservice.com` verwendet. Geben Sie in diesem Fall einfach einen Wert für **Portal-Hostname** ein, der an den Standarddomänennamen angefügt wird. Prisma Access for Users erstellt automatisch die erforderlichen Zertifikate und veröffentlicht den Hostnamen auf den öffentlichen DNS-Servern.

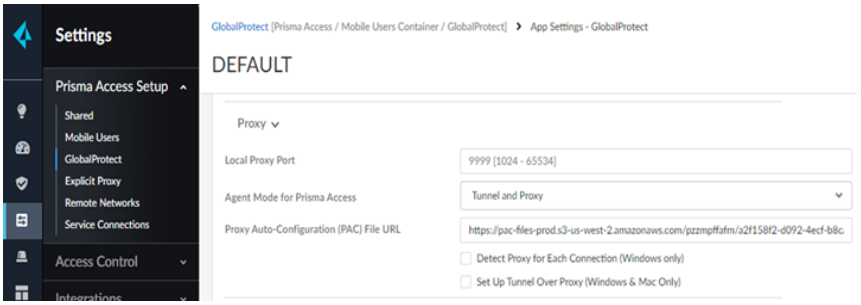
 ©2025 Palo Alto Networks, Inc.

- **Benutzerdefinierte Domäne** – Sie können die Portal-Adresse auch anpassen, wenn die Domäne im Portal-Hostnamen mit dem Domänennamen Ihres Unternehmens übereinstimmen soll (z. B. meinportal.meinedomäne.com).

2. Mobilen Benutzern die Authentifizierung bei Prisma Access ermöglichen.
3. Aktivieren Sie den GlobalProtect-Tunnel-Modus und den Proxy-Modus für Prisma Access in den Einstellungen der GlobalProtect-App, um den Internetverkehr an den agentenbasierten Proxy zu senden.
   - Wählen Sie **Workflows** > **Prisma Access-Einrichtung** > **GlobalProtect** aus.
   - Klicken Sie auf der Registerkarte **GlobalProtect-App** auf **Standard**, um die App-Einstellungen anzupassen. Alternativ hierzu können Sie auch auf **App-Einstellungen hinzufügen** klicken, um eine neue Konfiguration hinzuzufügen.
   - Klicken Sie auf **Erweiterte Optionen anzeigen** und auf den Abschnitt **App-Konfiguration**.
   - Stellen Sie im Abschnitt **Proxy den Agentenmodus für Prisma Access** auf **Tunnel und Proxy** ein, um die GlobalProtect-App anzuweisen, den Internetverkehr an den expliziten Proxy in Prisma Access und den privaten App-Datenverkehr an das VPN zu senden. Nachdem Sie den Modus **Tunnel und Proxy** in Prisma Access konfiguriert haben, können Benutzer sicher über Prisma Access auf das Internet zugreifen. Dies gilt auch dann, wenn Benutzer die Verbindung zur GlobalProtect-App trennen oder die GlobalProtect-App deaktivieren.
   - (Optional) Konfigurieren Sie den lokalen Proxy-Port. Der Portbereich liegt zwischen 1024 und 65534 und der Standardport ist 9999. Wenn der Standardport nicht verfügbar ist, prüft GlobalProtect zehn andere Ports im Bereich von 9999 bis 10009 und verwendet den verfügbaren Port. Sie können auch Ihre eigene Portnummer innerhalb des Bereichs auswählen.
   - (Optional) Konfigurieren Sie die URL der Proxy Auto-Configuration-(PAC-)Datei, wenn Sie die neue PAC-URL für die Proxy-Einstellungen per Push an den Endpunkt übertragen möchten. Die PAC-URL wird per Push an den Endpunkt übertragen, sobald der Benutzer eine Verbindung herstellt. Wenn der Benutzer die Verbindung zur GlobalProtect-App trennt, werden die Endpunkt-Proxy-Konfigurationen automatisch deaktiviert und auf die vorherigen Einstellungen zurückgesetzt.
   - (Optional) Aktivieren Sie Benutzer darf Netzwerk erneut erkennen, wenn der Benutzer das Portal auf neue Einstellungen überprüfen soll.
   - (Optional) Konfigurieren Sie Konfigurationsaktualisierungsintervall für GlobalProtect-App (Stunden). Standardmäßig aktualisiert der GlobalProtect-Client die zwischengespeicherte Portalkonfiguration alle 24 Stunden. Sie können das Aktualisierungsintervall entsprechend Ihren Geschäftsanforderungen ändern.

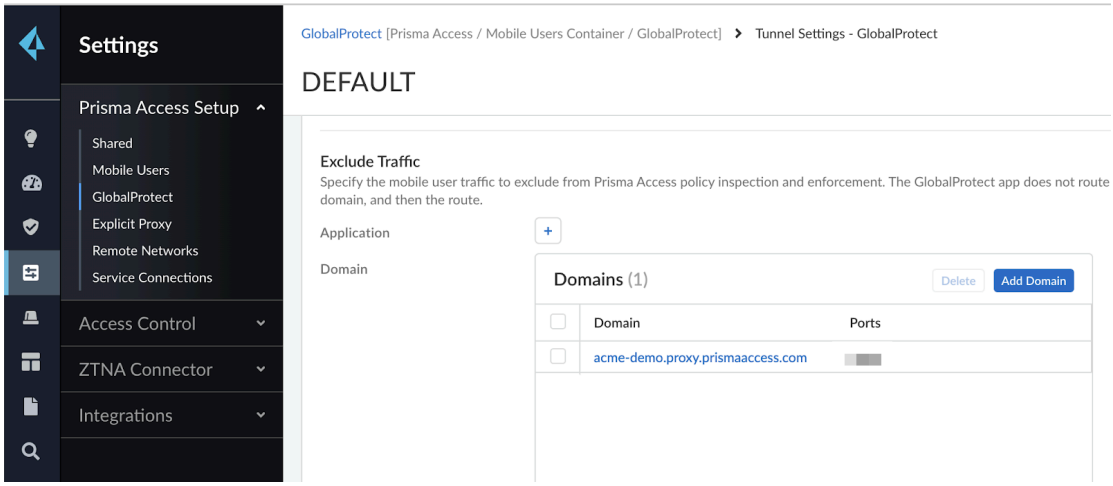
 ©2025 Palo Alto Networks, Inc.

- Deaktivieren Sie **Tunnel über Proxy einrichten (nur Windows und Mac)**.




 ©2025 Palo Alto Networks, Inc.

4. Schließen Sie in der **Split-Tunnel**-Konfiguration den FQDN des expliziten Proxy und den FQDN der PAC-Datei aus.
   - Wählen Sie **Workflows** > **Prisma Access-Einrichtung** > **GlobalProtect** aus.
   - Klicken Sie auf der Registerkarte **GlobalProtect-App** auf **Standard**, um die Tunneleinstellungen anzupassen, oder klicken Sie auf **Tunneleinstellungen hinzufügen**, um eine neue Konfiguration hinzuzufügen.
   - Wählen Sie unter **Datenverkehr ausschließen** die Option **Domäne hinzufügen** aus.




 ©2025 Palo Alto Networks, Inc.

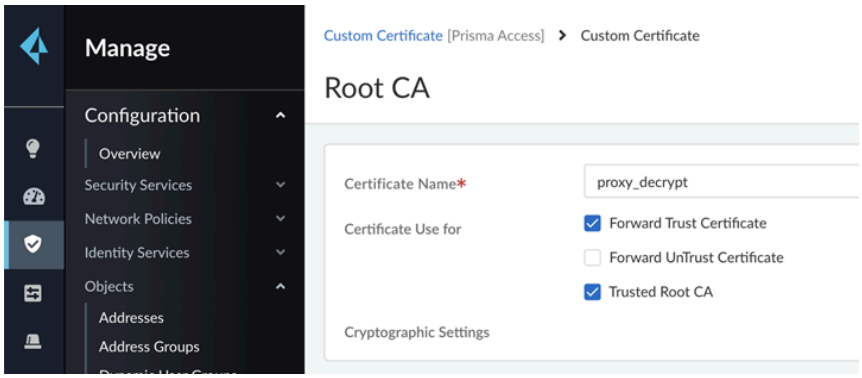
*Ersetzen Sie den FQDN in der Abbildung durch Ihren Proxy-FQDN.*

**STEP 3 |** Aktivieren Sie für die Sicherheit die Option „Immer aktiviert“, indem Sie die folgenden Einstellungen unter **Workflows** > **Prisma Access-Einrichtung** > **GlobalProtect** > **GlobalProtect-App** > **App-Einstellungen hinzufügen** konfigurieren:

1. Setzen Sie GlobalProtect deaktivieren auf **Nicht zulassen**, **Mit Passcode zulassen** oder auf **Mit Ticket zulassen**.
2. Deaktivieren Sie die Option Zulassen, dass sich Benutzer von der GlobalProtect-App abmelden.

**STEP 4 |** Konfigurieren Sie die Entschlüsselung für Datenverkehr für expliziten Proxy.

- Wählen Sie **Verwalten** > **Konfiguration** > **NGFW und** > **Sicherheitsdienste** > **Entschlüsselung** aus.
- Wenn Sie die Entschlüsselung aktivieren, stellen Sie sicher, dass Sie das Entschlüsselungszertifikat als vertrauenswürdige Stammzertifizierungsstelle einrichten.




**STEP 5 |** Konfigurieren Sie die Sicherheitsrichtlinienregeln für den Datenverkehr über expliziten Proxy.

- Wählen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Sicherheitsdienste** > **Sicherheitsrichtlinie** aus.
- Befolgen Sie die Best Practices der Internet-Gateway-Sicherheitsrichtlinie.

**STEP 6 |** (Optional) Konfigurieren Sie die GlobalProtect-App im Proxy- und Tunnel-Modus in einem Netzwerk ohne Standardroute.

- (Optional) Hosten Sie eine PAC-Datei intern und fügen Sie den FQDN des expliziten Proxy für Prisma Access als Proxy in der PAC-Datei hinzu, oder hosten Sie die PAC-Datei in einem Weiterleitungsprofil und fügen Sie Routen in Ihrem Netzwerk für IP-Adressen des PAC-Dienstes hinzu.
- Leiten Sie Authentifizierungsanforderungen für die Portal- und Gateway-FQDNs und für IdP-URLs an das Internet weiter.
- Richten Sie Routen zum FQDN des expliziten Proxy oder dessen IP-Adressen auf Perimetergeräten ein, damit Benutzer über den expliziten Proxy auf das Internet zugreifen können.

 ©2025 Palo Alto Networks, Inc.

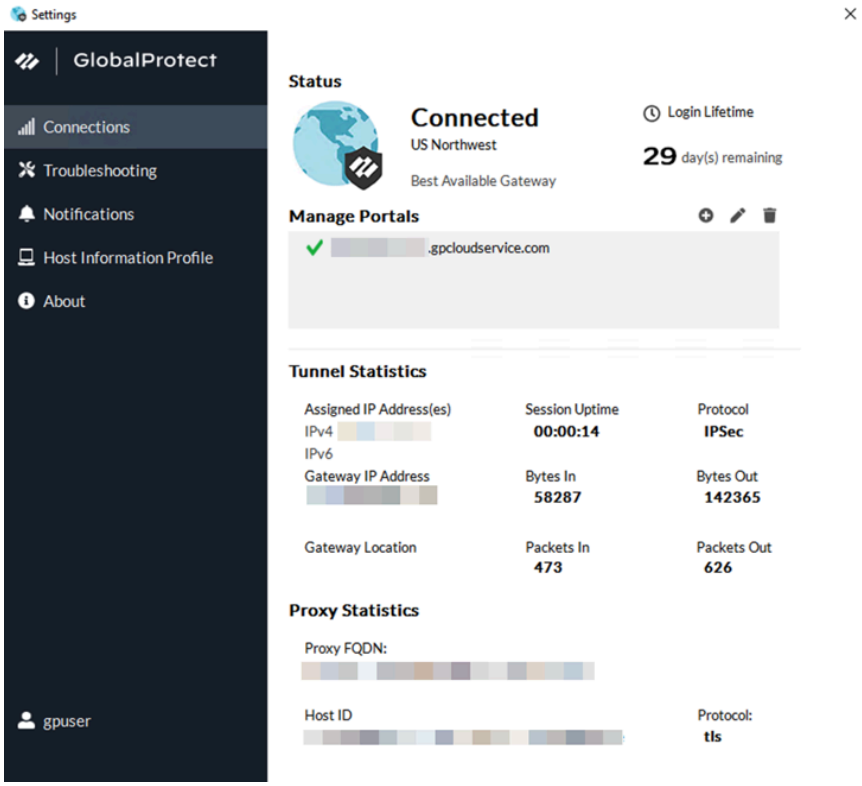
- (Optional) Fügen Sie DNS-Einträge hinzu, um den FQDN des expliziten Proxy für Prisma Access in eine interne IP-Adresse aufzulösen, wenn Benutzer öffentliche Domänen im Zweignetzwerk nicht auflösen können. Fügen Sie außerdem dem FQDN des expliziten Proxy oder dessen IP-Adresse die NAT (Network Address Translation) der Zieleinheit hinzu.
- So ermöglichen Sie Benutzern den direkten Zugriff auf private Apps, wenn sie im Büro sind:
  - **Direkter Zugriff:** Aktivieren Sie die interne Hosterkennung und lassen Sie die interne Gateway-Liste leer.

**STEP 7 |** Klicken Sie auf **Speichern** und **Konfiguration übertragen** an **GlobalProtect** und **Expliziten Proxy**.

 ©2025 Palo Alto Networks, Inc.

**STEP 8 |** Überprüfen Sie die Agent-Proxy-Bereitstellung und beheben Sie dabei gefundene Fehler.

1. Überprüfen Sie unter **Einstellungen** auf der Registerkarte **Verbindungen** die Informationen zu Ihrer Netzwerkverbindung in der GlobalProtect-App.
   1. Öffnen Sie die GlobalProtect-App.
   2. Wählen Sie **Einstellungen** aus, um die Anzeige mit den GlobalProtect-Einstellungen zu öffnen, und wählen Sie dann **Verbindungen** aus.




2. Zeigen Sie die GlobalProtect-Protokolle an und erfassen Sie diese.

   Zeigen Sie das PanGPS-Protokoll an, um die Konfiguration des Proxy-Modus im GlobalProtect-Portal zu überprüfen.

   Sie können überprüfen, ob der Proxy-Modus konfiguriert ist, indem Sie im PanGPS-Protokoll nach dem folgenden Ereignis suchen:

   ```
   OnProxyAgentMode: Hybridmodus
   ```

   Wenn Sie GlobalProtect-Protokolle in  anzeigen möchten, wählen Sie **Vorfälle und Benachrichtigungen** > **Protokoll-Viewer** aus und:

   - **GlobalProtect** für Authentifizierungsprotokolle
   - **Verkehr** und **Entschlüsselung** für Benutzerzugriffsprotokolle

**Trennen Sie die Verbindung zum Tunnel- und Proxy-Modus und inaktivieren Sie diesen Modus mit der Verbindungsmethode „Immer aktiviert“**

Ab GlobalProtect Version 6.3.1 müssen Sie die folgenden Schritte ausführen, wenn Sie den Modus **Tunnel und Proxy** für die GlobalProtect-App zusammen mit der Einstellung **Immer**

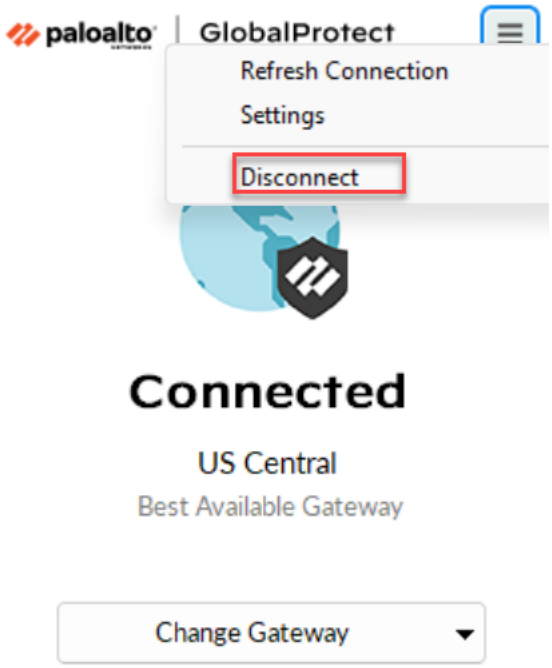
 ©2025 Palo Alto Networks, Inc.

**aktiviert** als Verbindungsmethode konfigurieren und die Verbindung zum Tunnel- und Proxy-Modus trennen möchten:

1. Trennen Sie die Verbindung zur GlobalProtect-App, um die Tunnelverbindung (VPN) zu trennen. Wenn Sie die Verbindung zur App trennen, wird die Tunnelverbindung (VPN) getrennt und die App bleibt weiterhin über den Proxy-Modus verbunden.
2. Deaktivieren Sie die GlobalProtect-App, um sowohl den Tunnel- als auch den Proxy-Modus zu trennen. Wenn Sie die App deaktivieren, wird sowohl die Verbindung zum Tunnel- als auch zum Proxy-Modus getrennt und die App ist nicht mehr verbunden.

Um die mit **Tunnel und Proxy** (Hybridmodus) und der Verbindungsmethode **Immer aktiviert** konfigurierte GlobalProtect-App zu trennen und zu deaktivieren, gehen Sie wie folgt vor:

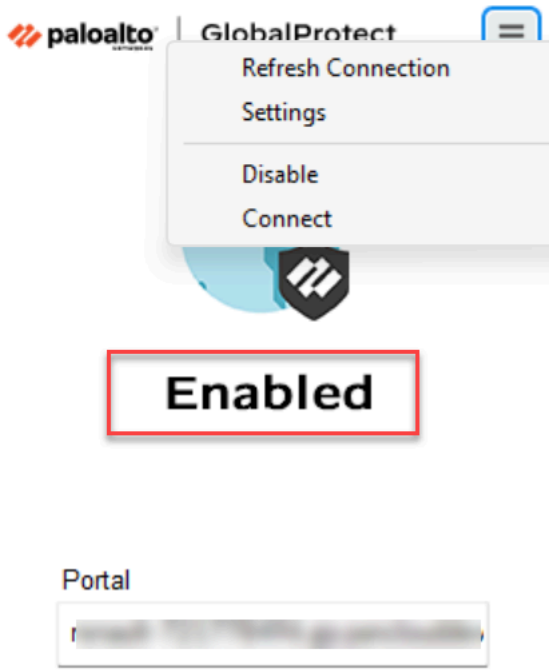
1. Trennen Sie die Verbindung zur GlobalProtect-App mithilfe der Option **Trennen** im Hamburger-Menü. Wenn Sie die Verbindung zur App trennen, wird die Tunnelverbindung (VPN) getrennt.



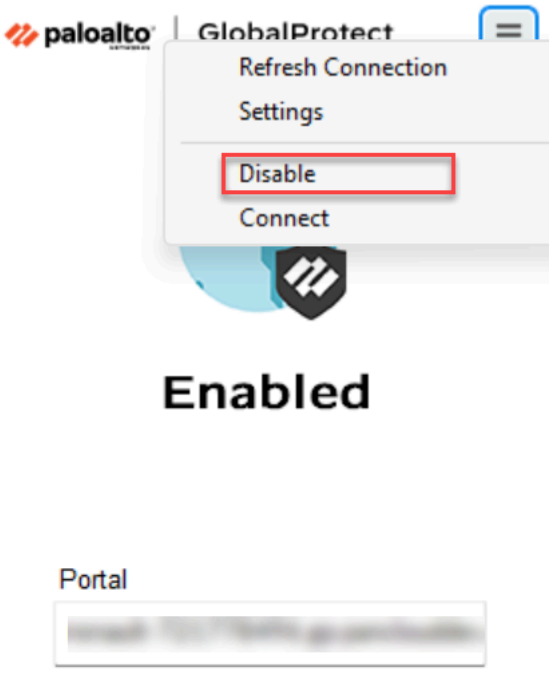

Nachdem Sie die Verbindung zur App getrennt haben, wird die VPN-Verbindung getrennt, der Proxy-Modus wird jedoch aktiviert. Die App ist weiterhin über den Proxy-Modus verbunden und zeigt den Status **Aktiviert** an.

*Wenn Sie die Tunnelverbindung (VPN) wiederherstellen möchten, können Sie die Option **Verbinden** im Hamburger-Menü verwenden.*


©2025 Palo Alto Networks, Inc.

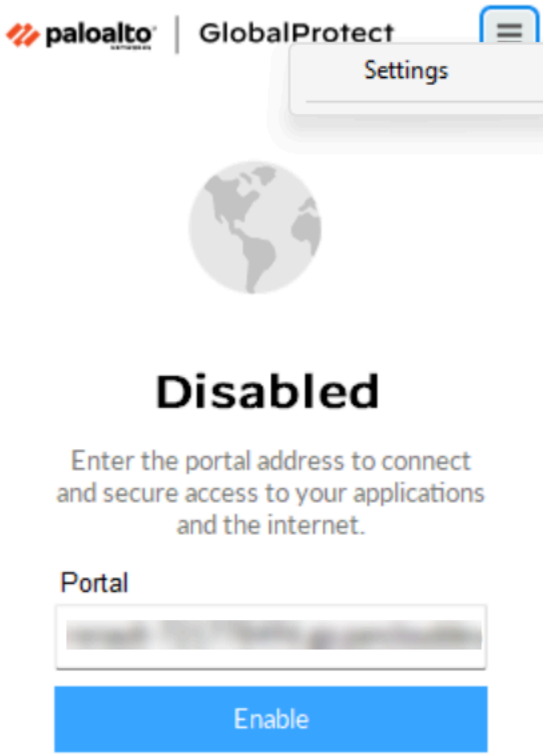



2. Deaktivieren Sie die GlobalProtect-App mit der Option **Deaktivieren** im Hamburger-Menü. Nachdem Sie die App deaktiviert haben, werden sowohl die Tunnel- als auch die Proxy-Verbindung getrennt.




Die App wird deaktiviert und der Status wird als **Deaktiviert** angezeigt.

 ©2025 Palo Alto Networks, Inc.



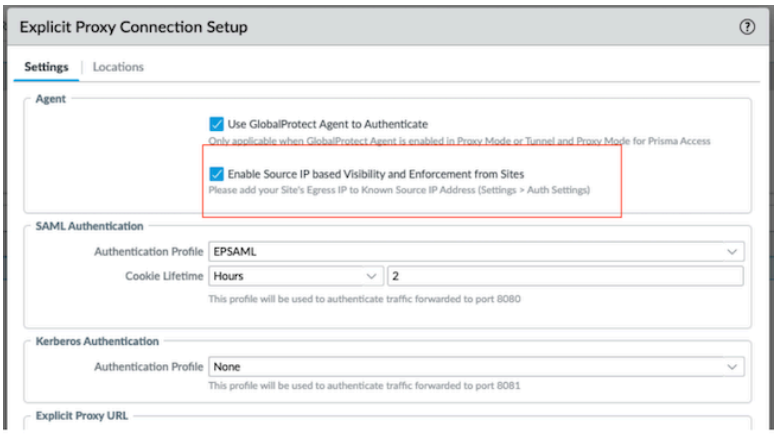

## GlobalProtect im Tunnel- und Proxy-Modus (Panorama)

*Wenn Sie einePrisma Access (Managed by Panorama)-Bereitstellung mit nur einem Mandanten in eine Bereitstellung mit mehreren Mandanten konvertieren, unterstützt nur der erste (d. h. der von Ihnen migrierte) Mandant diese Funktion. Außerdem müssen Sie für diesen ersten Mandanten Ihre Richtlinienregeln in der vordefinierten Gerätegruppe für expliziten Proxy (Explicit_Proxy_Device_Group) und nicht in einer benutzerdefinierten Gerätegruppe einrichten. Alle nachfolgenden Mandanten, die Sie für die Bereitstellung mit mehreren Mandanten nach dem ersten Mandanten erstellen, unterstützen diese Funktion nicht.*

 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** Aktivieren Sie die agentenbasierte Proxy-Funktionalität für mobile Benutzer.

1. Aktivieren Sie expliziten Proxy.
   1. Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Mobile Benutzer – Expliziter Proxy** aus.
   2. **Konfigurieren** Sie die Einrichtung des expliziten Proxy, um eine **URL des expliziten Proxy** anzugeben.
2. Wählen Sie **GlobalProtect-App zur Authentifizierung verwenden** aus, um die agentenbasierte Proxy-Funktionalität zu aktivieren. Optional kann außerdem **Quell-IP-basierte Sichtbarkeit und Durchsetzung über Websites aktivieren** ausgewählt werden.




3. Geben Sie die URL der **PAC-Datei** (PAC – Proxy Auto-Configuration) ein. Vergewissern Sie sich, dass in der PAC-Datei der Port 8080 eingegeben wurde.
   - Die Proxy-Anweisung in der PAC-Datei muss den Prisma Access-FQDN (Fully Qualified Domain Name) verwenden, den Sie oben konfiguriert haben.
   - Die PAC-Datei muss so konfiguriert werden, dass die GlobalProtect-Gateways (*.gp.gpcoudservice.com) ausgeschlossen sind.
4. Wählen Sie den **Verbindungsnamen** für die Einrichtung des expliziten Proxy aus, die Sie konfiguriert haben.
5. Wählen Sie die **Standorte** und Regionen aus, in denen Sie expliziten Proxy für mobile Benutzer bereitstellen möchten.

   Prisma Access fügt jedem von Ihnen ausgewählten Standort einen Proxy-Knoten hinzu. Expliziter Proxy unterstützt eine Teilmenge aller Prisma Access-Standorte. Wenn Sie die Anzahl der Standorte begrenzen möchten, wählen Sie zur Optimierung der Benutzererfahrung die Standorte mit der kürzesten Entfernung zu Ihren Endbenutzern aus. Wenn ein Standort in dem Land, in dem sich Ihre mobilen Benutzer befinden, nicht verfügbar ist, wählen Sie den Standort mit der kürzesten Entfernung zu Ihren mobilen Benutzern aus.

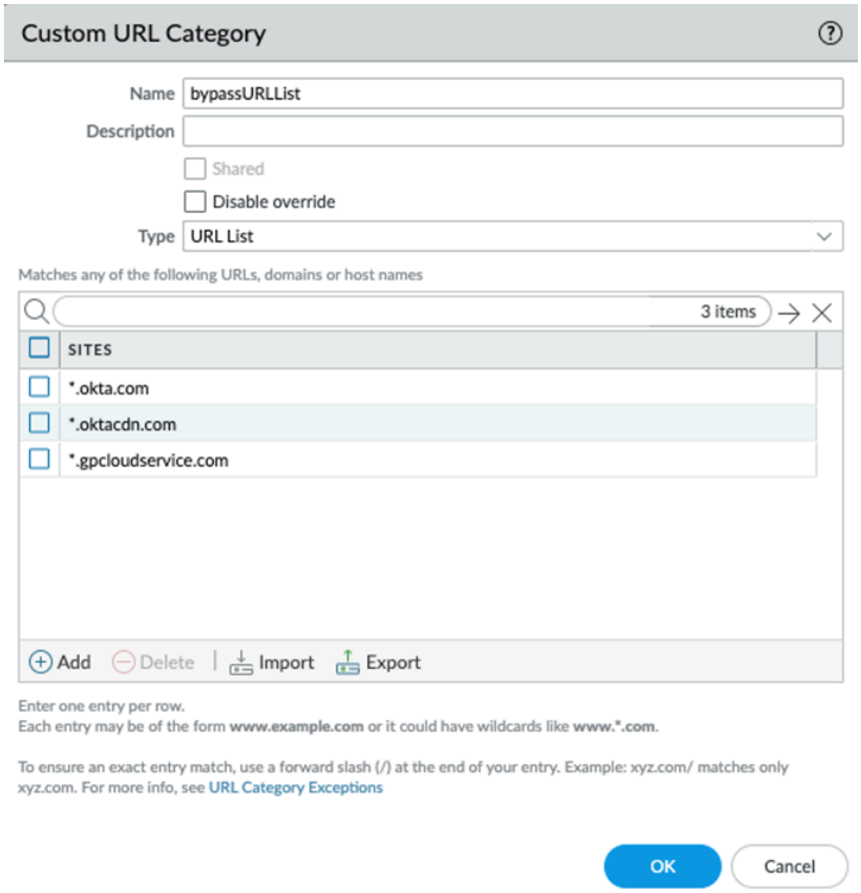
 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Identitätsanbieter (IdPs) umgehen.

Alle Anfragen an den Proxy werden authentifiziert. Wenn Sie jedoch IdP-Abläufe über den Proxy weiterleiten, müssen Sie diese umgehen, damit die Authentifizierung erfolgreich ausgeführt werden kann.

In diesem Beispiel werden das GlobalProtect-Portal und Okta umgangen. Diese Komponenten müssen jedoch an die jeweils verwendeten IdPs angepasst werden.

1. Wählen Sie die Gruppe **Explicit_Proxy_Device_Group** und dann die Optionen **Objekt** > **Benutzerdefinierte Objekte** > **URL-Kategorie** aus und erstellen Sie anschließend eine benutzerdefinierte URL-Kategorie.
2. Fügen Sie in der benutzerdefinierten URL-Kategorie alle FQDN-Domänen hinzu, die von der EP-Authentifizierung umgangen werden müssen.




3. Wählen Sie **Cloud Services** > **Konfiguration** > **Mobile Benutzer** > **Expliziter Proxy** > **Einstellungen** > **Authentifizierungseinstellungen** aus und fügen Sie die benutzerdefinierte URL-Kategorie hinzu.




 ©2025 Palo Alto Networks, Inc.

4. Führen Sie die Aktion „Commit und Push“ aus, um die Informationen festzuschreiben und an die Gruppe **Explicit_Proxy_Device_Group** zu übertragen.

**STEP 3 |** Konfigurieren Sie das GlobalProtect-Portal.

*Im Tunnel- und im Proxy-Modus gilt die von Ihnen festgelegte Verbindungsmethode nur für den durch GlobalProtect getunnelten Datenverkehr. Bei der agentenbasierten Proxy-Funktionalität ist die Internetsicherheit immer aktiviert. Auch wenn Sie eine On-Demand-Verbindungsmethode festlegen, wird der gesamte internetgebundene Datenverkehr weiterhin über einen Proxy geleitet, bei dem die Internetsicherheit immer aktiviert ist. Dies gilt auch dann, wenn Benutzer die Verbindung zur GlobalProtect-App trennen.*

1. Klicken Sie im Abschnitt für das Onboarding auf **Konfigurieren**.
2. Machen Sie auf der Registerkarte **Allgemein** die gewünschten Angaben für **Portal-Namenstyp**:

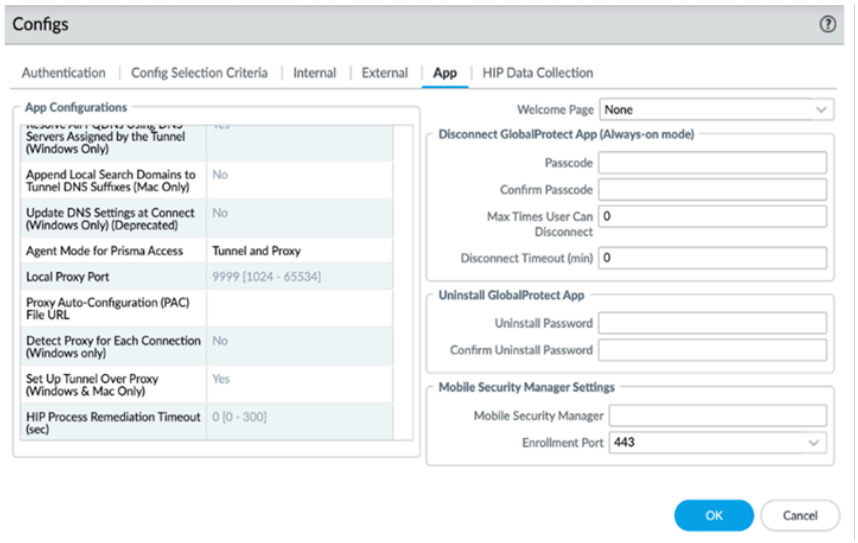
   **Standarddomäne verwenden –** Wenn Sie diese Option auswählen, verwendet Ihr Portal-Hostname den Standarddomänennamen: .gpcloudservice.com. In diesem Fall geben Sie einfach einen Portal-Hostnamen ein, der an den Standarddomänennamen angefügt wird.

 ©2025 Palo Alto Networks, Inc.

Prisma Access wird automatisch die erforderlichen Zertifikate erstellen und den Hostnamen auf öffentlichen DNS-Servern veröffentlichen.

**Unternehmensdomäne verwenden –** Wählen Sie diese Option aus, wenn die Domäne im Portal-Hostnamen mit dem Domänennamen Ihres Unternehmens übereinstimmen soll (z. B. myportal.mydomain.com).

3. Wählen Sie ein **Authentifizierungsprofil** aus, das angibt, wie Prisma Access mobile Benutzer authentifizieren soll oder erstellen Sie ein neues Profil.
4. (Optional) Wählen Sie ein **Authentifizierungsüberschreibungszertifikat** aus, um die sicheren Cookies zu verschlüsseln, die mobile Benutzer zur Authentifizierung beim Portal und Gateway verwenden.
   1. Aktivieren Sie den Tunnel- und Proxy-Modus in GlobalProtect.
      1. Wählen Sie **Netzwerk** > **GlobalProtect-Portale** aus.
      2. Wählen Sie die Portalkonfiguration aus, der Sie die Agentenkonfiguration hinzufügen möchten, und anschließend die Registerkarte **Agent**.
      3. Wählen Sie auf der Registerkarte **Agent** die Option **App** aus.
      4. Legen Sie im Bereich App-Konfigurationen den **Agentenmodus für Prisma Access** auf **Tunnel und Proxy** fest, um Internetdatenverkehr an den expliziten Proxy von Prisma Access und den privaten App-Datenverkehr an das VPN zu senden.




   2. Führen Sie die gewünschten optionalen Konfigurationsschritte aus.
      1. (Optional) Konfigurieren Sie den lokalen Proxy-Port. Der Portbereich liegt zwischen 1024 und 65534 und der Standardport ist 9999. Wenn der Standardport nicht verfügbar ist, prüft GlobalProtect zehn andere Ports im Bereich von 9999 bis 10009 und verwendet den verfügbaren Port. Sie können auch Ihre eigene Portnummer innerhalb des Bereichs auswählen.
      2. (Optional) Konfigurieren Sie die PAC-Autokonfigurationsdatei-URL, wenn Sie eine benutzerdefinierte PAC-URL für die Proxyeinstellungen per Push an den Endpunkt übertragen möchten. Die PAC-URL wird per Push an den Endpunkt übertragen, sobald der Benutzer eine Verbindung herstellt. Wenn der Benutzer die Verbindung zur GlobalProtect-App trennt, werden die Endpunkt-Proxy-Konfigurationen automatisch deaktiviert und auf die vorherigen Einstellungen zurückgesetzt.

 ©2025 Palo Alto Networks, Inc.

3. (Optional) Aktivieren Sie Benutzer darf Netzwerk erneut erkennen, wenn der Benutzer das Portal auf neue Einstellungen überprüfen soll.
4. (Optional) Konfigurieren Sie Konfigurationsaktualisierungsintervall für GlobalProtect-App (Stunden). Standardmäßig aktualisiert der GlobalProtect-Client die zwischengespeicherte Portalkonfiguration alle 24 Stunden. Sie können das Aktualisierungsintervall entsprechend Ihren Geschäftsanforderungen ändern.

3. Schließen Sie in der Split-Tunnel-Konfiguration den FQDN des expliziten Proxy und den FQDN der PAC-Datei aus.

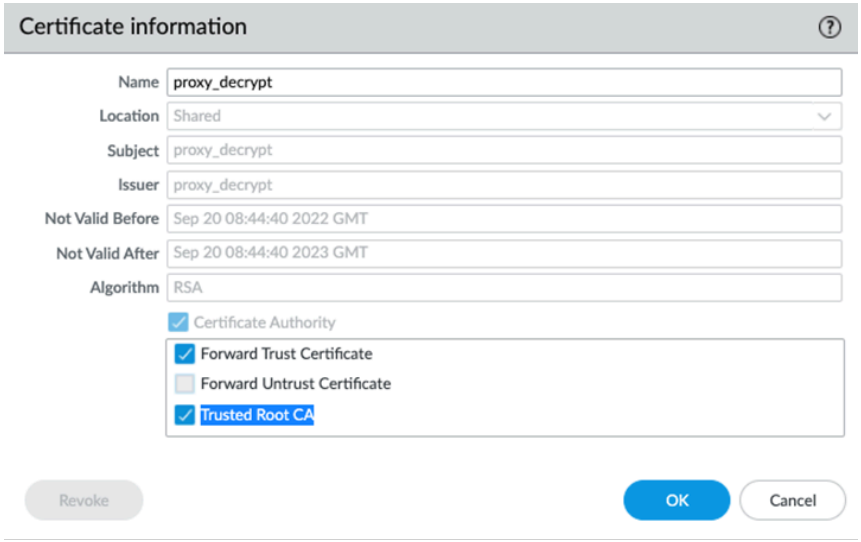
**STEP 4 |** Aktivieren Sie die Always-On-Internetsicherheit, indem Sie die folgenden Einstellungen konfigurieren:

1. Legen Sie für die Option Benutzern das Deaktivieren von GlobalProtect erlauben die Einstellung **Nicht zulassen**, **Mit Passcode zulassen** oder **Mit Ticket zulassen** fest.
2. Legen Sie für die Option Zulassen, dass sich Benutzer von der GlobalProtect-App abmelden die Einstellung **Nein** fest.

**STEP 5 |** (Optional) Konfigurieren Sie die Entschlüsselungsrichtlinie für Datenverkehr für expliziten Proxy.

Wenn Sie die Entschlüsselung aktivieren, stellen Sie sicher, dass das Entschlüsselungszertifikat auch als vertrauenswürdige Stammzertifizierungsstelle eingerichtet ist.

1. Wählen Sie **Gerät** > **Zertifikatverwaltung** > **Zertifikate** aus und erstellen Sie ein Zertifikat, das eine vertrauenswürdige Stammzertifizierungsstelle und ein Forward-Trust-Zertifikat ist.




2. Erstellen Sie eine Entschlüsselungsregel unter **Explicit_Proxy_Device Group** mit SSL-Forward-Proxy.

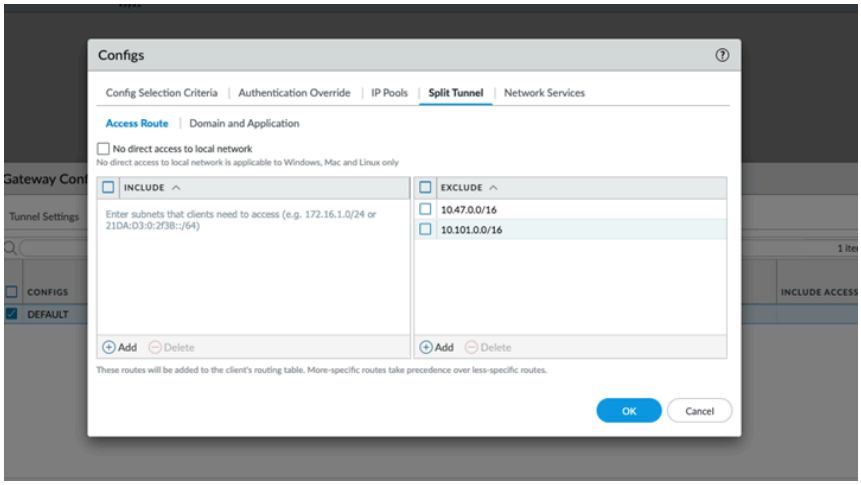
**STEP 6 |** Konfigurieren Sie die Sicherheitsrichtlinienregeln für den Datenverkehr über expliziten Proxy.

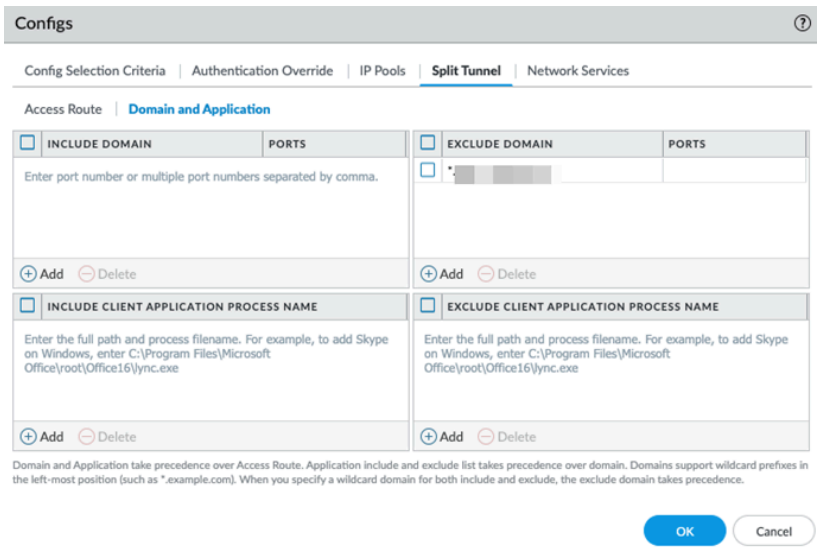
- Wählen Sie **Verwalten** > **Sicherheitsdienste** > **Sicherheitsrichtlinie** > **.** aus.
- Befolgen Sie die Best Practices der Internet-Gateway-Sicherheitsrichtlinie.

 ©2025 Palo Alto Networks, Inc.

**STEP 7 |** Konfigurieren Sie den Split-Tunnel in Panorama.

1. Wählen Sie **Netzwerk** > **Vorlage für mobile Benutzer** > **Gateways** > **GlobalProtect_ExternalGateway** > **Agent** > **Clienteinstellungen** > **Split** aus.
2. Konfigurieren Sie den Tunnel auf der Grundlage von Routen und Domänen.




**STEP 8 |** (Optional) Konfigurieren Sie die GlobalProtect-App im Tunnel- und Proxy-Modus in einem Netzwerk ohne Standardroute.

- (Optional) Hosten Sie eine PAC-Datei intern und fügen Sie den FQDN des expliziten Proxy für Prisma Access als Proxy in der PAC-Datei hinzu, oder hosten Sie die PAC-Datei in einem Weiterleitungsprofil und fügen Sie Routen in Ihrem Netzwerk für IP-Adressen des PAC-Dienstes hinzu.
- Überprüfen Sie, ob die GlobalProtect-Portal-URL und die IdP-URLs an den expliziten Proxy von Prisma Access weitergeleitet werden.
- Richten Sie Routen zum FQDN des expliziten Proxy oder dessen IP-Adressen auf Perimetergeräten ein, damit Benutzer über den expliziten Proxy auf das Internet zugreifen können.
- (Optional) Fügen Sie DNS-Einträge hinzu, um den FQDN des expliziten Proxy für Prisma Access in eine interne IP-Adresse aufzulösen, wenn Benutzer öffentliche Domänen

 ©2025 Palo Alto Networks, Inc.

im Zweignetzwerk nicht auflösen können. Fügen Sie außerdem dem FQDN des expliziten Proxy oder dessen IP-Adresse die NAT (Network Address Translation) der Zieleinheit hinzu.

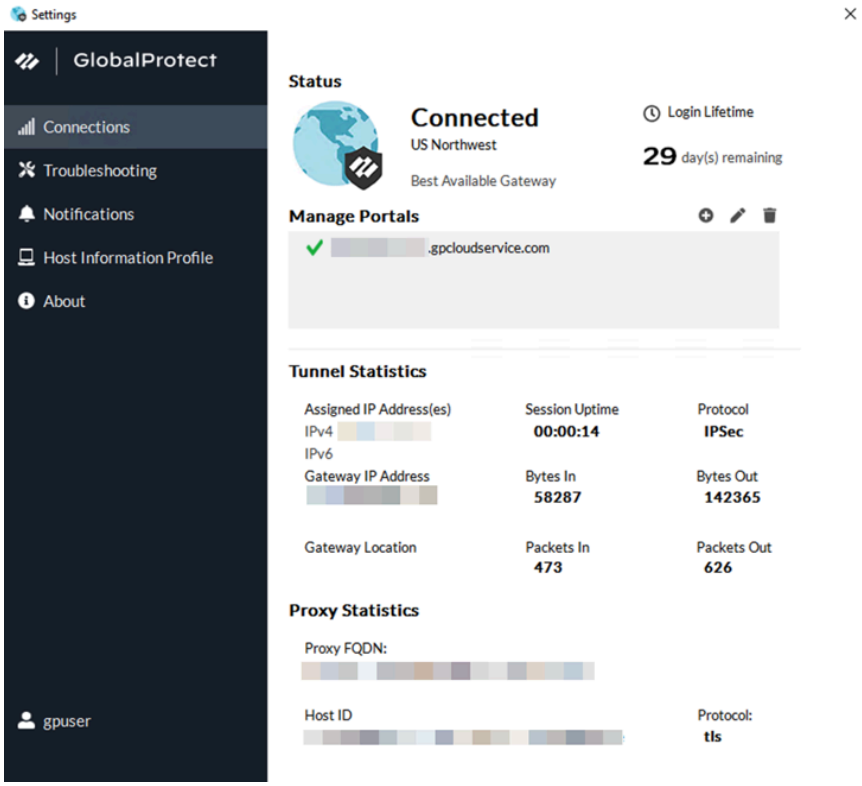
- So ermöglichen Sie Benutzern den direkten Zugriff auf private Apps, wenn sie im Büro sind:
  - **Direktzugriff** – Aktivieren Sie die interne Hosterkennung und lassen Sie die interne Gateway-Liste leer.

**STEP 9 |** Führen Sie die Aktion **Commit** aus, um Ihre Änderungen in Panorama festzuschreiben. Mit **Commit und Push** können Sie die Konfigurationsänderungen für die **Mobilen Benutzer** von Prisma Access und dem **Expliziten Proxy** festschreiben und übertragen.

 ©2025 Palo Alto Networks, Inc.

**STEP 10 |** Überprüfen Sie die Agent-Proxy-Bereitstellung und beheben Sie dabei gefundene Fehler.

1. Überprüfen Sie unter **Einstellungen** auf der Registerkarte **Verbindungen** die Informationen zu Ihrer Netzwerkverbindung in der GlobalProtect-App.
   1. Öffnen Sie die GlobalProtect-App.
   2. Wählen Sie **Einstellungen** aus, um die Anzeige mit den GlobalProtect-Einstellungen zu öffnen, und wählen Sie dann **Verbindungen** aus.




2. Zeigen Sie die GlobalProtect-Protokolle an und erfassen Sie diese.

   Zeigen Sie das PanGPS-Protokoll an, um die Konfiguration des Proxy-Modus im GlobalProtect-Portal zu überprüfen.

   Sie können überprüfen, ob der Proxy-Modus konfiguriert ist, indem Sie im PanGPS-Protokoll nach dem folgenden Ereignis suchen:

   ```
   OnProxyAgentMode: Hybridmodus
   ```

   Um GlobalProtect-Protokolle in Panorama anzuzeigen, wählen Sie **Überwachen** > **Protokolle** und:

   - **GlobalProtect**, für Authentifizierungsprotokolle
   - **Datenverkehr** und **Entschlüsselung** für Benutzerzugriffsprotokolle

**Trennen Sie die Verbindung zum Tunnel- und Proxy-Modus und inaktivieren Sie diesen Modus mit der Verbindungsmethode „Immer aktiviert“**

Ab GlobalProtect Version 6.3.1 müssen Sie die folgenden Schritte ausführen, wenn Sie den Modus **Tunnel und Proxy** für die GlobalProtect-App zusammen mit dem Modus **Immer**

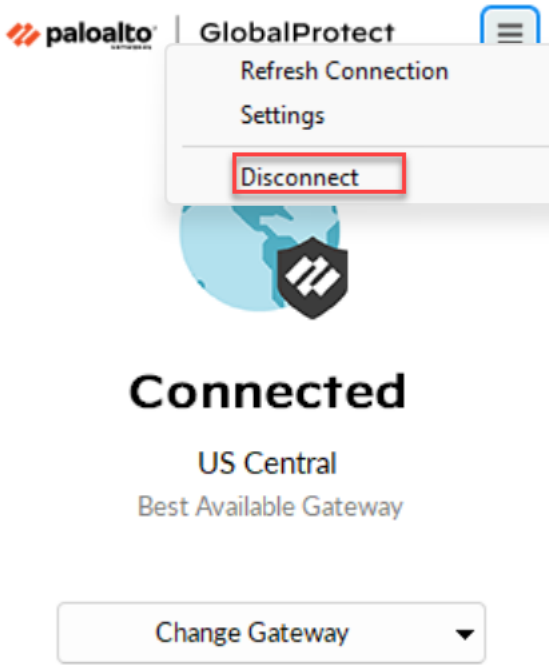
 ©2025 Palo Alto Networks, Inc.

**aktiviert** als Verbindungsmethode konfigurieren und den Tunnel- und Proxy-Modus trennen möchten:

1. Trennen Sie die Verbindung zur GlobalProtect-App, um die Tunnelverbindung (VPN) zu trennen. Wenn Sie die Verbindung zur App trennen, wird die Tunnelverbindung (VPN) getrennt und die App bleibt weiterhin über den Proxy-Modus verbunden.
2. Deaktivieren Sie die GlobalProtect-App, um sowohl den Tunnel- als auch den Proxy-Modus zu trennen. Wenn Sie die App deaktivieren, wird sowohl die Verbindung zum Tunnel- als auch zum Proxy-Modus getrennt und die App ist nicht mehr verbunden.

Um die mit **Tunnel und Proxy** (Hybridmodus) und der Verbindungsmethode **Immer aktiviert** konfigurierte GlobalProtect-App zu trennen und zu deaktivieren, gehen Sie wie folgt vor:

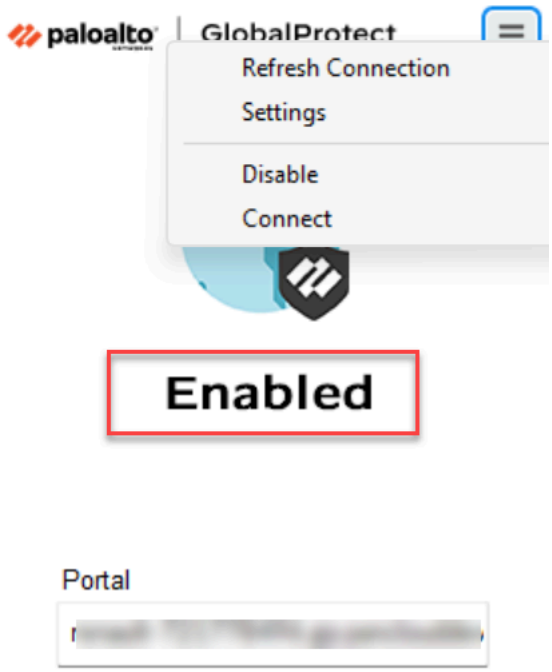
1. Trennen Sie die Verbindung zur GlobalProtect-App mithilfe der Option **Trennen** im Hamburger-Menü. Wenn Sie die Verbindung zur App trennen, wird die Tunnelverbindung (VPN) getrennt.



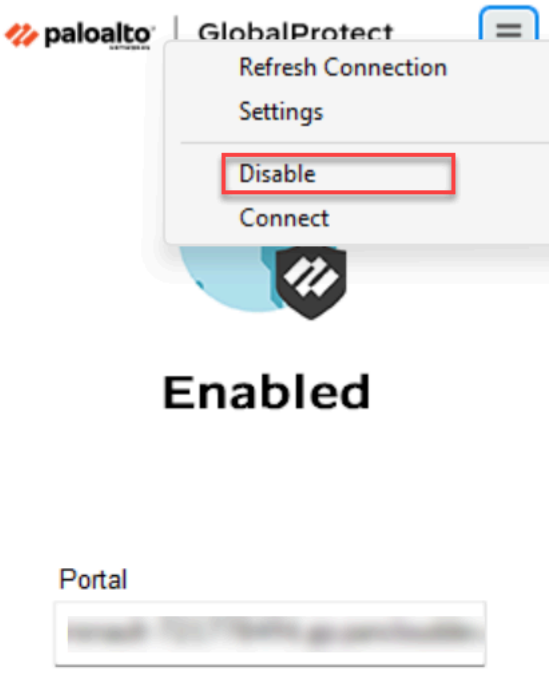

Nachdem Sie die Verbindung zur App getrennt haben, wird die VPN-Verbindung getrennt, der Proxy-Modus wird jedoch aktiviert. Die App ist weiterhin über den Proxy-Modus verbunden und zeigt den Status **Aktiviert** an.

*Wenn Sie die Tunnelverbindung (VPN) wiederherstellen möchten, können Sie die Option **Verbinden** im Hamburger-Menü verwenden.*


©2025 Palo Alto Networks, Inc.

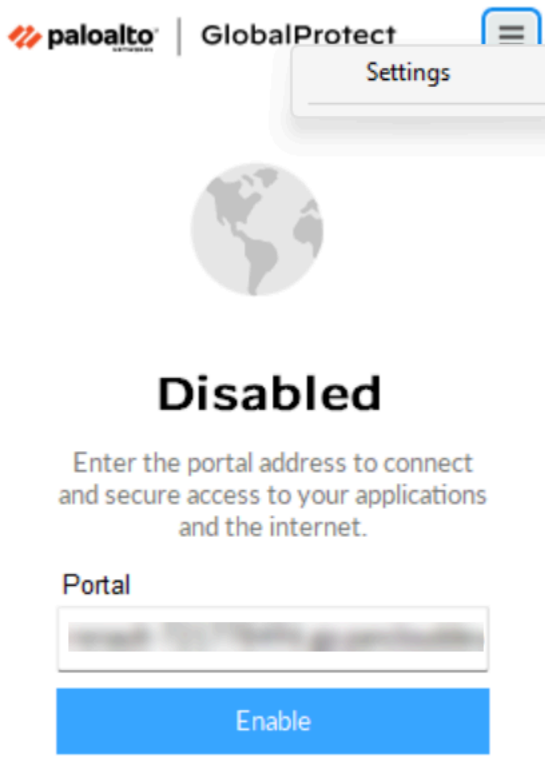



2. Deaktivieren Sie die GlobalProtect-App mit der Option **Deaktivieren** im Hamburger-Menü. Nachdem Sie die App deaktiviert haben, werden sowohl die Tunnel- als auch die Proxy-Verbindung getrennt.




Die App wird deaktiviert und der Status wird als **Deaktiviert** angezeigt.

 ©2025 Palo Alto Networks, Inc.




# Sichtbarkeit und Durchsetzung privater IP-Adressen für agentenbasierten Proxy-Verkehr

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama)<br>• Prisma Access (Managed by Strata Cloud Manager) | • Prisma Access Version 5.2<br>• GlobalProtect-App Version 6.3.1 für Windows oder macOS<br>• Prisma Access Dataplane Version 10.2.4<br>• Prisma Access Mobile-Benutzer-Lizenz<br>• Panorama-Plug-in Version 5.2.0 |

Benutzer, die über den GlobalProtect-Agenten von Zweigstellen aus eine Verbindung zum expliziten Proxy von Prisma Access herstellen, können private IP-Adressen von Endpunkten für die Protokollierung oder die Anwendung der Durchsetzung auf Basis von IP-Adressen nutzen.

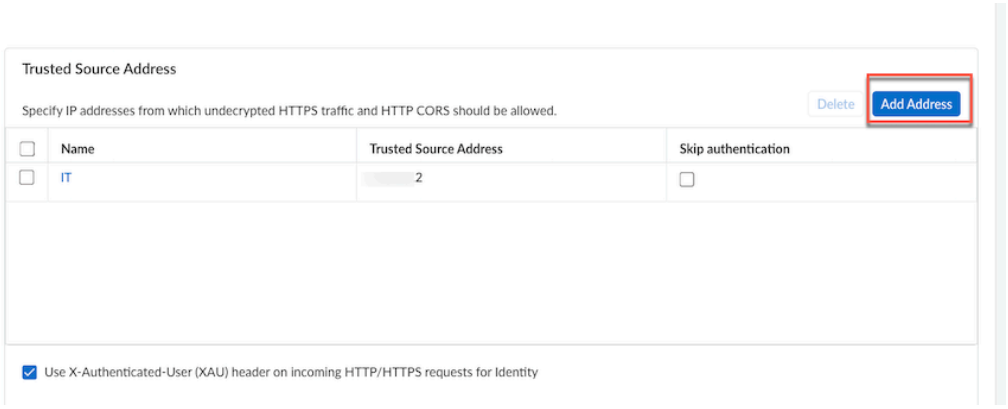
- Strata Cloud Manager
- Panorama

## Sichtbarkeit und Durchsetzung privater IP-Adressen für agentenbasierten Proxy-Datenverkehr (Strata Cloud Manager)

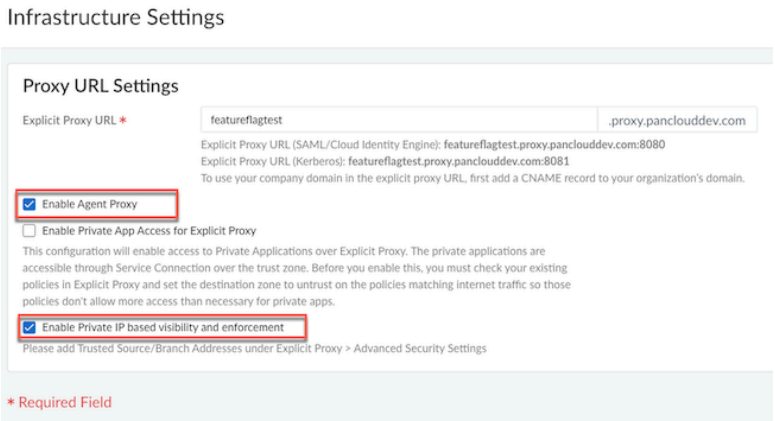
**STEP 1 |** Aktivieren Sie die agentenbasierte Proxy-Funktionalität (Proxy-Modus oder Tunnel- und Proxy-Modus) für mobile Benutzer.

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Navigieren Sie zu **Workflows** > **Einrichtung Prisma Access** > **Expliziter Proxy** > **Erweiterte Sicherheitseinstellungen**, und klicken Sie dann auf das Symbol „Einstellungen“. Fügen Sie unter **Adresse der vertrauenswürdigen Quelle** die Ausgangs-IP-Adresse der Zweigstelle hinzu.




**STEP 3 |** Navigieren Sie zu **Workflows** > **Einrichtung Prisma Access** > **Expliziter Proxy** > **Infrastruktureinstellungen**. Aktivieren Sie unter **Proxy-URL-Einstellungen Quell-IP-basierte Sichtbarkeit und Durchsetzung aktivieren** und klicken Sie dann auf **Speichern**.




**STEP 4 |** (Optional) Konfigurieren Sie die Sicherheitsregeln mit der Quell-IP-Adresse des Endpunkts.

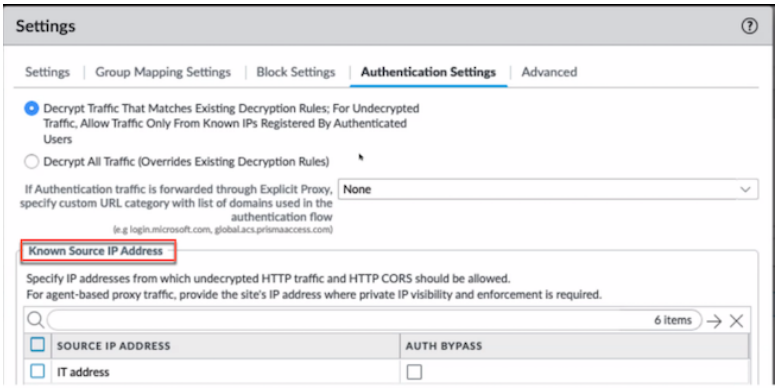
**STEP 5 |** **Konfiguration übertragen** auf **Expliziten Proxy**.

## Sichtbarkeit und Durchsetzung privater IP-Adressen für agentenbasierten Proxy-Datenverkehr (Panorama)

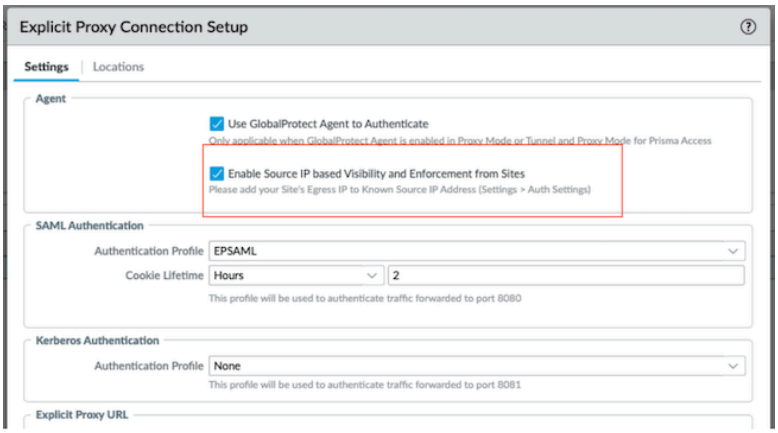
**STEP 1 |** Aktivieren Sie die agentenbasierte Proxy-Funktionalität (Proxy-Modus und Tunnel- und Proxy-Modus) für mobile Benutzer.

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Navigieren Sie zu **Cloud Services** > **Konfiguration** > **Mobile Benutzer** > **Expliziter Proxy** > **Einstellungen** > **Authentifizierungseinstellungen** und fügen Sie die Ausgangs-IP-Adresse des Zweigs unter **Bekannte Quell-IP-Adresse** hinzu.




**STEP 3 |** Navigieren Sie zu **Cloud Services** > **Konfiguration** > **Mobile Benutzer – Expliziter Proxy**. Aktivieren Sie unter **Agent Quell-IP-basierte Sichtbarkeit und Durchsetzung von Websites aktivieren** und klicken Sie dann auf **OK**.




**STEP 4 |** (Optional) Konfigurieren Sie die Sicherheitsregeln mit der Quell-IP-Adresse des Endpunkts.

**STEP 5 |** „Commit und Push“ an **Explicit_Proxy_Device_Group**.

## SAML-Authentifizierung für expliziten Proxy

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

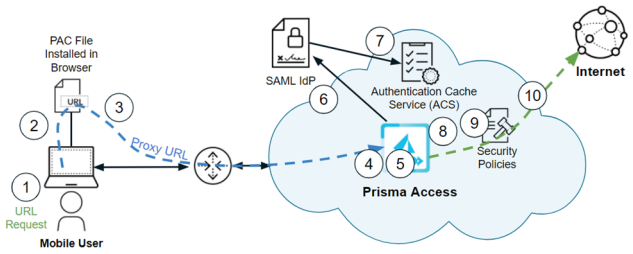
Erfahren Sie, wie der explizite Proxy mit SAML funktioniert und wie Sie ihn konfigurieren.

- Datenverkehrsverarbeitung des expliziten Proxy mit SAML
- Expliziten Proxy mit SAML konfigurieren

 ©2025 Palo Alto Networks, Inc.

## Datenverkehrsverarbeitung des expliziten Proxy mit SAML

So funktioniert der explizite Proxy mit SAML. Im Folgenden ist der Pfad des Datenverkehrs beschrieben:




**STEP 1 |** Der mobile Benutzer surft im Internet oder greift auf die SaaS-Anwendung zu, indem er die URL oder IP-Adresse über einen Webbrowser eingibt.

**STEP 2 |** Der Browser auf dem Endpunkt der mobilen Benutzer sucht nach der PAC-Datei.

Diese PAC-Datei gibt an, dass die URL- oder SaaS-Anfrage an den expliziten Proxy von Prisma Access gehen soll.

**STEP 3 |** Der HTTPS-Client (der Browser auf dem Endpunkt des mobilen Benutzers) leitet die URL-Anfrage an die Proxy-URL weiter.

**STEP 4 |** Der Datenverkehr wird zum expliziten Proxy umgeleitet, und der Proxy entschlüsselt den Datenverkehr.

**STEP 5 |** Der Proxy prüft den Datenverkehr und prüft das vom expliziten Proxy von Prisma Access eingerichtete Authentifizierungscookie.

Das Cookie enthält Informationen, die den mobilen Benutzer identifizieren, und wird zur Authentifizierung des Benutzers verwendet.

**STEP 6 |** Stellt Prisma Access bei der Prüfung des Cookies fest, dass der Benutzer nicht authentifiziert ist, leitet es den Benutzer zur Authentifizierung weiter.

**STEP 7 |** Nachdem der IdP den Benutzer authentifiziert hat, speichert Prisma Access den Authentifizierungsstatus des Benutzers im Authentifizierungs-Cache-Dienst (Authentication Cache Service, ACS). Die Gültigkeitsdauer der Authentifizierung basiert auf dem Wert für **Cookie-Lebensdauer**, den Sie bei der Konfiguration des expliziten Proxy angeben.

**STEP 8 |** Der explizite Proxy prüft das Vorhandensein und die Gültigkeit des Cookies. Ist das Cookie nicht vorhanden oder ungültig, wird der Benutzer an den ACS weitergeleitet. Nachdem der ACS die Authentifizierung des Benutzers bestätigt hat, wird der Benutzer mit einem Token zurück zum expliziten Proxy geleitet. Der Proxy validiert dann dieses Token und setzt das Cookie für diese Domäne und für diesen Benutzer.

**STEP 9 |** Prisma Access wendet die Sicherheitsdurchsetzung basierend auf den vom Administrator konfigurierten Sicherheitsrichtlinienregeln an.

**STEP 10 |** Wenn die URL nicht durch Sicherheitsrichtlinienregeln blockiert wird, sendet Prisma Access die URL-Anfrage ins Internet.


©2025 Palo Alto Networks, Inc.

**STEP 11 |** (Optional) Konfigurieren Sie die Funktionalität Konnektivität für expliziten Proxy in GlobalProtect für die Always-On Internet Security. Aktivieren Sie diese Funktionalität, um eine jederzeit verfügbare Sicherheit für den Internet-Verkehr zu erreichen und gleichzeitig On-Demand-Zugriff auf private Apps über GlobalProtect oder ein VPN von Drittanbietern zu ermöglichen.

## Expliziten Proxy mit SAML konfigurieren

Gehen Sie wie folgt vor, um einen expliziten Proxy mit SAML-Authentifizierung zu konfigurieren.

- Strata Cloud Manager
- Panorama

## Expliziten Proxy mit SAML (Strata Cloud Manager) konfigurieren

**STEP 1 |** Richten Sie den expliziten Proxy ein.

**STEP 2 |** (Optional) Konfigurieren der Cloud Identity Engine Authentifizierung für den expliziten Proxy.

**STEP 3 |** Konfigurieren Sie die Sicherheitsrichtlinienregeln.

1. Wählen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Konfigurationsumfang aus: Expliziter Proxy** > **Sicherheitsdienste** > **Sicherheitsrichtlinie**.
2. Passen Sie die Standardrichtlinienregeln Ihren Anforderungen und den Best Practices für die Sicherheitsrichtlinien für Internet-Gateways an.

> *Mit Prisma Access Version 5.1 und dem Dataplane PAN-OS 10.2.10 oder einer neueren Version benötigen Sie lediglich die Sicherheitsrichtlinienregel **Bekannten Benutzern den Webzugriff erlauben**.*

**STEP 4 |** Übertragen Sie Ihre Konfigurationsänderungen.

## Expliziten Proxy mit SAML konfigurieren (Panorama)

**STEP 1 |** Richten Sie den expliziten Proxy ein.

**STEP 2 |** (Optional) Konfigurieren der Cloud Identity Engine Authentifizierung für den expliziten Proxy.

**STEP 3 |** Konfigurieren Sie je nach der Version von Prisma Access und der Version Ihrer Dataplane entweder eine einzelne Richtlinienregel oder mehrere solcher Regeln.

| Versionsanforderungen | Configuration (Konfiguration) |
|---|---|
| Prisma Access Version 5.1 oder eine neuere Version und die Dataplane-Version PAN-OS 10.2.10 oder eine neuere Version. | Konfigurieren einer Sicherheitsrichtlinienregel für den Benutzerdatenverkehr vor der Authentifizierung.<br>**1.** Wählen Sie die Gerätegruppe **Explicit_Proxy_Device_Group** aus. |

 ©2025 Palo Alto Networks, Inc.

| Versionsanforderungen | Configuration (Konfiguration) |
|---|---|
| | 2. Erstellen Sie einen Anwendungsfilter mit dem Tag **Web-App**.<br>3. Wählen Sie **Richtlinien** > **Vor-Regeln** > **Hinzufügen** aus.<br>4. Erstellen Sie die Regel.<br>1. **Fügen** Sie die Regel hinzu.<br>2. Ordnen Sie ihr einen aussagekräftigen Namen zu.<br>Beispiel: **`allow-pre-auth`**<br>3. Wählen Sie auf der Registerkarte **Anwendung** die Option **Hinzufügen** und den Anwendungsfilter **Web-App** auswählen.<br>4. Auf der Registerkarte **Quelle** müssen Sie **Hinzufügen** und **Bekannter Benutzer** auswählen. |
| Alle anderen Prisma Access- und Dataplane-Versionen. | Konfigurieren Sie Sicherheitsrichtlinienregeln entsprechend Ihren Anforderungen und den Best Practices für die Sicherheitsrichtlinien für Internet-Gateways. |

**STEP 4 |** Schreiben Sie die Konfiguration mit **Commit** fest.

## „Expliziter Proxy“ einrichten

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>Wenn Sie private Quell-IP-basierte Sichtbarkeit und Durchsetzung auf „Expliziter Proxy“ in Ihrer Prisma Access-Umgebung aktivieren möchten, wenden Sie sich an Ihr Account-Team, um mehr zu erfahren. | • Prisma Access-Lizenz |

Verwenden Sie „Expliziter Proxy“, um mobile Benutzer zu schützen, indem Sie Browser-Datenverkehr auf Prisma Access umleiten.

**Onboarding-Richtlinien** – Verwenden Sie die folgenden Richtlinien, wenn Sie Ihre Bereitstellung des Typs „Expliziter Proxy“ lizenzieren und einbinden:

- „Expliziter Proxy“ unterstützt eine Teilmenge von Prisma Access-Standorten.

 ©2025 Palo Alto Networks, Inc.

- Mit zwei Sternchen gekennzeichnete Standorte können nicht hinzugefügt werden, da es sich dabei um lokale Zonen handelt, die mit Prisma Access nicht unterstützt werden.
- Wenn Sie über eine lokale Lizenz oder eine Evaluierungslizenz für Prisma Access für Benutzer verfügen und sowohl mit einer Bereitstellung des Typs „Mobile Benutzer – GlobalProtect“ als auch mit einer Bereitstellung des Typs „Mobile Benutzer – Expliziter Proxy“ arbeiten, können Sie jeweils maximal fünf Standorte bereitstellen (maximal fünf Standorte für „Mobile Benutzer – GlobalProtect“ und maximal fünf Standorte für „Mobile Benutzer – Expliziter Proxy“). Wenn Sie eine weltweite Lizenz besitzen, gibt es keine Einschränkungen für die maximale Anzahl von Standorten.
- „Expliziter Proxy“ unterstützt Mehrmandantenfähigkeit unter folgenden Bedingungen: Wenn Sie über eine vorhandene Prisma Access-Bereitstellung ohne Mehrmandantenfähigkeit verfügen und diese in eine Mehrmandanten-Bereitstellung umwandeln, wird „Expliziter Proxy“ nur vom ersten Mandanten (dem Mandanten, den Sie migriert haben) unterstützt. Alle nachfolgenden Mandanten, die Sie für die Bereitstellung mit mehreren Mandanten nach dem ersten Mandanten erstellen, unterstützen „Expliziter Proxy“ nicht.
- Beim Onboarding einer Bereitstellung des Typs „Expliziter Proxy“ empfiehlt Palo Alto Networks, die gesamte Konfiguration in einem einzigen Browser durchzuführen. Sie können jedoch Sicherheitsrichtlinien aus mehreren Browsern oder Browsersitzungen hinzufügen.
- Die URL-Filteraktionen **Weiter** oder **Überschreiben** werden nicht unterstützt und funktionieren nicht mit „Expliziter Proxy“.

Erfahren Sie, wie Sie „Expliziter Proxy“ einrichten.

- Strata Cloud Manager
- Panorama

## Cloud Management

Richten Sie eine Verbindung mit explizitem Proxy für mobile Benutzer ein. Mit explizitem Proxy leitet eine Proxy-Autokonfigurationsdatei (PAC) auf mobilen Benutzergeräten den Browserverkehr zu Prisma Access um.

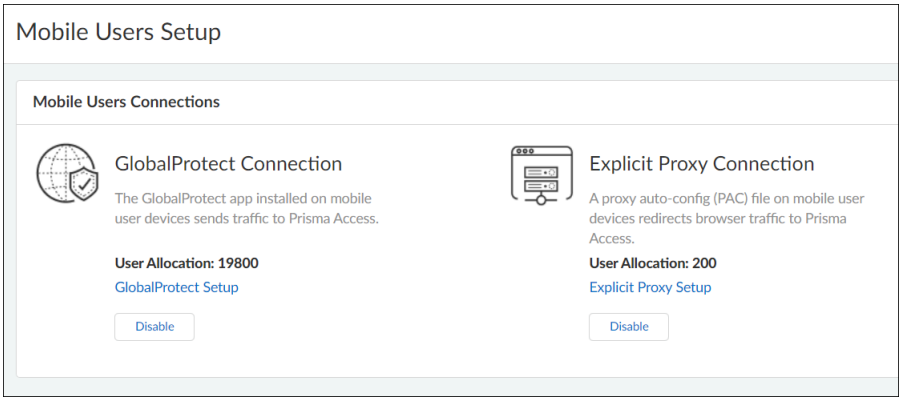
Lesen Sie vor Beginn unbedingt die Richtlinien zum expliziten Proxy.

### STEP 1 | Expliziten Proxy aktivieren und Benutzer zuweisen

Gehen Sie zu **Workflows** > **Einrichtung Prisma Access** > **Mobile Benutzer**, um mit der Einrichtung eines expliziten Proxys zu starten. Wenn Sie den expliziten Proxy aktivieren,

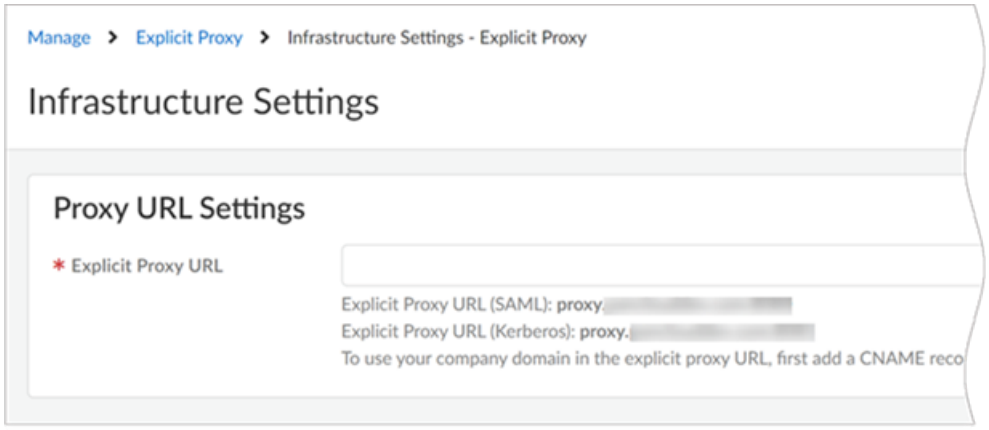
 ©2025 Palo Alto Networks, Inc.

werden Sie aufgefordert, die Anzahl der mobilen Benutzer anzugeben, die diesen Verbindungstyp verwenden sollen.




**STEP 2 | Fügen Sie die Proxy-Einstellungen hinzu, die mobile Benutzer für die Verbindung mit Prisma Access verwenden**

Wechseln Sie zu **Infrastruktureinstellungen**:




1. Geben Sie die URL eines expliziten Proxy an.

   Der Standardname lautet *proxyname*.proxy.prismaaccess.com, wobei *proxyname* die von Ihnen angegebene Subdomäne ist, die Port 8080 verwendet. Um Ihre Unternehmensdomäne in der URL des expliziten Proxy zu verwenden, fügen Sie einen CNAME-Datensatz zur Domäne Ihres Unternehmens hinzu.

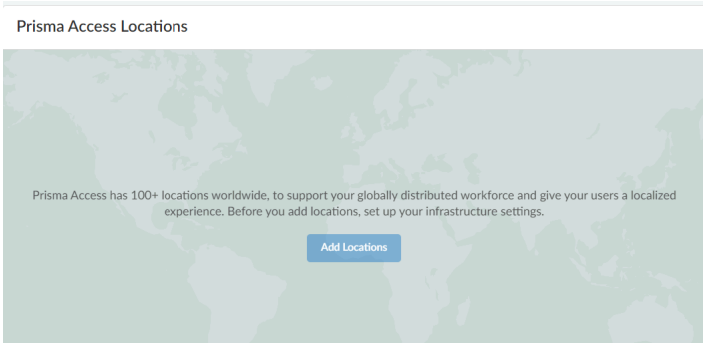
   Sie können SAML- oder Kerberos-Authentifizierungstypen verwenden, um mobile Benutzer zu authentifizieren.
2. (Optional) Wählen Sie **Agent-Proxy aktivieren** aus, um die agentenbasierte Proxy-Funktionalität zu aktivieren.

   Aktivieren Sie diese Funktion, um „Expliziter Proxy“ im Proxymodus oder im Tunnel- und Proxymodus einzurichten.
3. Verwenden Sie Weiterleitungsregeln, um eine PAC-Datei zu erstellen, die Ihren Anforderungen entspricht, oder laden Sie Ihre eigene PAC-Datei in ein Weiterleitungsprofil hoch.

 ©2025 Palo Alto Networks, Inc.

**STEP 3 | Wählen Sie den Prisma Access-Standort aus, mit dem sich Ihre mobilen Benutzer verbinden werden**

Fügen Sie die Prisma Access-Standorte hinzu, an denen Sie mobile Benutzer unterstützen möchten.




Auf der Karte sind die Prisma Access-Standorte dargestellt.

Wenn Sie die Anzahl der Standorte begrenzen, wählen Sie für ein optimales Benutzererlebnis die Standorte aus, die Ihren Benutzern am nächsten sind oder die sich im selben Land wie Ihre Benutzer befinden. Wenn ein Standort in dem Land, in dem sich Ihre mobilen Benutzer befinden, nicht verfügbar ist, wählen Sie für eine optimale Leistung den Standort aus, der Ihren Benutzern am nächsten ist.

*Sie sollten Standorte mit explizitem Proxy in mindestens zwei Regionen aktivieren, um regionale Redundanz zu gewährleisten.*

**STEP 4 | Mobile Benutzer authentifizieren**

Richten Sie die **Benutzerauthentifizierung** ein, damit nur legitime Benutzer Zugriff auf Ihre Dienste und Anwendungen erhalten.

SAML und Kerberos sind die unterstützten Authentifizierungsprotokolle. Prisma Access unterstützt PingOne, Azure AD und Okta als SAML-Authentifizierungsanbieter. Sie sollten jedoch jeden Anbieter verwenden können, der SAML 2.0 als SAML-Identitätsanbieter (IdP) unterstützt. Erfahren Sie mehr darüber, wie Sie die Authentifizierung mobiler Benutzer bei Prisma Access aktivieren.

**STEP 5 | Standardmäßig aktivierte Best-Practice-Sicherheitsregeln überprüfen**

Prisma Access setzt standardmäßig Best-Practice-Sicherheitsrichtlinienregeln durch. Diese Regeln ermöglichen es Ihren Benutzern, sicher auf allgemeine Internetseiten zu navigieren. Für die Benutzer gilt Folgendes:

- Der Besuch bekannter bösartiger Websites wird basierend auf der URL blockiert
- Bekanntermaßen bösartige Dateien können nicht hoch- oder heruntergeladen werden
- Sie werden vor unbekannten, nie zuvor gesehenen Bedrohungen geschützt
- Sie werden vor Viren, Spyware (Command-and-Control-Angriffen) und Sicherheitslücken geschützt

Nach der Ersteinrichtung können Sie diese Standardregeln überprüfen und aktualisieren, um Ihren Unternehmensanforderungen zu entsprechen.

 ©2025 Palo Alto Networks, Inc.

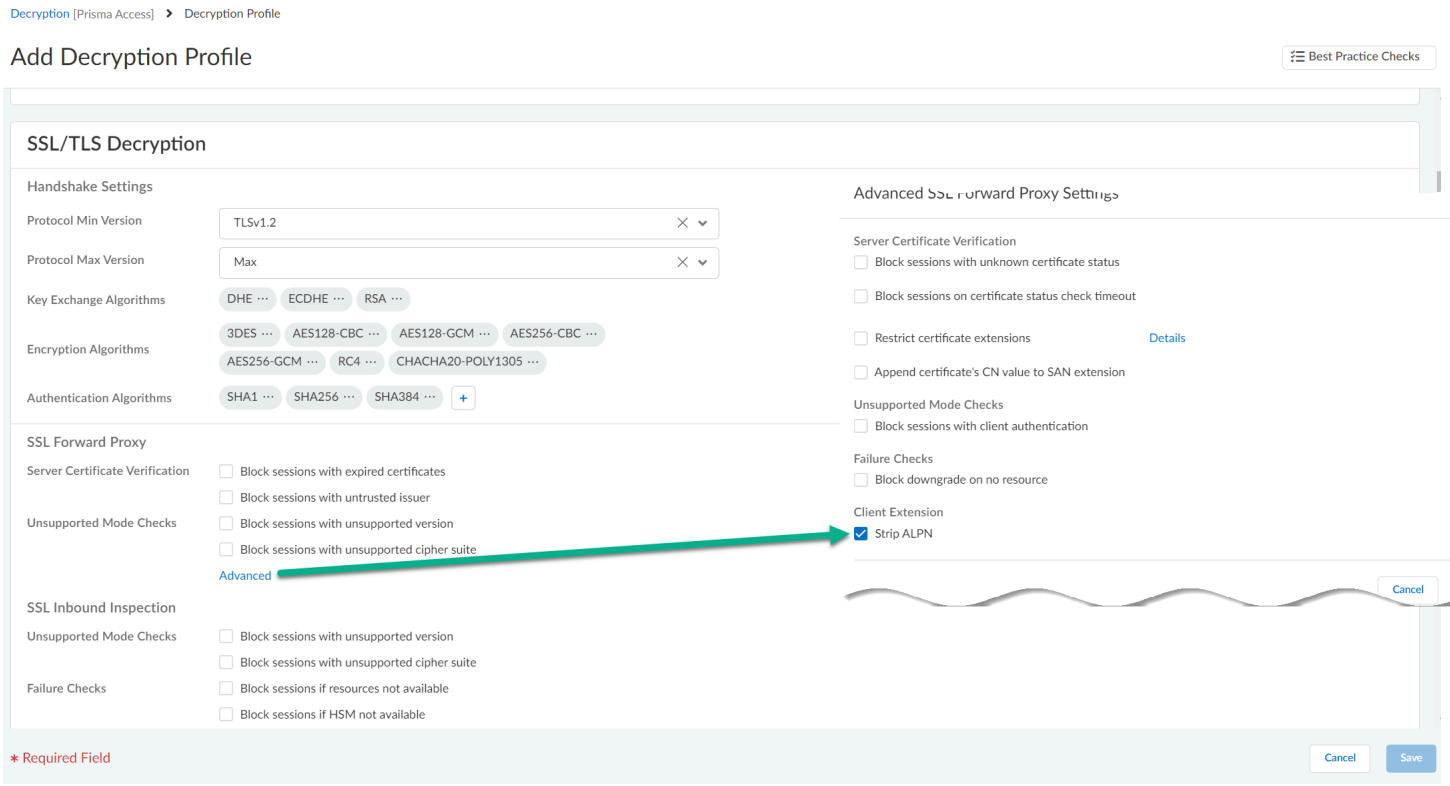
## STEP 6 | Überprüfen, ob der Standort der mobilen Benutzer aktiv ist

Nachdem Sie Ihre anfängliche Konfiguration an Prisma Access übertragen haben, beginnt Prisma Access mit der Bereitstellung der Umgebung Ihrer mobilen Benutzer. Dies kann bis zu 15 Minuten dauern. Sobald die Standorte Ihrer mobilen Benutzer eingerichtet und aktiv sind, können Sie diese auf den Einrichtungsseiten für mobile Benutzer, auf der Übersichtsseite und innerhalb von Insights einsehen.

*Sie können Ihre Einrichtung auch validieren, indem Sie **Verwalten** > **Diensteinrichtung** > **Mobile Benutzer** auswählen und die Infrastruktureinstellungen bearbeiten, um zu bestätigen, dass an jedem der von Ihnen bereitgestellten Standorte ein Gateway eingerichtet ist.*

## STEP 7 | Entschlüsselung für Datenverkehr für expliziten Proxy aktivieren

- Legen Sie die maximal unterstützte TLS-Version auf 1.2 fest.
- Legen Sie **ALPN entfernen** (Advanced SSL Forward Proxy-Einstellungen) fest, da der explizite Proxy natives HTTP/2 nicht unterstützt und Sie die ALPN-Header entfernen müssen.




## STEP 8 | Laden Sie die Stamm-Zertifizierungsstelle herunter und installieren Sie sie auf Ihrem Endpunkt zur SSL-Entschlüsselung.

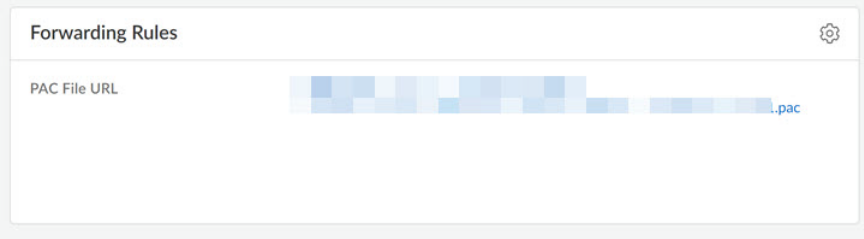
 ©2025 Palo Alto Networks, Inc.

**STEP 9 | Bearbeiten Sie den Inhalt der PAC-Datei.**

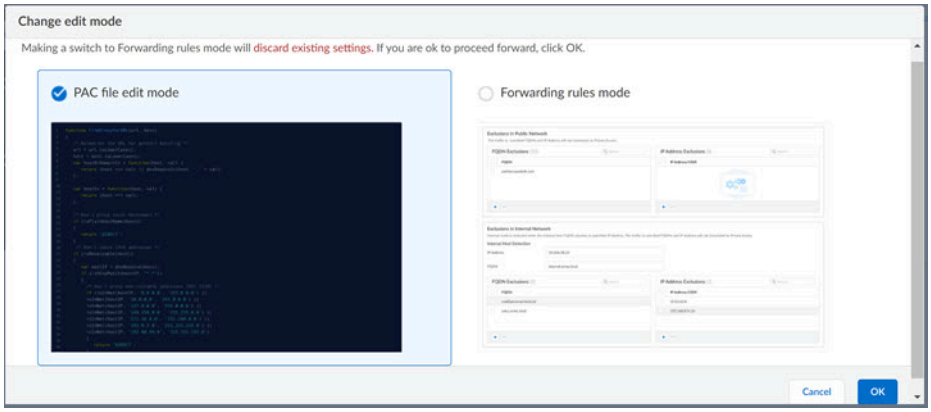
*Verwalten Sie PAC-Dateien mithilfe von* Weiterleitungsprofilen.

Passen Sie eine Proxy-Autokonfigurationsdatei (PAC) für explizite Proxys an Ihre Anforderungen an. Die GlobalProtect-App leitet den Datenverkehr basierend auf Weiterleitungsregeln und Logik aus der PAC-Datei über einen Proxy an Prisma Access weiter.

Wählen Sie **Weiterleitungsregeln** aus.




1. Laden Sie die PAC-Datei herunter und passen Sie sie an Ihre Anforderungen an. Importieren Sie sie dann wieder an diesen Ort, und wir nennen Ihnen die URL für den Standort, an dem Prisma Access die PAC-Datei hostet.
2. Bearbeiten Sie die PAC-Datei im Modus **PAC-Dateieditor** oder im Modus **Weiterleitungsregeln**.
3. Der Modus **PAC-Dateieditor** ist standardmäßig ausgewählt. Klicken Sie auf **OK**, um den Bearbeitungsmodus für PAC-Dateien zu aktivieren.
4. Wählen Sie **Modus „Weiterleitungsregel“** aus und klicken Sie auf **OK**, um im Modus „Weiterleitungsregeln“ fortzufahren. Beim Wechsel in den Modus „Weiterleitungsregeln“ werden die vorhandenen Einstellungen verworfen.



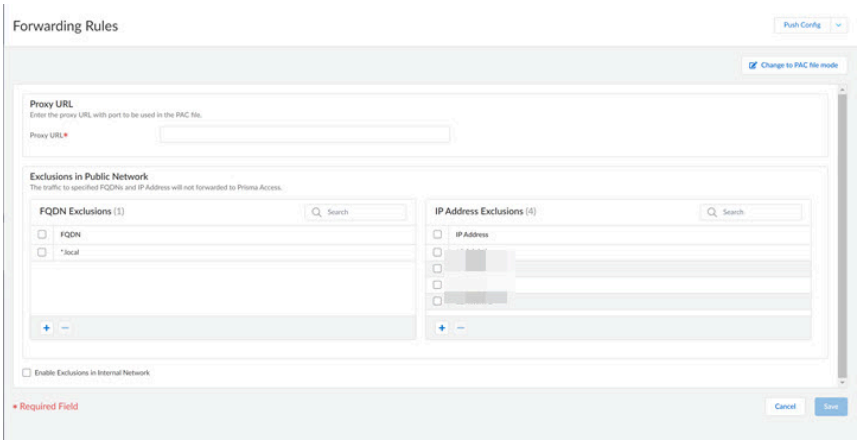

- Geben Sie die **URL des expliziten Proxy** und den Port ein, die in der PAC-Datei verwendet werden sollen.

  Standardmäßig lautet der Name proxyname.proxy.prismaaccess.com. Dabei ist „proxyname“ die von Ihnen angegebene Subdomäne, die Port 8080 verwendet.
- Konfigurieren Sie **Ausschlüsse im öffentlichen Netzwerk**, wenn sich Ihre mobilen Benutzer des expliziten Proxy über ein öffentliches Netzwerk mit Prisma Access verbinden.

 ©2025 Palo Alto Networks, Inc.

- Konfigurieren Sie **FQDN-Ausschlüsse** und **IP-Adressausschlüsse**. Die ausgeschlossenen FQDNs und IP-Adressen werden nicht von Prisma Access weitergeleitet.

- Aktivieren Sie **Ausschlüsse im internen Netzwerk zulassen**, um Ausschlüsse für bestimmte IP-Adressen oder FQDNs zu konfigurieren, wenn sich die mobilen Benutzer des expliziten Proxy mit Prisma Access im internen Netzwerk verbinden.
  - Geben Sie die folgenden Ausschlüsse an, um unterschiedliche Datenverkehrsausschlüsse festzulegen, wenn sich der Benutzer im internen Netzwerk befindet.
    - Geben Sie die **IP-Adresse** eines Hosts ein, der nur vom internen Netzwerk aufgelöst werden kann.
    - Geben Sie den **FQDN** ein, der in die von Ihnen eingegebene IP-Adresse aufgelöst wird.
  - Konfigurieren Sie Ausschlüsse für bestimmte FQDNs und IP-Adressen. Der Datenverkehr zu den angegebenen FQDNs und IP-Adressen wird von Prisma Access nicht weitergeleitet.
- **Speichern** Sie die Änderungen.

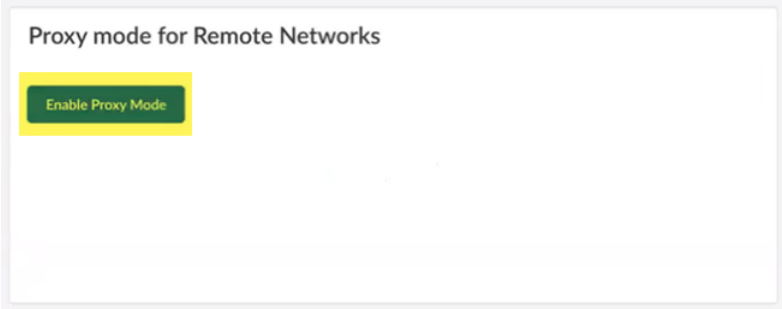



**STEP 10 |** Konfigurieren Sie **Erweiterte Sicherheitseinstellungen**.

- Wenn Sie Datenverkehr von Ihren Zweigstellen über einen sicheren IPSec-Tunnel an „Expliziter Proxy“ weiterleiten möchten, wählen Sie **Proxy-Modus aktivieren** aus und rufen

 ©2025 Palo Alto Networks, Inc.

Sie Anycast-IP-Adressen ab, wenn Sie „Expliziter Proxy“ in Verbindung mit einem Prisma Access-Remote-Netzwerk verwenden möchten.




Diese Lösung verwendet Anycast-Adressen mit einem Remote-Netzwerk-IPSec-Tunnel, um die Verwendung von „Expliziter Proxy“ für Benutzer und Geräte an einem Remote-Netzwerkstandort oder einem Zweigstellenstandort zu ermöglichen.

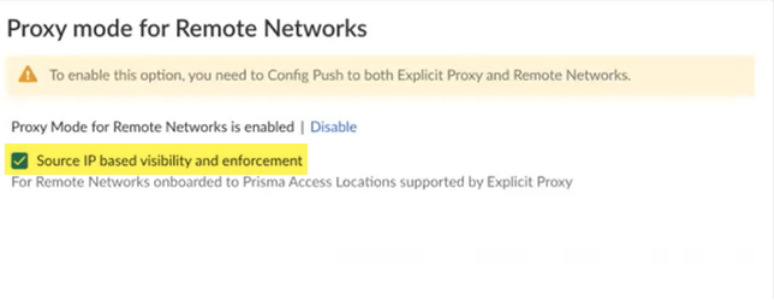
- Nur Bereitstellungen mit aktiviertem Proxy-Modus Wenn der Proxy-Modus in Ihren Remote-Netzwerken aktiviert ist, fügen Sie eine Richtlinie hinzu, um Datenverkehr zuzulassen, der an Anycast- und Unicast-IP in Remote-Netzwerken gebunden ist. Wenn Sie **Transparenz und Durchsetzung der Quell-IP** aktiviert haben, verwenden Sie das Feld **Quell-IP** in den Sicherheitsrichtlinien von „Expliziter Proxy“, um den Datenverkehr abzusichern. Sie benötigen zusätzliche Richtlinien in den Remote-Netzwerken.

 ©2025 Palo Alto Networks, Inc.

- (Optional) Wenn Sie den Proxy-Modus aktivieren, um die privaten IP-Adressen der Systeme an Ihren Zweigstellenstandorten zu nutzen, die Datenverkehr an „Expliziter Proxy“ weiterleiten, wählen Sie **Quell-IP-basierte Sichtbarkeit und Durchsetzung** aus.

  Für diese Funktionalität gelten folgende Anforderungen:

  - Mindestens Prisma Access-Dataplane 10.2.4
  - Eine Prisma Access (Managed by Panorama)-Bereitstellung mit einem Cloud Services-Plug-in von mindestens 4.1
  - Die Quell-IP-Adressen werden nur für Remote-Netzwerkstandorte angezeigt, die mit „Expliziter Proxy“ unterstützt werden.




- Geben Sie **Quellen blockieren** an.

  Fügen Sie der Liste **Quelladresse blockieren** den Quell-IP-Adressverkehr hinzu, der blockiert werden soll.

  Geben Sie eine Adresse, eine Adressgruppe oder EDL an.

  Um IP-Adresslisteneinträge von der Durchsetzung auszuschließen, wählen Sie **Ausnahme hinzufügen** aus, um die IP-Adressen auszuwählen, die von der Blockierung ausgeschlossen werden sollen.
- Geben Sie **Blockierte Domänen** an.

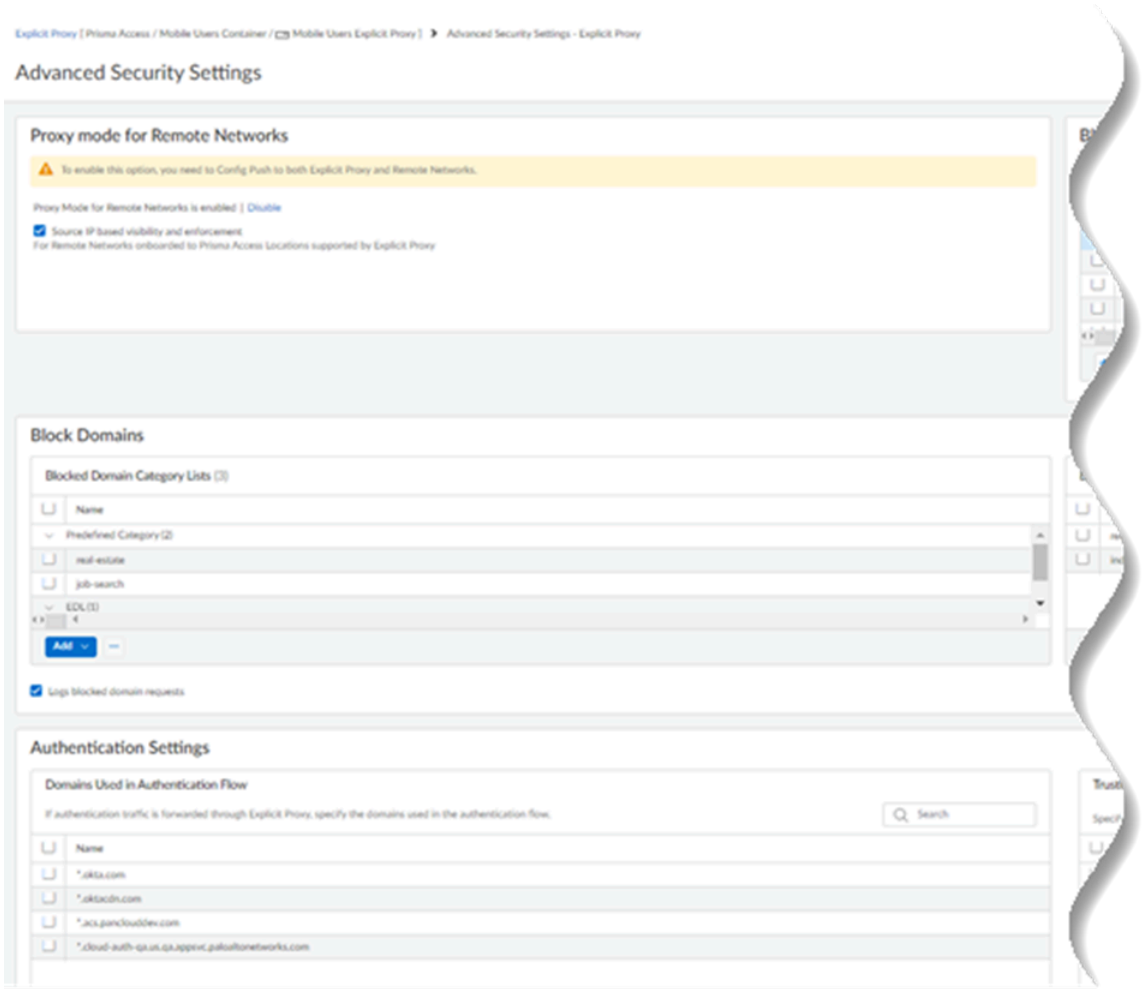
  Geben Sie die Domänen oder Domänenkategorien für bösartige Websites oder für Websites an, auf die Benutzer nicht zugreifen sollen. Prisma Access verhindert, dass Benutzer auf die URLs und IP-Adressen zugreifen, die Sie in diesem Bereich angeben, wenn Benutzer den Befehl HTTP GET (für unverschlüsselte Anfragen) oder HTTP CONNECT

 ©2025 Palo Alto Networks, Inc.

(für verschlüsselte Anfragen) absetzen. Benutzer erhalten eine Blockierungsseite, wenn sie versuchen, auf blockierte Websites zuzugreifen.

- Wenn Sie Domänen ausnehmen möchten, die in einer Liste blockierter Domänenkategorien enthalten sind, geben Sie diese in der **Ausnahmenliste** an.

  Alle eingegebenen Domänen sind von der Blockierung ausgenommen. Dies gilt auch dann, wenn sie in einer Domänenkategorie angezeigt werden, die Sie blockiert haben.
- „Expliziter Proxy“ erfordert Entschlüsselung, um Benutzer zu authentifizieren. Geben Sie die **im Authentifizierungsablauf verwendeten Domänen** ein.
-




- Geben Sie alle IP-Adressen ein, von denen unverschlüsselter HTTPS- oder HTTP-Cross-Origin Resource Sharing-(CORS-)Datenverkehr an die **Adresse der vertrauenswürdigen Quelle** zugelassen werden soll.
- Um die Authentifizierung aller von Ihnen eingegebenen vertrauenswürdigen Quelladressen zu umgehen, wählen Sie die Option **Authentifizierung überspringen** aus.

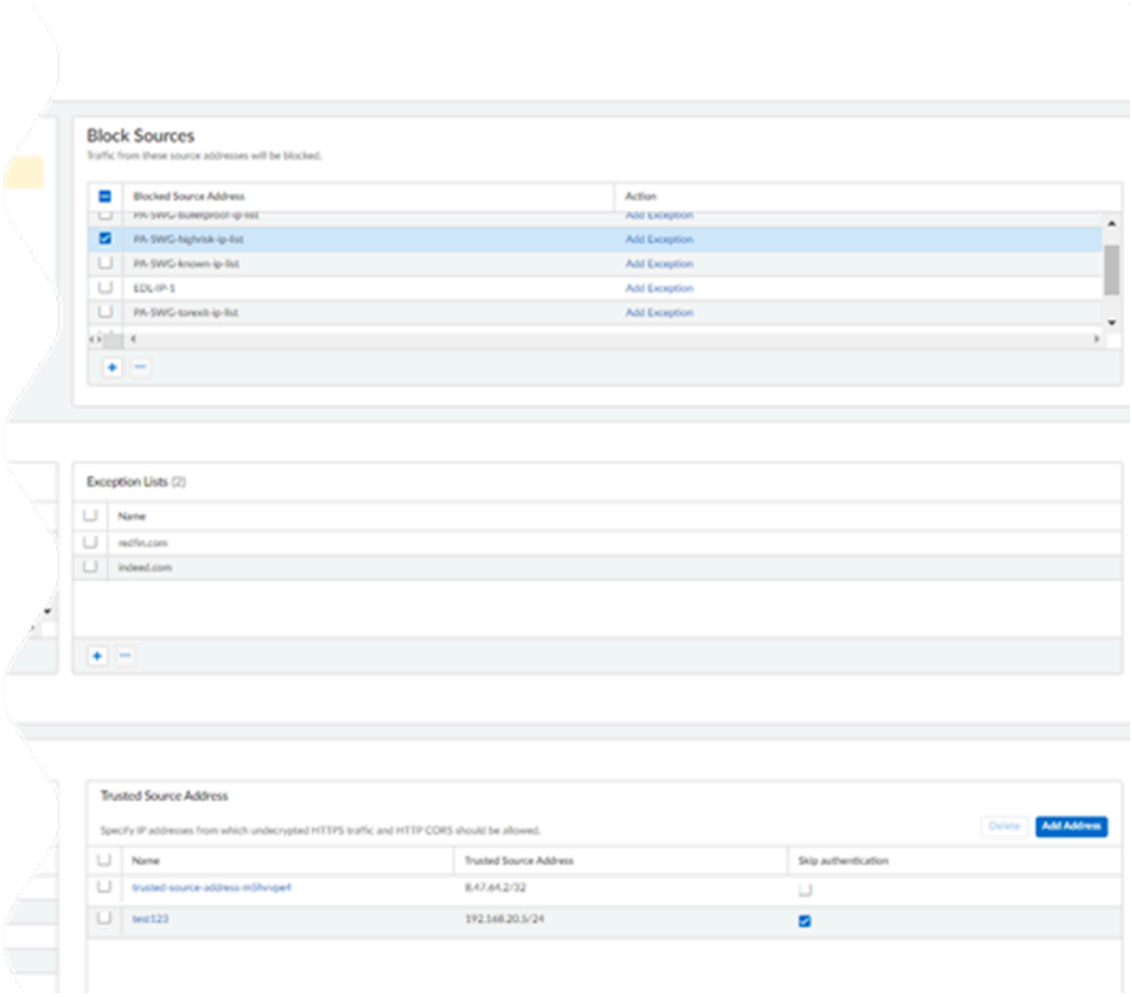
  Sie können die Option **Authentifizierung überspringen** mit der Einstellung **Quell-IP-basierte Sichtbarkeit und Durchsetzung** verwenden, um die Authentifizierung von monitorlosen Systemen zu überspringen, die sich nicht authentifizieren können, um Sicherheitsrichtlinien

 ©2025 Palo Alto Networks, Inc.

einzurichten und Einblicke in den Datenverkehr auf Prisma Access mit explizitem Proxy zu erhalten.

*Sie können entweder IP-Adressen oder Subnetze hinzufügen. Nach der Erweiterung der Subnetze werden maximal 100.000 IP-Adressen unterstützt.*

Wenn Sie die Option **Authentifizierung überspringen** auswählen, um die Authentifizierung für ein Adressobjekt zu überspringen, und dann später die Authentifizierung aktivieren möchten, indem Sie **Authentifizierung überspringen** für dieses Adressobjekt deaktivieren, kann es bis zu 24 Stunden dauern, bis die Änderung wirksam wird, nachdem Sie die Änderung vorgenommen und sie per Commit und Push festgeschrieben und übertragen haben.

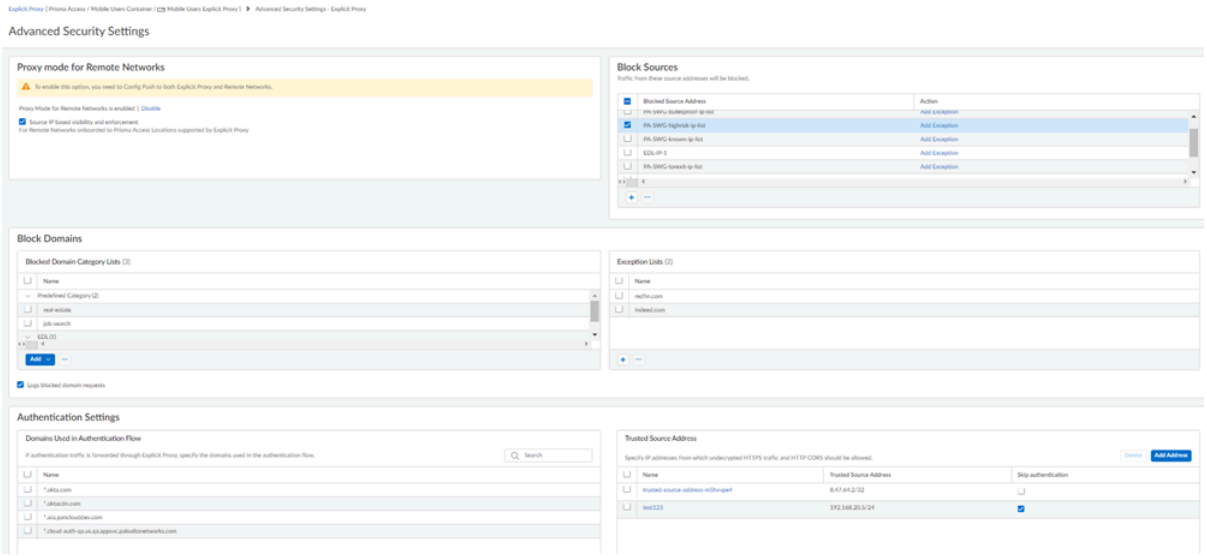
- 


- Wenn Sie über eine Bereitstellung des Typs „Expliziter Proxy“ verfügen und eine Liste vertrauenswürdiger Quell-IP-Adressen hinzugefügt haben, können Sie **X-Authenticated-User-(XAU-)Header für eingehende HTTP/HTTPS-Anfragen für Identität verwenden**.

 ©2025 Palo Alto Networks, Inc.

Verwenden Sie diese Funktion, um Benutzer zuzulassen, die von einem anderen Proxy angemeldet wurden und XAU-Header zur Authentifizierung verwenden.

*Sie müssen auf **Speichern** klicken, damit die XAU-Einstellung wirksam wird.*




## „Expliziter Proxy“ einrichten (Panorama)

Gehen Sie wie folgt vor, um mobile Benutzer mit einem expliziten Proxy zu schützen.

Bevor Sie „Expliziter Proxy“ konfigurieren, lesen Sie die Planungscheckliste, um zu erfahren, wie Sie die PAC-Datei für „Expliziter Proxy“ einrichten.

 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** Richten Sie die Authentifizierung für „Expliziter Proxy“ ein.

SAML und Kerberos werden als Authentifizierungstypen unterstützt.

Verwenden Sie die folgenden Richtlinien, wenn Sie die SAML-Authentifizierung für den IdP und in Panorama konfigurieren:

- **Richtlinien für Panorama:**
  - Konfigurieren Sie für Prisma Access einen **SAML-Identitätsanbieter** und ein **Authentifizierungsprofil**. Sie geben das Authentifizierungsprofil an, das Sie in einem späteren Schritt erstellen.
  - Stellen Sie sicher, dass Sie das Authentifizierungsprofil unter der Vorlage **Explicit_Proxy_Template** konfigurieren.
  - Verwenden Sie **mail** als Benutzerattribut im IdP-Serverprofil und im **Authentifizierungsprofil** auf Panorama.
  - „Expliziter Proxy“ unterstützt die Einstellung **SAML-Nachrichten an Identitätsanbieter signieren** im Serverprofil des SAML-Identitätsanbieters nicht.
  - Wenn Sie die Cloud Identity Engine zum Abrufen von Benutzer- und Gruppenzuordnungsinformationen konfigurieren, verwenden Sie in der Gruppenzuordnung für **SamAccountName** die Werte **mail** oder **userPrincipalName**.
  - Verwenden Sie beim Konfigurieren der **Einstellungen für die Gruppenzuordnung** während der Einrichtung von „Expliziter Proxy“ dasselbe Verzeichnisattribut für den primären Benutzernamen und E-Mail. Anderenfalls spiegelt Prisma Access die Benutzeranzahl nicht genau wider. Angenommen es liegt folgendes Benutzerprofil vor:

    ```
    sAMAccountName: muser Netbios: example userPrincipalName:
     muser@example.com mail: mobile.user@example.com
    ```

    Wenn Sie in der Konfiguration der Cloud Identity Engine für den **primären Benutzernamen** den Wert `userPrincipalName` und für **E-Mail** den Wert `mail` verwenden, unterscheiden sich die Benutzerinformationen, die der Strata Logging Service in Datenverkehrsprotokollen zurückgibt, und die Benutzerinformationen, die ACS in Authentifizierungsprotokollen zurückgibt. In diesem Beispiel sendet ACS das Attribut **mail** (mobile.user@example.com) an die Authentifizierungsprotokolle und der Strata Logging Service sendet das Attribut **userPrincipalName** (muser@example.com) an die Datenverkehrsprotokolle. Aufgrund dieser Diskrepanz wird Ihre Benutzeranzahl in den Feldern **Aktuelle Benutzer** und **Benutzer (letzte 90 Tage)** nicht korrekt sein, wenn Sie den Status von „Expliziter Proxy“ auf der Seite „Status“ (**Panorama** > **Cloud Services** > **Status** > **Status**) überprüfen. Verwenden Sie daher bei der Angabe der **Einstellungen für die Gruppenzuordnung** dasselbe Verzeichnisattribut für **Primärer Benutzername** und **E-Mail** (z. B. **mail**).
  - Wenn Sie Panorama zum Verwalten von Prisma Access verwenden, fügt die Cloud Identity Engine Benutzer- und Gruppeninformationen nicht automatisch in Sicherheitsrichtlinienregeln ein.

 ©2025 Palo Alto Networks, Inc.

- **IdP-Richtlinien:**
  - Verwenden Sie bei der Konfiguration von SAML die folgenden URLs:

    URL des **SAML Assertion Consumer Service**: **`https://global.acs.prismaaccess.com/saml/acs`**

    URL der **Entitäts-ID**: **`https://global.acs.prismaaccess.com/saml/metadata`**
  - Wenn Sie Okta als IdP verwenden, verwenden Sie **EmailAddress** für die Einstellung **Namens-ID-Format**.
  - Geben Sie die folgende einzelne Anmelde-URL ein: `https://global.acs.prismaaccess.com/saml/acs`.
  - Einzelabmeldung (Single Logout, SLO) wird nicht unterstützt.
  - Um Probleme mit der IdP-Authentifizierung zu beheben, verwenden Sie die Überwachungs- und Fehlerbehebungsfunktionen des IdP. Der ACS protokolliert keine IdP-Authentifizierungsfehler.
  - Wenn Sie ein **Authentifizierungsprofil** für den SAML-IdP erstellen, wählen Sie auf der Registerkarte **Erweitert** in der **Zulassungsliste alle** aus, da anderenfalls „Expliziter Proxy“ keine Gruppenzuordnung abrufen kann.

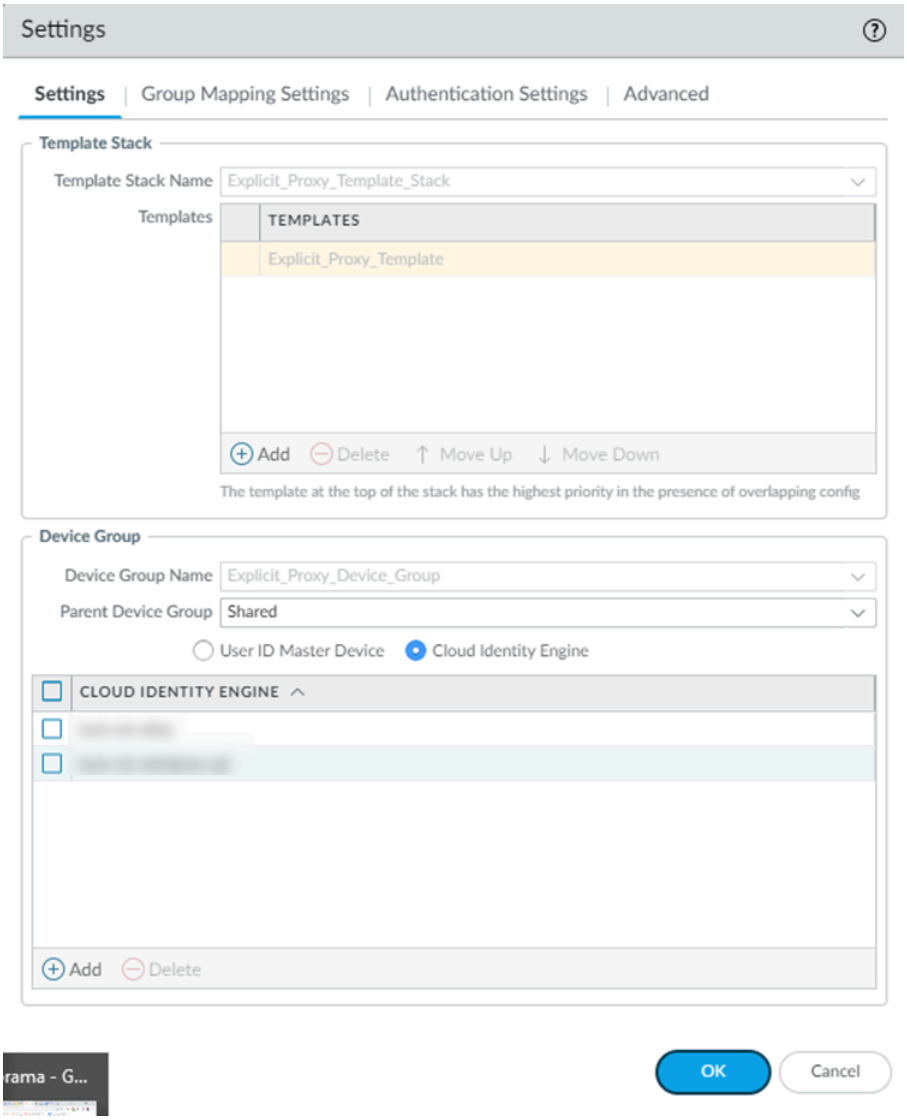
**STEP 2 |** Konfigurieren Sie die Einstellungen für „Expliziter Proxy“.

1. Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Mobile Benutzer – Expliziter Proxy** aus und klicken Sie auf das Zahnradsymbol, um die **Einstellungen** für „Expliziter Proxy“ zu bearbeiten.
2. Ändern Sie auf der Registerkarte **Einstellungen** die folgenden Einstellungen:
   - (Optional) Überprüfen Sie die Namen der Vorlage und des Vorlagenstacks.

     Standardmäßig erstellt Prisma Access einen neuen Vorlagenstack, **Explicit_Proxy_Template_Stack**, und eine neue Vorlage, **Explicit_Proxy_Template**. Vergewissern Sie sich, dass Sie diese Vorlage verwenden, wenn Sie Ihre Einstellungen für das **Gerät** in Panorama erstellen und bearbeiten.
   - Wählen Sie im Abschnitt „Gerätegruppe“ die **übergeordnete Gerätegruppe** aus, die die Konfigurationseinstellungen enthält, die Sie für „Expliziter Proxy“ erzwingen möchten, oder belassen Sie die übergeordnete Gerätegruppe als **freigegeben**, um die freigegebene Hierarchie der Prisma Access-Gerätegruppe zu verwenden. Der **Gerätegruppenname** kann nicht geändert werden.
   - (Optional) Wenn Sie eine Firewall der nächsten Generation als Mastergerät konfiguriert oder ein Cloud Identity Engine-Profil hinzugefügt haben, um Benutzer- und Gruppeninformationen in Sicherheitsrichtlinienregeln einzufügen, wählen Sie „Benutzer-ID-Mastergerät“ oder „Cloud Identity Engine“ aus. Anschließend wählen Sie entweder das von Ihnen erstellte Mastergerät oder Cloud Identity Engine-Profil aus.

 ©2025 Palo Alto Networks, Inc.

- Geben Sie im Abschnitt „Lizenzzuweisung“ die Anzahl der mobilen Benutzer an, die für „Expliziter Proxy“ zugewiesen werden sollen.



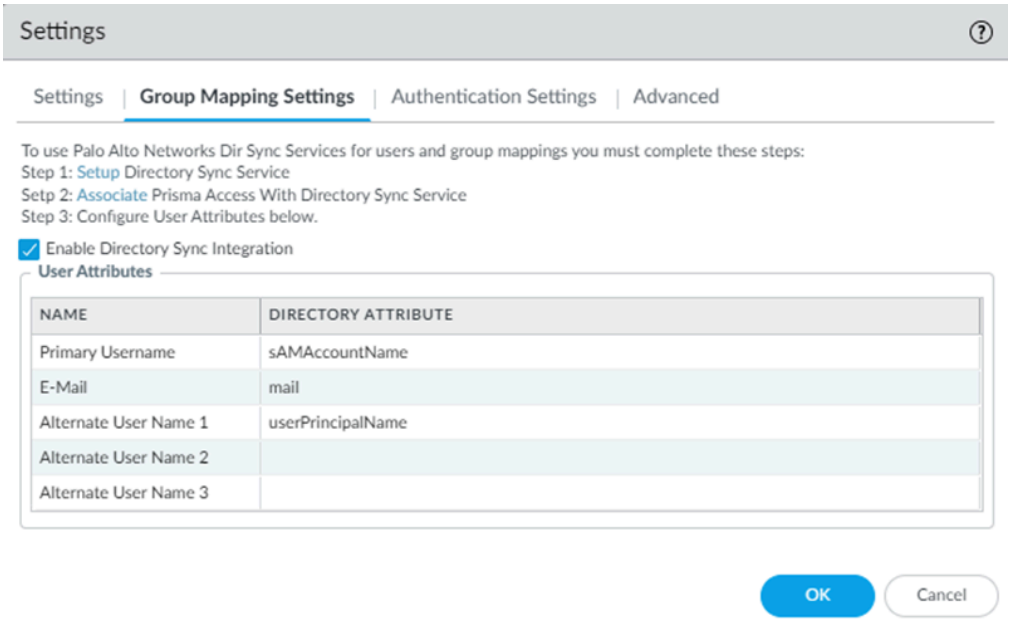

3. Aktivieren Sie auf der Registerkarte **Einstellungen für die Gruppenzuordnung** die Einstellung **Integration der Verzeichnissynchronisierung aktivieren** (jetzt „Cloud Identity

 ©2025 Palo Alto Networks, Inc.

Engine“ genannt), um Prisma Access so zu konfigurieren, dass die Cloud Identity Engine in der Lage ist, Benutzer- und Gruppeninformationen abzurufen.

Sie verwenden die Cloud Identity Engine, um Benutzer- und Gruppenzuordnungsinformationen für eine Bereitstellung des Typs „Expliziter Proxy“ einzufügen.

Geben Sie in das Feld **Primärer Benutzername** das Verzeichnisattribut **mail** und in das Feld **E-Mail** das Verzeichnisattribut **mail** ein.




4. Klicken Sie abschließend auf **OK**.

**STEP 3 |** (Optional) Konfigurieren Sie Blockeinstellungen.

Verwenden Sie Blockeinstellungen, um den Zugriff auf ein Internetziel in der DNS-Auflösungsphase zu blockieren.

*Um den Zugriff auf „Expliziter Proxy“ auf bestimmte Quell-IP-Adressen zu beschränken, können Sie auch bestimmte Objekte verwenden. Diese Adressobjekte, Adressgruppen und externen dynamischen Listen (EDL), die bestimmte Namen verwenden, ermöglichen die von Ihnen angegebenen IP-Adressen für den Internet-Verkehr und blockieren alle anderen IP-Adressen.*

**STEP 4 |** Konfigurieren Sie auf der Registerkarte **Authentifizierungseinstellungen** die Entschlüsselungs-, X-Authenticated-User-(XAU-) und Authentifizierungseinstellungen.

1. Konfigurieren Sie Ihre Einstellungen für entschlüsselten Datenverkehr.
   - Wählen Sie **Datenverkehr entschlüsseln, der bestehenden Entschlüsselungsregeln entspricht. Bei unverschlüsseltem Datenverkehr nur Datenverkehr von bekannten**

 ©2025 Palo Alto Networks, Inc.

**IPs zulassen, die von authentifizierten Benutzern registriert wurden** aus, um die folgenden Entschlüsselungsregeln zu konfigurieren:

- Datenverkehr, der den Entschlüsselungsrichtlinienregeln entspricht, die Sie mit einer **Aktion** zum **Entschlüsseln** oder **Entschlüsseln und Weiterleiten** konfiguriert haben, wird entschlüsselt.

  Wenn ein Benutzer auf eine unverschlüsselte HTTPS-Seite zugreift und sich ein Benutzer von dieser IP-Adresse aus noch nicht bei „Expliziter Proxy“ authentifiziert hat, wird der Benutzer blockiert. Der Benutzer kann jedoch auf eine entschlüsselte Seite zugreifen, die Authentifizierung abschließen und dann auf unverschlüsselte Seiten zugreifen.
- Unverschlüsselter Datenverkehr ist von IP-Adressen erlaubt, von denen sich mobile Benutzer bereits authentifiziert haben.

„Expliziter Proxy“ erfordert Entschlüsselung, um Benutzer zu authentifizieren. Geben Sie die Domänen ein, die in einer benutzerdefinierten URL-Kategorie entschlüsselt werden können. Anschließend geben Sie diese Kategorien in **Wenn der Authentifizierungsverkehr über den expliziten Proxy weitergeleitet wird, geben Sie die im Authentifizierungsablauf verwendeten Domänen an** an.

*Fügen Sie nur die Domänen hinzu, die für die Authentifizierung bei der von Ihnen angegebenen benutzerdefinierten URL-Kategorie erforderlich sind, einschließlich aller ACS- und IdP-FQDNs. Sie müssen Authentifizierungs-URLs der benutzerdefinierten URL-Kategorie auch dann hinzufügen, wenn Sie diese bereits einer Entschlüsselungsrichtlinie hinzugefügt haben.*

- Um die Entschlüsselung des gesamten Datenverkehrs zu ermöglichen, wählen Sie **Gesamten Datenverkehr entschlüsseln (Überschreibung vorhandener Entschlüsselungsregeln)** aus.

  Wenn Sie dieses Optionsfeld aktivieren, müssen Sie Folgendes sicherstellen:

  - Sie haben keine Ausnahmen in Ihrer Entschlüsselungsrichtlinie festgelegt.
  - Sie wenden in Ihrer Sicherheitsrichtlinie Quell-IP-Adressen-basierte Beschränkungen an.

  *Bei Nichtbeachtung dieser Empfehlungen kann „Expliziter Proxy“ als offener Proxy verwendet werden, der weithin als Weiterleitungsdienst zur Durchführung von Denial-of-Service-Angriffen missbraucht werden kann.*

  - Sie haben mindestens ein SSL-Forward-Proxy-Zertifikat als **Forward-Trust-Zertifikat** angegeben.

    Wenn Sie kein Forward-Trust-Zertifikat haben, erstellen Sie eines in Panorama. Anschließend können Sie Ihre Änderungen mit **Commit und Push** festschreiben und an Prisma Access übertragen. Wenn Sie kein Forward-Trust-Zertifikat haben,

 ©2025 Palo Alto Networks, Inc.

wird ein Commit-Fehler ausgelöst, sobald Sie Ihre Änderungen an „Expliziter Proxy“ festschreiben.

2. (Optional) Geben Sie alle IP-Adressen ein, von denen unverschlüsselter HTTP- oder HTTP-Cross-Origin Resource Sharing-(CORS-)Verkehr zur **Authentifizierungsumgehung der Adresse der vertrauenswürdigen Quelle** zugelassen werden soll.

   Fügen Sie IP-Adressen zu Adressobjekten hinzu, die auf IP-Adressen basieren, und **fügen** Sie die Adressobjekte im Feld hinzu.

   Geben Sie maximal 100.000 Adressen ein. Stellen Sie sicher, dass das Adressobjekt nur IP-Adressen verwendet.

3. (Optional) Um die Authentifizierung der eingegebenen Adressen vertrauenswürdiger Quellen zu umgehen, wählen Sie **Authentifizierung umgehen** aus.

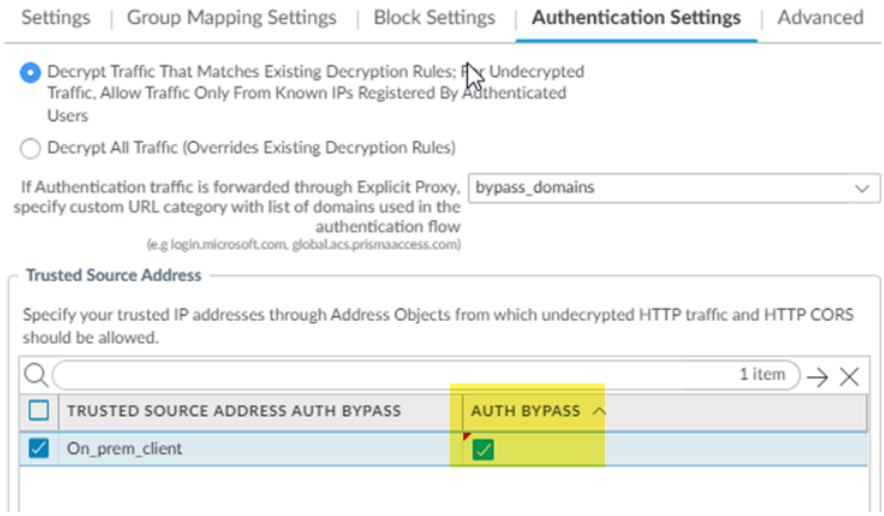
   Sie können die Option **Authentifizierung umgehen** mit der Einstellung **Quell-IP-basierte Sichtbarkeit und Durchsetzung** verwenden, um die Authentifizierung von monitorlosen Systemen zu überspringen, die sich nicht authentifizieren können, um Sicherheitsrichtlinien einzurichten und Einblicke in den Datenverkehr auf Prisma Access mit explizitem Proxy zu erhalten.

   *Sie können entweder IP-Adressen oder Subnetze hinzufügen. Nach Erweiterung der Subnetze werden maximal 100.000 IP-Adressen unterstützt.*

   Wenn Sie **Authentifizierung umgehen** auswählen, um die Authentifizierung für ein Adressobjekt zu überspringen, und dann später die Authentifizierung wieder aktivieren möchten, indem Sie **Authentifizierung umgehen** für dieses Adressobjekt deaktivieren, kann es bis zu 24 Stunden dauern, bis die Änderung wirksam wird, nachdem Sie die

 ©2025 Palo Alto Networks, Inc.

Änderung vorgenommen und Ihre Änderungen mit „Commit und Push“ festgeschrieben und übertragen haben.




4. (Optional) Damit die vertrauenswürdigen Quell-IP-Adressen XAU für Identität verwenden können, wählen Sie **Verwenden Sie den Header X-Authenticated-User (XAU) bei eingehenden HTTP/HTTPS-Anfragen für Identität** aus.

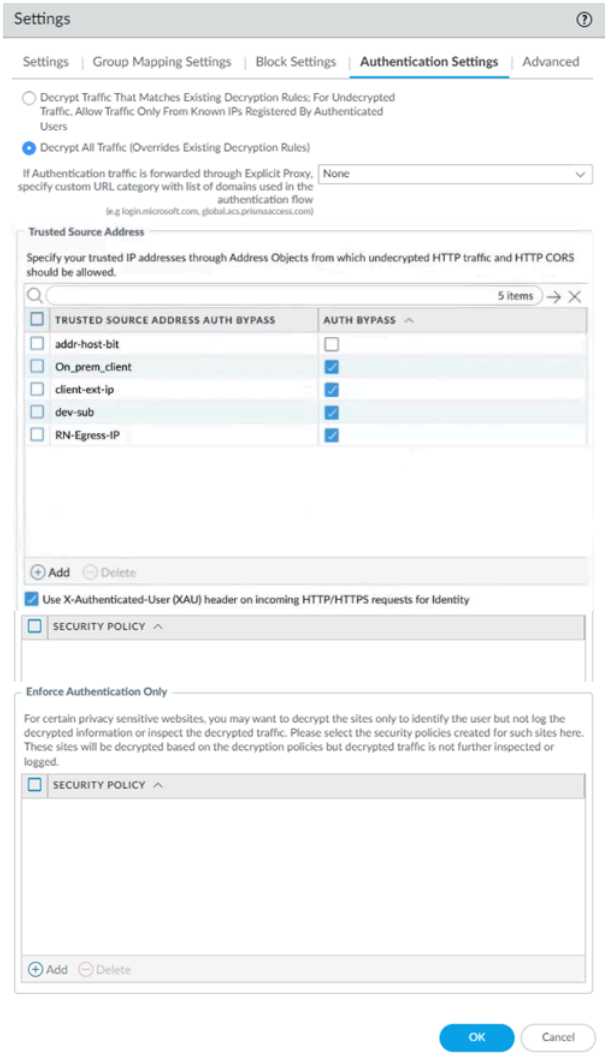
   Wählen Sie diese Option aus, wenn Sie Proxy-Verkettung von einem Drittanbieter-Proxy zu „Expliziter Proxy“ verwenden, Benutzer sich bei diesem Proxy authentifiziert haben und der Proxy XAU-Header verwendet.

   XAU-Header sind die einzigen HTTP-Header, die für die Erfassung der Header von „Expliziter Proxy“ unterstützt werden. X-Forwarded-For-(XFF-)Header werden nicht unterstützt.
5. (Optional) Geben Sie Einstellungen für datenschutzrelevante Websites an, indem Sie Sicherheitsrichtlinienregeln für diese Websites erstellen und dann die **Sicherheitsrichtlinie** oder Richtlinien für diese Websites im Bereich **Nur Authentifizierungsdurchsetzung** angeben.

   Für alle Websites, die Sie in der **Sicherheitsrichtlinie** oder den Richtlinien angeben, die Sie hinzufügen, entschlüsselt „Expliziter Proxy“ die Websites basierend auf

 ©2025 Palo Alto Networks, Inc.

den Entschlüsselungsrichtlinien, überprüft oder protokolliert den entschlüsselten Datenverkehr jedoch nicht.




**STEP 5 |** (Optional) Konfigurieren Sie **erweiterte** Einstellungen.

1. Wenn Sie Datenverkehr von Ihren Zweigstellen über einen sicheren IPSec-Tunnel an „Expliziter Proxy“ weiterleiten möchten, wählen Sie **Proxy-Modus aktivieren** aus und

 ©2025 Palo Alto Networks, Inc.

rufen Sie Anycast-IP-Adressen ab, wenn Sie „Expliziter Proxy“ in Verbindung mit einem Prisma Access-Remote-Netzwerk verwenden möchten.

Diese Lösung verwendet Anycast-Adressen mit einem Remote-Netzwerk-IPSec-Tunnel, um die Verwendung von „Expliziter Proxy“ für Benutzer und Geräte an einem Remote-Netzwerkstandort oder einem Zweigstellenstandort zu ermöglichen.

2. (Optional) Um die privaten IP-Adressen der Systeme an Ihren Niederlassungsstandorten zu nutzen, die Datenverkehr an den expliziten Proxy weiterleiten, wählen Sie **Quell-IP-basierte Sichtbarkeit und Durchsetzung** aus.

   Für diese Funktionalität gelten folgende Anforderungen:

   - Mindestens Prisma Access-Dataplane 10.2.4
   - Eine Prisma Access (Managed by Panorama)-Bereitstellung mit einem Cloud Services-Plug-in von mindestens 4.1
   - Die Quell-IP-Adressen werden nur für IP-Adressen aus einem Remote-Netzwerk angezeigt, nachdem Sie eine Remote-Netzwerkbereitstellung des Typs „Expliziter Proxy“ konfiguriert haben, und nur für Quelladressen an Remote-Netzwerkstandorten, die mit „Expliziter Proxy“ unterstützt werden.

3. Nur Bereitstellungen mit aktiviertem Proxy-Modus Wenn der Proxy-Modus in Ihren Remote-Netzwerken aktiviert ist, fügen Sie eine Richtlinie hinzu, um Datenverkehr zuzulassen, der an Anycast- und Unicast-IP in Remote-Netzwerken gebunden ist. Wenn Sie **Transparenz und Durchsetzung der Quell-IP** aktiviert haben, verwenden Sie das Feld **Quell-IP** in den Sicherheitsrichtlinien von „Expliziter Proxy“, um den Datenverkehr abzusichern. Sie benötigen zusätzliche Richtlinien in den Remote-Netzwerken.
4. Klicken Sie auf **OK**.

**STEP 6 |** Klicken Sie auf **Konfigurieren**, um die Einrichtung von „Expliziter Proxy“ zu konfigurieren.

1. Geben Sie einen **FQDN für den expliziten Proxy** an.

   Der Standardname lautet *proxyname*.proxy.prismaaccess.com, wobei *proxyname* die von Ihnen angegebene Subdomäne ist, die Port 8080 verwendet. Wenn Sie den Domänennamen Ihrer Organisation in der URL des expliziten Proxy verwenden möchten (z. B. thisproxy.proxy.mycompany.com), geben Sie einen CNAME-Eintrag für die Domäne Ihrer Organisation ein.

   Um beispielsweise eine Proxy-URL mit dem Namen thisproxy.prismaaccess.com einem Proxy mit dem Namen thisproxy.proxy.mycompany.com zuzuordnen, können Sie dem CNAME-Eintrag in der Domäne Ihrer Organisation den CNAME thisproxy.proxy.prismaaccess.com hinzufügen.
2. (Optional) Wählen Sie **GlobalProtect-Agent zur Authentifizierung verwenden** aus, um die agentenbasierte Proxy-Funktionalität zu aktivieren.

   Aktivieren Sie diese Funktion, um „Expliziter Proxy“ im Proxymodus oder im Tunnel- und Proxymodus einzurichten. Sie müssen dieses Kontrollkästchen auch aktivieren, um **Quell-IP-basierte Sichtbarkeit und Durchsetzung** zu aktivieren.

 ©2025 Palo Alto Networks, Inc.

3. Geben Sie ein **Authentifizierungsprofil** und die **Cookie-Lebensdauer** an.
   - Geben Sie das in Schritt 1 verwendete SAML-**Authentifizierungsprofil** an oder fügen Sie ein **neues** Authentifizierungsprofil hinzu, das mit Prisma Access verwendet werden soll.

     Sie müssen die SAML-Authentifizierung konfigurieren, einschließlich der Konfiguration eines **SAML-Identitätsanbieters** (IdP) und eines **Authentifizierungsprofils**, um einen expliziten Proxy zu verwenden.
   - (Optional) Geben Sie eine **Cookie-Lebensdauer** für das Cookie an, das die Authentifizierungsdaten der Benutzer speichert.

     Prisma Access legt die Anmeldeinformationen des Benutzers im Cache ab und speichert sie in Form eines Cookies. Um den Wert zu ändern, geben Sie die Dauer der Verwendung in Sekunden, Minuten, Stunden oder Tagen an.

     *Um zu verhindern, dass Benutzer Probleme mit dem Download großer Dateien vor Ablauf der Cookie-Lebensdauer haben oder das Cookie abläuft, wenn Benutzer über einen längeren Zeitraum auf eine einzelne Website zugreifen, empfiehlt Palo Alto Networks, eine Cookie-Lebensdauer von mindestens einem Tag zu konfigurieren. Wenn Benutzer des expliziten Proxy ein Problem mit dem Ablauf der Cookie-Lebensdauer haben, können sie zu einer anderen Website wechseln, um sich erneut bei ACS zu authentifizieren und das ACS-Cookie zu aktualisieren.*

     Wenn Sie eine Datei herunterladen und der Download länger dauert als die **Cookie-Lebensdauer**, wird der Dateidownload beendet, sobald die Cookie-Lebensdauer abläuft. Aus diesem Grund sollten Sie eine längere **Cookie-Lebensdauer** in Betracht ziehen, wenn Sie große Dateien herunterladen, deren Download lange dauert.

**STEP 7 |** Wählen Sie die **Standorte** und die Regionen aus, die den Standorten zugeordnet sind, an denen Sie Ihren expliziten Proxy für mobile Benutzer bereitstellen möchten. Prisma Access fügt jedem ausgewählten Standort einen Proxy-Knoten hinzu.

„Expliziter Proxy“ unterstützt eine Teilmenge aller Prisma Access-Standorte. Informationen zur Standortliste finden Sie unter Konfigurationsrichtlinien für den expliziten Proxy.

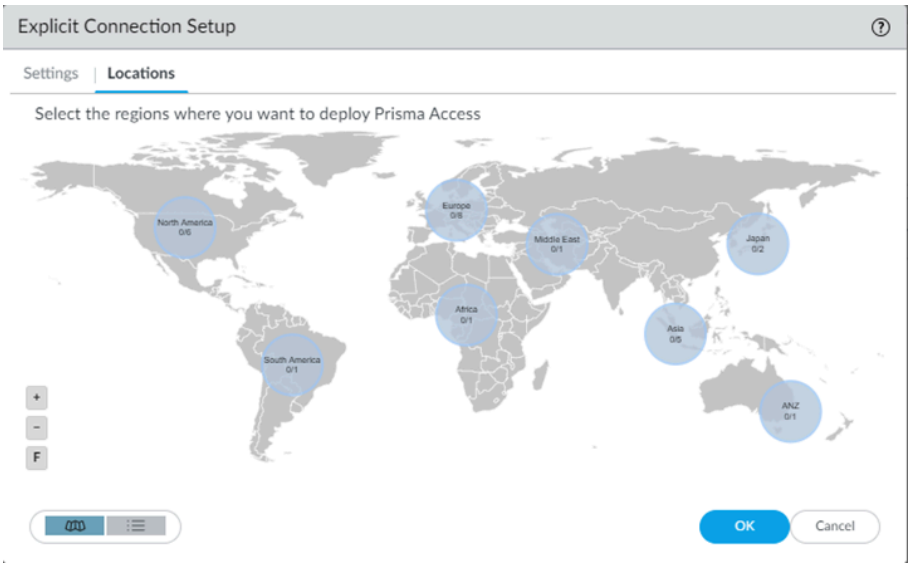
Auf der Registerkarte **Standorte** wird eine Karte angezeigt. Wenn Sie die Karte hervorheben, werden die globalen Regionen (Amerika, Europa und Asien-Pazifik) und die verfügbaren

 ©2025 Palo Alto Networks, Inc.

Standorte innerhalb der einzelnen Region angezeigt. Wählen Sie eine Region und anschließend die Standorte aus, die Sie in jeder Region bereitstellen möchten.

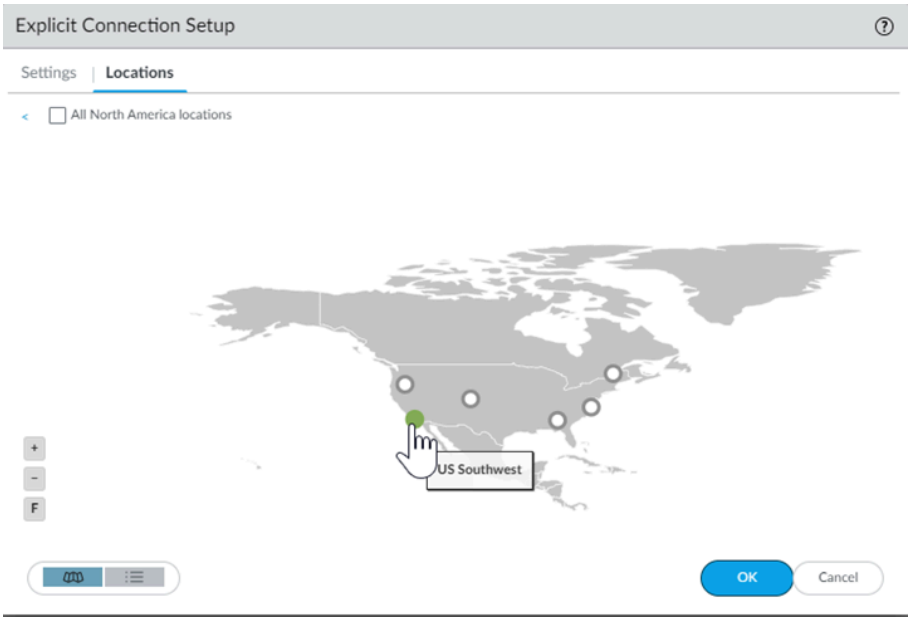
*Sie sollten Standorte mit explizitem Proxy in mindestens zwei Regionen aktivieren, um regionale Redundanz zu gewährleisten.*

1. Klicken Sie auf die Registerkarte **Standorte** und wählen Sie eine Region aus.




2. Wählen Sie mithilfe der Karte mindestens einen Standort mit explizitem Proxy in Ihrer ausgewählten Region aus.

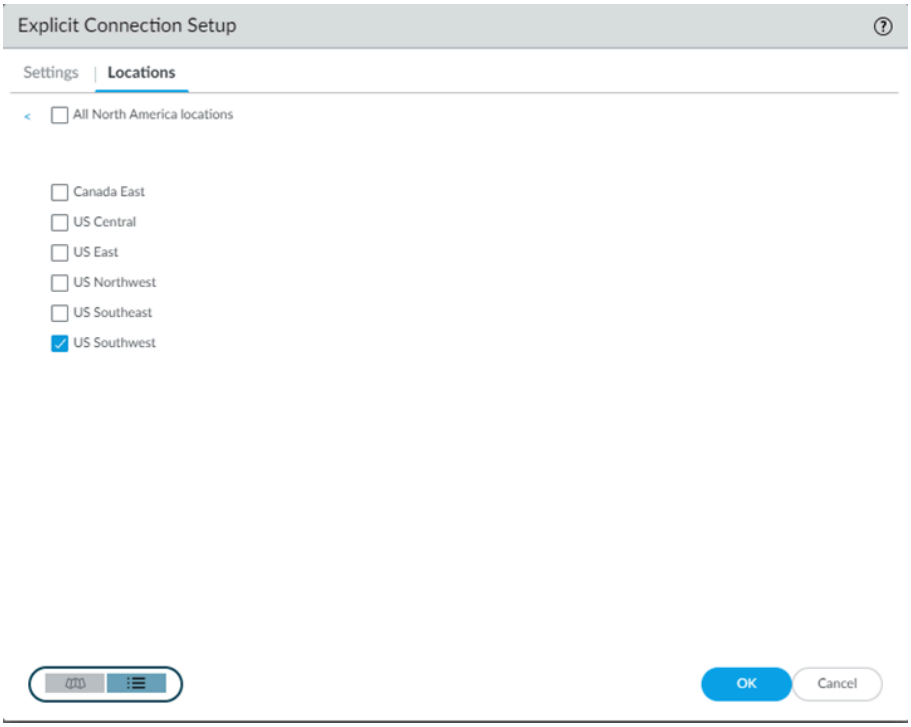
   Wenn Sie den Cursor über einen Standort bewegen, wird dieser hervorgehoben. Weiße Kreise zeigen einen verfügbaren Standort an, grüne Kreise zeigen an, dass Sie diesen Standort ausgewählt haben.




   Zusätzlich zur Kartenansicht können Sie eine Liste von Regionen und Standorten anzeigen. Sie können in der unteren linken Ecke zwischen der Karten- und der

 ©2025 Palo Alto Networks, Inc.

Listenansicht umschalten. In der Listenansicht werden Regionen nach Spalten sortiert angezeigt, wobei alle Orte nach Regionen angeordnet sind. Sie können **alle** Standorte innerhalb einer Region auswählen (oben im Dialogfenster).




3. Klicken Sie auf **OK**, um die Standorte hinzuzufügen.

**STEP 8 |** Konfigurieren Sie Sicherheitsrichtlinienregeln, um die Sicherheitsrichtlinien Ihrer Organisation durchzusetzen.

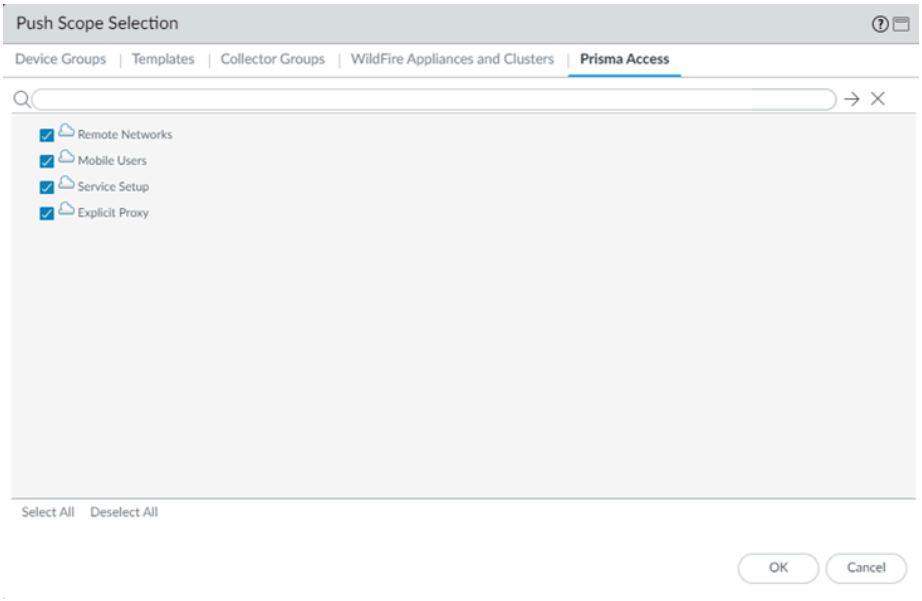
Verwenden Sie Sicherheitsrichtlinien, um erforderliche Konfigurationsänderungen vorzunehmen und die URLs zu steuern, auf die mobile Benutzer über „Expliziter Proxy“ zugreifen können. Verwenden Sie beim Konfigurieren Ihrer Sicherheitsrichtlinien die folgenden Richtlinien und Anforderungen:

- Erstellen Sie basierend auf Ihren Geschäftszielen Sicherheitsrichtlinien für sanktionierte Internet- und SaaS-Apps. Verwenden Sie dazu App-ID- und Benutzergruppen, die Zugriff auf diese Anwendungen benötigen.
- Verknüpfen Sie Sicherheitsprofile mit allen Sicherheitsrichtlinienregeln, damit Sie bekannte und unbekannte Bedrohungen gemäß den Best Practices des Sicherheitsprofils verhindern können.

 ©2025 Palo Alto Networks, Inc.

**STEP 9 |** Schreiben Sie Ihre Änderungen in Panorama fest und übertragen Sie die Konfigurationsänderungen per Push an Prisma Access.

1. Klicken Sie auf **Commit** > **Commit und Push**.
2. Wählen Sie **Auswahl bearbeiten** aus und vergewissern Sie sich, dass auf der Registerkarte **Prisma Access** die Einstellung **Expliziter Proxy** im **Übertragungsumfang** ausgewählt ist. Klicken Sie anschließend auf **OK**.




3. Klicken Sie auf **Commit und Push**.

**STEP 10 |** Wählen Sie die PAC-Datei aus, die mit „Expliziter Proxy“ verwendet werden soll.

1. Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Mobile Benutzer** > **Expliziter Proxy** aus.

   Geben Sie für den Port den Wert „8080“ in die PAC-Datei ein.
2. Wählen Sie den **Verbindungsnamen** für die soeben konfigurierte Einrichtung von „Expliziter Proxy“ aus.
3. Geben Sie die **PAC-Datei** ein, die für „Expliziter Proxy“ verwendet werden soll.

   *Sie müssen mit der Funktionsweise von PAC-Dateien vertraut sein und wissen, wie diese geändert werden, bevor Sie sie auf Prisma Access hochladen.*




   Wählen Sie **Durchsuchen** aus, um nach der Datei zu suchen, und laden Sie sie hoch.

   Prisma Access stellt Ihnen eine Beispiel-PAC-Datei zur Verfügung. Sie können die **Beispiel-PAC-Datei herunterladen**, die Werte ändern und diese Datei hochladen. Informationen zu den Anforderungen und Richtlinien für PAC-Dateien finden Sie unter PAC-Datei für „Expliziter Proxy“ einrichten. Dieser Abschnitt enthält unter anderem eine Beschreibung der Inhalte der Beispiel-PAC-Datei.

 ©2025 Palo Alto Networks, Inc.

# Kerberos-Authentifizierung für Bereitstellungen des Typs „Expliziter Proxy“

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

Bereitstellungen des Typs „Prisma Access Mobile – Expliziter Proxy“ unterstützen die Kerberos-Authentifizierung. Wenn Sie mit Servern, IoT-Geräten oder monitorlosen Computern arbeiten, die sich nicht mithilfe von SAML authentifizieren können, haben Sie die Möglichkeit, stattdessen die Kerberos-Authentifizierung zu verwenden.

Wenn Ihre Bereitstellung sowohl SAML als auch Kerberos zur Authentifizierung verwendet, können Sie beide Authentifizierungstypen in einer einzigen Bereitstellung des Typs „Expliziter Proxy“ konfigurieren. Auf diese Weise können Sie mobile Benutzer mit SAML authentifizieren, während Sie Server, IoT-Geräte oder monitorlose Computer mit Kerberos authentifizieren. Prisma Access mit explizitem Proxy verarbeitet die Authentifizierung abhängig vom Port, der für den Authentifizierungsverkehr verwendet wird:

- Wenn der Authentifizierungsverkehr Port 8080 verwendet, verwendet der explizite Proxy die SAML-Authentifizierung.
- Wenn der Authentifizierungsverkehr Port 8081 verwendet, verwendet der explizite Proxy die Kerberos-Authentifizierung.

Wenn nur ein Port konfiguriert ist, verwendet der nicht konfigurierte Port dasselbe Authentifizierungsprofil wie der konfigurierte Port.

*Kerberos SSO ist nur für Endpunkte und Systeme verfügbar, die Zugriff auf Ihre Kerberos-Infrastruktur haben. Endpunkte und Systeme ohne Zugriff auf die Kerberos-Infrastruktur müssen SAML SSO verwenden.*

- Anforderungen und Empfehlungen für die Bereitstellung von Kerberos für Bereitstellungen mit explizitem Proxy
- Kerberos-Schlüsseltabelle erstellen
- Konfigurieren der Kerberos-Authentifizierung für Bereitstellungen mit explizitem Proxy

## Anforderungen und Empfehlungen für die Bereitstellung von Kerberos für Bereitstellungen mit explizitem Proxy

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | ☐ Prisma Access-Lizenz<br>☐ Mindestens erforderliche Dataplane-Version: PAN-OS 10.1.3 oder höher |


©2025 Palo Alto Networks, Inc.

Bevor Sie eine Kerberos-Schlüsseltabelle erstellen, um Kerberos in einer Bereitstellung mit explizitem Proxy zu implementieren, sollten Sie sicherstellen, dass Ihre Kerberos-Bereitstellung folgende Anforderungen und Voraussetzungen erfüllt:

- Aktualisieren Sie Ihre Dataplane-Version auf PAN-OS 10.1.3 oder höher.
- Stellen Sie sicher, dass Sie über ein Kerberos-Konto verfügen, das Sie für Prisma Access zur Authentifizierung von Servern oder Geräten verwenden können.

  Ein Konto ist erforderlich, um eine Kerberos-Schlüsseltabelle zu erstellen. Dabei handelt es sich um eine Datei, die den Prinzipalnamen und das verschlüsselte Kerberos-Passwort enthält.
- Stellen Sie sicher, dass die Server und Endpunkte in die Domäne eingebunden sind, damit Benutzer und Computer mithilfe ihrer Anmeldeinformationen für das Arbeitsnetzwerk eine sichere Verbindung mit ihrer Arbeitsdomäne herstellen können.
- Stellen Sie sicher, dass Sie den Kerberos-Authentifizierungsverkehr an Port 8081 in der PAC-Datei der mobilen Benutzer oder in Ihren Proxy-Einstellungen auf dem Endpunkt oder den Servern weiterleiten.

  Der explizite Proxy verwendet Port 8081 für die Kerberos-Authentifizierung und Port 8080 für die SAML-Authentifizierung.
- Stellen Sie sicher, dass Ihr Kerberos-Administrator über die Fähigkeit zum Erstellen und Exportieren von Schlüsseltabellen verfügt.
- Stellen Sie sicher, dass Sie über die Ausgangs-IP-Adressen der Zweigstelle oder des Campus verfügen, an dem sich Ihre Server, IoT-Geräte oder monitorlosen Computer befinden.

  Sie fügen diese IP-Adressen der Liste der Adressen hinzu, die vom expliziten Proxy als vertrauenswürdig eingestuft werden.
- Befolgen Sie die Best Practices für die Kerberos-Benutzerauthentifizierung und -erstellung.

  Es liegt in der Verantwortung des Kerberos-Kontoadministrators, die Best Practices zu befolgen, um seine Kerberos-Umgebung zu schützen und zu verhindern, dass Passwörter

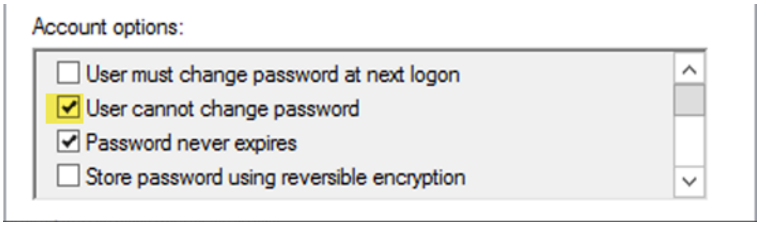
 ©2025 Palo Alto Networks, Inc.

kompromittiert werden. Verwenden Sie folgende Best Practices, wenn Sie die Benutzerkonten, das Kennwort und die ServicePrincipalNames (SPNs) erstellen.

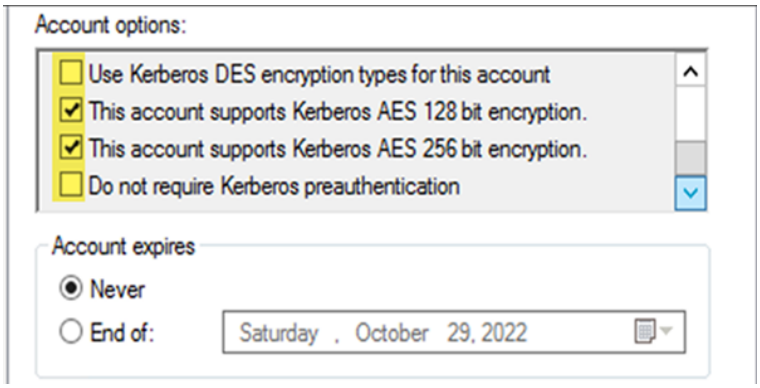
**Best Practices für die Erstellung von Kerberos-Benutzerkonten**:

- Verwenden Sie Admin-Benutzerkonten nicht wieder.

  Erstellen Sie einen eindeutigen Kontonamen für das Kerberos-Konto, das mit dem expliziten Proxy von Prisma Access verwendet werden soll.
- Teilen Sie dieses Konto nicht mit anderen Diensten. Verwenden Sie ein dediziertes Benutzerkonto für den expliziten Proxy von Prisma Access.
- Stellen Sie sicher, dass der Benutzer das Passwort für das Kerberos-Konto nicht ändern kann.

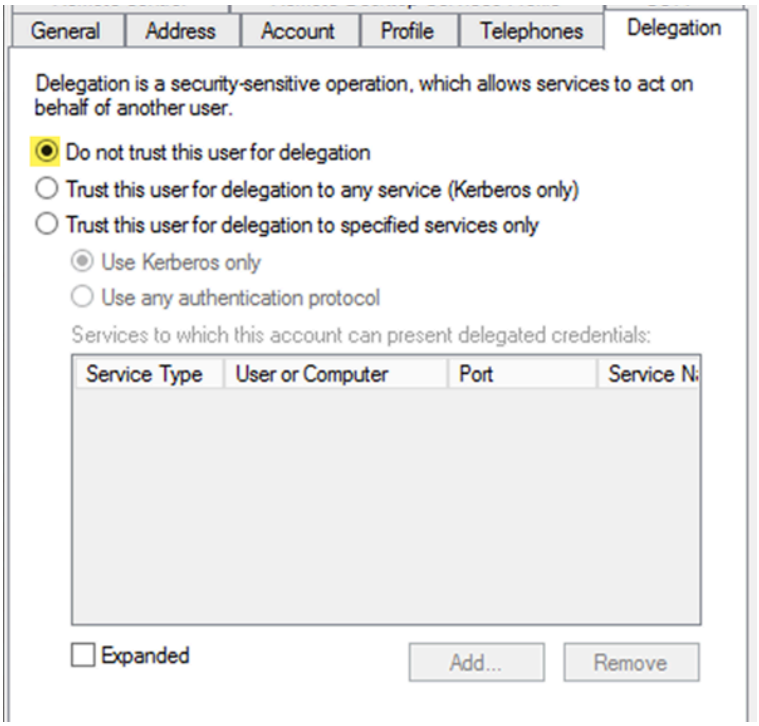



- Wenn Sie Kerberos-Kontooptionen auswählen, deaktivieren Sie die Optionen **Kerberos DES-Verschlüsselungstypen für dieses Konto verwenden** und **Kerberos-Vorauthentifizierung nicht erforderlich**.
- Aktivieren Sie die AES-128- und AES-256-Bit-Verschlüsselung.

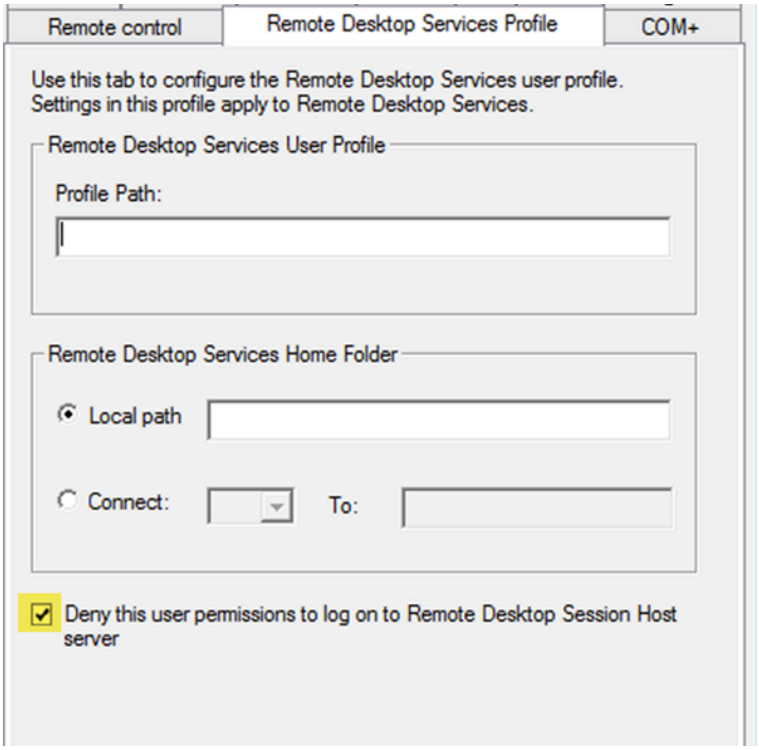



- Deaktivieren Sie die Delegierung für Benutzer.

 ©2025 Palo Alto Networks, Inc.

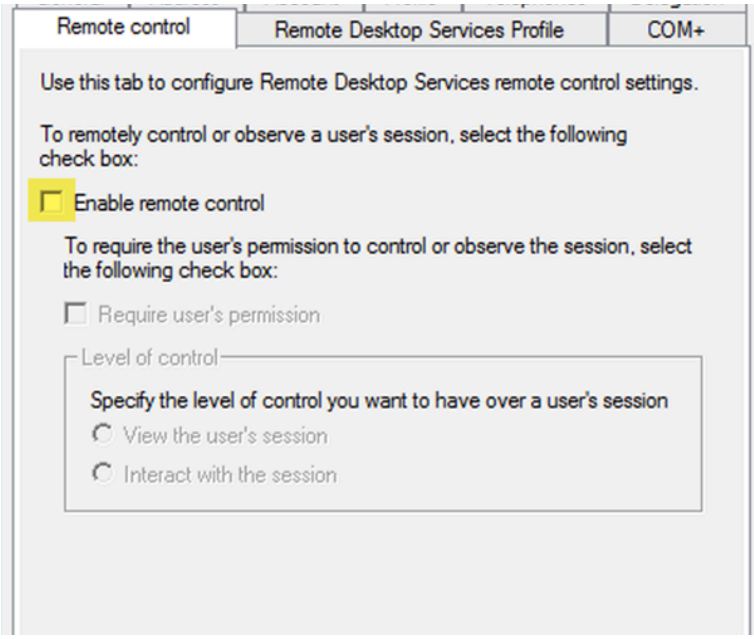



- Lehnen Sie die Möglichkeit ab, sich bei einer Remote-Desktopsitzung anzumelden.

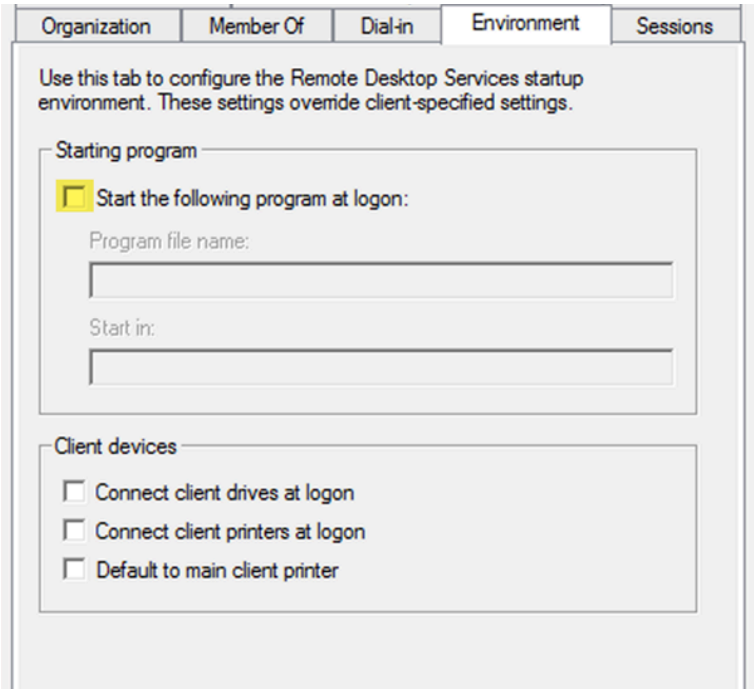



- Aktivieren Sie nicht die Fernsteuerung.

 ©2025 Palo Alto Networks, Inc.




- Lassen Sie nicht zu, dass Benutzer bei der Anmeldung Programme starten.




- Sie können Benutzer oder Benutzergruppen in der Zulassungsliste des von Ihnen erstellten Authentifizierungsprofils angeben, um die Authentifizierung auf die Benutzer oder Computer zu beschränken, die über legitime Geschäftsanforderungen verfügen.

**Best Practices für SPN und Schlüsseltabellen**:

- Stellen Sie sicher, dass der SPN nicht mehreren Benutzerkonten zugeordnet ist, da dies zu doppelten SPN-Fehlern führen kann.

 ©2025 Palo Alto Networks, Inc.

- RC4-HMAC-NT verwendet einen schwachen NTML-Hash. Befolgen Sie die Sicherheitsrichtlinien und Leitlinien Ihres Unternehmens, um die RC5-Verschlüsselung ein- oder auszuschließen.
- Die Verschlüsselungen DES-CBC-CRC und DES-CBC-MD5 sind veraltet und werden von Prisma Access nicht unterstützt.
- Wechseln Sie regelmäßig das Passwort für den SPN. Befolgen Sie die Sicherheitsrichtlinien und Leitlinien Ihres Unternehmens für die Passwortrotation.
- Befolgen Sie die Methoden Ihres Unternehmens für die Passwortkomplexität (erstellen Sie z. B. die SPN-Kennwörter auf wirklich zufällige Weise, die für Menschen nicht lesbar und zu erraten sind).
- Wenn Sie das Passwort für den Dienstbenutzer oder andere Attribute ändern, aktualisieren und generieren Sie die neue Schlüsseltabelle erneut und laden Sie sie in Prisma Access hoch.
- Wenn Sie eine neue PA-Region einbinden, müssen Sie eine neue Schlüsseltabelle für diese Region generieren, wie in den folgenden Schritten gezeigt.

Die folgende Beispielausgabe zeigt ein Konto, das mit den Best Practices für Kerberos erstellt wurde.

```
PS C:\Users\Administrator> Get-ADUser example -Properties "*"
 AccountNotDelegated : True AllowReversiblePasswordEncryption:
 False CannotChangePassword : True CN : example Deleted :
 DoesNotRequirePreAuth : False Enabled : True GivenName :
 PrismaAccess EP Service User KerberosEncryptionType :
 {AES128, AES256} msDS-SupportedEncryptionTypes : 24 Name :
 example PasswordExpired : False PasswordNeverExpires : True
 PasswordNotRequired : False PrincipalsAllowedToDelegateToAccount :
 {} ProtectedFromAccidentalDeletion : True SamAccountName :
 example servicePrincipalName : {HTTP/us-west-2.prisma-
abcde12345.proxy.prismaaccess.com@EXMP.COM, HTTP/us-east-2.prisma-
abcde12345.proxy.prismaaccess.com@EXMP.COM, HTTP/us-south-1.prisma-
abcde12345.proxy.prismaaccess.com@EXMP.COM} ServicePrincipalNames :
 {HTTP/us-west-2.prisma-abcde12345.proxy.prismaaccess.com@EXMP.COM,
 HTTP/us-east-2.prisma-abcde12345.proxy.prismaaccess.com@EXMP.COM,
 HTTP/us-south-1.prisma-abcde12345.proxy.prismaaccess.com@EXMP.COM}
 SmartcardLogonRequired : False TrustedForDelegation :
 False TrustedToAuthForDelegation : False UseDESKeyOnly :
 False UserPrincipalName : HTTP/us-south-1.prisma-
abcde12345.proxy.prismaaccess.com@EXMP.COM
```

## Kerberos-Schlüsseltabelle erstellen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | ☐ Prisma Access-Lizenz<br>☐ Erforderliche minimale Dataplane-Version: PAN-OS 10.1.3 oder höher |


©2025 Palo Alto Networks, Inc.

Nachdem Sie die Anforderungen und Empfehlungen für die Bereitstellung von Kerberos für expliziten Proxy überprüft haben, können Sie eine Kerberos-Schlüsseltabelle erstellen.

*Um eine optimale Leistung zu erzielen, sollte die Schlüsseltabellendatei kleiner als 60 KB sein.*

**STEP 1 |** Richten Sie Ihre Bereitstellung des expliziten Proxy ein.

**STEP 2 |** Rufen Sie den FQDN, die Proxy-FQDNs und DNS-CNAMEs ab, die zum Einrichten Ihrer Kerberos-Authentifizierung erforderlich sind.

Bei der Kerberos-Authentifizierung werden die Informationen verwendet, die aus dem Prisma Access-API-Skript abgerufen wurden, um die Kerberos-Schlüsseltabellen zu erstellen und zu konfigurieren. Das API-Skript ruft die folgenden Informationen ab:

- **ep_geo_lb_fqdn**: Der DNS-FQDN für explizite Proxys, der in der Konfiguration des Load-Balancers des Netzwerks für explizite Proxys verwendet wird. Dieser FQDN ist identisch mit der **URL des expliziten Proxy**, die in der Prisma Access-Benutzerschnittstelle unter **Workflows** > **Einrichtung Prisma Access** > **Expliziter Proxy** > **Infrastruktureinstellungen** > **URL des expliziten Proxy** festgelegt wird.
- **ep_geo_lb_cname**: Der DNS-CNAME für den Mandanten des expliziten Proxy.
- **ep_regional_fqdn**: Die FQDNs, die für die eingebundenen Standorte des expliziten Proxy verwendet werden.

  Expliziter Proxy weist jedem Standort eine öffentliche IP-Adresse für den Load Balancer des Netzwerks zu. ep_regional_fqdn ist der FQDN, der dieser IP-Adresse zugeordnet ist. Wenn

 ©2025 Palo Alto Networks, Inc.

mehrere Standorte dieselbe öffentliche IP-Adresse verwenden, verwenden diese Standorte denselben regionalen FQDN.

1. Generieren Sie einen API-Schlüssel, der als Teil eines curl-Befehls verwendet werden soll.
   - Wählen Sie in Prisma Access (Managed by Strata Cloud Manager) die Optionen **Workflows** > **Einrichtung Prisma Access** > **Prisma Access** > **Infrastruktureinstellungen** > **Neuen API-Schlüssel generieren** aus.
   - Wählen Sie in Panorama Managed Prisma Access die Optionen **Panorama** > **Cloud Services** > **Konfiguration** > **Diensteinrichtung** > **API-Schlüssel generieren** aus.
2. Erstellen Sie eine Datei mit der Endung .txt und geben Sie die folgenden Befehlsoptionen in die Datei ein:

   ```
   { "serviceType": "swg_proxy", "location": "deployed",
    "addrType": "network_load_balancer" }
   ```
3. Geben Sie den folgenden Befehl ein, um die erforderlichen FQDNs für die Verwendung der Kerberos-Authentifizierung abzurufen:

   ```
   curl -X POST --data @option.txt -H header-api-key:Current-
   API-Key "https://api.prod.datapath.prismaaccess.com/
   getPrismaAccessIP/v2"
   ```

   Dabei ist `option.txt` die Datei mit der Endung .txt, die Sie in einem vorherigen Schritt erstellt haben, und `Current-API-Key` ist der Prisma Access-API-Schlüssel.
4. Notieren Sie sich die FQDNs.

   Es gibt mindestens einen **ep_geo_lb_fqdn**, einen **ep_geo_lb_cname** und einen **ep_regional_fqdn** pro eingebundenem Standort.

**STEP 3 |** Erstellen Sie einen neuen Benutzer für den Prisma Access-Dienst mit explizitem Proxy im Active Directory (AD) Ihrer Organisation, indem Sie den folgenden Befehl eingeben:

```
New-ADUser -Name "USER_NAME" -GivenName "USER_GIVEN_NAME"
 -SamAccountName "USER_SAMACCOUNTNAME" -UserPrincipalName
 "USER_NAME@DNS_DOMAIN_NAME" -Path "X_500_PATH" –AccountPassword
```

 ©2025 Palo Alto Networks, Inc.

```
(ConvertTo-SecureString “PASSWORD” -AsPlainText -force) -Enabled
$true -KerberosEncryptionType RC4,AES128,AES256
```

Dabei gilt:

- *USER_NAME* ist der Name des Benutzerobjekts.
- *USER_GIVEN_NAME* ist der Vorname des Benutzers.
- *USER_SAMACCOUNTNAME* ist der Security Account Manager(SAM)-Name des Benutzers.
- *USER_NAME@DNS_DOMAIN_NAME* ist der Benutzer-Principal-Name (User Principal Name, UPN) des Benutzers.
- *X_500_PATH* ist der X.500-Pfad der Organisationseinheit oder des Containers, in der bzw. dem das neue Objekt erstellt wird (z. B. `DC=EXAMPLE,DC=COM`.)
- *PASSWORD* ist das Passwort, das für das Konto verwendet werden soll.

Das folgende CLI-Beispiel umfasst den Benutzernamen `example`, den SAM-Namen `example`, den Vornamen `PrismaAccess EP Service User`, den UPN `example@exmp.com`, den Pfad `DC=EXMP,DC=COM` und das Passwort Ex@mple123:

```
New-ADUser -Name "example" -GivenName "PrismaAccess EP
 Service User" -SamAccountName "example" -UserPrincipalName
 "example@exmp.com" -Path "DC=EXMP,DC=COM" –AccountPassword
 (ConvertTo-SecureString “Ex@mple123” -AsPlainText -force) -Enabled
 $true -KerberosEncryptionType RC4,AES128,AES256
```

*Im obigen Befehl wird der Verschlüsselungstyp RC4 angegeben, der einen schwachen NTLM-Hash verwendet. Befolgen Sie die Sicherheitsrichtlinien und Leitlinien Ihrer Organisation, um RC4 in diesen Befehl ein- oder aus diesem Befehl auszuschließen.*

**STEP 4 |** Geben Sie den folgenden Befehl ein, um zu verhindern, dass das Passwort abläuft und geändert wird:

```
Get-ADUser USER_NAME|Set-ADUser -PasswordNeverExpires:$True -
CannotChangePassword:$true
```

*Befolgen Sie die Sicherheitsrichtlinien und Leitlinien Ihrer Organisation sowie die Richtlinien für den Ablauf und die Rotation von Passwörtern.*

**STEP 5 |** Geben Sie den folgenden Befehl ein, um das neu erstellte Benutzerkonto anzuzeigen:

```
Get-ADUser USER_NAME -property msDS-KeyVersionNumber
```

**STEP 6 |** Ordnen Sie die SPNs zu und exportieren Sie Schlüsseltabellendateien, die mit der Kerberos-Authentifizierung in Ihrem Windows AD verwendet werden sollen.

Eine Schlüsseltabellendatei ermöglicht es dem expliziten Proxy, die Kerberos-Authentifizierungstoken zu validieren, die während der Datenverkehrsflüsse von Benutzern, Servern, IoT-Geräten oder anderen monitorlosen Computern bereitgestellt werden. Während der Erstellung der Schlüsseltabellendatei erfordert der explizite Proxy, dass die Werte, die Sie

 ©2025 Palo Alto Networks, Inc.

in einem früheren Schritt mithilfe der API abgerufen haben, als ServicePrincipalNames (SPNs) dem Benutzerkonto zugeordnet werden, das Sie im Schritt danach erstellt haben.

Verwenden Sie die Werte **ep_geo_lb_fqdn**, **ep_geo_lb_cname** und **ep_regional_fqdn**. Diese Werte ermöglichen es dem expliziten Proxy, Datenverkehrsflüsse zu einer dieser Proxy-Domänen zu authentifizieren.

1. Generieren und exportieren Sie eine Schlüsseltabelle, indem Sie den Wert **ep_geo_lb_fqdn** als Dienst-Principal-Namen (Service Principal Name, SPN) verwenden und die folgenden Befehle eingeben:

   ```
   ktpass -princ HTTP/ep_geo_lb_fqdn@REALM -
   mapuser DOMAIN\USER_NAME -ptype KRB5_NT_PRINCIPAL -crypto all
    -pass PASSWORD -out KEYTAB_NAME_1.keytab
   ```

   Dabei gilt:

   - *ep_geo_lb_fqdn* ist der **ep_geo_lb_fqdn**-Wert, der vom API-Skript des expliziten Proxy zurückgegeben wird.
   - *REALM* ist der Bereich (z. B. `EXMP.COM`).

     In den meisten Fällen geben Sie den Bereich in Großbuchstaben ein.
   - *DOMAIN\USER_NAME* ist der Anmeldename auf Domänenebene (z. B. `EXMP\example`).
   - *PASSWORD* ist das Passwort, das für die Schlüsseltabelle verwendet werden soll. Dieses Passwort muss nicht mit dem Benutzerpasswort übereinstimmen, sondern mit dem Wert, den Sie für die SPNs **ep_geo_lb_cname** und **ep_regional_fqdn** in den nächsten Schritten erstellen.
   - *KEYTAB_NAME_1* ist der Name der Schlüsseltabelle. Der Name der Schlüsseltabelle muss für diesen SPN eindeutig sein.

   *Befolgen Sie unbedingt die Best Practices zum Erstellen von SPNs und Passwörtern.*

   Im folgenden CLI-Beispiel wird für *ep_geo_lb_fqdn* `example.proxy.prismaaccess.com`, für *REALM* `EXMP.COM`, für

 ©2025 Palo Alto Networks, Inc.

*DOMAIN\USER_NAME* EXMP\example, für *PASSWORD* Ex@mple123 und als Name der exportierten Schlüsseltabelle exmp1.keytab verwendet:

```
ktpass -princ HTTP/example.proxy.prismaaccess.com@EXMP.COM -
mapuser EXMP\example -ptype KRB5_NT_PRINCIPAL -crypto all -
pass Ex@mple123 -out exmp1.keytab
```

2. Generieren und exportieren Sie eine Schlüsseltabelle, indem Sie den Wert **ep_geo_lb_cname** mithilfe der folgenden Befehle als SPN eingeben:

```
ktpass -princ HTTP/ep_geo_lb_cname@REALM -
mapuser DOMAIN\USER_NAME -ptype KRB5_NT_PRINCIPAL -crypto all
 -pass PASSWORD -out KEYTAB_NAME_2.keytab
```

Dabei gilt:

- *ep_geo_lb_cname* ist der **ep_geo_lb_cname**-Wert, der vom AP-Skript des expliziten Proxy zurückgegeben wird.
- *REALM* ist der Bereich, z. B: EXMP.COM
- *DOMAIN\USER_NAME* ist der Anmeldename auf Domänenebene (z. B. EXMP \example).
- *PASSWORD* ist das Passwort, das für die Schlüsseltabelle verwendet werden soll. Dieses Passwort muss mit den SPN-Passwörtern **ep_geo_lb_fqdn** und **ep_regional_fqdn** übereinstimmen.
- *KEYTAB_NAME_2* ist der Name der Schlüsseltabelle, die Sie exportieren möchten. Dieser Name sollte sich von den anderen SPN-Schlüsseltabellennamen unterscheiden, die Sie erstellen.

Im folgenden CLI-Beispiel wird für *ep_geo_lb_cname* prisma-abcde12345.proxy.prismaaccess.com, für *REALM* EXMP.COM, für *DOMAIN\USER_NAME* EXMP\example, für *PASSWORD* Ex@mple123 und als Name der exportierten Schlüsseltabellendatei exmp2.keytab verwendet:

```
ktpass -princ HTTP/prisma-
abcde12345.proxy.prismaaccess.com@EXMP.COM -mapuser EXMP
```

 ©2025 Palo Alto Networks, Inc.

```
\example -ptype KRB5_NT_PRINCIPAL -crypto all -pass Ex@mple123
 -out exmp2.keytab
```

3. Generieren und exportieren Sie eine Schlüsseltabelle, indem Sie den Wert **ep_regional_fqdn** mithilfe der folgenden Befehle als SPN eingeben:

   ```
   ktpass -princ HTTP/ep_regional_fqdn@REALM -
   mapuser DOMAIN\USER_NAME -ptype KRB5_NT_PRINCIPAL -crypto all
    -pass PASSWORD -out KEYTAB_NAME_3.keytab
   ```

   Dabei gilt:

   - *ep_regional_fqdn* ist der **ep_regional_fqdn**-Wert, der vom API-Skript des expliziten Proxy zurückgegeben wird.
   - *REALM* ist der Bereich (z. B. `EXMP.COM`).
   - *DOMAIN\USER_NAME* ist der Anmeldename auf Domänenebene (z. B. `EXMP\example`).
   - *PASSWORD* ist das Passwort, das für die Schlüsseltabelle verwendet werden soll. Dieses Passwort muss mit den SPN-Passwörtern **ep_geo_lb_fqdn** und **ep_geo_lb_cname** übereinstimmen.
   - *KEYTAB_NAME_3* ist der Name der Schlüsseltabelle, die Sie exportieren möchten. Dieser Name sollte sich von den anderen SPN-Schlüsseltabellennamen unterscheiden, die Sie erstellen.

   Im folgenden CLI-Beispiel wird für *ep_regional_fqdn* `us-west-2.prisma-abcde12345.proxy.prismaaccess.com`, für *REALM* `EXMP.COM`, für *DOMAIN\USER_NAME* `EXMP\example`, für *PASSWORD* `Ex@mple123` und als Name der exportierten Schlüsseltabellendatei `exmp3.keytab` verwendet:

   ```
   ktpass -princ HTTP/us-west-2.prisma-
   abcde12345.proxy.prismaaccess.com@EXMP.COM -mapuser EXMP
   \example -ptype KRB5_NT_PRINCIPAL -crypto all -pass Ex@mple123
    -out exmp3.keytab
   ```

4. (Optional) Wenn Sie mit weiteren Standorten arbeiten, die unterschiedliche **ep_regional_fqdn**-Werte verwenden und Sie Schlüsseltabellen für diese Standorte erstellen möchten, generieren und exportieren Sie mindestens eine zusätzliche Schlüsseltabelle, indem Sie Schritt 6.c wiederholen und dabei den Wert **ep_regional_fqdn** für diese Positionen verwenden.

   Erstellen Sie einen eindeutigen Schlüsseltabellennamen für jeden eindeutigen **ep_regional_fqdn**. Wenn z. B. **ep_regional_fqdn** für einen anderen Standort `us-east-2.prisma-abcde12345.proxy.prismaaccess.com` ist, geben Sie die folgende Beispiel-CLI mit einem eindeutigen Namen für die exportierte Schlüsseltabellendatei ein:

   ```
   ktpass -princ HTTP/us-east-2.prisma-
   abcde12345.proxy.prismaaccess.com@EXMP.COM -mapuser EXMP
   \example -ptype KRB5_NT_PRINCIPAL -crypto all -pass Ex@mple123
    -out exmp4.keytab
   ```

 ©2025 Palo Alto Networks, Inc.

**STEP 7 |** Löschen Sie nicht unterstützte Verschlüsselungen in erstellten Schlüsseltabellen, indem Sie folgende `ktutil`-Befehle in Ubuntu eingeben.

Die folgende Systemausgabe umfasst Beispiele für die Bereinigung verschiedener Verschlüsselungen:

```
slot KVNO Principal ---- ----
 ---------------------------------------------------------------------
 1 3 HTTP/us-west-2.prisma-
abcde12345.proxy.prismaaccess.com@PANW.COM (des-cbc-crc) 2 3
 HTTP/us-west-2.prisma-abcde12345.proxy.prismaaccess.com@PANW.COM
 (des-cbc-md5) 3 3 HTTP/us-west-2.prisma-
abcde12345.proxy.prismaaccess.com@PANW.COM (arcfour-hmac) 4 3
 HTTP/us-west-2.prisma-abcde12345.proxy.prismaaccess.com@PANW.COM
 (aes256-cts-hmac-sha1-96) 5 3 HTTP/ us-west-2.prisma-
abcde12345.proxy.prismaaccess.com@PANW.COM (AES128-CTS-HMAC-
SHA1-96)
```

```
# Alle Schlüsseltabellen anzeigen, die Schlüsseleingabezahlen
 abrufen, um DES-CBC-MD5 und DES-CBC-CRC zu entfernen. # Und RC4-
HMAC basierend auf der Richtlinie Ihrer Organisation aktivieren
 oder deaktivieren. for i in `ls keytab_name*.keytab`; do echo
 $i; klist -Kte -k $i; done # cleanup unsupported ciphers #
 entry #1 is typically des-cbc-crc # entry #2 is typically
 des-cbc-md5 # entry #3 is typically arcfour-hmac ktutil
 rkt KEYTAB_NAME_1.keytab delent 2 delent 1 wkt new1.keytab quit
 ktutil rkt KEYTAB_NAME_2.keytab delent 2 delent 1 wkt new2.keytab
 quit ktutil rkt KEYTAB_NAME_3.keytab delent 2 delent 1 wkt
 new3.keytab quit
```

Dabei gilt: *KEYTAB_NAME_1*.keytab, *KEYTAB_NAME_2*.keytab und *KEYTAB_NAME_3*.keytab sind die Schlüsseltabellen, die Sie im vorherigen Schritt erstellt haben.

**STEP 8 |** (Optional) Wenn Sie weitere Schlüsseltabellen für andere Regionen erstellt haben, entfernen Sie nicht unterstützte Verschlüsselungen für diese Schlüsseltabellen, indem Sie den obigen `ktutil`-Befehl eingeben und dabei *KEYTAB_NAME_1*.keytab durch den Schlüsseltabellennamen, den Sie für die Region oder Regionen verwendet haben, ersetzen und eine andere Ausgabedatei angeben (z. B. `new4.keytab`, `new5.keytab` usw.).

**STEP 9 |** Führen Sie die von Ihnen erstellten Schlüsseltabellen zusammen, indem Sie den folgenden `ktutil`-Befehl eingeben. Dabei sind new1.keytab, new2.keytab und new3.keytab die Schlüsseltabellen, die Sie im vorherigen Schritt erstellt haben. Stellen Sie sicher, dass Sie alle regionsspezifischen Schlüsseltabellen in diesen Befehl einschließen:

```
ktutil rkt new1.keytab rkt new2.keytab rkt new3.keytab # Wenn Sie
 zusätzliche regionsspezifische Schlüsseltabellendateien erstellt
 haben, fügen Sie diese hier hinzu. wkt papxv1.keytab quit
```

Wenn Sie fertig sind, verwenden Sie die von Ihnen erstellte Schlüsseltabelle (in diesem Beispiel `papxv1.keytab`) als Schlüsseltabelle für den expliziten Proxy.

 ©2025 Palo Alto Networks, Inc.

## Konfigurieren der Kerberos-Authentifizierung für Bereitstellungen mit explizitem Proxy

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

- Strata Cloud Manager
- Panorama

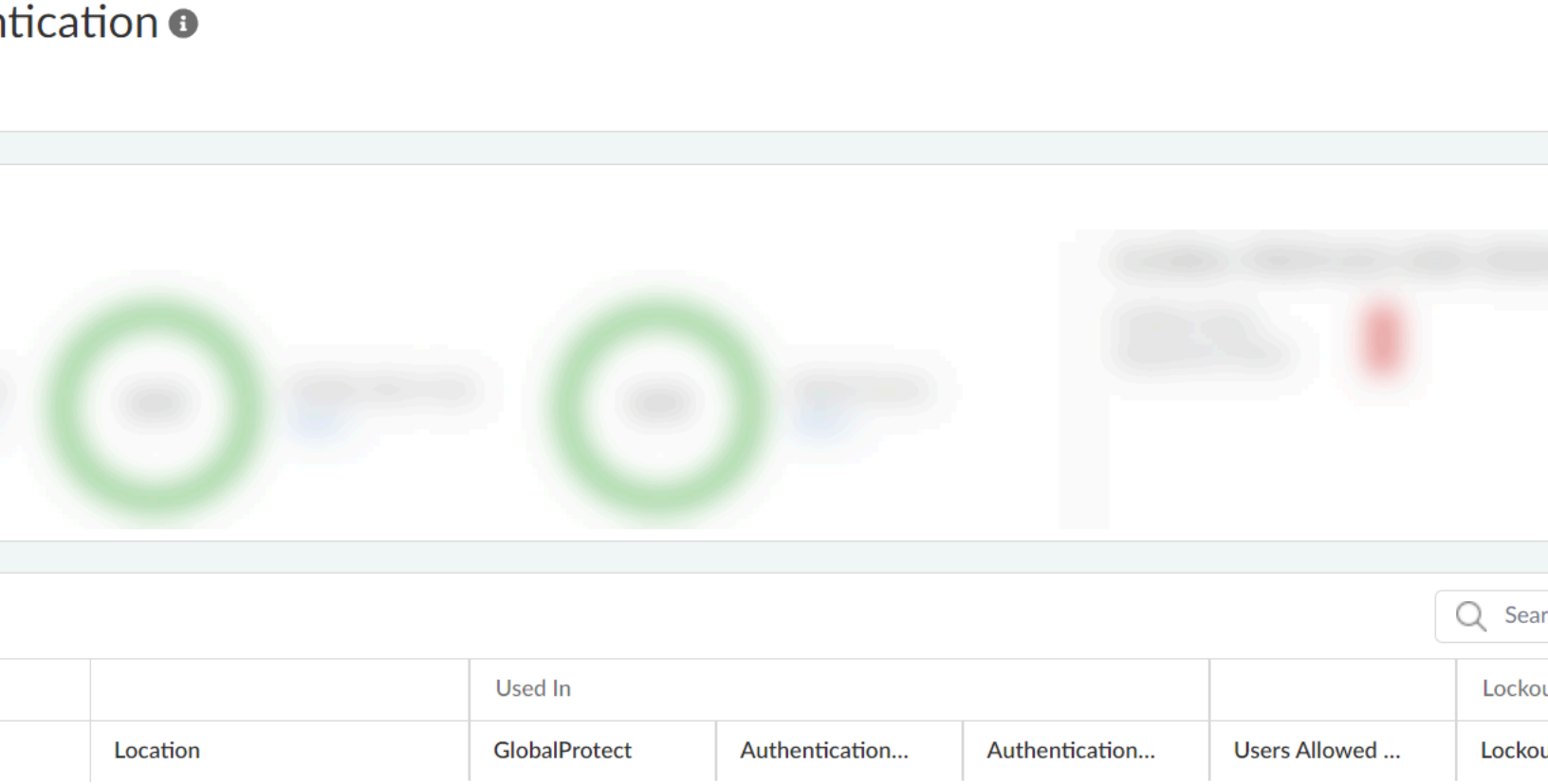
 ©2025 Palo Alto Networks, Inc.

### Konfigurieren der Kerberos-Authentifizierung für Bereitstellungen mit explizitem Proxy (Strata Cloud Manager)

**STEP 1 |** Richten Sie ein Kerberos-Authentifizierungsprofil ein.

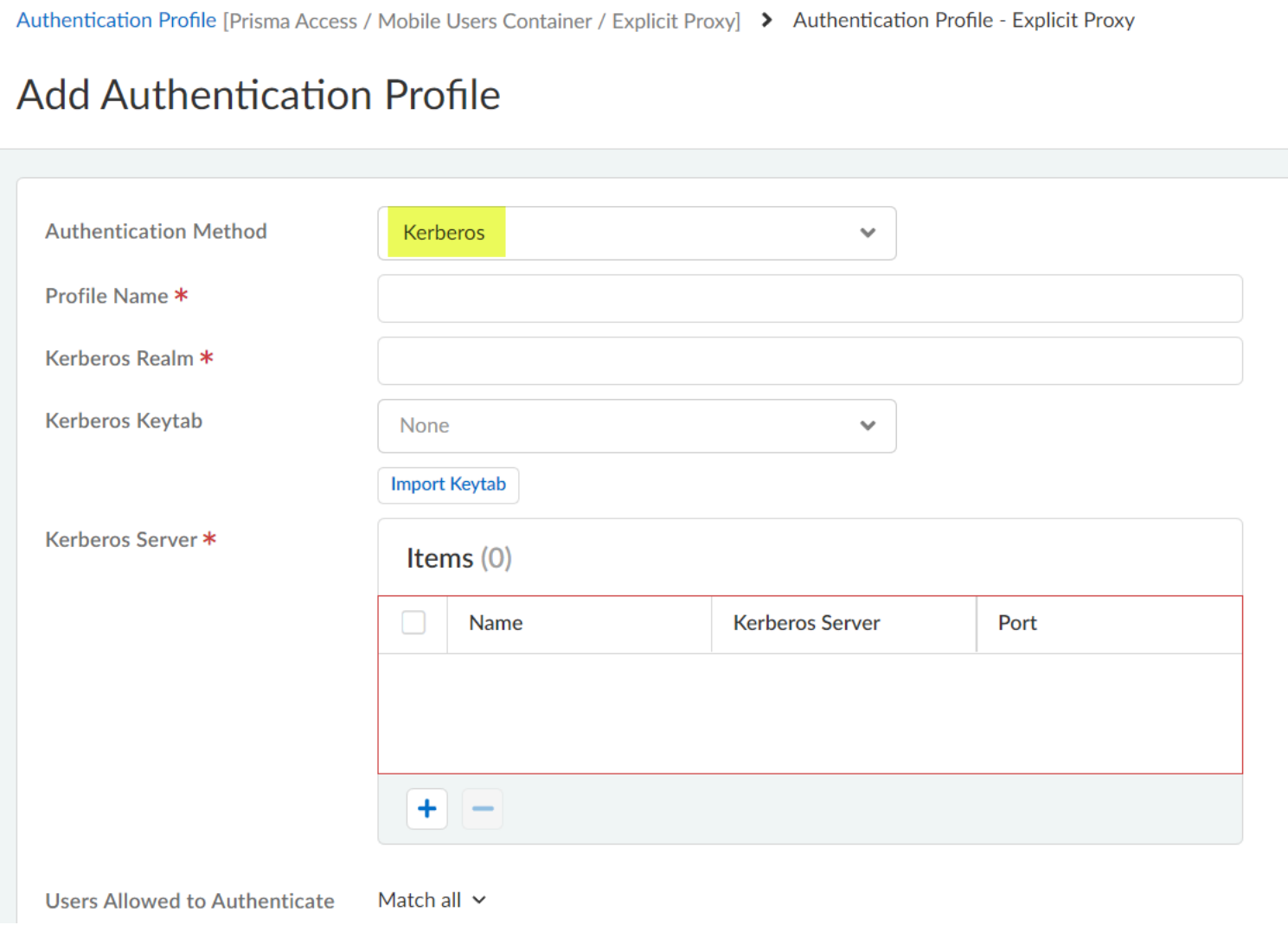
Das Profil definiert, wie der explizite Proxy für die Authentifizierung mobiler Benutzer eine Verbindung zum Kerberos-Server herstellt.

1. Rufen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Identitätsdienste** > **Authentifizierung** > **Authentifizierungsprofile** und dann **Profil hinzufügen** auf.




2. Wählen Sie die **Authentifizierungsmethode** aus: **Kerberos**.

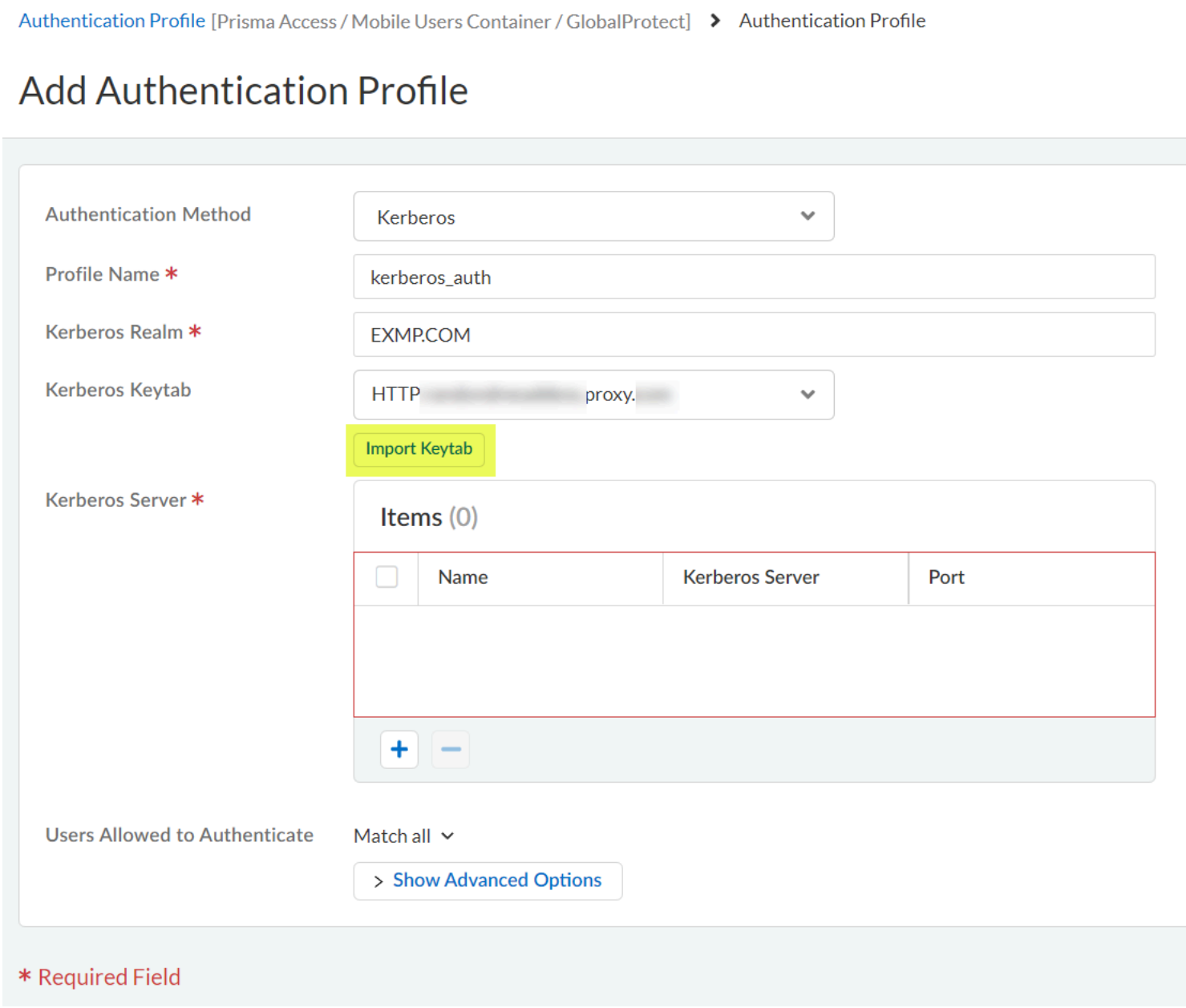
 ©2025 Palo Alto Networks, Inc.




3. Geben Sie einen eindeutigen **Profilnamen** ein, um das Profil zu identifizieren.

   Das Authentifizierungsprofil gibt das Serverprofil an, das vom Portal oder den Gateways zur Benutzerauthentifizierung verwendet wird.
4. Geben Sie den **Kerberos-Bereich** (bis zu 127 Zeichen) ein, um den Hostnamen-Teil des Benutzer-Anmeldenamens anzugeben. Beispielsweise ist dem Benutzerkontonamen „user@EXMP.COM“ der Bereich „EXMP.COM“ zugeordnet.
5. Importieren Sie die **Kerberos-Schlüsseltabelle** (**Schlüsseltabelle importieren**), die Sie bereits erstellt haben.

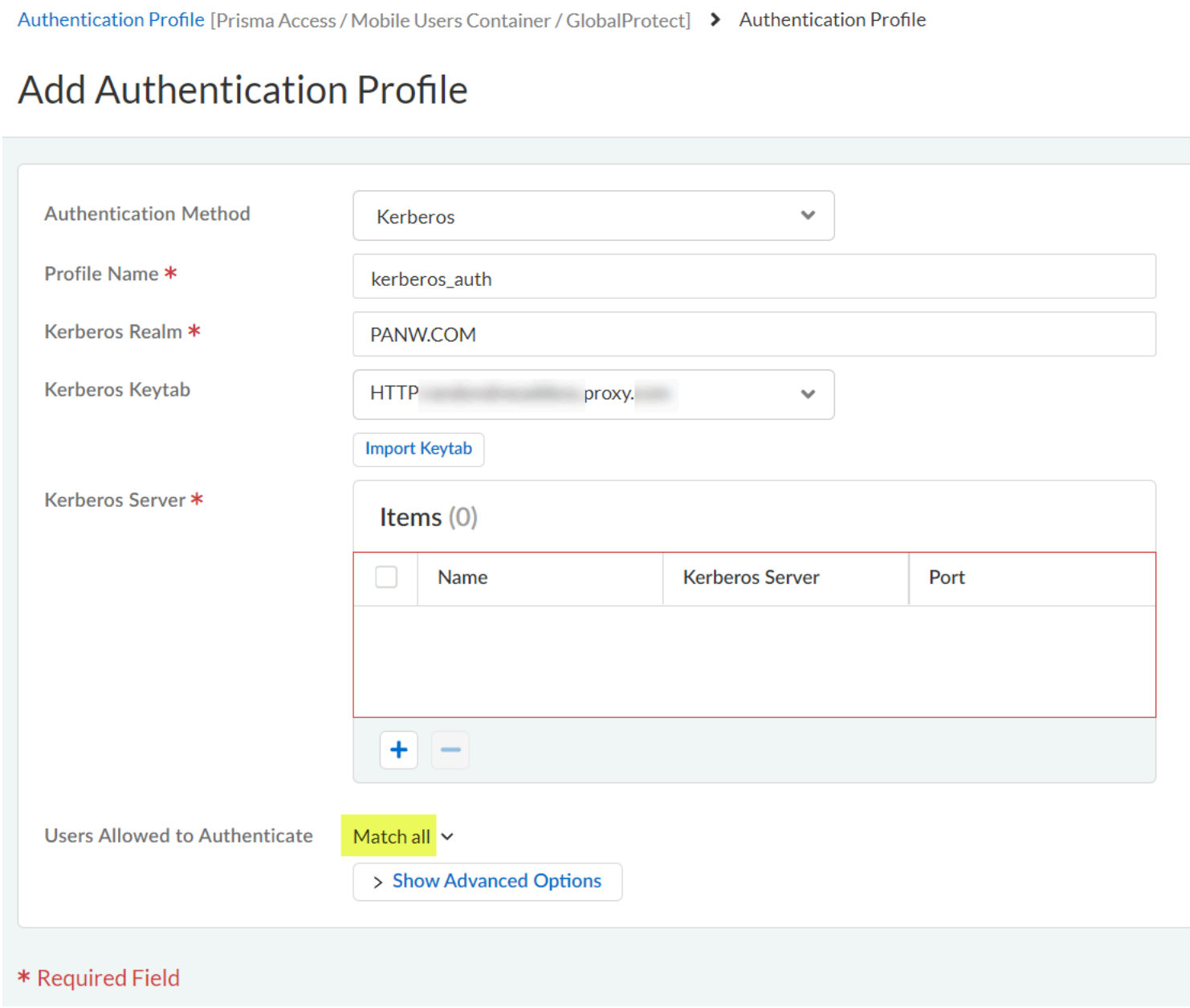
 ©2025 Palo Alto Networks, Inc.




6. Fügen Sie diesem Profil unter **Benutzer, die sich authentifizieren dürfen** die dazu berechtigten Benutzer hinzu.
   - Um alle Benutzer auszuwählen, wählen Sie die Option zum **Abgleichen aller Benutzer** aus.
   - Wenn Sie die Cloud Identity Engine verwenden, um die Liste der Benutzer auszufüllen, wählen Sie die Benutzer in einer Liste aus, oder wählen Sie **Alle** aus, um allen Benutzern die Authentifizierung zu erlauben.
   - Um lokale Benutzer hinzuzufügen, die sich mit Kerberos anmelden können, wählen Sie **Lokalen Benutzer hinzufügen** aus und geben Sie anschließend einen Wert für **Name** ein. Erstellen Sie dann ein **Passwort**.


©2025 Palo Alto Networks, Inc.

- Verwenden Sie zur Konfiguration der Benutzerauthentifizierung und der Benutzerzuordnung das UPN-Format (userPrincipalName); andere Formate (wie beispielsweise samAccountName) werden nicht unterstützt.
- In Unicode-Zeichen angegebene Benutzernamen werden nicht unterstützt.

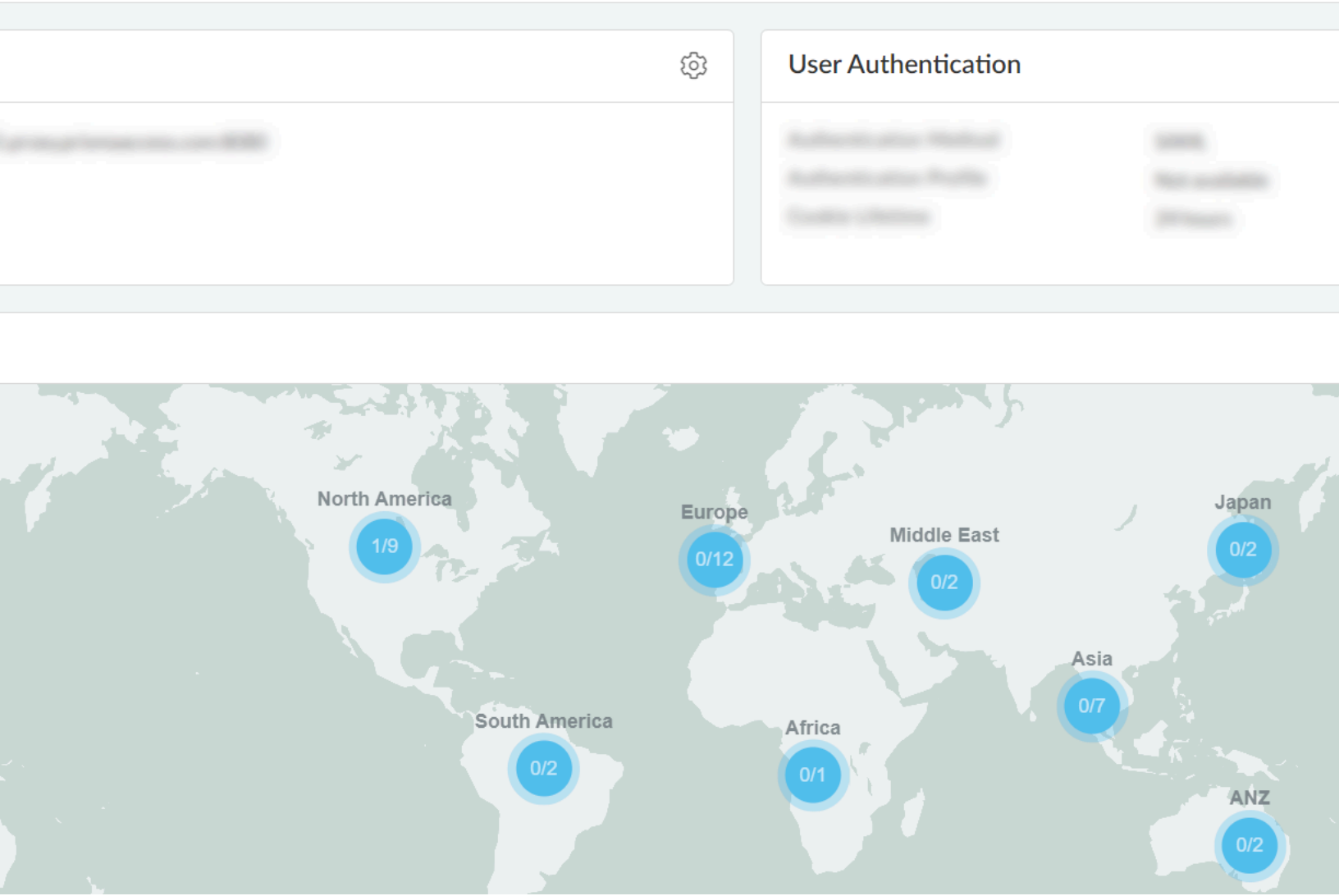



7. **Save (Speichern)** Sie Ihre Änderungen.

 ©2025 Palo Alto Networks, Inc.

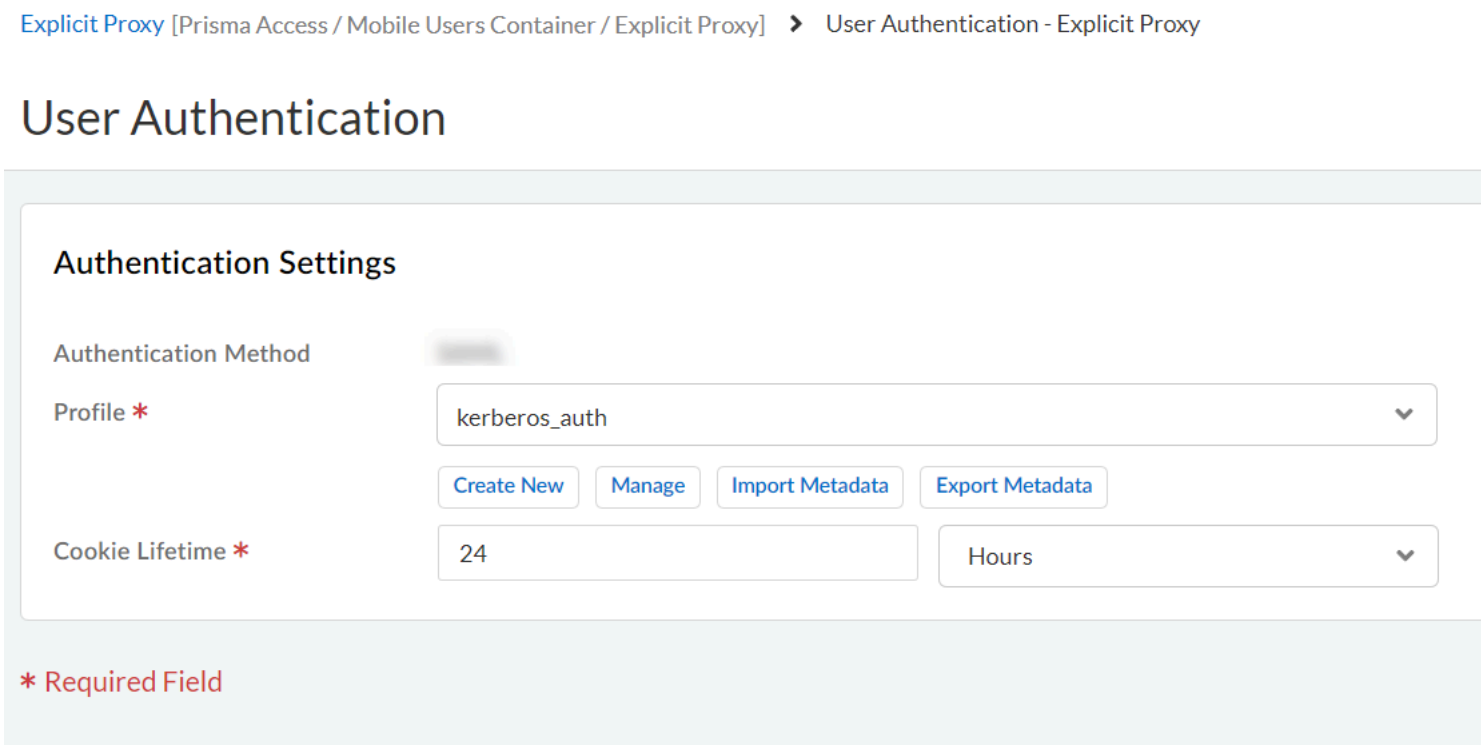
**STEP 2 |** Verknüpfen Sie das Authentifizierungsprofil mit einer Authentifizierungsmethode.

1. Wählen Sie **Workflows** > **Prisma Access-Einrichtung** > **Expliziter Proxy** > **Benutzerauthentifizierung** aus.




2. Wählen Sie **Verbindungsname** aus.
3. Wählen Sie als **Authentifizierungsmethode** die Option **Kerberos** und anschließend das von Ihnen erstellte **Profil** für Kerberos aus.


©2025 Palo Alto Networks, Inc.




4. **Save (Speichern)** Sie Ihre Änderungen.

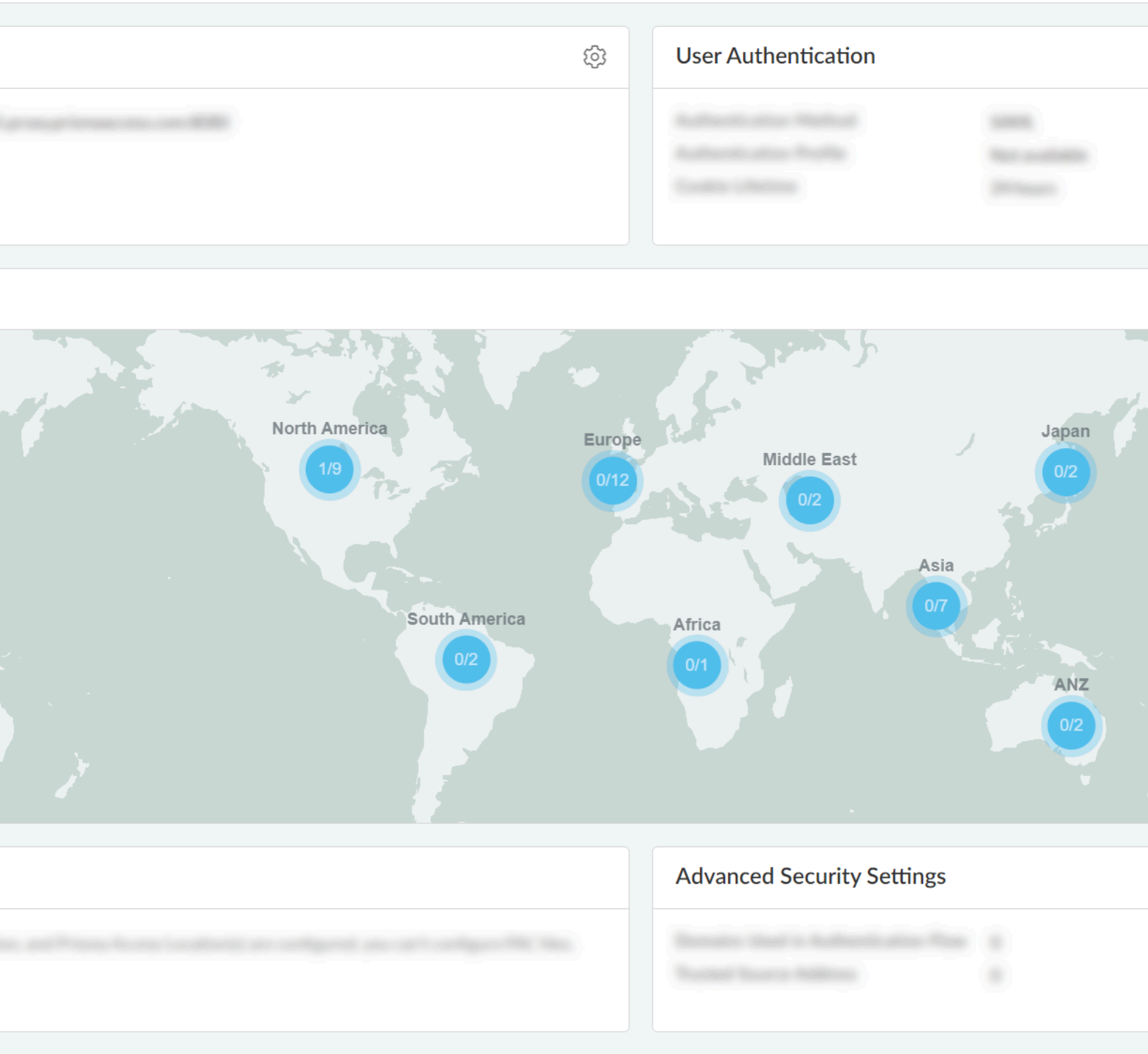
 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** (Optional) Fügen Sie die Ausgangs-IP-Adressen des Zweigstellen- oder Campus-Standorts, an dem sich Ihre Benutzer, Server, IoT-Geräte oder monitorlosen Maschinen befinden, der Liste vertrauenswürdiger expliziter Proxy-Adressen hinzu.

Diesen Arbeitsschritt müssen Sie nur ausführen, wenn Sie für bestimmte IP-Adressen die **Authentifizierung überspringen** wollen oder den **XAU-Header (X-Authenticated User) für eingehende HTTP/HTTPS-Identitätsanforderungen verwenden** möchten.

1. Rufen Sie **Workflows** > **Prisma Access-Einrichtung** > **Expliziter Proxy** > **Erweiterte Sicherheitseinstellungen** auf.

 ©2025 Palo Alto Networks, Inc.

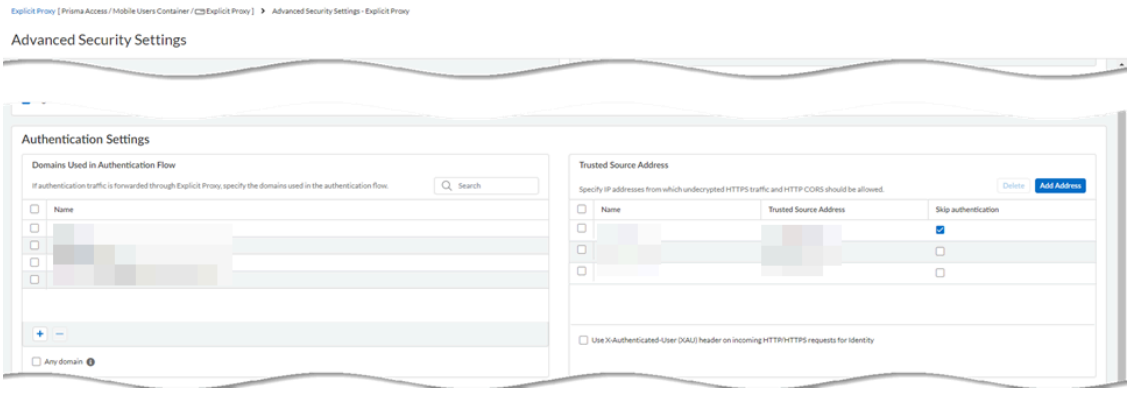



2. Fügen Sie mit **Adresse hinzufügen** (mindestens) eine Adresse zum Feld **Adresse der vertrauenswürdigen Quelle** hinzu.


©2025 Palo Alto Networks, Inc.

Wenn Sie die Ausgangs-Endpunkt-IP-Adressen nicht zur vertrauenswürdigen Liste hinzufügen, erzwingt der explizite Proxy bei Benutzern und Maschinen die Authentifizierung mit SAML sowie mit Kerberos.

Geben Sie maximal 100.000 IP-Adressen ein.




3. **Save (Speichern)** Sie Ihre Änderungen.

**STEP 4 |** Erstellen Sie für die Benutzerauthentifizierung eine Allow-All-Richtlinienregel.

1. Wählen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Sicherheitsdienste** > **Sicherheitsrichtlinie** > **Regel hinzufügen** > **Vor-Regeln** > **aus.**.
2. Ordnen Sie der Regel einen Namen zu.
3. Legen Sie für alle erforderlichen Übereinstimmungskriterien die Einstellung **Beliebig** fest.
4. Legen Sie für Benutzer die Einstellung **Bekannt** fest.
5. Legen Sie für die Aktion **Zulassen** fest.
6. **Speichern** Sie die Regel.

**STEP 5 |** Übertragen Sie Ihre Konfigurationsänderungen.


©2025 Palo Alto Networks, Inc.

**STEP 6 |** Überprüfen Sie, ob die Kerberos-Authentifizierung mit Prisma Access ordnungsgemäß funktioniert, indem Sie die Datenverkehrs- und Authentifizierungsprotokolle anzeigen.

1. (Nur entschlüsselter Datenverkehr) Wählen Sie **Aktivität** > **Protokoll-Viewer** > **Firewall/Datenverkehr** aus und überprüfen Sie, ob die Kerberos-Authentifizierung korrekt funktioniert.

   *Wenn Sie mit Strata Cloud Manager arbeiten, dann rufen Sie **Vorfälle und Benachrichtigungen** > **Protokoll-Viewer** > **Firewall/Datenverkehr** auf.*

   *Für entschlüsselten Datenverkehr wird der Benutzername in den Datenverkehrs-Protokollen angezeigt.*

2. (Nur nicht entschlüsselter Datenverkehr) Wählen Sie **Aktivität** > **Protokoll-Viewer** > **Firewall/Authentifizierung** aus und überprüfen Sie, ob die Kerberos-Authentifizierung korrekt funktioniert.

   *Wenn Sie mit Strata Cloud Manager arbeiten, dann rufen Sie **Vorfälle und Benachrichtigungen** > **Protokoll-Viewer** > **Firewall/Authentifizierung** auf.*

   Die folgenden Felder enthalten weitere Informationen zum Authentifizierungsereignis:

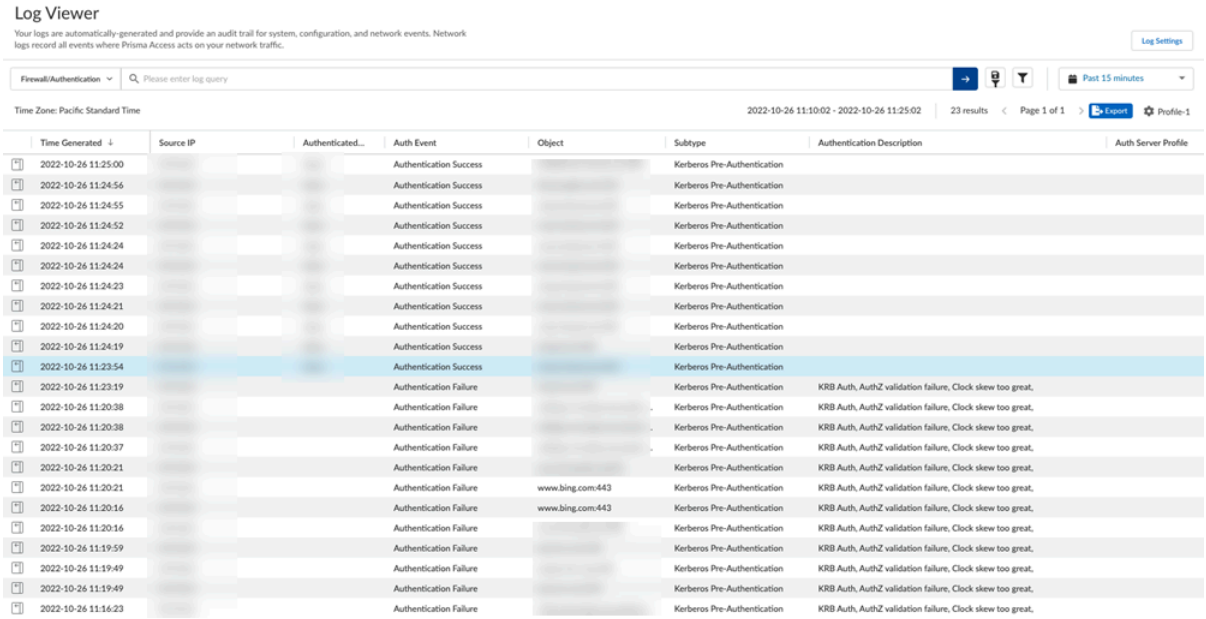
   - **Objekt** – Die Website, auf die der Benutzer zuzugreifen versuchte, bevor er zur Authentifizierung an Kerberos umgeleitet wurde.
   - **Auth-Ereignis** – Der Status des Authentifizierungsversuchs.

     Mit **Authentifizierungserfolg** wird angezeigt, dass das Authentifizierungsereignis erfolgreich ausgeführt werden konnte; **Authentifizierungsfehler** zeigt an, dass der Versuch fehlgeschlagen ist, und generiert ein Protokoll.
   - **Authentifizierungsbeschreibung** – Wenn der Authentifizierungsversuch fehlgeschlagen ist, erhalten Sie hier zusätzliche Informationen zur Art des Fehlers.

     Beispielsweise weist die Meldung **Benutzer nicht erlaubt** darauf hin, dass der Benutzer oder die Gruppe Kerberos nicht zur Authentifizierung verwenden darf.

 ©2025 Palo Alto Networks, Inc.

Dies kann darauf zurückzuführen sein, dass der Benutzer oder die Gruppe nicht zur **Zulassungsliste** im Authentifizierungsprofil hinzugefügt wurde.



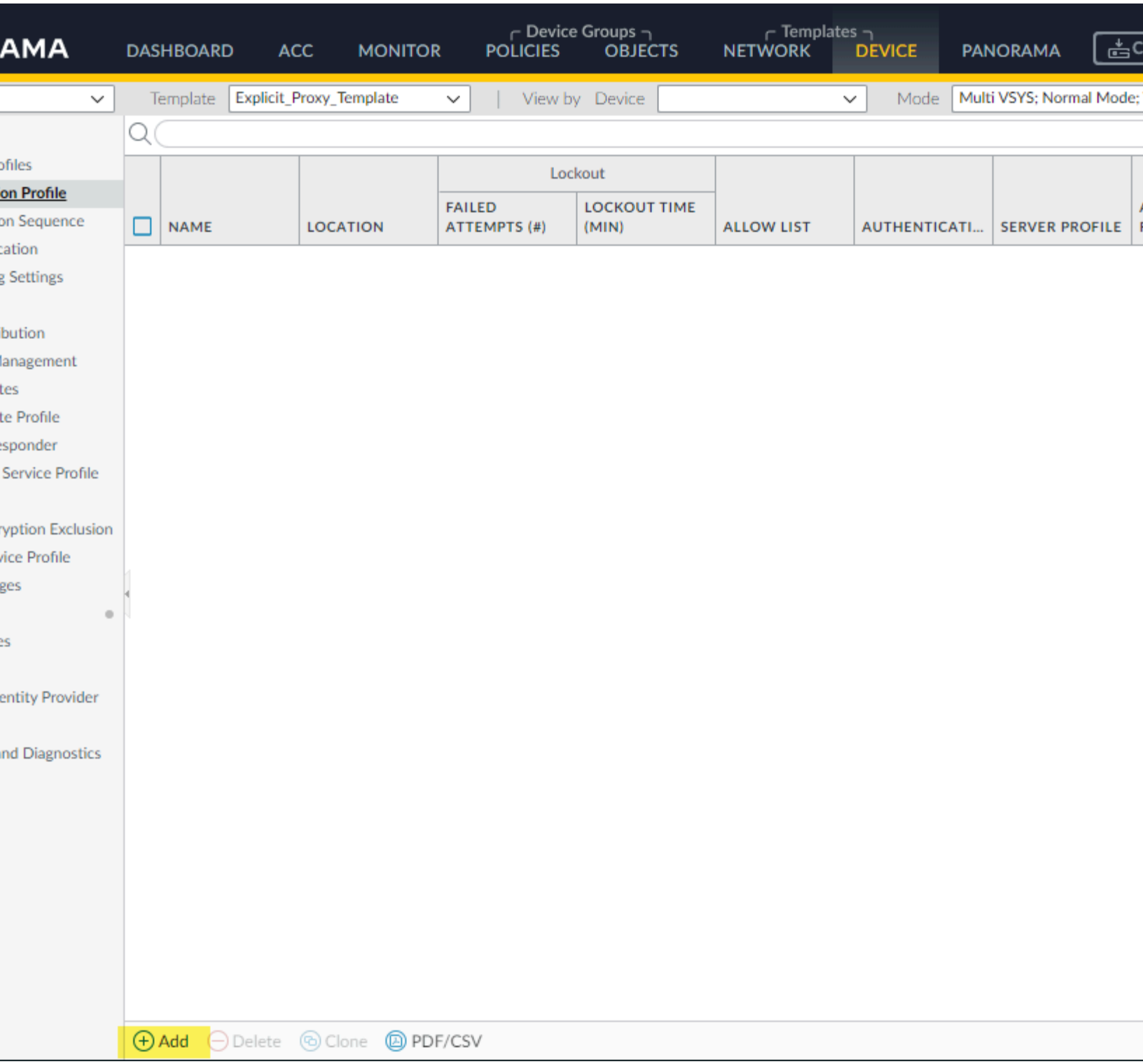

## Konfigurieren der Kerberos-Authentifizierung für Bereitstellungen mit explizitem Proxy (Panorama)

 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** Richten Sie ein Kerberos-Authentifizierungsprofil ein.

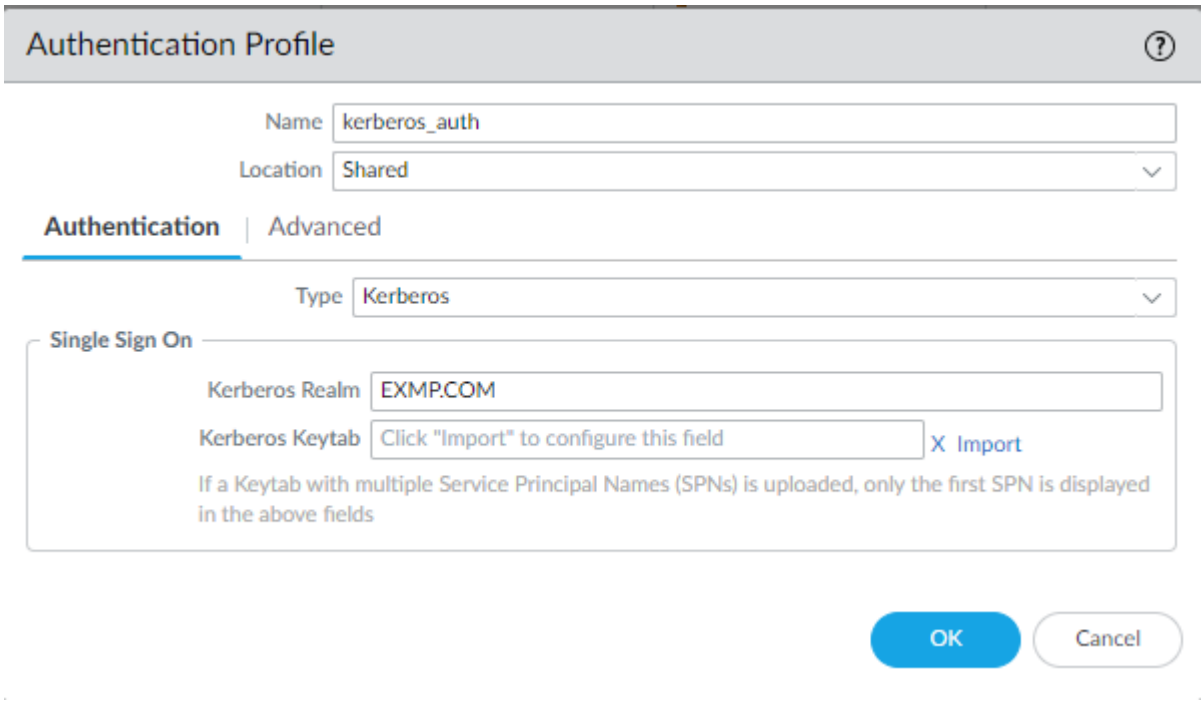
Das Profil definiert, wie der explizite Proxy für die Authentifizierung mobiler Benutzer eine Verbindung zum Kerberos-Server herstellt.

1. Rufen Sie **Gerät** > **Authentifizierungsprofil** > **+ Hinzufügen** auf.

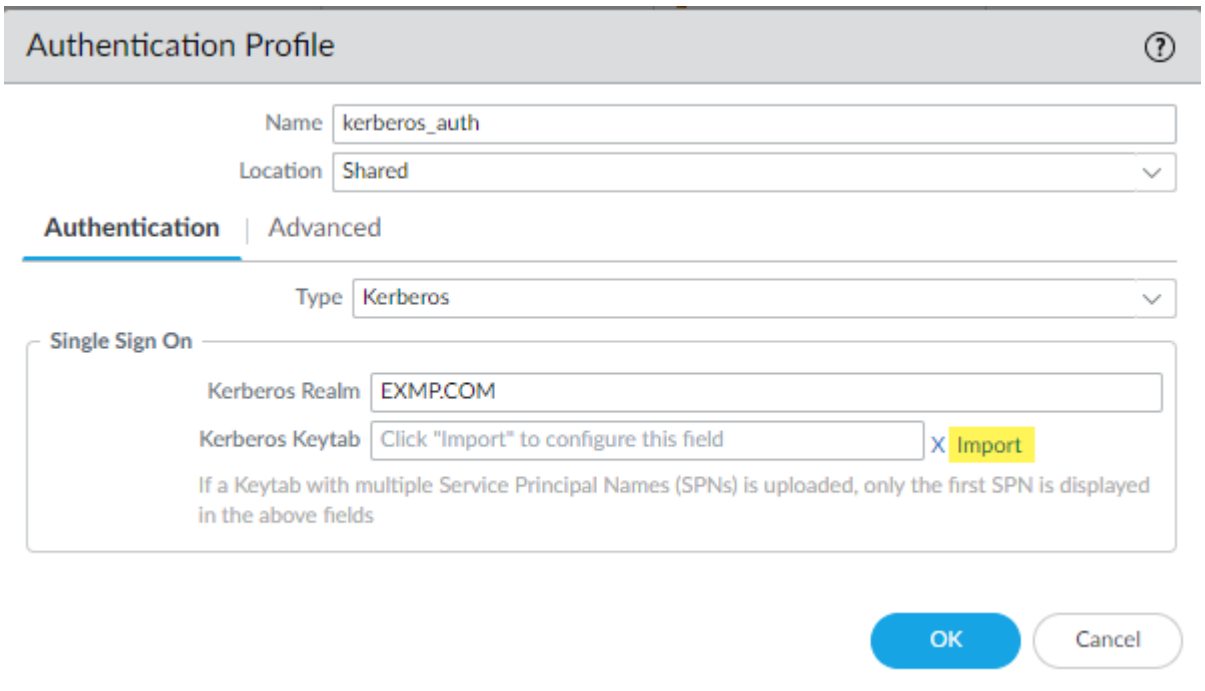



2. Wählen Sie den **Typ** aus: **Kerberos**.

 ©2025 Palo Alto Networks, Inc.



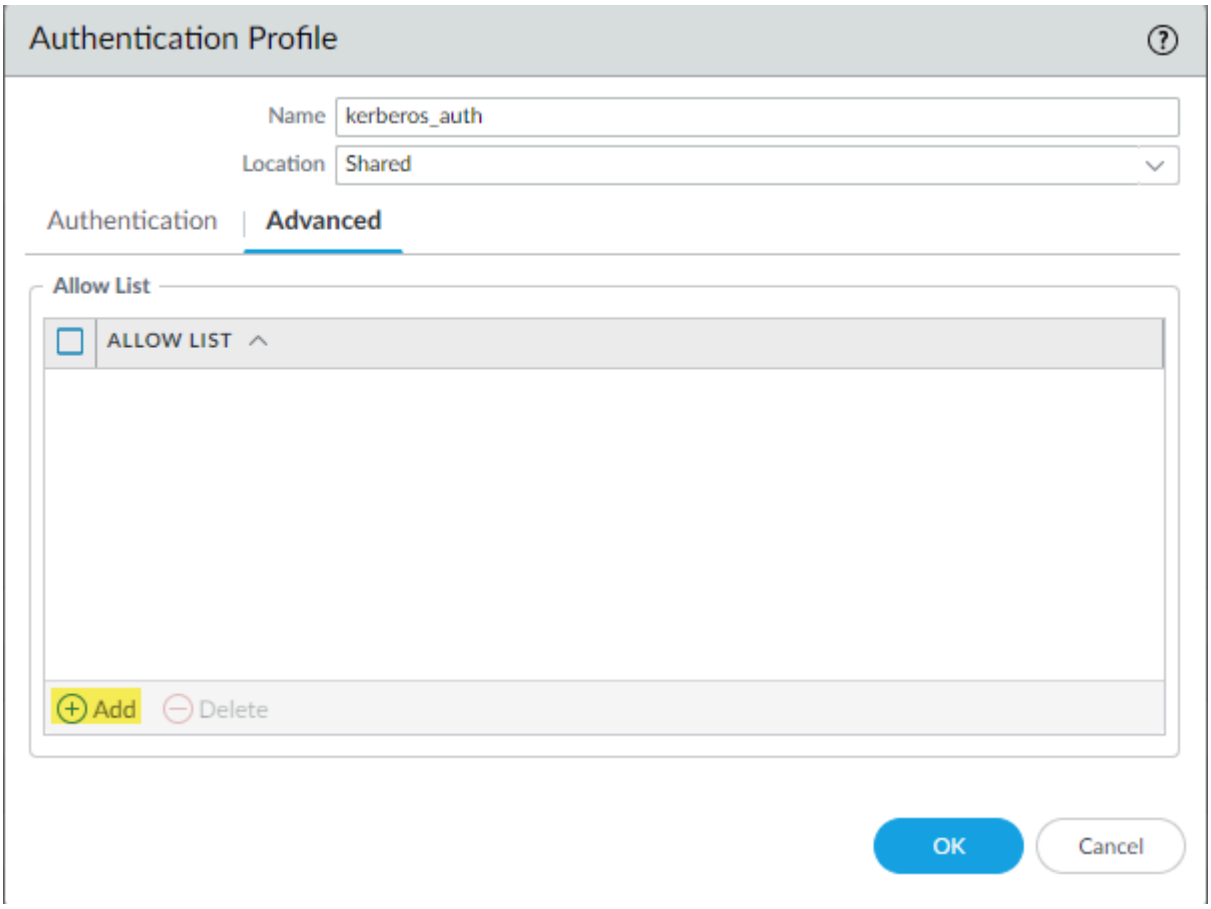

3. Geben Sie unter **Name** einen Namen ein, anhand dessen das Authentifizierungsprofil identifiziert werden kann.
4. Geben Sie den **Kerberos-Bereich** (bis zu 127 Zeichen) ein, um den Hostnamen-Teil des Benutzer-Anmeldenamens anzugeben. Beispielsweise ist dem Benutzerkontonamen „user@EXMP.COM“ der Bereich „EXMP.COM“ zugeordnet.
5. **Importieren** Sie die Kerberos-Schlüsseltabelle, die Sie bereits erstellt haben.




6. Fügen Sie Benutzer hinzu, die sich mit diesem Profil authentifizieren dürfen.
   - Wählen Sie **Erweitert** > **+ Hinzufügen** aus.

 ©2025 Palo Alto Networks, Inc.

- Um alle Benutzer auszuwählen, wählen Sie **Alle** aus.
- Wenn Sie die Cloud Identity Engine verwenden, um die Liste der Benutzer auszufüllen, wählen Sie die Benutzer in einer Liste aus, oder wählen Sie **Alle** aus, um allen Benutzern die Authentifizierung zu erlauben.
- Um lokale Benutzer hinzuzufügen, die sich mit Kerberos anmelden können, geben Sie deren Benutzernamen ein.
  - Verwenden Sie zur Konfiguration der Benutzerauthentifizierung und der Benutzerzuordnung das UPN-Format (userPrincipalName); andere Formate (wie beispielsweise samAccountName) werden nicht unterstützt.
  - In Unicode-Zeichen angegebene Benutzernamen werden nicht unterstützt.



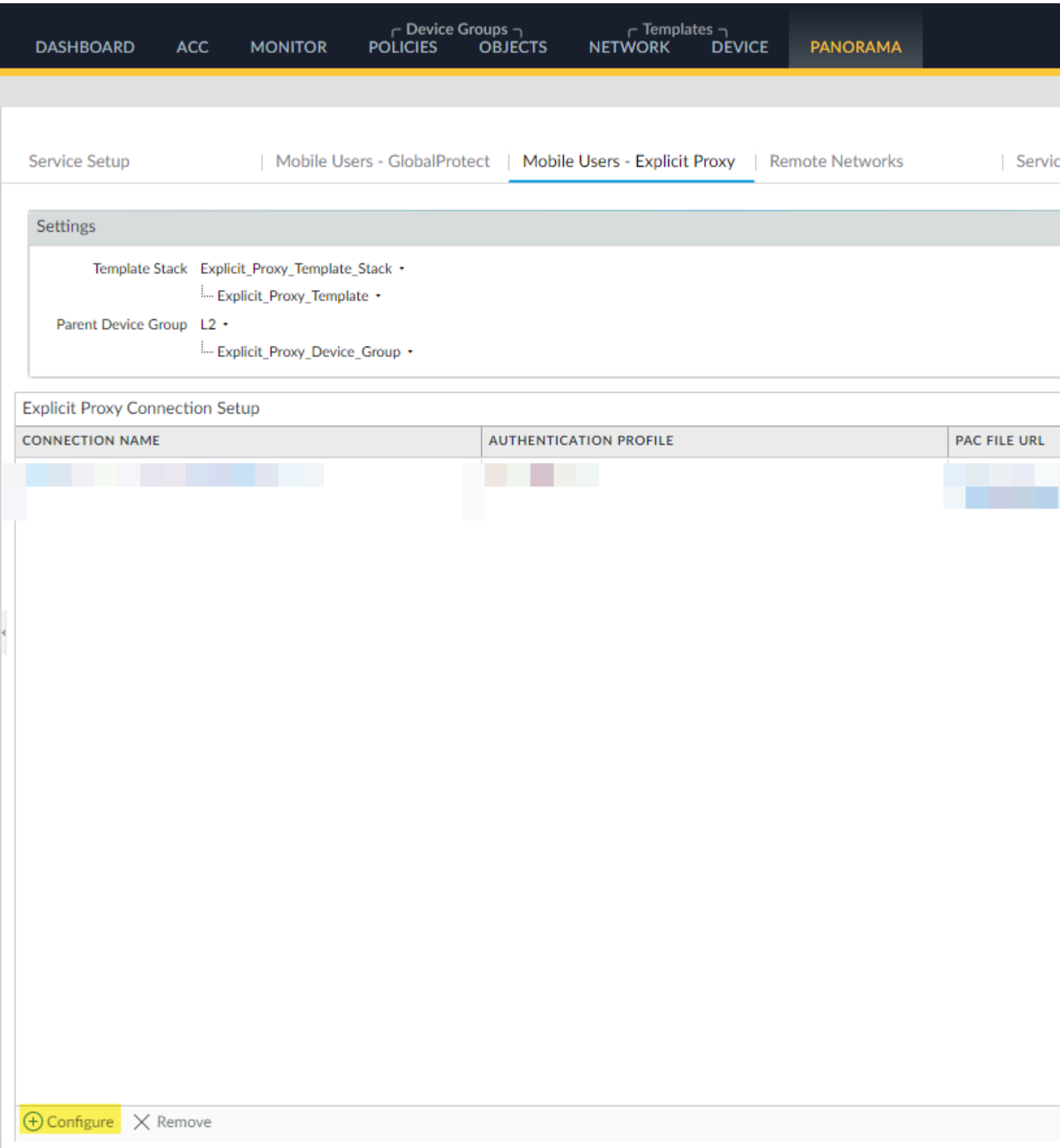

7. **Save (Speichern)** Sie Ihre Änderungen.


©2025 Palo Alto Networks, Inc.

**STEP 2 |** Verknüpfen Sie das Authentifizierungsprofil mit einer Authentifizierungsmethode.

1. Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **+ Konfigurieren** aus.

 ©2025 Palo Alto Networks, Inc.




 ©2025 Palo Alto Networks, Inc.

2. Legen Sie den **FQDN des expliziten Proxys** fest.
3. Wählen Sie das von Ihnen erstellte Kerberos-**Profil** aus.
4. Wählen Sie dann **OK** aus, um Ihre Änderungen zu speichern.

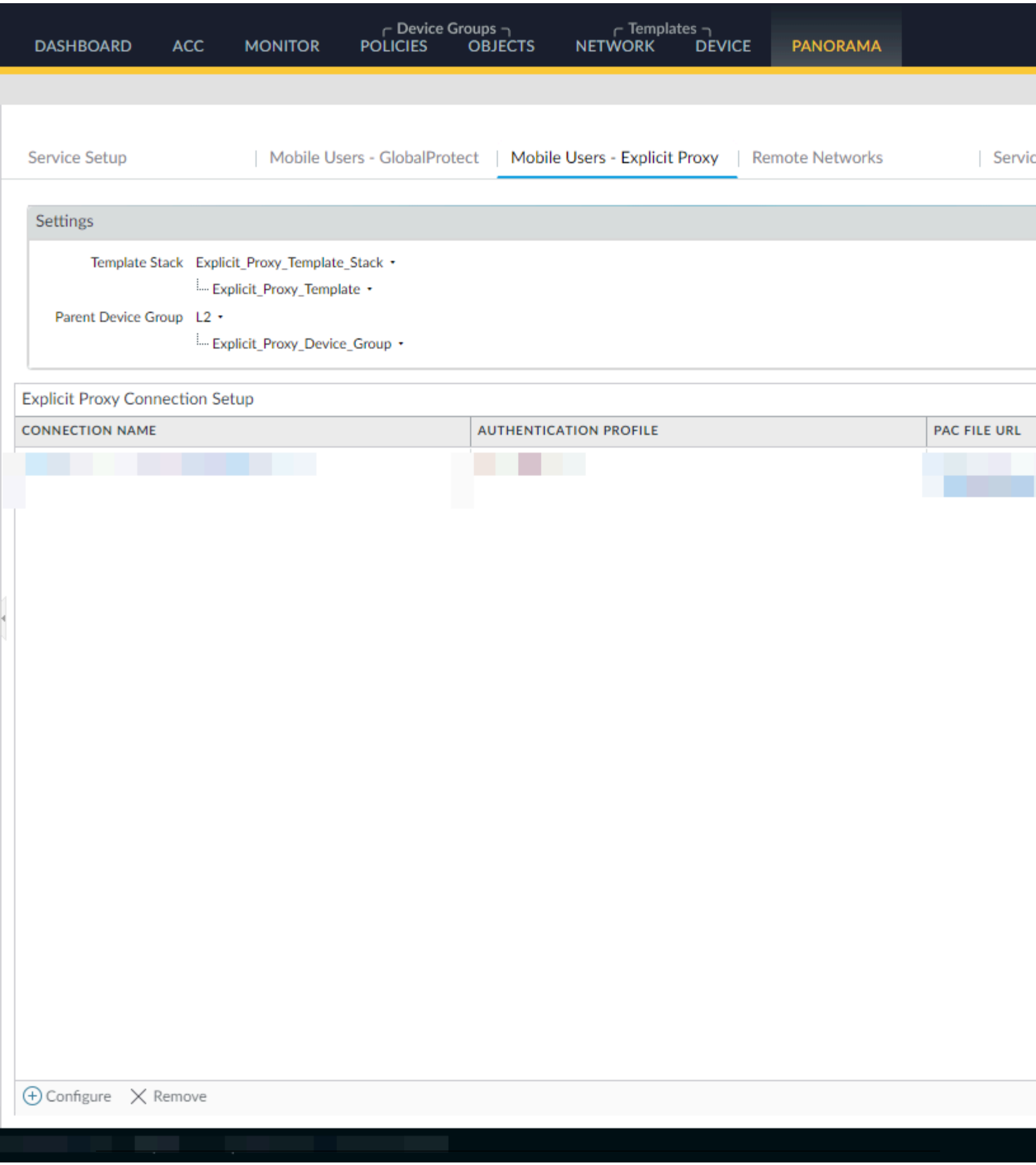

©2025 Palo Alto Networks, Inc.

**STEP 3 |** (Optional) Fügen Sie die Ausgangs-IP-Adressen des Zweigstellen- oder Campus-Standorts, an dem sich Ihre Benutzer, Server, IoT-Geräte oder monitorlosen Maschinen befinden, der Liste vertrauenswürdiger expliziter Proxy-Adressen hinzu.

Diesen Arbeitsschritt müssen Sie nur ausführen, wenn Sie für bestimmte IP-Adressen die **Authentifizierung überspringen** wollen oder den **XAU-Header (X-Authenticated User) für eingehende HTTP/HTTPS-Identitätsanforderungen verwenden** möchten.

1. Rufen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Zahnrad für Einstellungen** > **Authentifizierungseinstellungen** auf.

 ©2025 Palo Alto Networks, Inc.



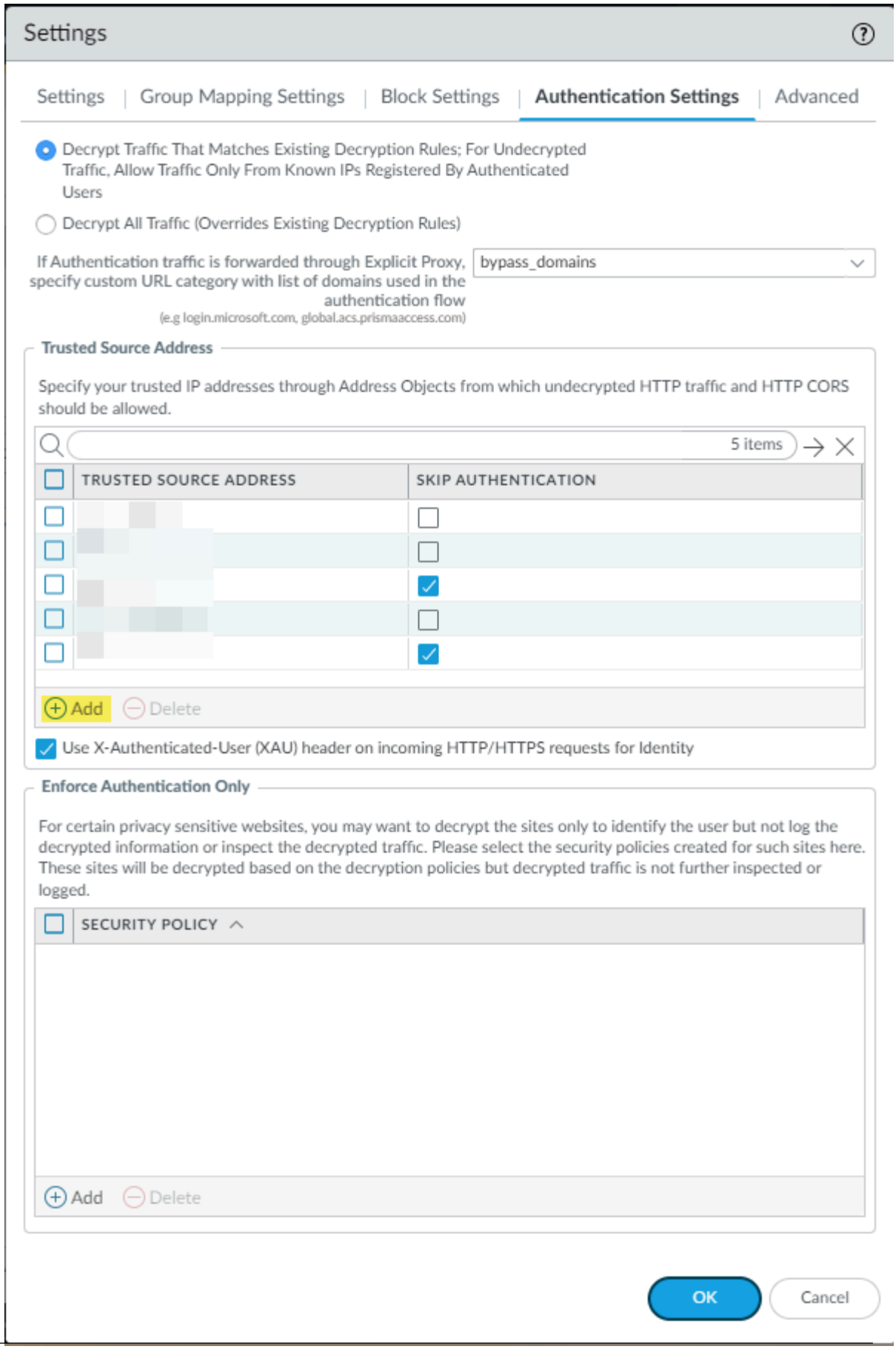

 ©2025 Palo Alto Networks, Inc.

2. Wählen Sie **Hinzufügen** aus, um Adressen zum Feld **Adresse der vertrauenswürdigen Quelle** hinzuzufügen.

   Wenn Sie die Ausgangs-Endpunkt-IP-Adressen nicht zur vertrauenswürdigen Liste hinzufügen, erzwingt der explizite Proxy bei Benutzern und Maschinen die Authentifizierung mit SAML sowie mit Kerberos.

   Geben Sie maximal 100.000 IP-Adressen ein.

 ©2025 Palo Alto Networks, Inc.




 ©2025 Palo Alto Networks, Inc.

3. Wählen Sie dann **OK** aus, um Ihre Änderungen zu speichern.

**STEP 4 |** Erstellen Sie für die Benutzerauthentifizierung eine Allow-All-Richtlinienregel.

1. Wählen Sie **Richtlinien** > **Vor-Regeln** > **+ Hinzufügen** aus.
2. Ordnen Sie der Regel einen Namen zu.
3. Wählen Sie die **Quelle** aus.
4. Legen Sie für den Quellbenutzer die Option **Bekannter Benutzer** fest.
5. Setzen Sie alle anderen erforderlichen Werte auf **Beliebig**.
6. Wählen Sie **OK**, um die Regel zu speichern.

**STEP 5 |** Schreiben Sie Ihre Konfigurationsänderungen fest und übertragen Sie sie mit Commit und Push.

**STEP 6 |** Überprüfen Sie, ob die Kerberos-Authentifizierung mit Prisma Access ordnungsgemäß funktioniert, indem Sie die Datenverkehrs- und Authentifizierungsprotokolle anzeigen.

1. (Nur entschlüsselter Datenverkehr) Wählen Sie **Überwachen** > **Protokolle** > **Datenverkehr** aus und überprüfen Sie, ob die Kerberos-Authentifizierung ordnungsgemäß funktioniert.

   *Für entschlüsselten Datenverkehr wird der Benutzername in den Datenverkehrs-Protokollen angezeigt.*

2. (Nur nicht entschlüsselter Datenverkehr) Wählen Sie **Überwachen** > **Protokolle** > **Authentifizierung** aus und überprüfen Sie, ob die Kerberos-Authentifizierung korrekt funktioniert.

   Die folgenden Felder enthalten weitere Informationen zum Authentifizierungsereignis:

   - **Objekt** – Die Website, auf die der Benutzer zuzugreifen versuchte, bevor er zur Authentifizierung an Kerberos umgeleitet wurde.
   - **Auth-Ereignis** – Der Status des Authentifizierungsversuchs.

     Mit **Authentifizierungserfolg** wird angezeigt, dass das Authentifizierungsereignis erfolgreich ausgeführt werden konnte; **Authentifizierungsfehler** zeigt an, dass der Versuch fehlgeschlagen ist, und generiert ein Protokoll.
   - **Authentifizierungsbeschreibung** – Wenn der Authentifizierungsversuch fehlgeschlagen ist, erhalten Sie hier zusätzliche Informationen zur Art des Fehlers.

     Beispielsweise weist die Meldung **Benutzer nicht erlaubt** darauf hin, dass der Benutzer oder die Gruppe Kerberos nicht zur Authentifizierung verwenden darf. Dies kann darauf zurückzuführen sein, dass der Benutzer oder die Gruppe nicht zur **Zulassungsliste** im Authentifizierungsprofil hinzugefügt wurde.

 ©2025 Palo Alto Networks, Inc.

# Cloud Identity Engine-Authentifizierung für Bereitstellungen mit explizitem Proxy

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

Verwenden Sie die Cloud Identity Engine, um sowohl die Benutzeridentifikation als auch die Benutzerauthentifizierung für mobile Benutzer in einer Bereitstellung von Prisma Access mit explizitem Proxy bereitzustellen.

Die Cloud Identity Engine bietet Funktionen für die Benutzeridentifikation und die Benutzerauthentifizierung für eine zentralisierte cloudbasierte Lösung in lokalen, cloudbasierten oder hybriden Netzwerkumgebungen. Die Cloud Identity Engine ermöglicht es Ihnen, Sicherheitsrichtlinien für Benutzer und Gruppen zu schreiben, und unterstützt Sie bei der Sicherung Ihrer Netzwerke, indem verhaltensbasierte Sicherheitsaktionen durchgesetzt werden.

Durch die kontinuierliche Synchronisierung der Informationen aus Ihren Verzeichnissen und unabhängig davon, ob diese lokal, cloudbasiert oder hybrid angelegt wurden, wird sichergestellt, dass Ihre Benutzerinformationen korrekt und aktuell sind und die Richtliniendurchsetzung auf Grundlage der Zuordnungen auch dann fortgesetzt werden kann, wenn der Cloud-Identitätsprovider vorübergehend nicht verfügbar ist.

- Cloud Identity Engine-Authentifizierung für Bereitstellungen mit explizitem Proxy (Strata Cloud Manager)
- Cloud Identity Engine-Authentifizierung für Bereitstellungen mit explizitem Proxy (Panorama)

## Cloud Identity Engine-Authentifizierung für Bereitstellungen mit explizitem Proxy (Strata Cloud Manager)

Die Cloud Identity Engine ermöglicht sowohl die Benutzeridentifikation als auch die Benutzerauthentifizierung für mobile Benutzer in einer Bereitstellung von Prisma Access mit explizitem Proxy. Die Cloud Identity Engine ist im expliziten Proxy Authentication Cache Service (ACS) integriert und verwendet SAML-Identitätsanbieter (IdPs), um die Authentifizierung für mobile Benutzer des expliziten Proxy bereitzustellen.

Führen Sie die folgenden Schritte aus, um die Authentifizierung für eine Bereitstellung mit explizitem Proxy für mobile Benutzer mithilfe der Cloud Identity Engine zu konfigurieren.

**STEP 1 |** Führen Sie in Prisma Access (Managed by Strata Cloud Manager) die Aktion Expliziten Proxy einrichten für Ihren Mandanten durch.

Bevor Sie expliziten Proxy konfigurieren, sollten Sie sich mit der Funktionsweise von explizitem Proxy vertraut machen und sich darüber informieren, welche Richtlinien verwendet werden müssen, um die Konfiguration durchzuführen.

Wenn Sie über mehrere Mandanten verfügen, dann konfigurieren Sie expliziten Proxy für jeden Ihrer Mandanten, für den dieser Schritt erforderlich ist.

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Melden Sie sich am Hub an und richten Sie über die Cloud Identity Engine-App einen Authentifizierungstyp und den Authentifizierungsanbieter ein.

Sie können Apps im Hub nach Mandanten oder Supportkonto geordnet anzeigen.

1. Konfigurieren Sie einen SAML-Authentifizierungstyp in der Cloud Identity Engine.

   Die Anleitung „Erste Schritte“ für Cloud Identity Engine enthält die Verfahren, die Sie zum Konfigurieren einer SAML-IdP in der Cloud Identity Engine benötigen:

   - Konfigurieren von Azure als IdP in der Cloud Identity Engine
   - Konfigurieren von Okta als IdP in der Cloud Identity Engine
   - Konfigurieren von PingOne als IdP in der Cloud Identity Engine
   - Konfigurieren von PingFederate als IdP in der Cloud Identity Engine
   - Konfigurieren von Google als IdP in der Cloud Identity Engine

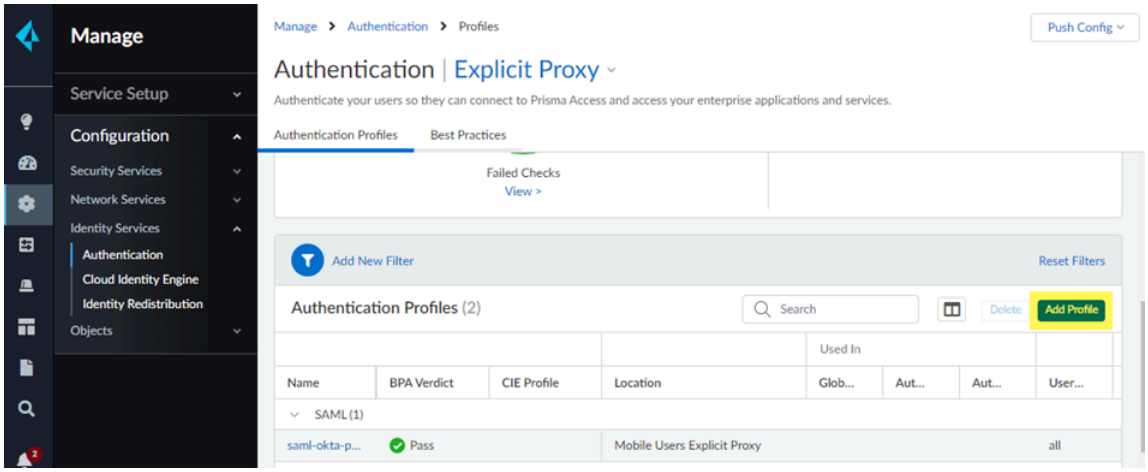
   Konfigurieren Sie keine Einzelabmeldung, da diese Funktion nicht unterstützt wird.
2. Richten Sie ein Authentifizierungsprofil in der Cloud Identity Engine ein und wählen Sie die Benutzer und Gruppen aus, die diese Authentifizierungsmethode verwenden können.

   Sie geben dieses Profil an, wenn Sie in einem späteren Schritt ein Authentifizierungsprofil in Prisma Access (Managed by Strata Cloud Manager) erstellen.

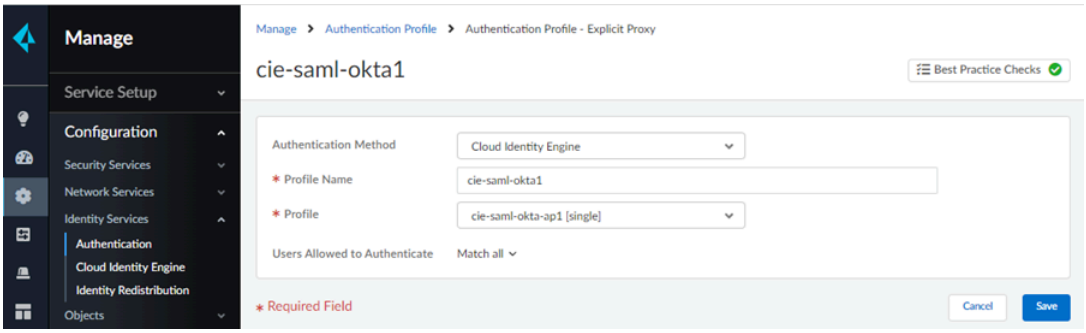
 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Kehren Sie zu Prisma Access (Managed by Strata Cloud Manager) zurück und erstellen Sie ein Authentifizierungsprofil, das Sie mit der Cloud Authentication Engine verwenden können.

1. Rufen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Identitätsdienste** > **Authentifizierung** auf und legen Sie als Geltungsbereich **Expliziter Proxy** fest. Fügen Sie dann mit **Profil hinzufügen** ein Authentifizierungsprofil hinzu.




2. Wählen Sie eine **Authentifizierungsmethode** der **Cloud Identity Engine** aus.
3. Ordnen Sie dem Profil unter **Profilname** einen Namen zu.
4. Wählen Sie das Cloud Identity Engine-Authentifizierungsprofil aus, das Sie in einem vorherigen Schritt erstellt haben.

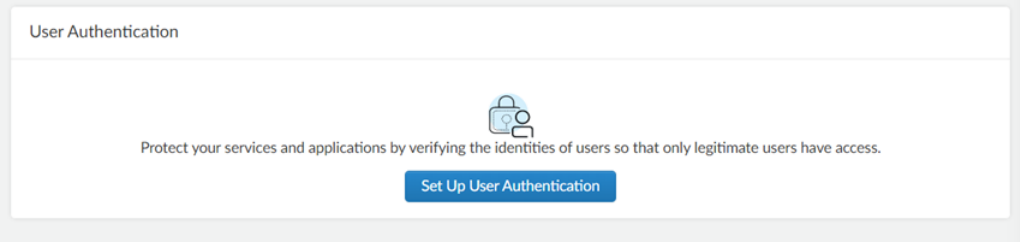



5. **Save (Speichern)** Sie Ihre Änderungen.

 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** Richten Sie die Benutzerauthentifizierung im expliziten Proxy ein.

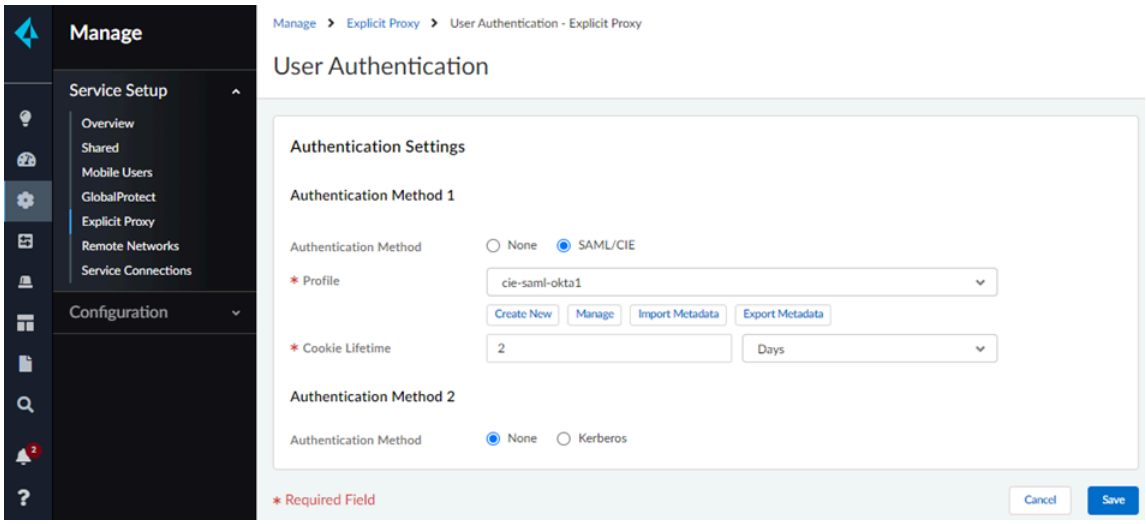
1. Rufen Sie **Workflows** > **Prisma Access-Einrichtung** > **Expliziter Proxy** und **Benutzerauthentifizierung einrichten** auf.




2. Wählen Sie als **Authentifizierungsmethode SAML/CIE** aus.
3. Wählen Sie das Authentifizierungsprofil aus, das Sie in Cloud-verwaltetes Prisma Access erstellt haben.
4. Geben Sie eine **Cookie-Lebensdauer** für das Cookie an, das die Authentifizierungsdaten der Benutzer speichert.

   Nachdem der IdP den Benutzer authentifiziert hat, speichert Prisma Access den Authentifizierungsstatus des Benutzers im ACS (Authentication Cache Service). Die Gültigkeitsdauer der Authentifizierung basiert auf dem Wert für die Cookie-Lebensdauer, den Sie hier angeben.

   Um zu verhindern, dass Benutzer Probleme mit dem Download großer Dateien vor Ablauf der Cookie-Lebensdauer haben oder das Cookie abläuft, wenn Benutzer über einen längeren Zeitraum auf eine einzelne Website zugreifen, empfiehlt Palo Alto Networks, eine **Cookie-Lebensdauer** von mindestens einem Tag zu konfigurieren. Wenn Benutzer des expliziten Proxy ein Problem mit dem Ablauf der Cookie-Lebensdauer haben, können sie zu einer anderen Website wechseln, um sich erneut bei ACS zu authentifizieren und das ACS-Cookie zu aktualisieren.

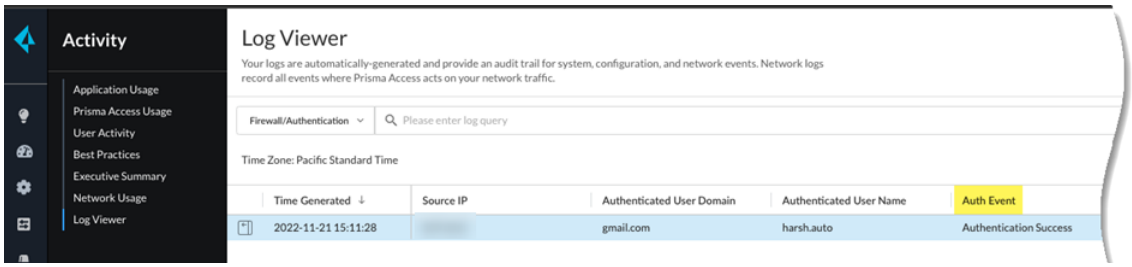



5. **Save (Speichern)** Sie Ihre Änderungen.

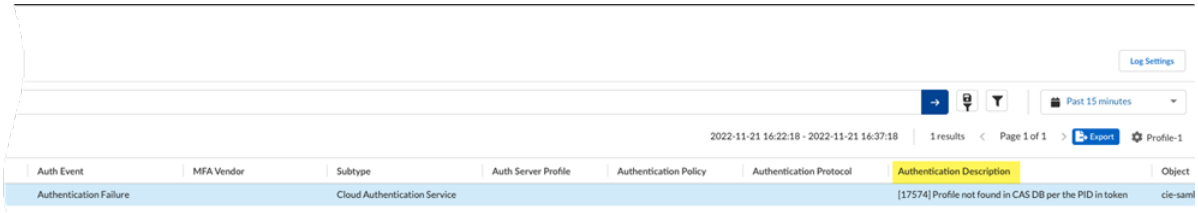
 ©2025 Palo Alto Networks, Inc.

**STEP 5 |** Stellen Sie sicher, dass die Cloud Identity Engine Ihre mobilen Benutzer des expliziten Proxy erfolgreich authentifizieren kann.

1. Wählen Sie in Prisma Access (Managed by Strata Cloud Manager) **Vorfälle und Benachrichtigungen** > **Protokoll-Viewer** > **Firewall/Authentifizierung** aus.
2. Zeigen Sie den Status für **Authentifizierungsereignis** an.

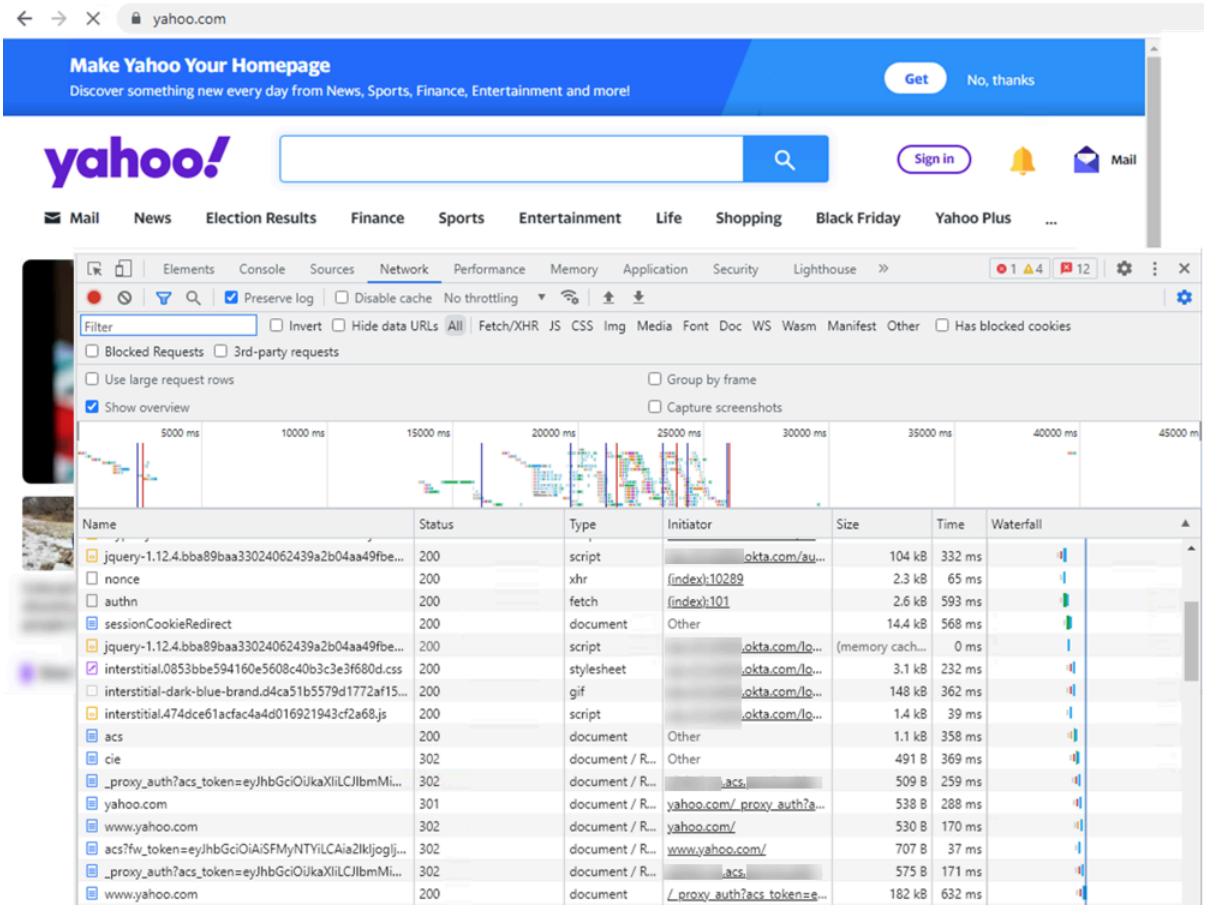



Wenn die Authentifizierung fehlschlägt, lesen Sie die weiterführenden Informationen zum Fehler in der **Authentifizierungsbeschreibung**.




3. Verwenden Sie über den Endpunkt des mobilen Benutzers Entwicklertools, um den Authentifizierungsfluss der Cloud Identity Engine anzuzeigen.

 ©2025 Palo Alto Networks, Inc.




### Cloud Identity Engine-Authentifizierung für Bereitstellungen mit explizitem Proxy (Panorama)

Authentifizieren Sie mobile Benutzer des expliziten Proxy von Prisma Access (Managed by Panorama) mit der Cloud Identity Engine

## Proxy-Modus in Remote-Netzwerken

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br><br>Wenn Sie private Quell-IP-basierte Sichtbarkeit und Durchsetzung auf „Expliziter Proxy“ in Ihrer Prisma Access-Umgebung aktivieren möchten, wenden Sie sich an Ihr Account-Team, um mehr zu erfahren. | • Prisma Access-Lizenz<br><br>Für den Proxy-Modus für Remote-Netzwerke sind eine Prisma Access-Lizenz für mobile Benutzer und eine Prisma Access-Lizenz für Remote-Netzwerke erforderlich. |

Der Proxy-Modus in Remote-Netzwerken hilft, ausgehenden Internet-Verkehr für Benutzer und Server in Ihren Zweigstellen abzusichern, die aus Vernetzungs- oder Compliance-Gründen eine PAC-basierte Verbindungsmethode benötigen.


©2025 Palo Alto Networks, Inc.

Sie können den Proxy-Modus für Remote-Netzwerke für Folgendes verwenden:

- Sichern des internetgebundenen Datenverkehrs von Zweigstellen, die nicht standardmäßige Routen verwenden.
- Sichern des internetgebundenen Datenverkehrs von Ihren Filialen, ohne diesen an den Standort eines Rechenzentrums oder einer Zentrale zurückzuleiten.
- Herstellen einer Verbindung mit Prisma Access Expliziter Proxy über private IP-Adressen.

  Prisma Access bietet Ihnen vier Anycast-IP-Adressen weltweit und eine Unicast-IP-Adresse pro Remote-Netzwerk, mit der Sie Datenverkehr an „Expliziter Proxy“ weiterleiten.
- Durchsetzen von Sicherheitskontrollen und Erzielen von Sichtbarkeit basierend auf der Quell-IP für die Systeme in der Niederlassung.
- Überspringen der Authentifizierung für Server, basierend auf der Quell-IP-Adresse.
- Herstellen einer Verbindung mit Prisma Access von Ihrer Niederlassung durch einen IPSec Tunnel.
- Wenn Sie mehr als 1.000 Mbit/s Bandbreite benötigen, können Sie eine Remote-Netzwerkverbindung mit hoher Bandbreite mithilfe mehrerer Remote-Netzwerkverbindungen erstellen und in jeder Verbindung die Anycast- und Unicast-Adressen für „Expliziter Proxy“ angeben.

Im folgenden Diagramm ist ein Remote-Netzwerk dargestellt, das für einen Standort konfiguriert wurde, für den keine Standardroute konfiguriert ist. Um Benutzer und monitorlose Geräte am Standort mit einer Bereitstellung des Typs „Expliziter Proxy“ zu schützen, hat der Administrator die folgenden Konfigurationsänderungen vorgenommen:

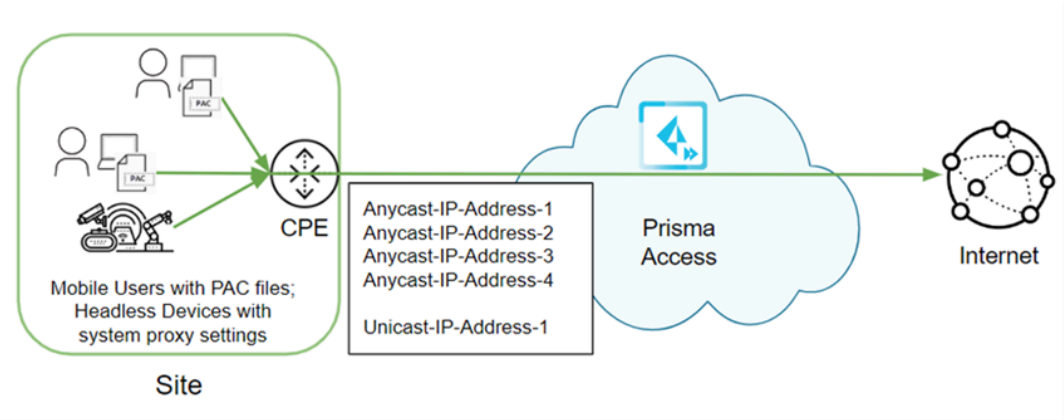
- Es wurden Standorte mit Bereitstellungen des Typs „Remote-Netzwerk“ und „Expliziter Proxy“ eingebunden und es wurden Anycast- sowie Unicast-IP-Adressen abgerufen, die Prisma Access aus seinem Infrastruktursubnetz übernimmt.

  *Sie können auch einen Hostnamen für von „Expliziter Proxy“ gesteuerten Datenverkehr erstellen und diesem Hostnamen die Unicast- und Anycast-IP-Adressen von „Expliziter Proxy“ hinzufügen.*
- Das CPE wurde so konfiguriert, dass es den Datenverkehr von „Expliziter Proxy“ an diese Anycast- und Unicast-Adressen weiterleitet.

  Verwenden Sie die Anycast-IP-Adressen in der PAC-Datei, um Prisma Access aus jedem eingebundenen Remote-Netzwerktunnel auswählen zu lassen, um Datenverkehr an „Expliziter Proxy“ weiterzuleiten. Verwenden Sie die Unicast-Adresse, damit Prisma Access Datenverkehr durch einen bestimmten Remote-Netzwerktunnel weiterleitet. In diesem Beispiel können Sie entweder Anycast- oder Unicast-Adressen verwenden, da der Datenverkehr nur über einen einzigen Remote-Netzwerk-IPSec-Tunnel geleitet wird.
- Geben Sie diese IP-Adressen in den PAC-Dateien der Endpunkte der Benutzer und in den System-Proxy-Einstellungen der monitorlosen Geräte an.

Nach Abschluss der Konfiguration leitet Prisma Access den Datenverkehr aus dem Remote-Netzwerk-Tunnel an „Expliziter Proxy“ weiter.

 ©2025 Palo Alto Networks, Inc.




- Strata Cloud Manager
- Panorama

## Proxy-Modus in Remote-Netzwerken (Strata Cloud Manager)

Gehen Sie wie folgt vor, um Benutzer in Remote-Netzwerken mithilfe von „Expliziter Proxy“ in cloudverwaltetem Prisma Access zu schützen.

**STEP 1 |** Konfigurieren Sie Ihre Einrichtung für „Expliziter Proxy“ und binden Sie die Standorte mit explizitem Proxy ein, die Sie hinzufügen möchten.

**STEP 2 |** Falls noch nicht geschehen, binden Sie Ihre Remote-Netzwerke ein.

*Sie müssen Prisma Access-Remote-Netzwerke an den Standorten aktivieren, die von „Expliziter Proxy“ unterstützt werden.*

**STEP 3 |** Wählen Sie **Konfiguration übertragen** aus, wobei sicherzustellen ist, dass die Optionen **Mobile Benutzer – Remote-Mitarbeiter** und **Remote-Netzwerke** im Bereich **Push** ausgewählt sind.

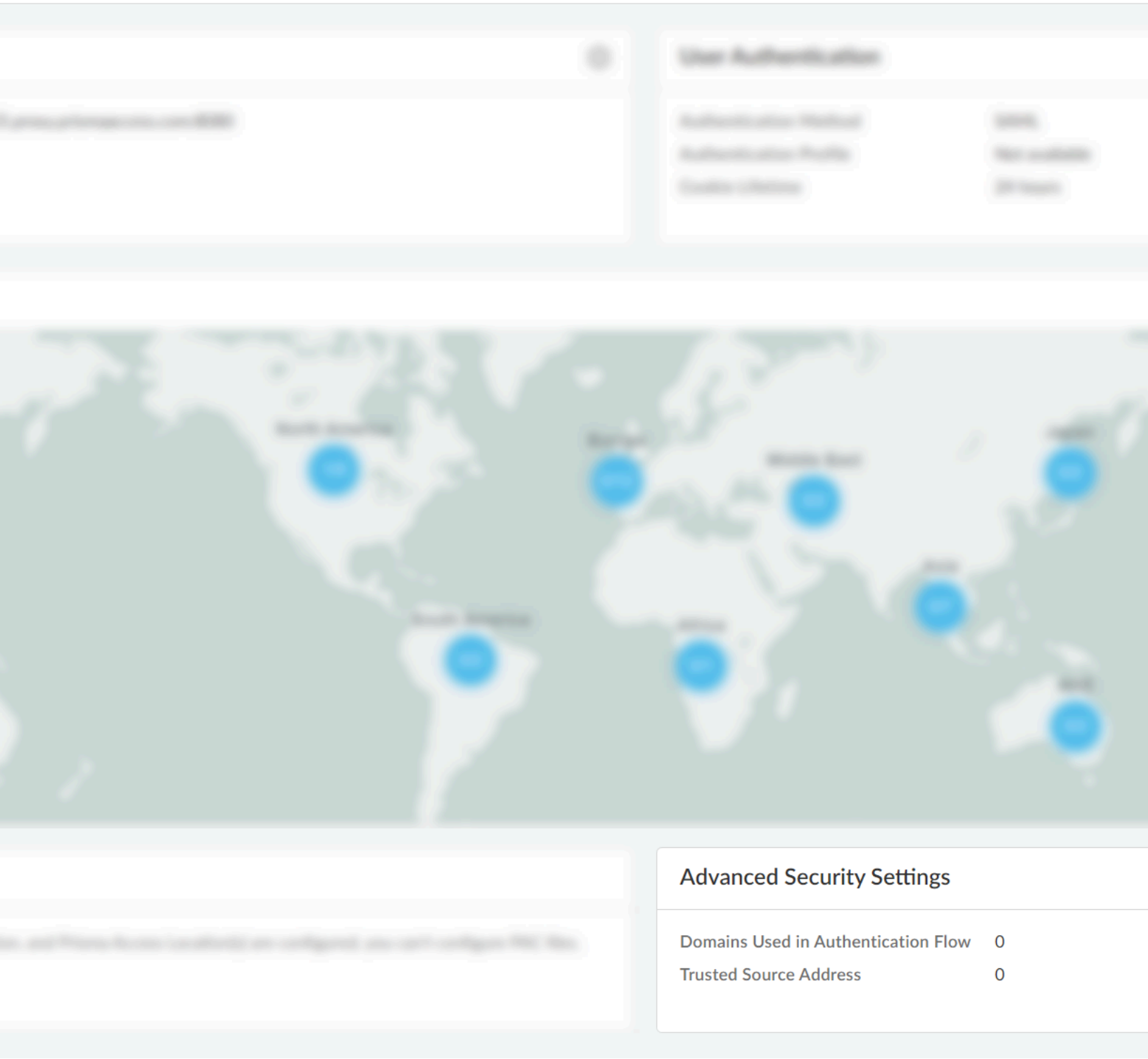
Der Push-Vorgang ruft Anycast-Adressen ab, die Sie benötigen, um „Expliziter Proxy“ in das Remote-Netzwerk zu integrieren.

 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** Rufen Sie die Anycast-IP-Adressen ab, die Sie für Ihre Bereitstellung des Typs „Expliziter Proxy“/„Remote-Netzwerk“ benötigen.

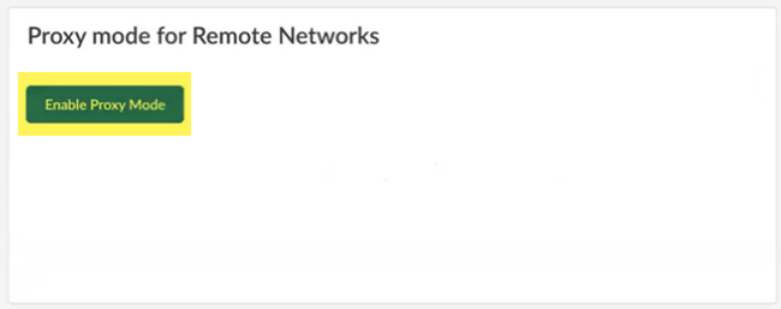
1. Wählen Sie **Workflows** > **Einrichtung Prisma Access** > **Expliziter Proxy** > **Erweiterte Sicherheitseinstellungen** aus.

 ©2025 Palo Alto Networks, Inc.




2. Wählen Sie **Proxy-Modus aktivieren** aus.

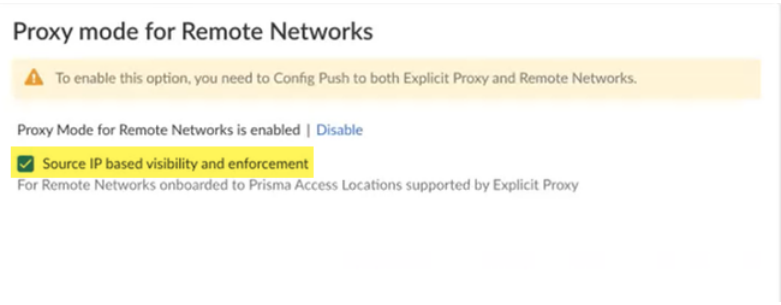

©2025 Palo Alto Networks, Inc.




3. Um die Quell-IP-Adressen der Systeme an Ihren Niederlassungsstandorten zu nutzen, die Datenverkehr an den expliziten Proxy weiterleiten, wählen Sie **Quell-IP-basierte Sichtbarkeit und Durchsetzung** aus.

   Für diese Funktionalität gelten folgende Anforderungen:

   - Mindestens Prisma Access-Dataplane 10.2.4
   - Sie dürfen nur Remote-Netzwerkstandorte verwenden, die von „Expliziter Proxy“ unterstützt werden.



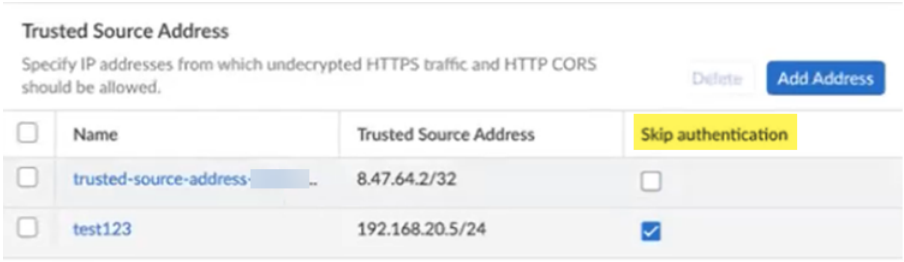

4. Ergänzen Sie eine Richtlinie, um Datenverkehr zuzulassen, der an Anycast- und Unicast-IP in Remote-Netzwerken gebunden ist. Wenn Sie die **Transparenz und Durchsetzung der Quell-IP** aktiviert haben, verwenden Sie das Feld **Quell-IP** in den Sicherheitsrichtlinien von „Expliziter Proxy“, um den Datenverkehr abzusichern. Sie benötigen zusätzliche Richtlinien in den Remote-Netzwerken.
5. (Optional) Um die Authentifizierung beliebiger, von Ihnen eingegebener vertrauenswürdiger Quelladressen zu umgehen, geben Sie im Bereich **Adresse der vertrauenswürdigen Quelle** IP-Adressen an, bei denen die Authentifizierung übersprungen werden soll, und wählen Sie **Authentifizierung überspringen** aus.

   Sie können die Option **Authentifizierung überspringen** mit der Einstellung **Quell-IP-basierte Sichtbarkeit und Durchsetzung** verwenden, um die Authentifizierung von monitorlosen Systemen zu überspringen, die keine Sicherheitsrichtlinien einrichten

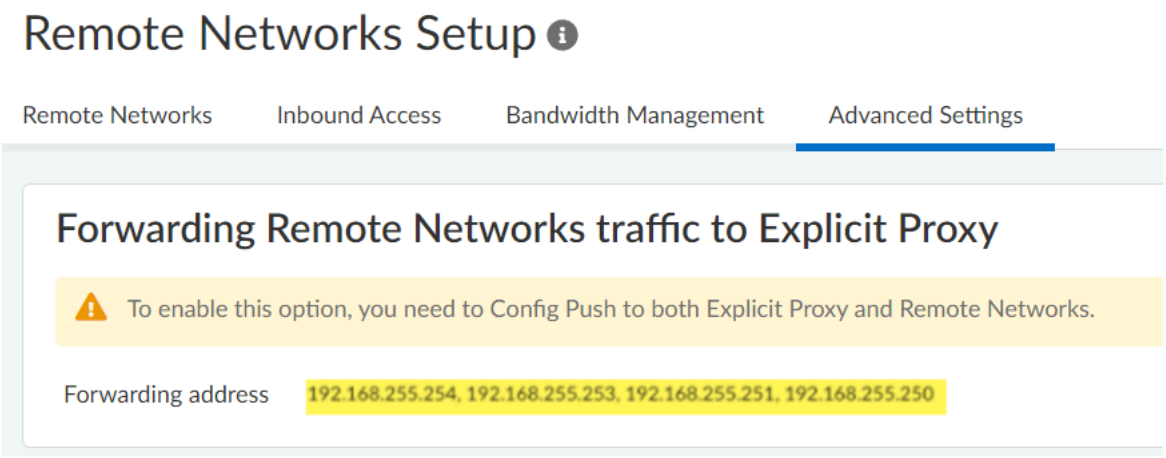
 ©2025 Palo Alto Networks, Inc.

können, und so Einblick in den Datenverkehr auf Prisma Access mit explizitem Proxy erhalten.

*Sie können entweder IP-Adressen oder Subnetze hinzufügen. Nach Erweiterung der Subnetze werden maximal 100.000 IP-Adressen unterstützt.*




6. Gehen Sie zu **Workflows** > **Einrichtung Prisma Access** > **Remote-Netzwerke**.
7. Wählen Sie **Konfiguration übertragen** aus, wobei sicherzustellen ist, dass die Optionen **Mobile Benutzer – Remote-Mitarbeiter** und **Remote-Netzwerke** im Bereich **Push** ausgewählt sind.
8. Wählen Sie **Erweiterte Einstellungen** in der Einrichtung Ihres Remote-Netzwerks aus und suchen Sie nach den Anycast-IP-Adressen, die zum Weiterleiten des Datenverkehrs an „Expliziter Proxy“ verwendet werden.




**STEP 5 |** (Optional) Suchen Sie nach der Unicast-Adresse, die für Ihre Bereitstellung des Typs „Expliziter Proxy“/„Remote-Netzwerk“ verwendet werden soll.

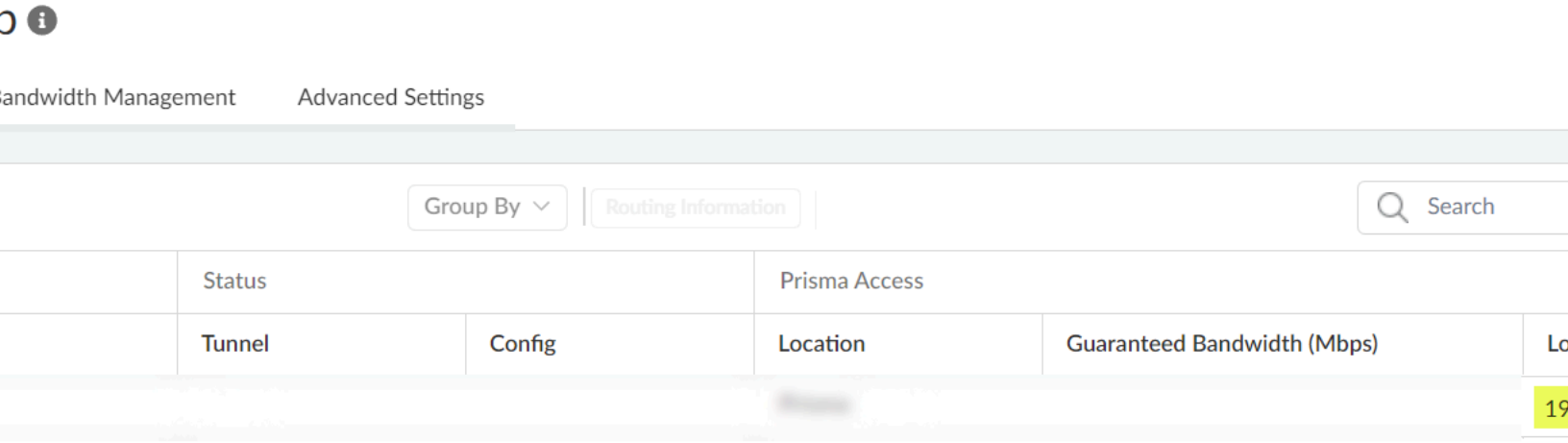
Verwenden Sie die Unicast-IP-Adresse in der PAC-Datei nur, wenn Sie ein bestimmtes Remote-Netzwerk als Ziel für die Weiterleitung von Datenverkehr an „Expliziter Proxy“

 ©2025 Palo Alto Networks, Inc.

verwenden möchten. Wenn Sie alle bereitgestellten Remote-Netzwerke verwenden möchten, um Datenverkehr an „Expliziter Proxy“ weiterzuleiten, verwenden Sie die Anycast-Adressen.

1. Gehen Sie zu **Workflows** > **Einrichtung Prisma Access** > **Remote-Netzwerke**.
2. Notieren Sie sich die **Loopback-IP**-Adresse.

   Wenn IPv4- und IPv6-Adressen vorliegen, notieren Sie sich die IPv4-Adresse.




## Proxy-Modus in Remote-Netzwerken (Panorama)

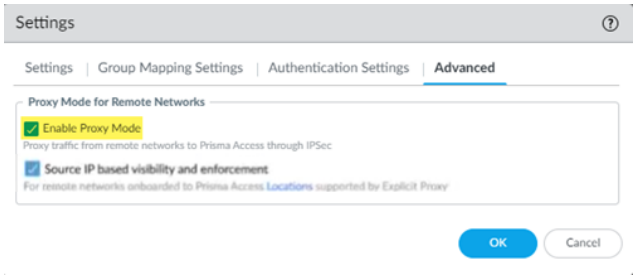
Gehen Sie wie folgt vor, um Benutzer in Remote-Netzwerken mithilfe von „Expliziter Proxy“ in Prisma Access (Managed by Panorama) Access zu schützen.

**STEP 1 |** Konfigurieren Sie Ihre Bereitstellung des Typs „Expliziter Proxy“ und binden Sie die Standorte mit explizitem Proxy ein, die Sie hinzufügen möchten.


©2025 Palo Alto Networks, Inc.

**STEP 2 |** Rufen Sie die Anycast-IP-Adressen ab, die Sie für Ihre Bereitstellung des Typs „Expliziter Proxy“/„Remote-Netzwerk“ verwenden.

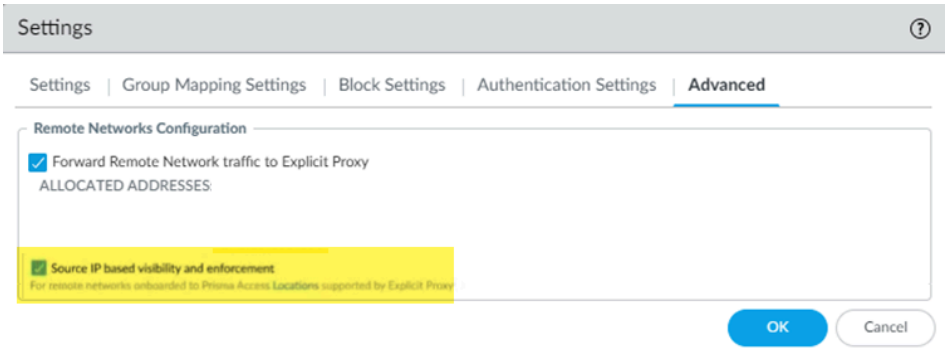
1. Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Mobile Benutzer – Expliziter Proxy** aus.
2. Wählen Sie das Zahnradsymbol aus, um die **Einstellungen** zu bearbeiten.
3. Wählen Sie **Proxy-Modus aktivieren** aus.




4. Um die privaten IP-Adressen der Systeme an Ihren Niederlassungsstandorten zu nutzen, die Datenverkehr an den expliziten Proxy weiterleiten, wählen Sie **Quell-IP-basierte Sichtbarkeit und Durchsetzung** aus.

   Für diese Funktionalität gelten folgende Anforderungen:

   - Eine minimale Prisma Access-Dataplane von 10.2.4
   - Eine Prisma Access (Managed by Panorama)-Bereitstellung mit einem minimalen Cloud Services-Plug-in von 4.1
   - Sie dürfen nur Remote-Netzwerkstandorte verwenden, die mit „Expliziter Proxy“ unterstützt werden.




5. Ergänzen Sie eine Richtlinie, um Datenverkehr zuzulassen, der an Anycast- und Unicast-IP in Remote-Netzwerken gebunden ist. Wenn Sie die **Transparenz und Durchsetzung der Quell-IP** aktiviert haben, verwenden Sie das Feld **Quell-IP** in den Sicherheitsrichtlinien von „Expliziter Proxy“, um den Datenverkehr abzusichern. Sie benötigen zusätzliche Richtlinien in den Remote-Netzwerken.
6. (Optional) Geben Sie unter **Authentifizierungseinstellungen** alle IP-Adressen ein, von denen unverschlüsselter HTTP- oder HTTP-Cross-Origin Resource Sharing(CORS)-

 ©2025 Palo Alto Networks, Inc.

Datenverkehr zur Authentifizierungsumgehung der **Adresse der vertrauenswürdigen Quelle** zugelassen werden soll.

Fügen Sie IP-Adressen zu Adressobjekten hinzu, die auf IP-Adressen basieren, und **ergänzen** Sie die Adressobjekte im Feld.

Geben Sie maximal 100.000 Adressen ein. Stellen Sie sicher, dass das Adressobjekt nur IP-Adressen verwendet.

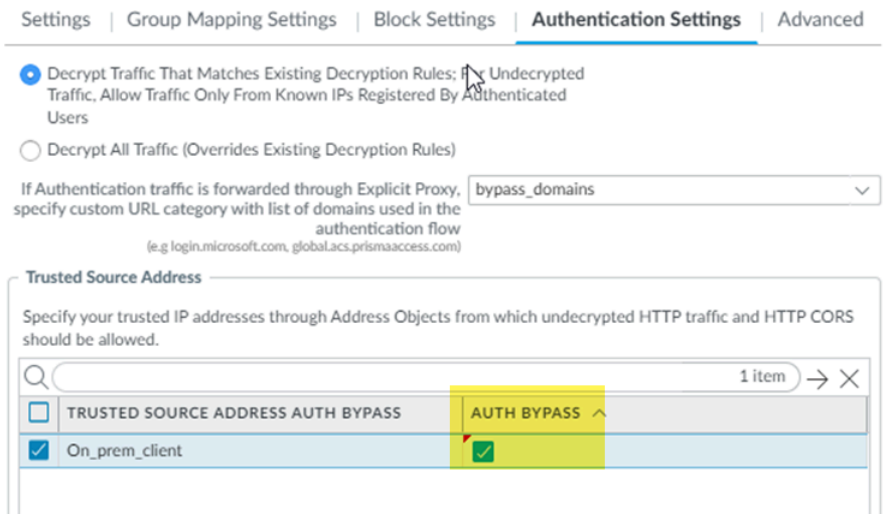
7. (Optional) Um die Authentifizierung der eingegebenen Adressen vertrauenswürdiger Quellen zu umgehen, wählen Sie **Authentifizierung umgehen** aus.

   Sie können die Option **Authentifizierung umgehen** mit der Einstellung **Quell-IP-basierte Sichtbarkeit und Durchsetzung** verwenden, um die Authentifizierung von monitorlosen Systemen zu überspringen, die sich nicht authentifizieren, keine Sicherheitsrichtlinien

 ©2025 Palo Alto Networks, Inc.

einrichten und keinen Einblick in den Datenverkehr auf Prisma Access mit explizitem Proxy erhalten können.

*Sie können entweder IP-Adressen oder Subnetze hinzufügen. Nach Erweiterung der Subnetze werden maximal 100.000 IP-Adressen unterstützt.*



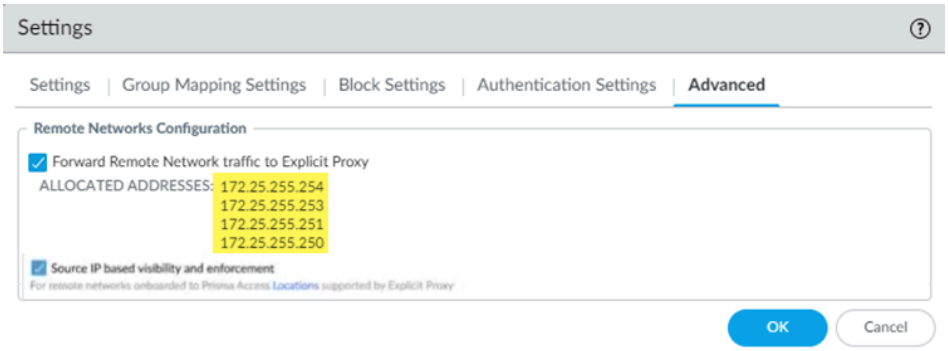

8. Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Remote-Netzwerke** aus.
9. Binden Sie Ihre Remote-Netzwerkstandorte ein, falls noch nicht geschehen.

   *Sie müssen Prisma Access-Remote-Netzwerke an den Standorten aktivieren, die von „Expliziter Proxy“ unterstützt werden.*
10. Klicken Sie auf **Commit** > **Commit und Push**.
11. Wählen Sie **Auswahl bearbeiten** aus und vergewissern Sie sich, dass auf der Registerkarte **Prisma Access** die Option **Prisma Access für Netzwerke** im Feld **Übertragungsumfang** ausgewählt wurde. Klicken Sie anschließend auf **OK**.
12. Führen Sie für Ihre Änderungen die Aktion **Commit und Push** aus.

    Sie müssen für Ihre Remote-Netzwerke einen Commit durchführen und die Änderungen per Push übertragen, damit Prisma Access die IP-Adressen abrufen kann, die in einer Bereitstellung des Typs „Expliziter Proxy“/„Remote-Netzwerk“ verwendet werden.
13. Kehren Sie zu den **Einstellungen** für „Expliziter Proxy“ zurück (**Panorama** > **Cloud Services** > **Konfiguration** > **Mobile Benutzer – Expliziter Proxy** > **Einstellungen** >

 ©2025 Palo Alto Networks, Inc.

**Erweitert**) und notieren Sie sich die **ZUGEORDNETEN ADRESSEN**, die unter **Remote-Netzwerk-Konfiguration** angezeigt werden.



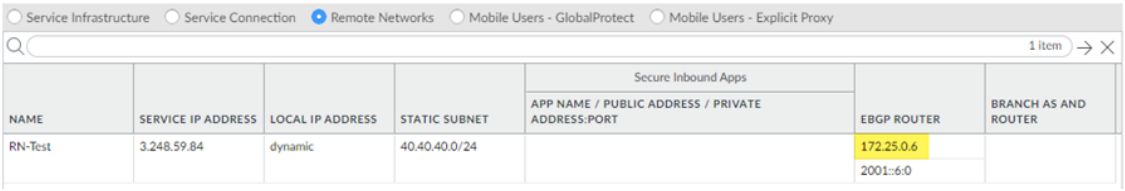

**STEP 3 |** (Optional) Suchen Sie nach der Unicast-Adresse, die Sie für Ihre Bereitstellung des Typs „Expliziter Proxy“/„Remote-Netzwerk“ verwenden möchten.

Verwenden Sie die Unicast-IP-Adresse in der PAC-Datei nur, wenn Sie ein bestimmtes Remote-Netzwerk als Ziel für die Weiterleitung von Datenverkehr an „Expliziter Proxy“ verwenden möchten. Wenn Sie alle bereitgestellten Remote-Netzwerke verwenden möchten, um Datenverkehr an „Expliziter Proxy“ weiterzuleiten, verwenden Sie die Anycast-Adressen.

1. Wählen Sie **Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Remote Netzwerke** aus.
2. Notieren Sie sich die Adresse des **EBGP-Routers**.

   Wenn IPv4- und IPv6-Adressen vorliegen, notieren Sie sich die IPv4-Adresse.

   *Diese Adresse wird auch als Loopback-Adresse bezeichnet. Wenn Sie Konfigurationsänderungen vorgenommen haben, durch die sich die EBGP-Routeradresse geändert hat, können Sie die Loopback-IP-Adresse mithilfe der Prisma Access-Legacy-API abrufen.*




**STEP 4 |** Stellen Sie sicher, dass das CPE in Ihrem Netzwerk korrekt eingerichtet ist, damit Endpunkte den Datenverkehr über die Anycast- und Unicast-IP-Adressen an „Expliziter Proxy“ weiterleiten.

## Wie der explizite Proxy Benutzer identifiziert

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |


©2025 Palo Alto Networks, Inc.

Der explizite Proxy identifiziert Benutzer in den Datenverkehrsprotokollen abhängig davon, wie sich die Benutzer beim Proxy authentifizieren (siehe die folgende Tabelle).

| Authentifizierungstyp | Benutzeridentifikation in Datenverkehrsprotokollen |
|---|---|
| Benutzer, die sich mit SAML-Authentifizierung und -Entschlüsselung anmelden | Der Benutzername. |
| Benutzer, die sich über einen anderen Proxy anmelden, der X-Authenticated-User(XAU)-Header verwendet | XAU-Header-Informationen.<br>Der explizite Proxy lässt die Verwendung von XAU zur Authentifizierung nur für Datenverkehr von bestimmten IP-Adressen zu. Sie erstellen ein Adressobjekt und geben die IP-Adressen an, für die Sie XAU für die Authentifizierung zulassen. Fügen Sie dann während der Einrichtung des expliziten Proxy das Adressobjekt im Feld **Adresse der vertrauenswürdigen Quelle** hinzu. |
| Authentifizierte Cross Origin Ressource Sharing(CORS)-Anfragen | Der Benutzer `swg-authenticated-ip-user`.<br>Ein Teil des Datenverkehrs stammt von authentifizierten Benutzern, deren Browser keine Cookies senden oder Authentifizierungsumleitungen durchführen können, wie z. B. CORS-Anfragen. In solchen Fällen fügt der explizite Proxy den Benutzer `swg-authenticated-ip-user` zu den Datenverkehrsprotokollen hinzu. |
| Unverschlüsselter Datenverkehr (wenn Sie zugelassen haben, dass der explizite Proxy unverschlüsselten Datenverkehr von IP-Adressen zulässt, bei denen sich Benutzer zuvor authentifiziert haben) | Der Benutzer `swg-authenticated-ip-user`.<br>Sie können angeben, dass der explizite Proxy unverschlüsselten Datenverkehr von IP-Adressen zulässt, bei denen sich Benutzer authentifiziert haben. Legen Sie dazu Folgendes fest: **Datenverkehr entschlüsseln, der bestehenden Entschlüsselungsregeln entspricht. Bei unverschlüsseltem Datenverkehr nur Datenverkehr von bekannten IPs zulassen, die von authentifizierten Benutzern registriert wurden,** wenn Sie den expliziten Proxy konfigurieren. In diesen Konfigurationen fügt der explizite Proxy den Benutzer `swg-authenticated-ip-user` zu den Datenverkehrsprotokollen hinzu. |
| Datenverkehr für Domänen, für die Sie die Authentifizierung umgehen möchten | Der Benutzer *swg-known-auth-bypass*.<br>Wenn Sie den expliziten Proxy einrichten, können Sie die Authentifizierung bestimmter Domänen umgehen. Der Benutzername für Datenverkehr aus diesen Domänen wird in den Protokollen als *swg-known-auth-bypass* angezeigt. |


©2025 Palo Alto Networks, Inc.

# Weiterleitungsprofile des expliziten Proxys

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access-Lizenz für mobile Benutzer |

Weiterleitungsprofile des expliziten Proxys ermöglichen es Ihnen, mithilfe mehrerer PAC-Dateien zu definieren, welcher Datenverkehr an Prisma Access weitergeleitet werden soll. Mit Weiterleitungsprofilen können Sie zudem einfach zu bedienende Weiterleitungsregeln erstellen, anstatt sich mit der Komplexität der Erstellung und Pflege einer PAC-Datei zu beschäftigen.

- Definieren mehrerer PAC-Dateien mithilfe von Weiterleitungsprofilen
- Definieren, welcher Datenverkehr mit Weiterleitungsregeln an explizite Proxys weitergeleitet werden soll
- Anhängen von Weiterleitungsprofilen an GlobalProtect App-Konfiguration

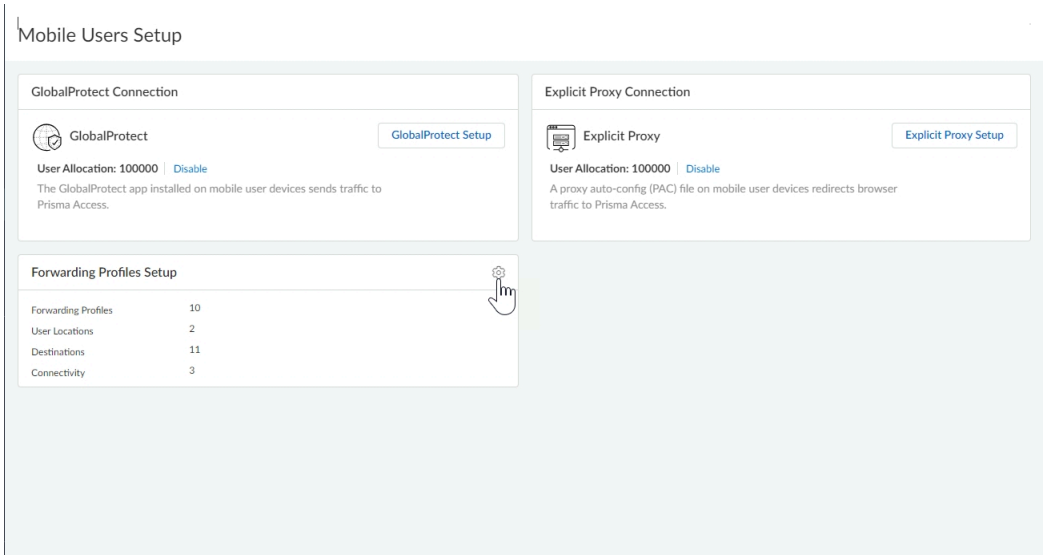
## Definieren mehrerer PAC-Dateien mithilfe von Weiterleitungsprofilen

Mit Weiterleitungsprofilen können Sie mehrere PAC-Dateien gleichzeitig in Ihrer Bereitstellung verwenden, sodass Sie definieren können, welcher Datenverkehr an Prisma Access weitergeleitet werden soll.

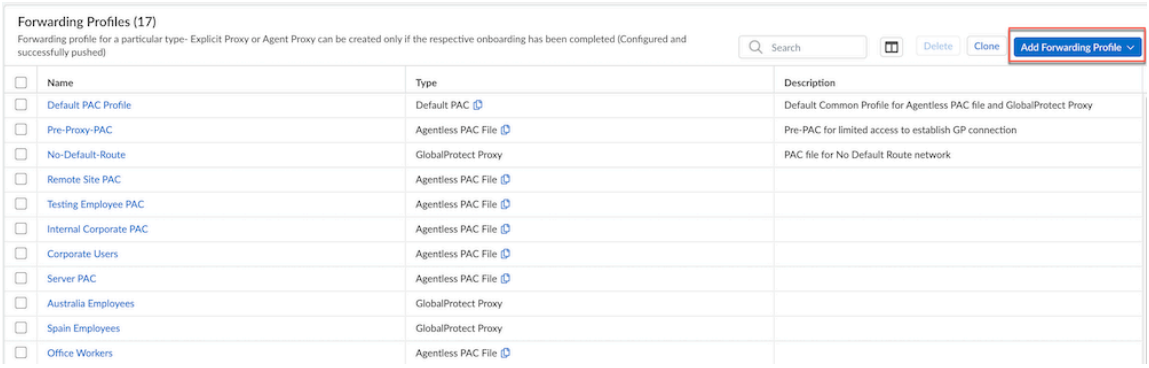

©2025 Palo Alto Networks, Inc.

**STEP 1 |** Erstellen Sie ein Weiterleitungsprofil.

1. Wählen Sie von Strata Cloud Manager aus **Workflows** > **Einrichtung Prisma Access** > **Mobile Benutzer** > **Einrichtung von Weiterleitungsprofilen** aus.




2. Klicken Sie auf **Weiterleitungsprofil hinzufügen**.



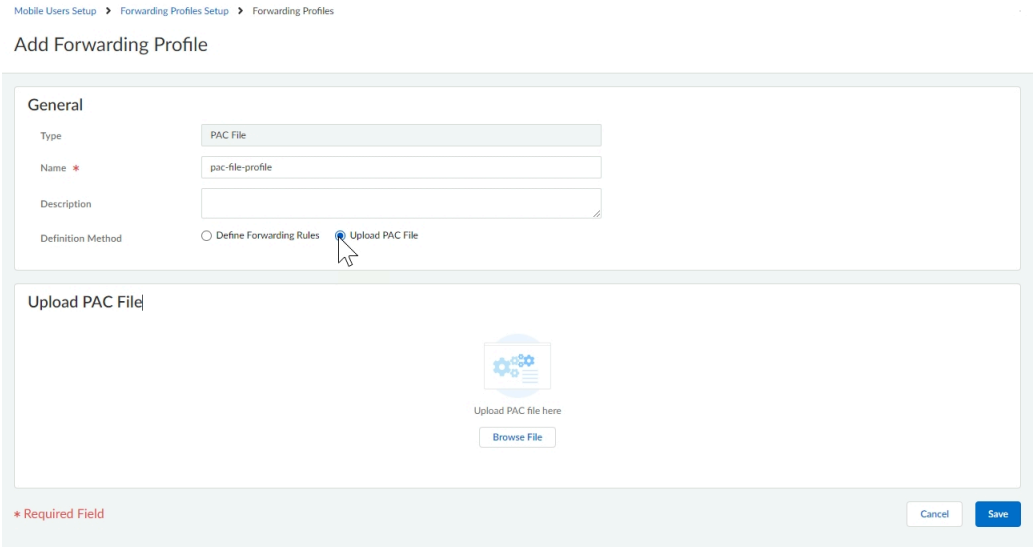

**STEP 2 |** Wählen Sie **PAC-Datei** aus.

**PAC-Datei** ist für den expliziten Proxy für Prisma Access. **GlobalProtect-Proxy** ist für die Verwendung von GlobalProtect im Proxy-Modus.

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Laden Sie eine PAC-Datei hoch.

1. Wählen Sie **PAC-Datei hochladen** aus, um eine vorhandene PAC-Datei hochzuladen, oder erstellen Sie eine PAC-Datei mithilfe der Richtlinien für PAC-Dateien.




2. Klicken Sie auf **Datei durchsuchen**, um Ihr Dateisystem nach der PAC-Datei zu durchsuchen.
3. **Speichern** Sie das Profil.

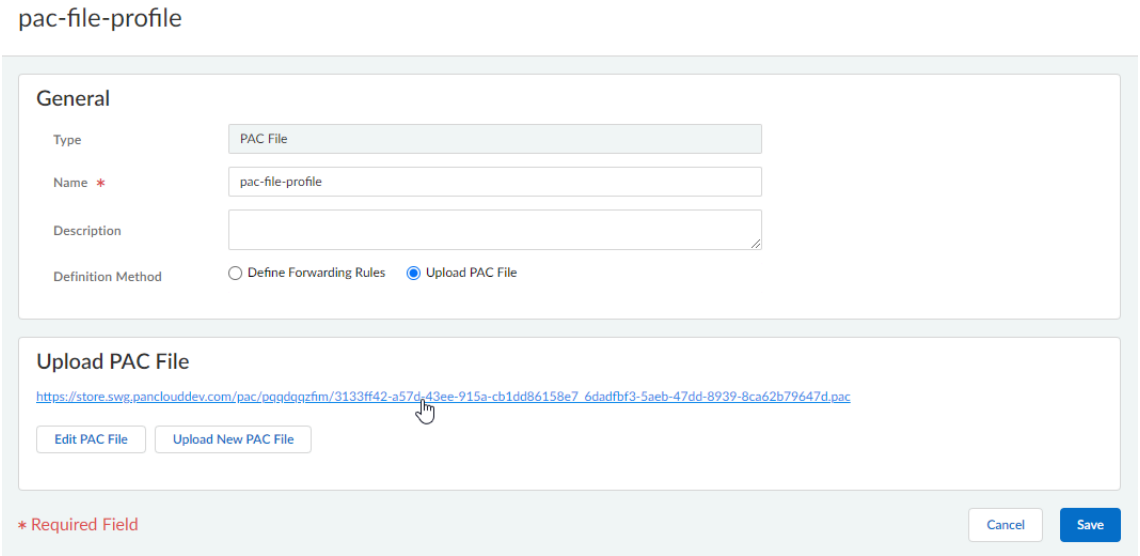
**STEP 4 |** Wiederholen Sie die beiden vorherigen Schritte, um ein weiteres Weiterleitungsprofil mit einer anderen PAC-Datei zu erstellen.

Beide PAC-Dateien werden nun gleichzeitig in Ihrer Bereitstellung verwendet.

**STEP 5 |** Rufen Sie die URL der PAC-Datei ab.

1. Kehren Sie zu dem Profil zurück, in das Sie die PAC-Datei hochgeladen haben.

   Sie sollten die URL sehen, in der die PAC-Datei gehostet wird.




 ©2025 Palo Alto Networks, Inc.

**STEP 6 |** (Optional) Bearbeiten Sie die PAC-Datei.

Um schnell Änderungen an der PAC-Datei vorzunehmen, können Sie sie direkt in der Webschnittstelle bearbeiten.

1. Klicken Sie im Weiterleitungsprofil auf **PAC-Datei bearbeiten**.
2. Nehmen Sie Änderungen vor und **speichern** Sie sie.



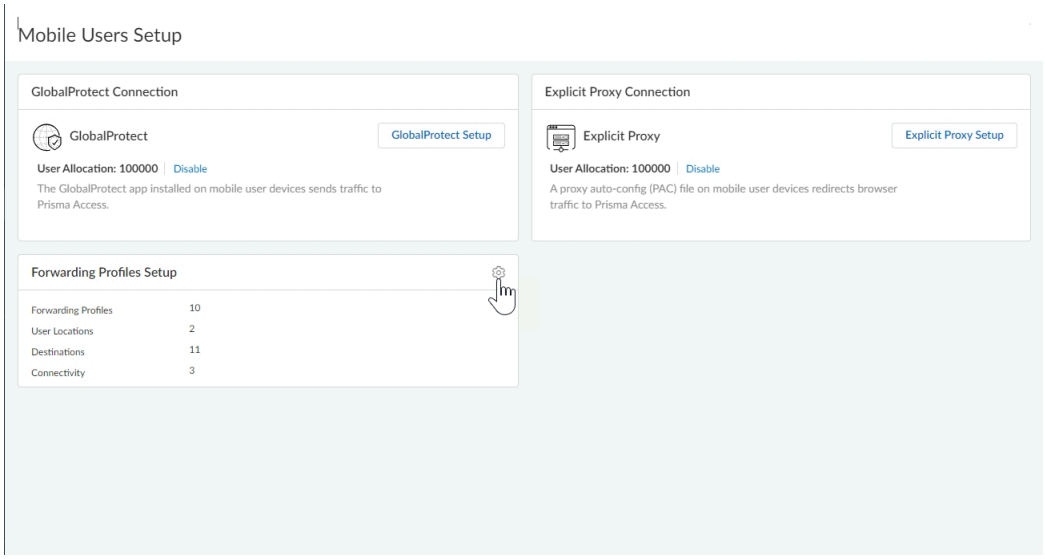

## Definieren, welcher Datenverkehr mit Weiterleitungsregeln an explizite Proxys weitergeleitet werden soll

Anstatt Ihre eigene PAC-Datei von Grund auf neu zu erstellen, können Sie einfache Weiterleitungsregeln erstellen, um eine PAC-Datei zu generieren.

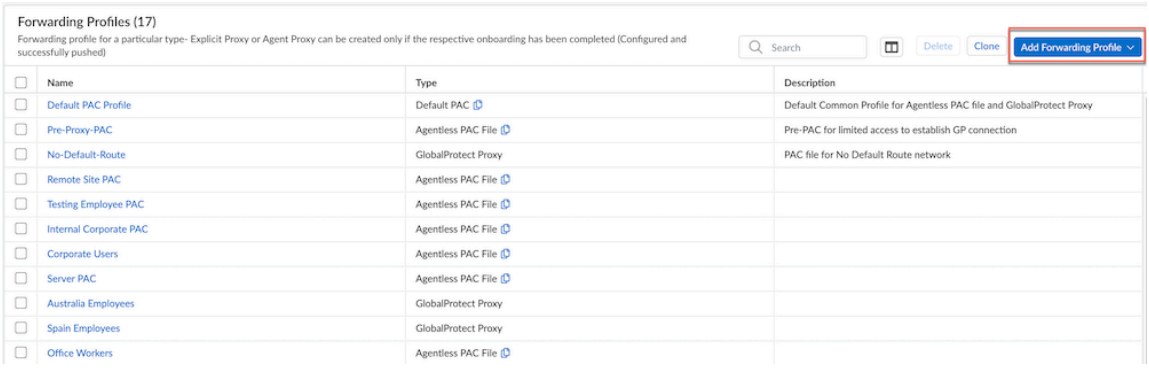
 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** Erstellen Sie ein Weiterleitungsprofil.

1. Wählen Sie von Strata Cloud Manager aus **Workflows** > **Einrichtung Prisma Access** > **Mobile Benutzer** > **Einrichtung von Weiterleitungsprofilen** aus.




2. Klicken Sie auf **Weiterleitungsprofil hinzufügen**.



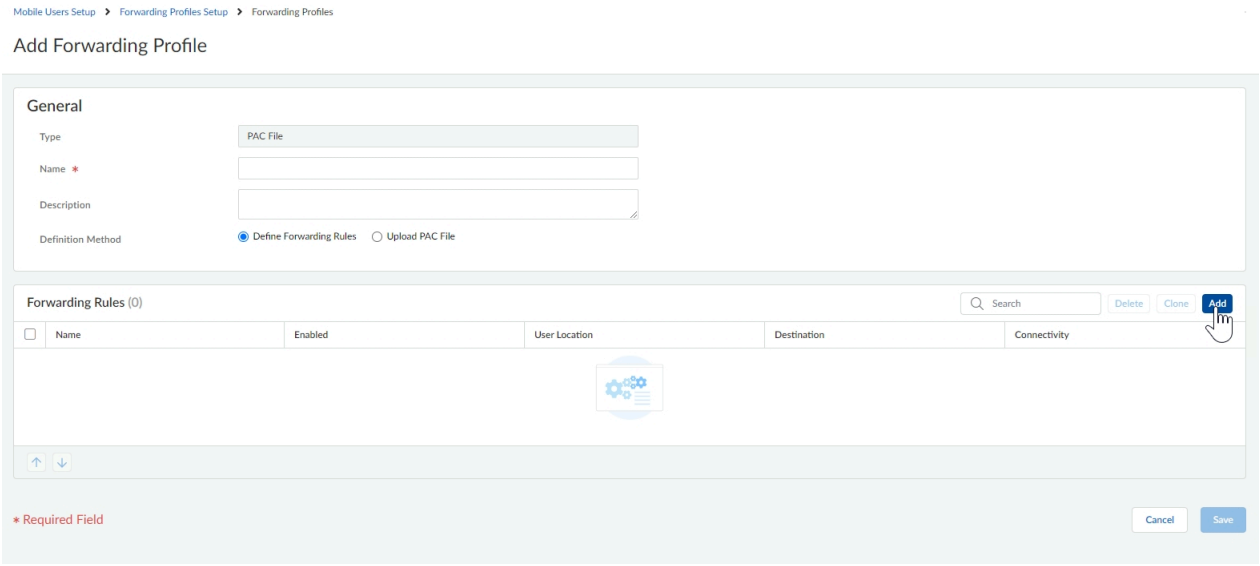

**STEP 2 |** Wählen Sie **PAC-Datei** aus.

**PAC-Datei** ist für den expliziten Proxy für Prisma Access. **GlobalProtect-Proxy** ist für die Verwendung von GlobalProtect im Proxy-Modus.

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Fügen Sie eine Weiterleitungsregel hinzu.

1. Wählen Sie **Hinzufügen** aus.




2. Füllen Sie die erforderlichen Felder aus:

| | |
|---|---|
| Name | Name des Profils. |
| Benutzerstandorte | Standort der Benutzer, für die Sie die Weiterleitungsregel erstellen. Sie können benutzerdefinierte Standorte über **Workflows** > **Einrichtung Prisma Access** > **Mobile Benutzer** > **Einrichtung von Weiterleitungsprofilen**<br><br>> **Benutzerstandorte** erstellen.<br><br>*Sie können keine Platzhalterzeichen verwenden, wenn Sie benutzerdefinierte Benutzerstandorte basierend auf der IP-Adresse konfigurieren.* |
| Ziele | Ziel des Webdatenverkehrs. Sie können aus vordefinierten Zielen auswählen oder Sie können benutzerdefinierte Ziele über **Workflows** > **Einrichtung Prisma Access** > **Mobile Benutzer** > **Einrichtung von Weiterleitungsprofilen**<br><br>> **Ziele** erstellen. |

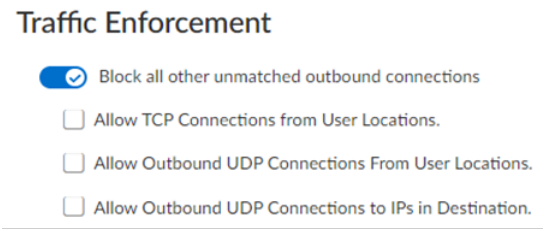
 ©2025 Palo Alto Networks, Inc.

| | |
|---|---|
| Konnektivität | **Direkt** bewirkt, dass der Datenverkehr den Proxy umgeht.<br>**Global Proxy** bewirkt, dass der Datenverkehr über den Proxy läuft. |

3. Wählen Sie **Hinzufügen** aus, wenn Sie fertig sind.
4. Aktivieren Sie **Datenverkehrsüberwachung**, wenn Sie den gesamten ausgehenden Datenverkehr (z. B. UDP) blockieren möchten, der den Weiterleitungsregeln nicht entspricht. Diese Option erfordert GlobalProtect Agent Version 6.3.1 und ist standardmäßig deaktiviert. Wenn Sie Anwendungen haben, in denen Sie UDP-Verbindungen zulassen müssen, können Sie diese Ausnahmen mithilfe von **Benutzerstandort**- oder **Ziel**-Objekten hinzufügen.

   Sie können Ihre Blockieraktionen wie folgt anpassen:

   - Blockieren Sie alle ausgehenden UDP-Verbindungen von den Endpunkten.
   - Erlauben Sie TCP von bestimmten Standorten. Sie können beispielsweise den gesamten TCP-Datenverkehr von Ihrem Büro aus zulassen.
   - Erlauben Sie UDP von bestimmten Standorten. Sie können beispielsweise den gesamten TCP-Datenverkehr von Ihrem Büro aus zulassen.
   - Wenn bestimmte Anwendungen UDP-Verbindungen benötigen, können Sie ausgehende UDP-Verbindungen zu bestimmten Zielen zulassen.

5. **Speichern** Sie das Profil mit der von Ihnen erstellten Weiterleitungsregel.

   Das Profil wird in Ihrer Liste der Weiterleitungsprofile angezeigt. Beim Öffnen wird eine URL zur PAC-Datei angezeigt, die aus der Regel generiert wurde. **Zeigen Sie die PAC-Datei an**, um ihren Inhalt zu sehen.

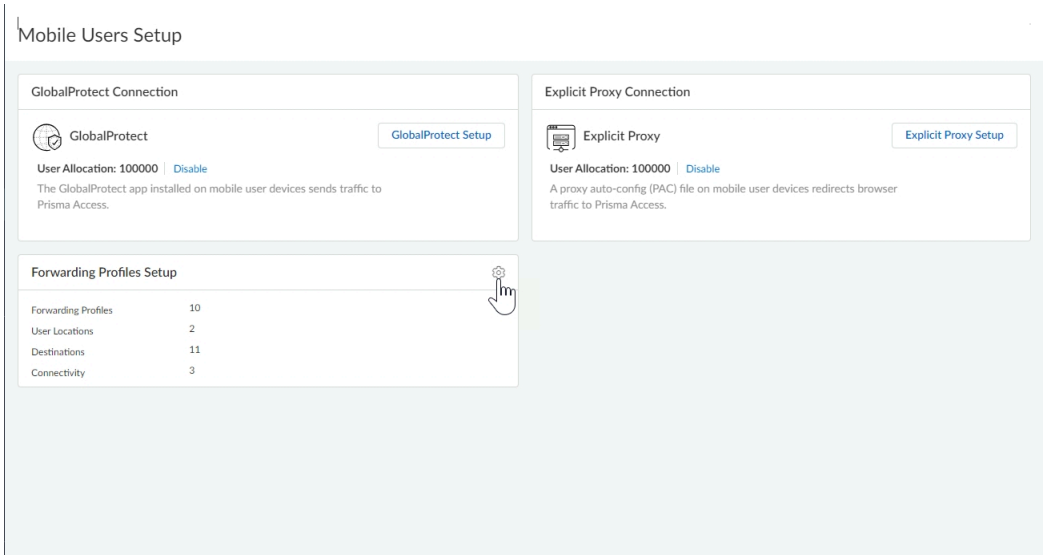
## Anhängen von Weiterleitungsprofilen an GlobalProtect App-Konfiguration

Sie können Weiterleitungsprofile verwenden, um die Konfiguration Ihres GlobalProtect-App-Proxys zu vereinfachen.

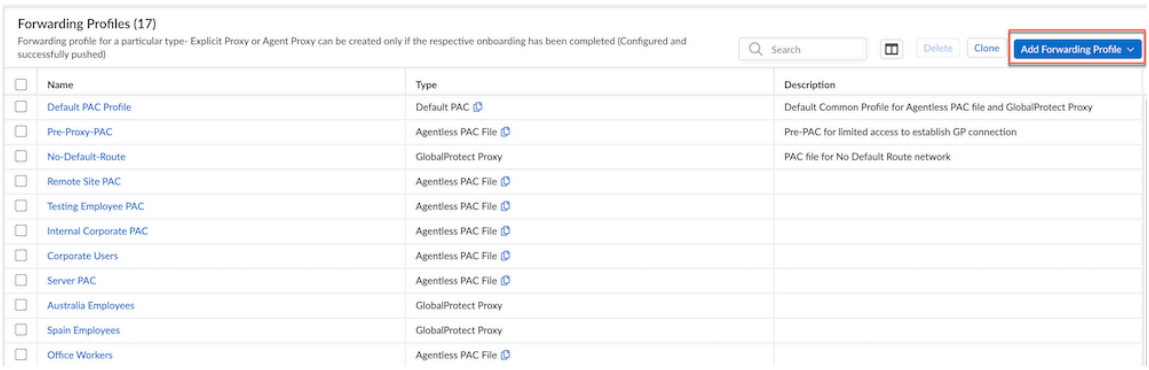

©2025 Palo Alto Networks, Inc.

**STEP 1 |** Erstellen Sie ein Weiterleitungsprofil.

1. Wählen Sie von Strata Cloud Manager aus **Workflows** > **Einrichtung Prisma Access** > **Mobile Benutzer** > **Einrichtung von Weiterleitungsprofilen** aus.




2. Klicken Sie auf **Weiterleitungsprofil hinzufügen**.



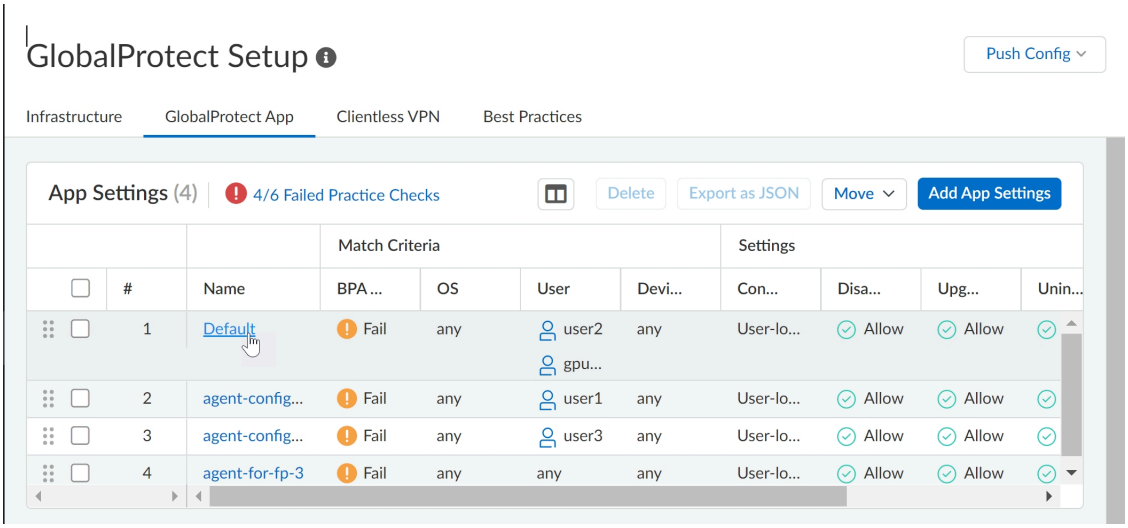

**STEP 2 |** Wählen Sie **GlobalProtect-Proxy** aus.

**STEP 3 |** Konfigurieren Sie das Weiterleitungsprofil durch Hochladen einer PAC-Datei oder Erstellen von Weiterleitungsregeln.

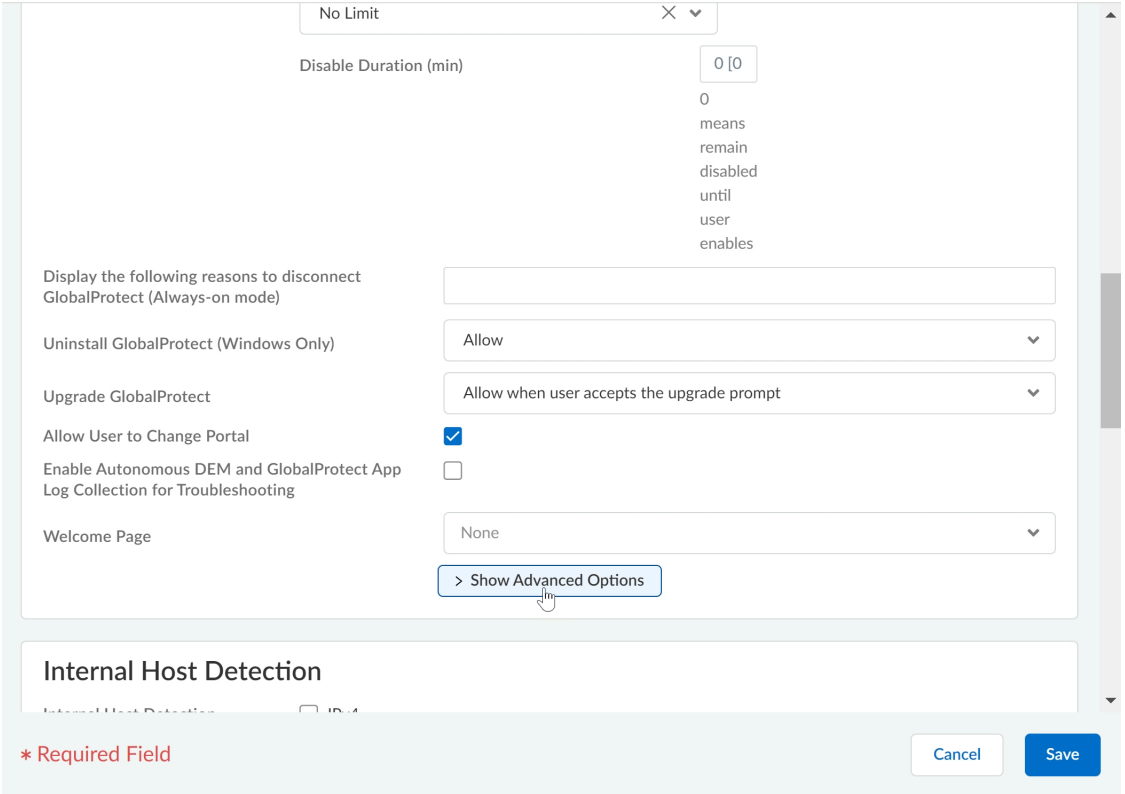
 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** Fügen Sie Ihrer GlobalProtect app-Proxykonfiguration das Weiterleitungsprofil hinzu.

1. Wählen Sie **Workflows** > **Einrichtung Prisma Access** > **GlobalProtect** > **GlobalProtect-App** aus.
2. Wählen Sie eine Konfigurationsdatei aus.




3. Klicken Sie unter „App-Konfiguration“ auf **Erweiterte Optionen anzeigen**.

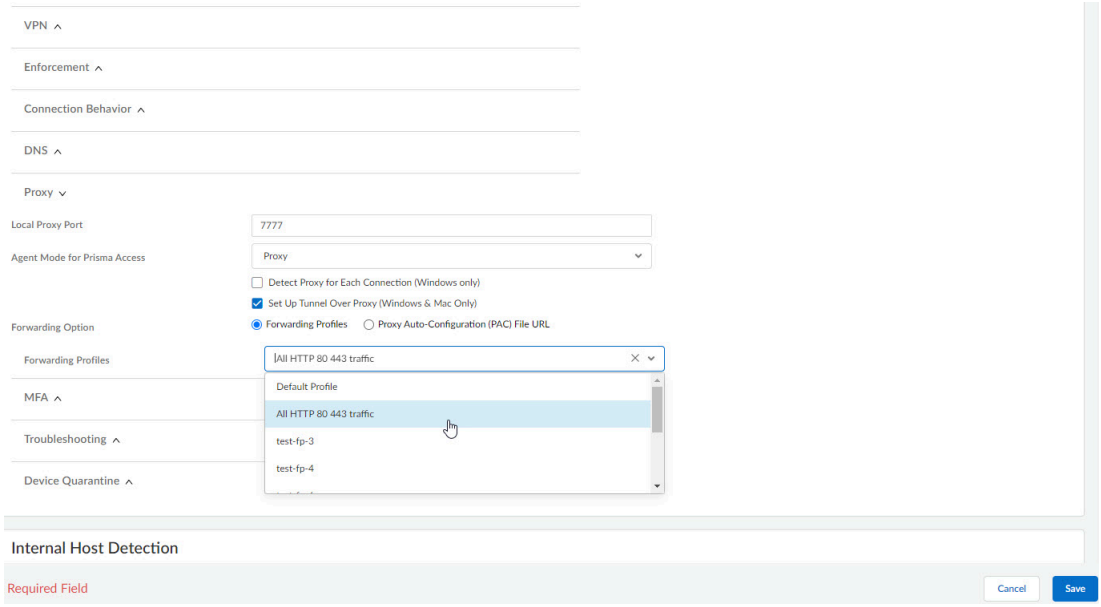



4. Erweitern Sie die Einstellungen für **Proxy**.
5. Wählen Sie je nach GlobalProtect Agent-Modus entweder **Proxy** oder **Tunnel und Proxy** aus.

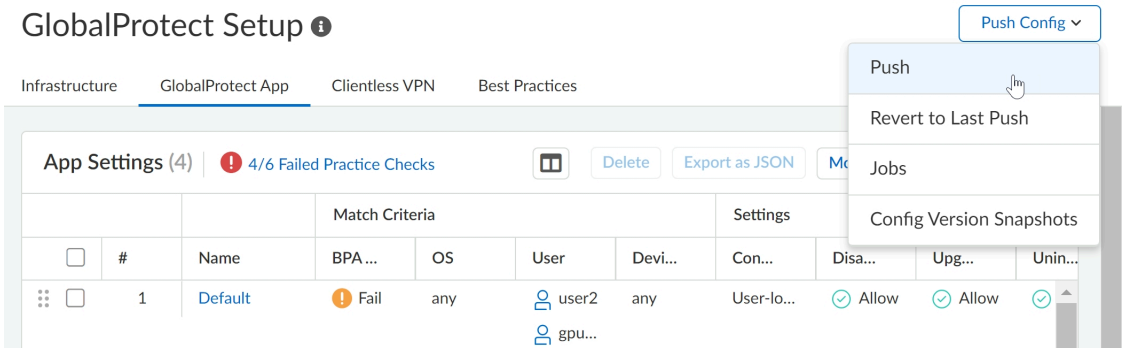
 ©2025 Palo Alto Networks, Inc.

*Sie können kein Weiterleitungsprofil hinzufügen, wenn Sie den Modus **Tunnel** auswählen.*

6. Wählen Sie **Weiterleitungsprofile** und dann das gewünschte Weiterleitungsprofil aus.




7. **Save (Speichern)** Sie Ihre Änderungen.
8. Wählen Sie **Konfiguration übertragen** > **Push** aus.




# Richtlinien für PAC-Dateien

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

- Strata Cloud Manager
- Panorama


©2025 Palo Alto Networks, Inc.

## Richtlinien für PAC-Dateien (Strata Cloud Manager)

Beachten Sie beim Konfigurieren der PAC-Datei zur Verwendung mit „Expliziter Proxy“ die folgenden Richtlinien und Anforderungen:

- Beachten Sie, dass der Agent bei Verwendung des GlobalProtect Agent im Proxy-Modus die PAC-Datei an Ihre Hosts verteilt. Der Agent greift über HTTPS auf die PAC-Datei zu. Die PAC-Datei ist öffentlich.
- PAC-Dateien leiten den Benutzerdatenverkehr an „Expliziter Proxy“.
- Sie können nur eine PAC-Datei für die Verwendung mit Prisma Access hosten, und die PAC-Datei von „Expliziter Proxy“ wird in den Vereinigten Staaten gehostet. Wenn Sie einen alternativen PAC-Dateizugriff außerhalb der USA benötigen, können Sie die PAC-Datei in Ihrem Unternehmen hosten.
- Um auf die PAC-Datei zuzugreifen, müssen Sie sicherstellen, dass Ihre Endpunkte die folgenden IP-Adressen erreichen können:
  - 34.111.7.85
  - 34.160.172.204
  - 34.110.206.116
  - 34.95.107.244
  - 34.149.8.36

  *Wenn Sie mit einem Netzwerk ohne Standardroute arbeiten, müssen Sie Routen für diese IP-Adressen hinzufügen, um auf die PAC-Datei zuzugreifen.*
- Für PAC-Dateien wird nur das ASCII-Textformat unterstützt. Palo Alto Networks empfiehlt, die PAC-Datei in einem Texteditor wie VI oder Vim zu erstellen und zu speichern.
- Nachdem Sie Ihre Konfiguration für expliziten Proxy erstellt und Ihre Änderungen festgeschrieben und per Push übertragen haben, laden Sie Ihre PAC-Datei hoch oder geben Sie Ihre PAC-Konfiguration im PAC-Datei-Editor an.
- Am Anfang der Anweisung `return"PROXY foo.proxy.prismaaccess.com:8080";` muss mindestens eine URL für den expliziten Proxy für den in Prisma Access eingehenden Datenverkehr vorhanden sein. Verwenden Sie entweder eine konfigurierte Domäne, die beim Übertragen Ihrer Änderungen per Push verwendet wird, oder verwenden Sie eine gültige IPv4-Adresse oder ein DIRECT-Schlüsselwort wie `PROXY paloaltonetworks-245139.proxy.prismaaccess.com:8080` oder `PROXY 1.2.3.4:8080` usw.
- Wenn der Proxy nicht umgangen wird, müssen Sie ein PROXY-Schlüsselwort angeben. Eine gültige Proxy-Anweisung ist erforderlich, wenn kein `DIRECT`-Schlüsselwort für die Proxy-Umgehung konfiguriert ist.
- Wenn eine gültige PROXY-Anweisung vor einer ungültigen PROXY-Anweisung gefunden wird, überspringt „Expliziter Proxy“ die Gültigkeitsprüfung für alle PROXY-Anweisungen nach der ersten. Beispielsweise würde eine PAC-Datei mit der gültigen Anweisung `PROXY paloaltonetworks-245139.proxy.prismaaccess.com:8080` gefolgt von der ungültigen Anweisung `PROXY foo.proxy.prismaacess.com:8080` als gültig angesehen, da der explizite Proxy die Gültigkeitsprüfung für `foo.proxy.prismaacess.com:8080` überspringt.

 ©2025 Palo Alto Networks, Inc.

- Wenn Sie eine PROXY-Anweisung verwenden, damit ACS-Datenverkehr den Prisma Access-Proxy umgeht, darf die PROXY-Anweisung nicht die URL des expliziten Proxy verwenden. In dieser Konfiguration gibt „Expliziter Proxy“ eine Fehlermeldung aus, ermöglicht Ihnen jedoch das Hochladen der PAC-Datei. Sie können den ACS-Datenverkehr mit einem gültigen FQDN oder einer gültigen IPv4-Adresse an andere Proxys oder mit dem Schlüsselwort `DIRECT` direkt an das Internet weiterleiten.
- In PROXY-Anweisungen werden nur IPv4-Adressen unterstützt. Verwenden Sie keine IPv6-Adressen in PROXY-Anweisungen.
- Die maximale Dateigröße für eine PAC-Datei beträgt 750 KB.
- Wenn ACS/IdP-Datenverkehr „Expliziter Proxy“ durchlaufen muss, fügen Sie diese Domänen einer Authentifizierungsumgehungsliste und einer Richtlinienregel „Keine Entschlüsselung“ hinzu.
- Wenn Sie „Expliziter Proxy“ in einer Umgebung mit Standardroute einrichten, müssen Sie die Portal-, Gateway- und SAML-FQDNs ausschließen. Sie können die PAC-Datei verwenden, um die FQDNs zu umgehen.
- Sie können eine PAC-Datei nach dem Hochladen nicht mehr löschen. Sie können jedoch eine neue PAC-Datei hochladen oder sie im PAC-Dateieditor bearbeiten, um die vorhandene Datei zu überschreiben.

„Expliziter Proxy“ stellt Ihnen eine Beispiel-PAC-Datei bereit, die Sie ändern und als PAC-Datei für Ihre Bereitstellung des Typs „Expliziter Proxy“ verwenden können. Die Beispiel-PAC-Datei, die Prisma Access bereitstellt, enthält die folgenden Daten:

```
function FindProxyForURL(url, host) { /* Bypass localhost and Private
 IPs */ var resolved_ip = dnsResolve(host); if (isPlainHostName(host)
 || shExpMatch(host, "*.local") || isInNet(resolved_ip, "10.0.0.0",
 "255.0.0.0") || isInNet(resolved_ip, "172.16.0.0", "255.240.0.0")
 || isInNet(resolved_ip, "192.168.0.0", "255.255.0.0") ||
 isInNet(resolved_ip, "127.0.0.0", "255.255.255.0")) return
 "DIRECT"; /* Bypass FTP */ if (url.substring(0,4) == "ftp:")
 return "DIRECT"; /* Bypass SAML, e.g. Okta */ if (shExpMatch(host,
 "*.okta.com") || shExpMatch(host, "*.oktacdn.com"))
 return "DIRECT"; /* Bypass ACS */ if (shExpMatch(host,
 "*.acs.prismaaccess.com")) return "DIRECT"; /* Forward to Prisma
 Access */ return "PROXY foo.proxy.prismaaccess.com:8080";
```

Wenn Sie die Standard-PAC-Datei verwenden möchten, die Prisma Access bereitstellt, können Sie die Felder in der PAC-Datei optional wie in der folgenden Tabelle beschrieben ändern.

| Text | Beschreibung |
|---|---|
| `var resolved_ip = dnsResolve(hos t); ... return "DIRECT";` | Wenn Sie die Daten in dieser Datei nicht ändern, wird „Expliziter Proxy“ von den folgenden Hostnamen und IP-Adressen umgangen:<br>• `if (isPlainHostName(host)` – „Expliziter Proxy“ wird für Hostnamen, die keine Punkte enthalten (z. B. http://intranet), umgangen. |

 ©2025 Palo Alto Networks, Inc.

| Text | Beschreibung |
| --- | --- |
| | • `shExpMatch(host, "*.local") ||` – Der Proxy wird für alle Hostnamen, die im internen Netzwerk (localhost) gehostet werden, umgangen.<br>• `isInNet(resolved_ip, "10.0.0.0", "255.0.0.0") || isInNet(resolved_ip, "172.16.0.0", "255.240.0.0") || isInNet(resolved_ip, "192.168.0.0", "255.255.0.0") || isInNet(resolved_ip, "127.0.0.0", "255.255.255.0"))` – „Expliziter Proxy“ wird für alle IP-Adressen, die sich im privaten oder Loopback-IP-Adressbereich befinden, umgangen. |
| `if (url.substring(0,4) == "ftp:" ) return "DIRECT";` | „Expliziter Proxy“ wird für FTP-Sitzungen umgangen. |
| `if (shExpMatch(host, "*.okta.com ") || shExpMatch(host, "*.oktacd n.com")) return "DIRECT";` | „Expliziter Proxy“ wird für SAML-IdP umgangen. Vergewissern Sie sich, dass Sie alle vom IdP verwendeten FQDNs hinzufügen.<br>Wenn Sie Okta als IdP für die SAML-Authentifizierung verwenden, geben Sie **`*.okta.com`** und **`*.oktacdn.com`**ein. |
| `if (shExpMatch(host, "*.acs.pri smaaccess.com")) return "DIRECT ";` | „Expliziter Proxy“ wird für den Prisma Access-Authentifizierungs-Cache-Dienst (ACS) umgangen.<br>Anstatt ein Platzhalterzeichen zu verwenden, können Sie den spezifischen **ACS-FQDN** für Ihre Bereitstellung hinzufügen. Suchen Sie diesen FQDN unter **Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Mobile Benutzer – Expliziter Proxy** > **ACS-FQDN**. |
| `return "PROXY foo.proxy.prismaac cess.com:8080"` | „Expliziter Proxy“ wird für die URL des expliziten Proxy umgangen.<br>In der Anweisung `return"PROXY foo.proxy.prismaaccess.com:8080";` muss mindestens eine URL für den expliziten Proxy für den in Prisma Access eingehenden Datenverkehr vorhanden sein. Verwenden Sie entweder eine konfigurierte Domäne, die beim Übertragen Ihrer Änderungen per |

 ©2025 Palo Alto Networks, Inc.

| Text | Beschreibung |
| --- | --- |
| | Push verwendet wird, oder verwenden Sie eine gültige IPv4-Adresse oder ein DIRECT-Schlüsselwort wie PROXY `paloaltonetworks-245139.proxy.prismaaccess.c` oder PROXY `1.2.3.4:8080`. |

## Richtlinien für PAC-Dateien (Panorama)

Beachten Sie beim Konfigurieren der PAC-Datei zur Verwendung mit „Expliziter Proxy“ die folgenden Richtlinien und Anforderungen:

- Beachten Sie, dass der Agent bei Verwendung des GlobalProtect Agent im Proxy-Modus die PAC-Datei an Ihre Hosts verteilt. Der Agent greift über HTTPS auf die PAC-Datei zu. Die PAC-Datei ist öffentlich.
- PAC-Dateien leiten den Benutzerdatenverkehr an „Expliziter Proxy“.
- Sie können nur eine PAC-Datei für die Verwendung mit Prisma Access hosten, und die PAC-Datei von „Expliziter Proxy“ wird in den Vereinigten Staaten gehostet. Wenn Sie einen alternativen PAC-Dateizugriff außerhalb der USA benötigen, können Sie die PAC-Datei in Ihrem Unternehmen hosten.
- Um auf die PAC-Datei zuzugreifen, müssen Sie sicherstellen, dass Ihre Endpunkte die folgenden IP-Adressen erreichen können:
  - 34.111.7.85
  - 34.160.172.204
  - 34.110.206.116
  - 34.95.107.244
  - 34.149.8.36
- Für PAC-Dateien wird nur das ASCII-Textformat unterstützt. Palo Alto Networks empfiehlt, die PAC-Datei in einem Texteditor wie VI oder Vim zu erstellen und zu speichern.
- Laden Sie die PAC-Datei hoch, nachdem Sie Ihre Konfiguration für „Expliziter Proxy“ erstellt und Ihre Änderungen festgeschrieben und per Push übertragen haben. Nachdem Sie Ihre PAC-Datei hochgeladen haben, ist ein Festschreiben und Übertragen der Änderungen per Push nicht mehr möglich.
- Am Anfang der Anweisung `return"PROXY foo.proxy.prismaaccess.com:8080";` muss mindestens eine URL für den expliziten Proxy für den in Prisma Access eingehenden Datenverkehr vorhanden sein. Verwenden Sie entweder eine konfigurierte Domäne, die beim Übertragen Ihrer Änderungen per Push verwendet wird, oder verwenden Sie eine gültige IPv4-Adresse oder ein DIRECT-Schlüsselwort wie PROXY `paloaltonetworks-245139.proxy.prismaaccess.com:8080` oder PROXY `1.2.3.4:8080` usw.
- Wenn der Proxy nicht umgangen wird, müssen Sie ein PROXY-Schlüsselwort angeben. Eine gültige Proxy-Anweisung ist erforderlich, wenn kein `DIRECT`-Schlüsselwort für die Proxy-Umgehung konfiguriert ist.

 ©2025 Palo Alto Networks, Inc.

- Wenn eine gültige PROXY-Anweisung vor einer ungültigen PROXY-Anweisung gefunden wird, überspringt „Expliziter Proxy“ die Gültigkeitsprüfung für alle PROXY-Anweisungen nach der ersten. Beispielsweise würde eine PAC-Datei mit der gültigen Anweisung PROXY `paloaltonetworks-245139.proxy.prismaaccess.com:8080` gefolgt von der ungültigen Anweisung PROXY `foo.proxy.prismaaccess.com:8080` als gültig angesehen, da der explizite Proxy die Gültigkeitsprüfung für `foo.proxy.prismaaccess.com:8080` überspringt.
- Wenn Sie eine PROXY-Anweisung verwenden, damit ACS-Datenverkehr den Prisma Access-Proxy umgeht, darf die PROXY-Anweisung nicht die URL des expliziten Proxy verwenden. In dieser Konfiguration gibt „Expliziter Proxy“ eine Fehlermeldung aus, ermöglicht Ihnen jedoch das Hochladen der PAC-Datei. Sie können den ACS-Datenverkehr mit einem gültigen FQDN oder einer gültigen IPv4-Adresse an andere Proxys oder mit dem Schlüsselwort `DIRECT` direkt an das Internet weiterleiten.
- In PROXY-Anweisungen werden nur IPv4-Adressen unterstützt. Verwenden Sie keine IPv6-Adressen in PROXY-Anweisungen.
- Die maximale Dateigröße für eine PAC-Datei beträgt 256 KB.
- Wenn ACS/IdP-Datenverkehr „Expliziter Proxy“ durchlaufen muss, fügen Sie diese Domänen einer Authentifizierungsumgehungsliste und einer Richtlinienregel „Keine Entschlüsselung“ hinzu.
- Wenn Sie „Expliziter Proxy“ in einer Umgebung mit Standardroute einrichten, müssen Sie die Portal-, Gateway- und SAML-FQDNs ausschließen. Sie können die PAC-Datei verwenden, um die FQDNs zu umgehen.
- Sie können eine PAC-Datei nach dem Hochladen nicht mehr löschen. Sie können jedoch eine neue PAC-Datei hochladen, um die vorhandene Datei zu überschreiben.
- Wenn Sie die URL des expliziten Proxy in Prisma Access ändern, aber die PAC-Datei unverändert lassen, um die Änderung widerzuspiegeln, wird die Änderung nicht angewendet. Sie müssen eine neue PAC-Datei hochladen, die die neue URL des expliziten Proxy angibt.

„Expliziter Proxy“ stellt Ihnen eine Beispiel-PAC-Datei bereit, die Sie ändern und als PAC-Datei für Ihre Bereitstellung des Typs „Expliziter Proxy“ verwenden können. Die Beispiel-PAC-Datei, die Prisma Access bereitstellt, enthält die folgenden Daten:

```
function FindProxyForURL(url, host) { /* Bypass localhost and Private
 IPs */ var resolved_ip = dnsResolve(host); if (isPlainHostName(host)
 || shExpMatch(host, "*.local") || isInNet(resolved_ip, "10.0.0.0",
 "255.0.0.0") || isInNet(resolved_ip, "172.16.0.0", "255.240.0.0")
 || isInNet(resolved_ip, "192.168.0.0", "255.255.0.0") ||
 isInNet(resolved_ip, "127.0.0.0", "255.255.255.0")) return
 "DIRECT"; /* Bypass FTP */ if (url.substring(0,4) == "ftp:")
 return "DIRECT"; /* Bypass SAML, e.g. Okta */ if (shExpMatch(host,
 "*.okta.com") || shExpMatch(host, "*.oktacdn.com"))
 return "DIRECT"; /* Bypass ACS */ if (shExpMatch(host,
 "*.acs.prismaaccess.com")) return "DIRECT"; /* Forward to Prisma
 Access */ return "PROXY foo.proxy.prismaaccess.com:8080";
```

Wenn Sie die Standard-PAC-Datei verwenden möchten, die Prisma Access bereitstellt, können Sie die Felder in der PAC-Datei optional wie in der folgenden Tabelle beschrieben ändern.

 ©2025 Palo Alto Networks, Inc.

| Text | Beschreibung |
| --- | --- |
| `var resolved_ip = dnsResolve(host); ... return "DIRECT";` | Wenn Sie die Daten in dieser Datei nicht ändern, wird „Expliziter Proxy“ von den folgenden Hostnamen und IP-Adressen umgangen:<br>• `if (isPlainHostName(host)` – „Expliziter Proxy“ wird für Hostnamen, die keine Punkte enthalten (z. B. http://intranet), umgangen.<br>• `shExpMatch(host, "*.local") ||` – Der Proxy wird für alle Hostnamen, die im internen Netzwerk (localhost) gehostet werden, umgangen.<br>• `isInNet(resolved_ip, "10.0.0.0", "255.0.0.0") || isInNet(resolved_ip, "172.16.0.0", "255.240.0.0") || isInNet(resolved_ip, "192.168.0.0", "255.255.0.0") || isInNet(resolved_ip, "127.0.0.0", "255.255.255.0"))` – „Expliziter Proxy“ wird für alle IP-Adressen, die sich im privaten oder Loopback-IP-Adressbereich befinden, umgangen. |
| `if (url.substring(0,4) == "ftp:") return "DIRECT";` | „Expliziter Proxy“ wird für FTP-Sitzungen umgangen. |
| `if (shExpMatch(host, "*.okta.com") \|\| shExpMatch(host, "*.oktacdn.com")) return "DIRECT";` | „Expliziter Proxy“ wird für SAML-IdP umgangen. Vergewissern Sie sich, dass Sie alle vom IdP verwendeten FQDNs hinzufügen.<br>Wenn Sie Okta als IdP für die SAML-Authentifizierung verwenden, geben Sie **`*.okta.com`** und **`*.oktacdn.com`**ein. |
| `if (shExpMatch(host, "*.acs.prismaaccess.com")) return "DIRECT";` | „Expliziter Proxy“ wird für den Prisma Access-Authentifizierungs-Cache-Dienst (ACS) umgangen.<br>Anstatt ein Platzhalterzeichen zu verwenden, können Sie den spezifischen **ACS-FQDN** für Ihre Bereitstellung hinzufügen. Suchen Sie diesen FQDN unter **Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Mobile Benutzer – Expliziter Proxy** > **ACS-FQDN**. |


©2025 Palo Alto Networks, Inc.

| Text | Beschreibung |
| --- | --- |
| `return "PROXY foo.proxy.prismaaccess.com:8080"` | „Expliziter Proxy“ wird für die URL des expliziten Proxy umgangen.<br>In der Anweisung `return"PROXY foo.proxy.prismaaccess.com:8080";` muss mindestens eine URL für den expliziten Proxy für den in Prisma Access eingehenden Datenverkehr vorhanden sein. Verwenden Sie entweder eine konfigurierte Domäne, die beim Übertragen Ihrer Änderungen per Push verwendet wird, oder verwenden Sie eine gültige IPv4-Adresse oder ein DIRECT-Schlüsselwort wie PROXY `paloaltonetworks-245139.proxy.prismaaccess.c` oder PROXY `1.2.3.4:8080`. |

## Expliziter Proxy – Best Practices

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

Verwenden Sie die empfohlenen Best Practices bei der Implementierung Ihrer Bereitstellung mit dem expliziten Proxy, um optimale Leistung und ideale Benutzererfahrung zu gewährleisten:

- **Allgemeine Best Practices für die Bereitstellung mit dem expliziten Proxy**:
  - Stellen Sie den expliziten Proxy aus Redundanzgründen in mindestens zwei Regionen bereit.
  - Wenn sich alle Benutzer hinter einem NAT-Gerät befinden und der explizite Proxy die IP-Adresse des NAT-Geräts als Quell-IP-Adresse ansieht, sollten Sie eine NAT-IP-Adresse pro 500 mobile Benutzer zuweisen.
  - Verwenden Sie Weiterleitungsprofile, um eine PAC-Datei zu konfigurieren.
- **Best Practices für PAC-Datei** – Umgehen Sie beim Einrichten der PAC-Datei alle URLs für SAML, CIE und Authentication Cache Service (ACS).
- **Best Practices für die SAML-Authentifizierung**:
  - Setzen Sie die **Cookie-Lebensdauer** der SAML-Authentifizierung auf 24 Stunden, um die beste Benutzererfahrung ohne Authentifizierungsunterbrechungen zu erzielen.
  - Wenn Sie GlobalProtect im Proxy-Modus oder GlobalProtect im Tunnel- und Proxy-Modus konfiguriert haben, setzen Sie die **Cookie-Lebensdauer** im GlobalProtect-Portal auf 12 Stunden.
- **Best Practices für die Kerberos-Authentifizierung** – Die Keytab-Datei sollte weniger als 60 KB groß sein.

 ©2025 Palo Alto Networks, Inc.

- **Best Practices für Sicherheitsrichtlinienregeln** – Verwenden Sie Best Practices für Sicherheitsrichtlinienregeln, indem Sie die **Aktion** in Richtlinien auf **Ablehnen** statt auf **Löschen** oder **Zurücksetzen** festlegen. Diese Aktionen helfen bei der schnellen Freigabe der Ressourcen innerhalb des Sicherheitsverarbeitungsknotens des expliziten Proxys (EP-SPN), um optimale Leistung zu gewährleisten.
- **Best Practices für die Entschlüsselung** – Konfigurieren Sie mindestens eine Entschlüsselungsrichtlinie und ein Entschlüsselungszertifikat.
- **Best Practices für IP-Quelladressen** – Um den Zugriff auf den expliziten Proxy auf bestimmte IP-Quelladressen zu beschränken, verwenden Sie spezielle Objekte, darunter Adressobjekte, Adressgruppen und externe dynamische Listen (EDLs).

# Expliziter Proxy – Überwachung und Fehlerbehebung

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

Erfahren Sie, wie Sie Ihre Prisma Access-Bereitstellung des Typs „Expliziter Proxy“ überwachen und eventuelle Fehler beheben.

- Strata Cloud Manager
- Panorama

## Expliziter Proxy (Strata Cloud Manager) – Überwachung und Fehlerbehebung

Überwachen Sie die Prisma Access-Bereitstellung des Typs „Expliziter Proxy“, um die Behebung von Problemen zu unterstützen.

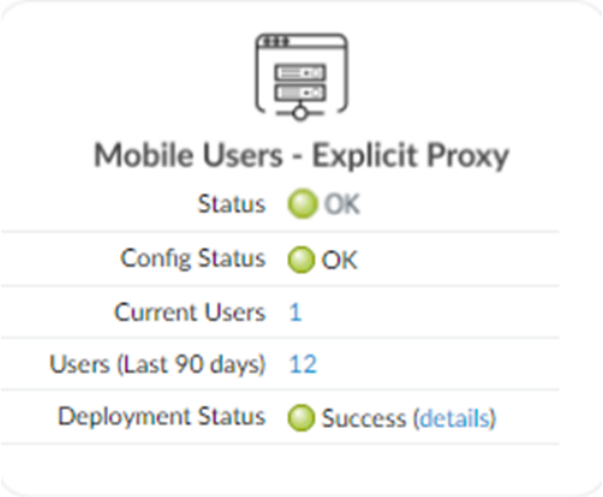
- Klicken Sie auf **Überwachen** > **Benutzer** und wählen Sie die verbundene Methode **Expliziter Proxy** aus.
- Wählen Sie **Überwachen** > **Benutzer** und anschließend die Verbindungsmethode **Expliziter Proxy** aus, um mobile Benutzer anzuzeigen, die über „Expliziter Proxy“ in einem Webbrowser auf ihren Geräten eine Verbindung zu Prisma Access-Sicherheitsdiensten herstellen.
- Wählen Sie **Überwachen > Prisma Access Standorte > Expliziter Proxy für mobile Benutzer** aus, um eine Übersicht über den Zustand Ihrer Prisma Access-Standorte für mobile Benutzer anzuzeigen.
- Überprüfen Sie die Datenverkehrsprotokolle (**Vorfälle und Benachrichtigungen > Protokoll-Viewer** und wählen Sie den Protokolltyp **Verkehr** aus) und Authentifizierungsprotokolle (**Vorfälle und Benachrichtigungen > Protokoll-Viewer** und wählen Sie den Protokolltyp **Authentifizierung** aus), um Probleme im Zusammenhang mit der Authentifizierung zu beheben.

## Expliziter Proxy (Panorama) – Überwachung und Fehlerbehebung

Nachdem Sie „Expliziter Proxy“ für mobile Benutzer konfiguriert haben, überwachen Sie den Status und beheben Probleme, indem Sie den Status Ihrer Prisma Access-Bereitstellung des Typs „Expliziter Proxy“ überprüfen.


©2025 Palo Alto Networks, Inc.

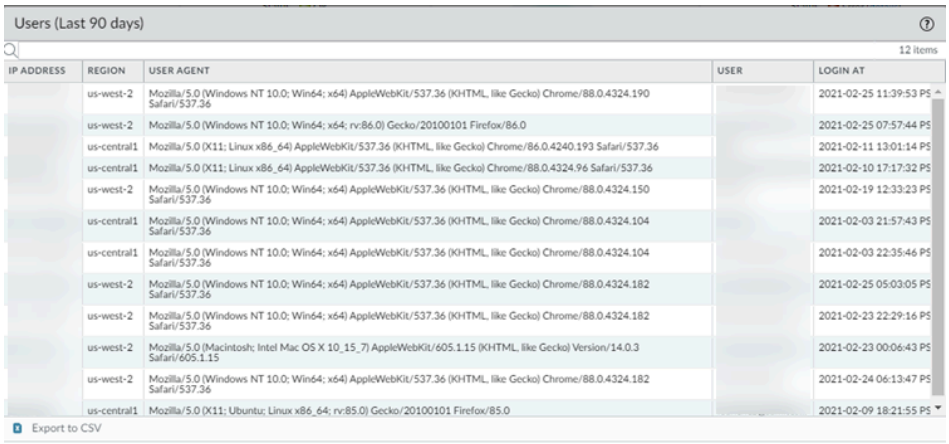
- Wählen Sie **Panorama** > **Cloud Services** > **Status** > **Status** aus, um den Status von „Expliziter Proxy“ anzuzeigen.




Die Felder **Status** und **Konfigurationsstatus** für mobile Benutzer informieren darüber, ob die Verbindung zwischen Prisma Access und Ihren mobilen Benutzern **OK** ist, ob der Status zum Tunnel nicht abgerufen werden kann (**Warnung**) oder ob die mobilen Benutzer keine Verbindung zu „Expliziter Proxy“ herstellen können (**Fehler**).

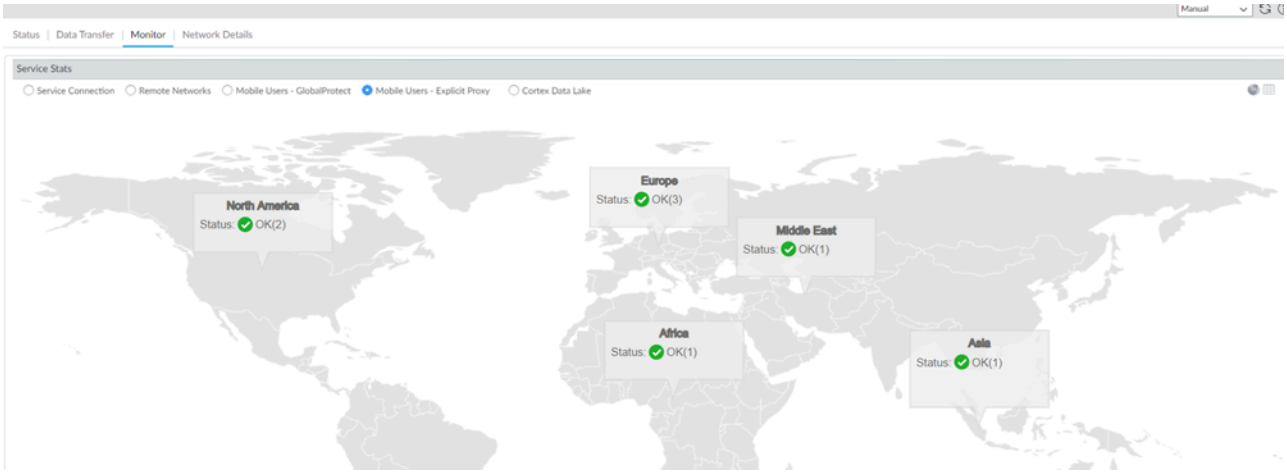
Klicken Sie auf den Hyperlink neben **Aktuelle Benutzer** und **Benutzer (letzte 90 Tage)**, um weitere Informationen über mobile Benutzer zu erhalten.

- **Aktuelle Benutzer** – Die aktuelle Anzahl authentifizierter Benutzer, die den Datenverkehr in den letzten fünf Minuten durchsucht haben.
- **Benutzer (letzte 90 Tage)** – Die Anzahl der eindeutig authentifizierten Benutzer von „Expliziter Proxy“ in den letzten 90 Tagen.

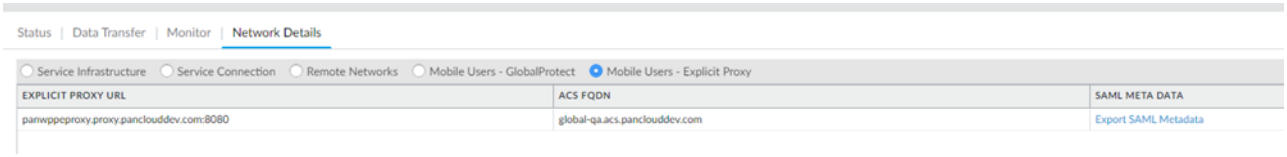



 ©2025 Palo Alto Networks, Inc.

- Wählen Sie **Panorama** > **Cloud Services** > **Status** > **Überwachen** > **Mobile Benutzer – Expliziter Proxy** aus, um eine Karte mit den bereitgestellten Standorten mit explizitem Proxy anzuzeigen.




- Wählen Sie **Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Mobile Benutzer – Expliziter Proxy** aus, um die folgenden Details anzuzeigen:




  - **URL des expliziten Proxy** – Die URL, die für „Expliziter Proxy“ verwendet wird.
  - **ACS FQDN** – Der FQDN des ACS.
  - **SAML-Metadaten** – Die von SAML verwendeten Authentifizierungsprofil-Metadaten. Sie können **SAML-Metadaten exportieren**, um die Metadatendatei zu speichern.
- Überprüfen Sie zur Behebung von Problemen im Zusammenhang mit der Authentifizierung die Datenverkehrsprotokolle (**Überwachen** > **Protokolle** > **Verkehr**) und die Authentifizierungsprotokolle (**Überwachen** > **Protokolle** > **Authentifizierung**). „Expliziter Proxy“ zeigt die folgenden IP-Adressen und Standorte in den Protokollen an:
  - **IP-Adressen** – Wenn mobile Benutzer den ACS-FQDN in der PAC-Datei umgehen, werden die IP-Adresse, die in der Spalte **Quelle** in den Datenverkehrsprotokollen angezeigt wird, sowie die Datenverkehrsprotokolle und die Spalte **IP-Adresse** in den Authentifizierungsprotokollen, wenn sie unter **Explicit_Proxy_Device_Group** angezeigt werden, mit der IP-Adresse des mobilen Benutzers übereinstimmen. Wenn Benutzer den ACS-FQDN in der PAC-Datei nicht umgehen, ist die Quell-IP-Adresse die öffentliche IP-Adresse der Cloud-Firewall von „Expliziter Proxy“, an der Umleitungen zu ACS erfolgen.
  - **Standorte** – Wenn mobile Benutzer den ACS-FQDN in der PAC-Datei umgehen, ist der Regionsname, der in der Spalte **Region** in **Authentifizierungsprotokolle**, **Aktuelle Benutzer** und **Benutzer (letzte 90 Tage)** angezeigt wird, eine der fünf Regionen (us-west-2, us-east-1, eu-west-2, eu-west-3, ap-south-1), in denen der ACS bereitgestellt wird, und zeigt die Region an, in der „Expliziter Proxy“ die Weiterleitungen vom Browser des Clients aus durchführt. Wenn Benutzer den ACS-FQDN in der PAC-Datei nicht umgehen, ist der Regionsname, der in der Spalte **Region** in **Authentifizierungsprotokolle**, **Aktuelle Benutzer** und **Benutzer (letzte 90 Tage)** angezeigt wird, eine der fünf Regionen (us-west-2, us-east-1, eu-west-2, eu-west-3, ap-south-1), in denen der ACS bereitgestellt wird, und zeigt die

 ©2025 Palo Alto Networks, Inc.

Region an, in der „Expliziter Proxy“ die Weiterleitungen von der Firewall des expliziten Proxy aus durchführt.

## Einstellungen für expliziten Proxy blockieren

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Panorama Managed Prisma Access | • Lizenz für Prisma Access |

**Um diese Funktion zu aktivieren, wenden Sie sich an Ihren Ansprechpartner bei Palo Alto Networks, der sich mit dem SRE-Team (Site Reliability Engineering) in Verbindung setzt und eine Anfrage stellt.**

Wenn Benutzer mit explizitem Proxy auf ein Internetziel zugreifen, wird die DNS-Auflösung für das Internetziel von explizitem Proxy durchgeführt. Um den Zugriff auf ein Internetziel in der DNS-Auflösungsphase zu blockieren, können Sie die Blockierungseinstellungen verwenden. Sie können die Blockierung auf Basis der DNS-Sicherheitskategorien, URL-Filterkategorien oder anhand externer dynamischer Listen (EDLs) durchführen.

Für die Domänen, die von Ihnen blockiert werden, führt Prisma Access die Blockierung der Domänen durch, sodass Benutzer während der Ausführung der HTTP-GET-Anforderung (für unverschlüsselte Websites) oder der HTTP-Verbindungsanforderung (für verschlüsselte Websites) eine Blockierungsseite erhalten, was bedeutet, dass Domänen während der ersten Verbindungsanforderung blockiert wurden. Wenn Sie den Zugriff auf die Website blockieren, wird den Benutzern eine Blockierungsseite angezeigt, nachdem sie den Authentifizierungsprozess durchlaufen haben, und der Benutzername wird für weitere Forensik- und SOC-Workflows (Security Operations Center) erfasst.

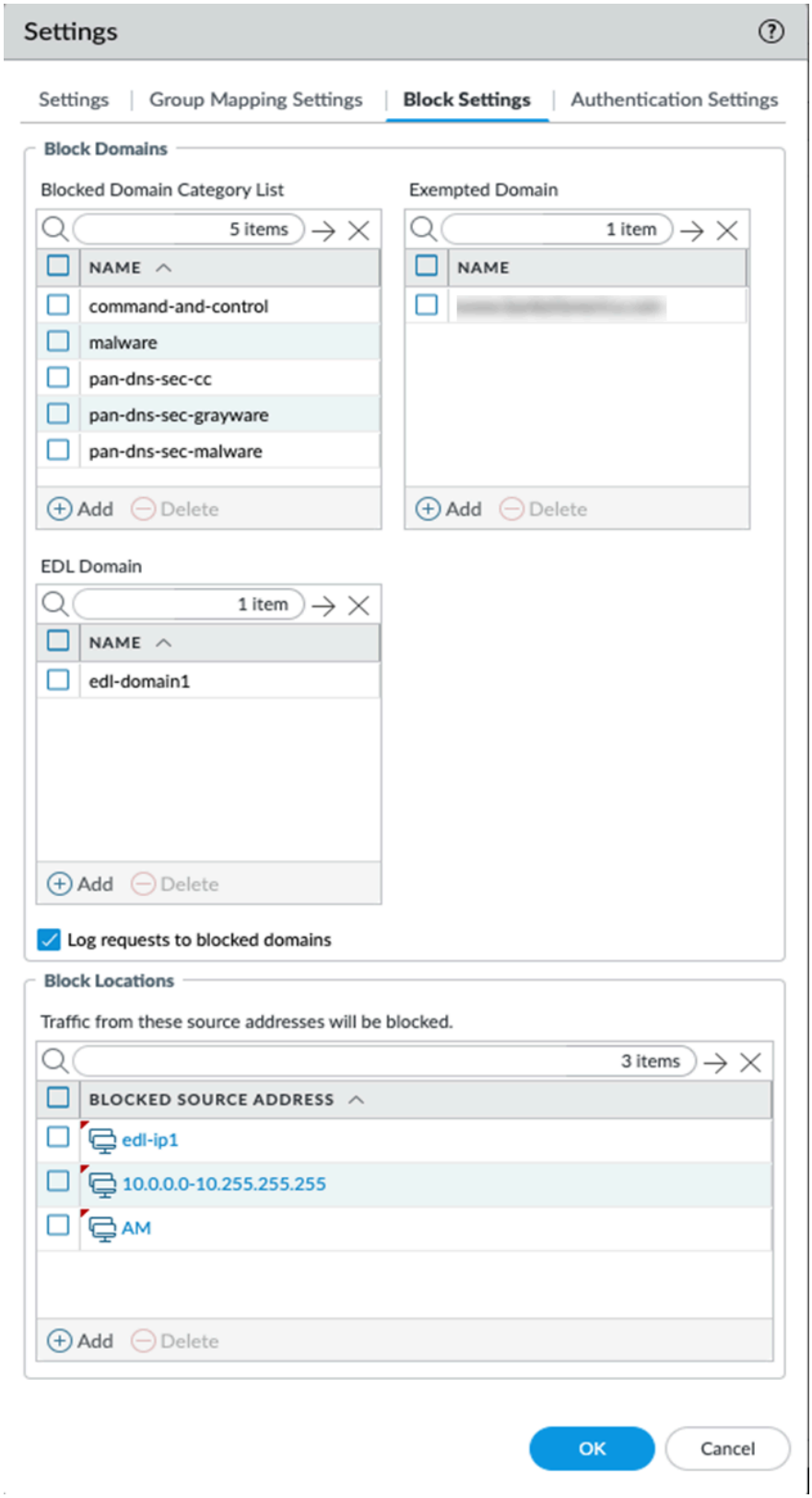
Wenn Sie Prisma Access (Managed by Strata Cloud Manager) verwenden, dann beachten Sie Schritt 8 unter Expliziten Proxy einrichten. Um die von Panorama mit Prisma Access verwalteten Blockierungseinstellungen zu konfigurieren, führen Sie die folgenden Schritte aus.

**STEP 1 |** Konfigurieren Sie **Blockierungseinstellungen**, um Domänen oder Domänenkategorien zu blockieren.

Geben Sie die Domänen oder Domänenkategorien für bösartige Websites oder für beliebige Websites an, auf die Benutzer keinen Zugriff erhalten sollen. Prisma Access verhindert, dass Benutzer auf die URLs und IP-Adressen zugreifen können, die Sie in diesem Bereich angeben, wenn Benutzer den Befehl HTTP GET (für unverschlüsselte Anfragen) oder

 ©2025 Palo Alto Networks, Inc.

HTTP-VERBINDUNG (für verschlüsselte Anfragen) absetzen. Benutzer erhalten eine Blockierungsseite, wenn sie versuchen, auf blockierte Websites zuzugreifen.




 ©2025 Palo Alto Networks, Inc.

1. In **Liste blockierter Domänenkategorien** geben Sie die vordefinierten Kategorien ein, die blockiert werden sollen.

   Benutzerdefinierte URL-Kategorien werden nicht unterstützt.
2. Geben Sie unter **EDL-Domäne** domänenbasierte externe dynamische Listen (EDLs) ein, die blockiert werden sollen.

   Sie können nur EDLs auswählen, die den EDL-Typ **Dynamische Domänenlisten** aufweisen. Dynamische IP-Listen und dynamische URL-Listen sind nicht zulässig.
3. Wenn Sie Domänen ausnehmen möchten, die in einer **Liste blockierter Domänenkategorien** enthalten sind, geben Sie diese Domänen als **Ausgenommene Domänen** an.

   Alle eingegebenen Domänen sind von der Blockierung ausgenommen. Dies gilt auch dann, wenn sie in einer Domänenkategorie erscheinen, die Sie blockiert haben.

   - Sie können maximal 100 Domänen eingeben.
   - Die maximale Länge von Domäneneinträgen beträgt 256 Zeichen.

**STEP 2 |** Wählen Sie die IP-Adressen aus, die im Bereich **Blockierte Quelladresse** blockiert werden sollen.

Sie können durch Auswahl von **Hinzufügen** Adressen, Adressgruppen, IP-Adressen-basierte EDLs oder regions- und länderbasierte IP-Adressen hinzufügen.

Verwenden Sie die folgenden Richtlinien für IP-Adressen:

- Verwenden Sie ausschließlich EDLs mit dem **Typ IP-Liste** oder **Vordefinierte IP-Liste**.
- Verwenden Sie ausschließlich Adressobjekte mit dem Typ **IP-Bereich** oder **IP-Netzmaske**.
- Adressgruppen mit dynamischer Objektmitgliedschaft werden nicht unterstützt.
- Verwenden Sie keine benutzerdefinierten Regionen in IP-Adressobjekten. Verwenden Sie stattdessen vordefinierte Regionen.

**STEP 3 |** Wählen Sie **Anfragen an blockierte Domänen protokollieren** aus, damit Prisma Access Anfragen an blockierte Domänen protokolliert.

Da Protokolle für blockierte Domänen ein hohes Aufkommen an Datenverkehr von Botnets generieren können, sollten Sie beim Aktivieren der Protokollierung mit Bedacht vorgehen. Alternativ hierzu können Sie diese Funktion auch ausschließlich zur Fehlerbehebung einsetzen. Wenn Sie die Proxy-Nutzung einschränken (z. B. wenn Sie die Nutzung auf bestimmte IP-Adressen beschränken), können Sie die Protokollierung möglicherweise ohne Einschränkung aktivieren.

## Expliziten Proxy-Internetverkehr mit speziellen Objekten auf bestimmte IP-Adressen beschränken

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | • Prisma Access-Lizenz |

 ©2025 Palo Alto Networks, Inc.

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Panorama) | |

Ein expliziter Proxy stellt spezielle Adressobjekte, Adressgruppen und externe dynamische Listen (EDLs) bereit, um den Zugriff auf den expliziten Proxy auf bestimmte Quell-IP-Adressen zu beschränken. Wenn Sie eines oder mehrere dieser speziellen Objekte mit den folgenden genauen Namen erstellen, lässt der explizite Proxy die von Ihnen angegebenen Quell-IP-Adressen zu und blockiert alle anderen IP-Adressen:

- **Adressobjekt**: Wählen Sie in der Gruppe „Explicit_Proxy_Device_Group“ die Optionen **Objekte** > **Adressen** aus und erstellen Sie ein Objekt mit dem Namen **Zulässige Quelladresse für expliziten Proxy von Palo Alto Networks**.
- **Adressgruppe**: Wählen Sie in der Gruppe „Explicit_Proxy_Device_Group“ die Optionen **Objekte** > **Adressgruppen** aus und erstellen Sie ein Objekt mit dem Namen **Zulässige Quelladressgruppe für expliziten Proxy von Palo Alto Networks**.
- **Externe dynamische Liste (EDL)**: Wählen Sie in der Gruppe „Explicit_Proxy_Device_Group“ die Optionen **Objekte** > **Externe dynamische Listen** aus. Erstellen Sie dann eine EDL mit dem Namen **Zulässige Quellliste für expliziten Proxy von Palo Alto Networks** und eine EDL des Typs **IP-Liste**.

Sie können IP-Adressen wie Ausgangs-IP-Adressen von Zweigstellen angeben.

Es ist nicht erlaubt, die explizite Proxy-Authentifizierung für eine große Anzahl von Domains mittels Platzhaltern (wie z. B. *.*) zu überspringen – es sei denn, Sie beschränken Ihren Quelldatenverkehr mit einem dieser speziellen Objekte auf bestimmte Quell-IP-Adressen.

Verwenden Sie Adressobjekte, Adressgruppen oder EDLs separat oder gemeinsam. Sie können beispielsweise nur eine Adressgruppe erstellen, ohne ein Adressobjekt oder eine EDL zu erstellen.

## Zugriff auf Ihr Rechenzentrum mit explizitem Proxy

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ☐ (Für ZTNA-Connector und Colo-Connect) Prisma Access Version 5.2.1<br>☐ (Für Dienstverbindungen) Prisma Access Version 5.0<br>☐ (Für privaten App-Zugriff und Partner-App-Zugriff) GlobalProtect app Version 6.2 für Windows oder macOS |

Sie können Dienstverbindungen, ZTNA-Connectoroder Colo-Connect verwenden, um auf Ressourcen in Ihrem Rechenzentrum zuzugreifen, z. B. auf externe dynamische Listen oder private Apps und Partner-Apps, während Sie weiterhin von einer Verbindung über expliziten Proxy profitieren können.

 ©2025 Palo Alto Networks, Inc.

*Die folgenden RFC 6598-IP-Adressen werden für den Zugriff auf private Anwendungen mithilfe des expliziten Proxy über Dienstverbindungen, Colo-Connect oder ZTNA-Connector nicht unterstützt:*

- *100.64.0.0/15*
- *100.88.0.0/15*
- *100.72.0.0/15*

*Die vorhandenen ZTNA-Connectors, die diese IP-Adressen in IP-Blöcken der ZTNA-Connector-Anwendung oder Connector-IP-Blöcken verwenden, können den Prisma Access Browser oder den GlobalProtect Agent im Proxy-Modus über expliziten Proxy nicht verwenden. Sie müssen sich an Ihren Ansprechpartner von Palo Alto Networks wenden, um Ihre IP-Adressen auf einen anderen Block zu migrieren.*

- Strata Cloud Manager
- Panorama

## Zugriff auf Ihr Rechenzentrum mit explizitem Proxy (Strata Cloud Manager)

**STEP 1 |** Konfigurieren Sie abhängig von Ihren Anforderungen eine Dienstverbindung, Colo-Connect oder ZTNA-Connector in Prisma Access.

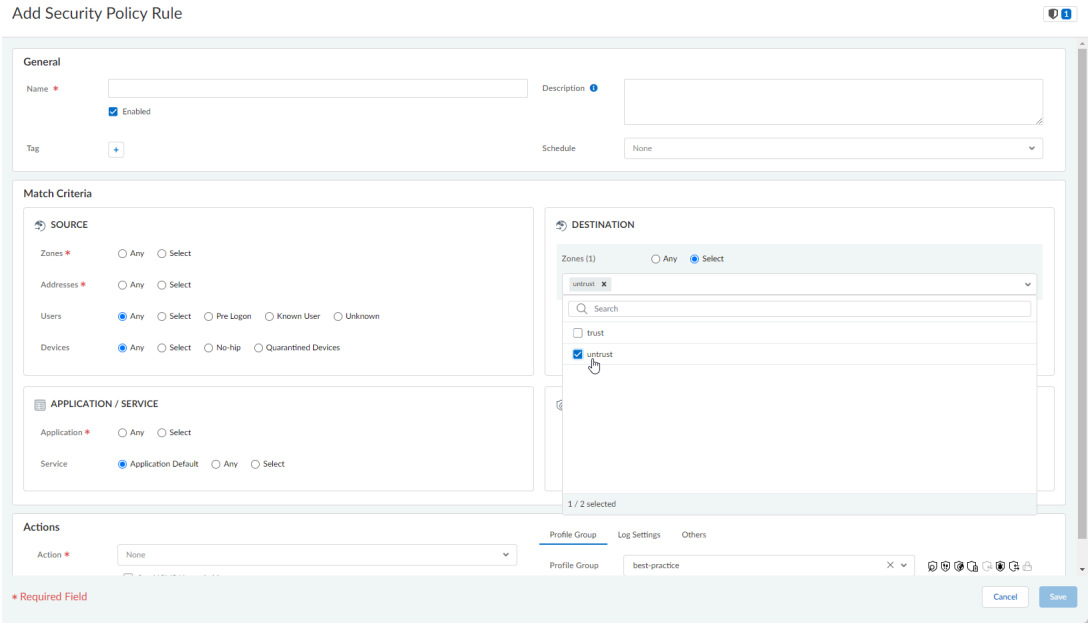
**STEP 2 |** Konfigurieren Sie die DNS-Einstellungen.

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Stellen Sie sicher, dass für **ZIEL-Zonen** für den internetgebundenen Datenverkehr die Einstellung **nicht vertrauenswürdig** anstelle von **beliebige** festgelegt wird.

*Wird dieser Schritt nicht ausgeführt, kann dies zu einem nicht erwünschten Zugriff auf Ihr Rechenzentrum führen.*

1. Rufen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access**auf, legen Sie für **Konfigurationsumfang** die Option **Prisma Access** > **Container für mobile Benutzer** > **Expliziter Proxy** fest und wählen Sie dann **Sicherheitsrichtlinie** > **Sicherheitsdienste** aus.
2. Öffnen Sie eine Regel für den internetgebundenen Datenverkehr.
3. Vergewissern Sie sich, dass für **Zonen** unter **ZIEL** die Option **nicht vertrauenswürdig** eingestellt wurde.




4. Wiederholen Sie diesen Arbeitsschritt für alle Regeln für den internetgebundenen Datenverkehr.

**STEP 4 |** Aktivieren Sie den privaten Anwendungszugriff.

- Aktivieren Sie den privaten Anwendungszugriff mit Prisma Access Browser.
  1. Wählen Sie **Workflows** > **Einrichtung Prisma Access** > **Expliziter Proxy** > **Infrastruktureinstellungen** aus und **aktivieren** Sie Prisma Access Browser. Wählen Sie unter **Proxy-URL-Einstellungen Privaten App-Zugriff für expliziten Proxy aktivieren** aus.

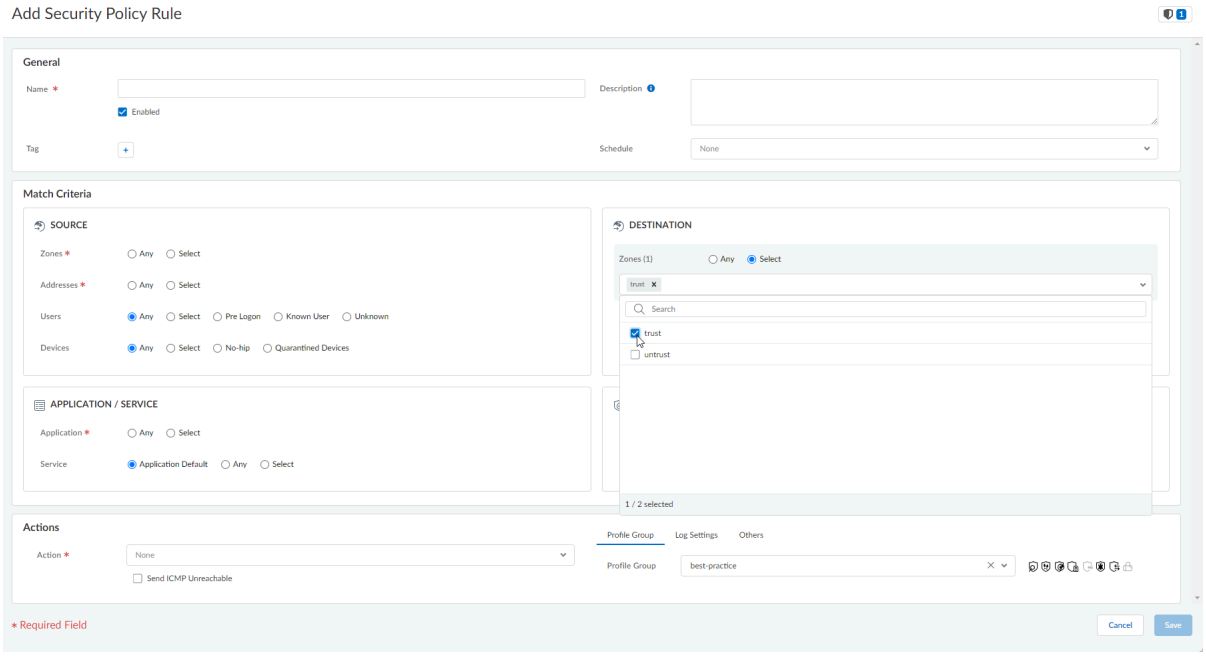
- Aktivieren Sie den privaten Anwendungszugriff mit einem regulären Browser.
  1. Wählen Sie **Workflows** > **Einrichtung Prisma Access** > **Expliziter Proxy** > **Infrastruktureinstellungen** > **Agent-Proxy aktivieren** > **Privaten Anwendungszugriff für expliziten Proxy aktivieren** aus.

 ©2025 Palo Alto Networks, Inc.

**STEP 5 |** Erstellen Sie Sicherheitsrichtlinienregeln für die Rechenzentrumsressourcen, auf die Sie zugreifen möchten.

1. Rufen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access**auf, legen Sie für **Konfigurationsumfang** die Option **Prisma Access** > **Container für mobile Benutzer** > **Expliziter Proxy** fest und wählen Sie dann **Sicherheitsrichtlinie** > **Sicherheitsdienste** aus.
2. Erstellen Sie Sicherheitsrichtlinienregeln.

Vergewissern Sie sich, dass für die Regeln für den Zugriff auf Rechenzentren unter ZIEL die Option **Zonen** auf **vertrauenswürdig** gesetzt wurde.




**STEP 6 |** Wenn Sie unter Expliziter Proxy den privaten Anwendungszugriff aktivieren, wählen Sie **Push Konfig** aus, um Ihre Konfigurationsänderungen nach dem Onboarding von ZTNA-Connector zu speichern.

## Zugriff auf Ihr Rechenzentrum mit explizitem Proxy (Panorama)

**STEP 1 |** Konfigurieren Sie abhängig von Ihren Anforderungen eine Dienstverbindung, Colo-Connect oder ZTNA-Connector in Prisma Access.

**STEP 2 |** DNS-Einstellungen konfigurieren.

**STEP 3 |** Zonenzuordnungen konfigurieren.

1. Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Mobile Benutzer – Expliziter Proxy** > **Zonenzuordnung** aus
2. Fügen Sie die Zonen, die Sie für den Zugriff auf die Ressourcen Ihres Rechenzentrums verwenden, zu **Vertrauenswürdige Zonen** hinzu.

 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** Stellen Sie sicher, dass die `Zielzone` in den Richtlinienregeln für den internetgebundenen Datenverkehr auf eine nicht vertrauenswürdige Zone anstatt auf `beliebige` eingestellt ist.

> *Wird dieser Schritt nicht ausgeführt, kann dies zu einem unerwünschten Zugriff auf Ihr Rechenzentrum führen.*

1. Wählen Sie **Richtlinien**aus.
2. Legen Sie als `Gerätegruppe` die Gruppe **Explicit_Proxy_Device_Group** fest.
3. Ändern Sie die `Zielzone` von `beliebige` in eine der nicht vertrauenswürdigen Zonen, die Sie in einem vorhergehenden Arbeitsschritt konfiguriert haben.

**STEP 5 |** Aktivieren Sie den privaten Anwendungszugriff.

- Aktivieren Sie den privaten Anwendungszugriff mit Prisma Access Browser.
  1. Gehen Sie zu **Panorama** > **Cloud Services** > **Konfiguration** > **Mobile Benutzer – Expliziter Proxy** > **Einstellungen** > **Erweitert** > **Prisma Access Browser aktivieren** > **Privaten Anwendungszugriff aktivieren**

- Aktivieren Sie den privaten Anwendungszugriff mithilfe eines regulären Browsers.
  1. Gehen Sie zu **Panorama** > **Cloud Services** > **Konfiguration** > **Mobile Benutzer – Explizierter Proxy** > **Einstellungen** > **Erweitert** > **GlobalProtect Agent zur Authentifizierung verwenden** > **Privaten Anwendungszugriff aktivieren**

**STEP 6 |** Erstellen Sie Sicherheitsrichtlinienregeln für die Rechenzentrumsressourcen, auf die Sie zugreifen möchten.

1. Wählen Sie **Richtlinien**aus.
2. Legen Sie als `Gerätegruppe` die Gruppe **Explicit_Proxy_Device_Group** fest.
3. Erstellen Sie Sicherheitsrichtlinienregeln.

   Stellen Sie bei Regeln für den Zugriff auf Rechenzentren sicher, dass Sie die **vertrauenswürdigen** Zonen verwenden, die Sie in einem früheren Schritt konfiguriert haben.

## App-basierte Office 365-Integration mit explizitem Proxy

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Lizenz für mobile Benutzer |

Erfahren Sie, wie Sie die browserbasierte Version von Office 365 mit explizitem Proxy integrieren.

- Strata Cloud Manager
- Panorama

 ©2025 Palo Alto Networks, Inc.

## App-basierte Office 365-Integration mit explizitem Proxy (Panorama)

Prisma Access für expliziten Proxy unterstützt die browserbasierte Version von Office 365 (M365), einschließlich Office Online (office.com). Befolgen Sie diese Schritte, um die browserbasierte Version von Office 365 mit explizitem Proxy zu integrieren.

Zwar unterstützt der explizite Proxy die App-basierte Version von Office 365 nicht, doch Sie können diese Richtlinien befolgen, um den expliziten Proxy mit auf Office 365-Apps basierten Richtlinien zu verwenden.

### Browserbasierte Office 365-Integration mit Prisma Access für expliziten Proxy einrichten

Wenn Sie die browserbasierte Version von Office 365 verwenden, gehen Sie wie folgt vor, um Office 365 mit dem expliziten Proxy zu integrieren.

**STEP 1 |** (Optional) Wenn Sie mandantenbasierte Einschränkungen verwenden möchten (Einschränken der Zugriffskontrolle auf Office 365 nur für eine bestimmte Anzahl von Mandanten), verwenden Sie HTTP-Header-Einfügung mit einer benutzerdefinierten URL-Kategorie, um bestimmten Mandanten den Zugriff auf Office 365 zu ermöglichen.

**STEP 2 |** Fügen Sie Entschlüsselungsrichtlinien für die URLs hinzu, die für Office 365 verwendet werden.

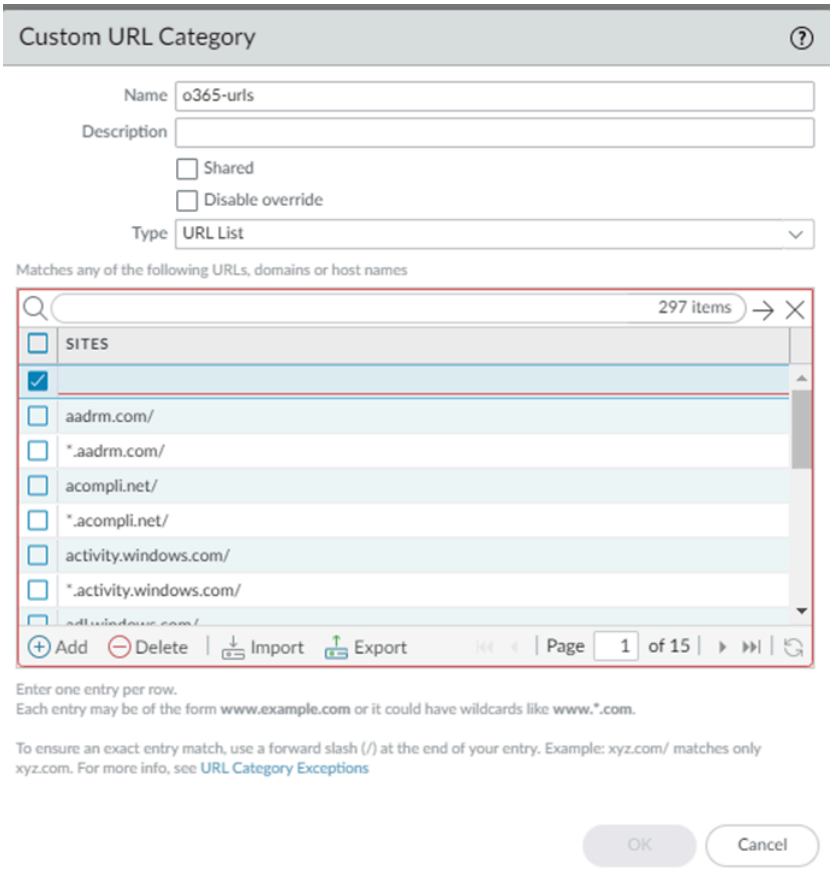
1. Wählen Sie **Objekte** > **Benutzerdefinierte Objekte** > **URL-Kategorie** aus, um eine benutzerdefinierte URL-Kategorie **hinzuzufügen**.

   Stellen Sie sicher, dass Sie sich in der Gruppe **Explicit_Proxy_Device_Group** befinden.
2. Geben Sie **URL-Liste** als **Typ** an.
3. Sie müssen die Liste der Standorte **hinzufügen**, um die Office 365-Integration zu aktivieren.

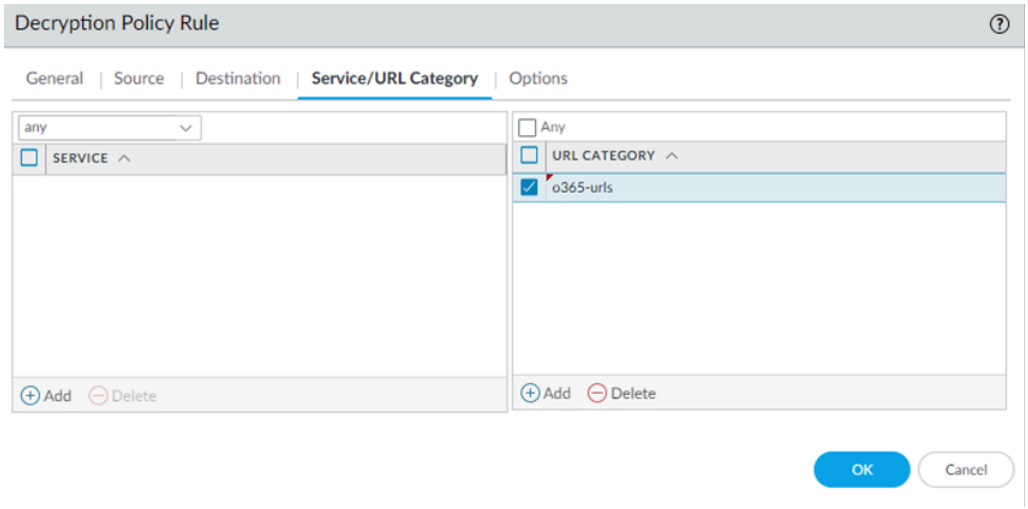
   Um das Hochladen der URLs zu vereinfachen, können Sie die Liste der Office 365-URLs unter https://saasedl.paloaltonetworks.com/feeds/m365/worldwide/any/all/url


©2025 Palo Alto Networks, Inc.

kopieren, diese URLs in einer Datei speichern und die Datei in die benutzerdefinierte URL-Kategorie **importieren**.




4. Wählen Sie **Richtlinien** > **Entschlüsselung** > **Vor-Regeln** aus, um eine Entschlüsselungsrichtlinienregel **hinzuzufügen**.
5. Geben Sie die von Ihnen erstellte **URL-Kategorie** an.




6.

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Fügen Sie Entschlüsselungsrichtlinien für Daten- und Bedrohungsschutzfunktionen wie Enterprise Data Loss Prevention (Enterprise DLP), WildFire, Threat Prevention oder SaaS Security hinzu.

**STEP 4 |** Sie können mit dem EDL-Hosting-Dienst eine externe dynamische Liste erstellen.

**STEP 5 |**

### App-basierte Office 365-Integration mit explizitem Proxy einrichten

Der explizite Proxy unterstützt keine vollständige clientbasierte (App-)Version von Office 365, da Office 365 Nicht-Web-Ports und -Protokolle sowie angeheftete Zertifikate verwendet, was die Verwendung von Entschlüsselung verhindert. Wenn Sie den Datenverkehr von Office 365-Client-Apps absichern müssen, können Sie dafür eine der folgenden Prisma Access-Funktionen verwenden:

- Stellen Sie eine Bereitstellung des Typs „Mobile Benutzer – GlobalProtect“ mit explizitem Proxy bereit und verwenden Sie Split-Tunnel-Optionen von GlobalProtect, um Datenverkehr von den Office 365-Apps an den GlobalProtect-Tunnel weiterzuleiten, während Sie anderen Internetdatenverkehr angeben, der an den GlobalProtect-Tunnel, direkt ins Internet oder an den expliziten Proxy gesendet werden soll, basierend auf Ihrer PAC-Datei und den Ein- und Ausschlussoptionen für GlobalProtect-Tunnel.
- Wenn Ihre Organisation erfordert, dass der internetgebundene Datenverkehr über einen expliziten Proxy läuft, oder wenn Ihr Netzwerk keine Standardroute hat, können Sie eine Remote-Netzwerkbereitstellung mit explizitem ProxyRemote-Netzwerkbereitstellung mit explizitem Proxy festlegen. In dieser Bereitstellung stellt Ihnen der explizite Proxy eine Liste von Anycast- und Unicast-Adressen zur Verfügung, und Sie konfigurieren Ihr CPE so, dass der Datenverkehr über diese Adressen an das Remote-Netzwerk und von dort an den expliziten Proxy und das Internet weitergeleitet wird.

  Um Office 365 mit diesem Bereitstellungstyp zu verwenden, geben Sie PAC-Dateiregeln an, um Office 365 ohne Webzugriff zu umgehen und direkt auf das Internet zuzugreifen.
- Wenn Sie GlobalProtect oder ein Prisma Access-Remote-Netzwerk nicht in Ihrer Umgebung bereitstellen können, haben Sie die Möglichkeit, die PAC-Datei des expliziten Proxy so zu konfigurieren, dass der Office 365-Datenverkehr umgangen wird. Verwenden Sie für die Umgehung die URL-Liste.

*Liste der URLs zum Aktivieren der Office 365-Integration mit Prisma Access für expliziten Proxy*

Eine Option, die Sie verwenden können, um Office 365-Apps ohne Browserzugriff mit explizitem Proxy zu integrieren, besteht darin, die Office 365-bezogenen URLs anzugeben und diese URLs in der PAC-Datei für expliziten Proxy zu umgehen. Verwenden Sie eine der folgenden Methoden, um die Liste der zu umgehenden URLs zu erhalten:

- Verwenden Sie die EDL-URL des EDL-Hosting-Dienstes von Palo Alto Networks für Microsoft 365-Apps.

  Die Verwendung des Hosting-Dienstes erleichtert die betriebliche Belastung durch die Absicherung des Datenverkehrs zu Ihren SaaS-Anwendungen, indem eine Feed-URL als

 ©2025 Palo Alto Networks, Inc.

EDL-Quelle verwendet wird. Wenn ein SaaS-Anbieter einen neuen Endpunkt für eine SaaS-Anwendung hinzufügt, wird die entsprechende Feed-URL aktualisiert.

Verwenden Sie für weltweite Microsoft 365-URLs die URL https://saasedl.paloaltonetworks.com/feeds/m365/worldwide/any/all/url. Weitere URLs werden für IPv4 und IPv6 sowie für länderspezifische und behördliche Anwendungen bereitgestellt.

- Rufen Sie die Liste der von Microsoft bereitgestellten Office 365-IP-Adressen und URLs unter https://learn.microsoft.com/de-us/microsoft-365/enterprise/urls-and-ip-address-ranges ab. Microsoft bietet unter https://learn.microsoft.com/de-us/microsoft-365/enterprise/microsoft-365-ip-web-service auch einen Webdienst für Office 365-IP-Adressen und -URLs.

# Konfigurieren der Proxy-Verkettung mit Blue Coat Proxy

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | ☐ Prisma Access-Lizenz. |

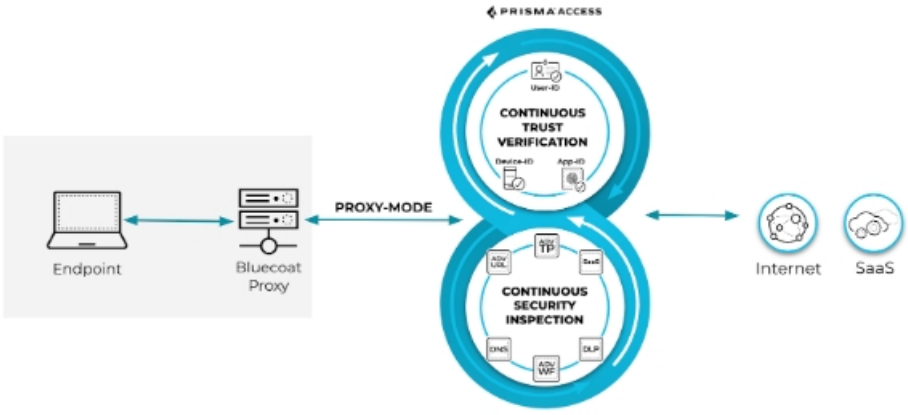
Die Proxy-Verkettung erzeugt einen Multihop-Internetpfad durch Kaskadierung mehrerer Proxyserver für eine zusätzliche Sicherheitsebene oder aufgrund der Compliance. Jeder Server leitet Ihren Datenverkehr an den nächsten weiter und erreicht so schließlich das Internet. Diese Technik nutzt Ihre vorhandene Netzwerkinfrastruktur und ermöglicht die Verbindung zu einem Upstream-Proxy für eine sichere HTTP- und HTTPS-Kommunikation. Die Integration erhält die Browsereinstellungen des Benutzers und verbessert gleichzeitig Sicherheit und Kontrolle.

Gründe für die Verwendung der Funktion für die Proxy-Verkettung durch Unternehmen:

1. Verbesserte Wahrung von Datenschutz und Anonymität durch mehrschichtigen Schutz und Umgehung geografischer Einschränkungen.
2. Sicherheit und Kontrolle durch Filterung bösartiger Inhalte, Spam und Phishing-Versuche durch eine zusätzliche Sicherheitsebene für das Surferlebnis des Benutzers.
3. Unternehmen können die Proxy-Verkettung verwenden, um interne Richtlinienregeln durchzusetzen, indem sie den Zugriff auf bestimmte Websites oder Dienste basierend auf Benutzerrollen oder Standorten einschränken.
4. Anstatt ein neues System bereitzustellen, können Sie mit der Proxy-Verkettung Ihre vorhandene Netzwerkinfrastruktur weiterhin nutzen, indem Sie für bestimmte Aufgaben eine Verbindung zu einem Upstream-Proxyserver herstellen. Auf diese Weise kann eine kostengünstige und effiziente Lösung bereitgestellt werden.

Erfahren Sie mehr darüber, wie Prisma Access-Expliziter Proxy funktioniert.

 ©2025 Palo Alto Networks, Inc.




Im Folgenden wird ein Szenario gezeigt, in dem Kunden den Datenverkehr über eine Proxy-Verkettung vom lokalen Blue Coat-Proxy zum Prisma Access expliziten Proxy weiterleiten möchten. Der lokale Blue Coat-Proxy authentifiziert Benutzer und übergibt den Benutzernamen an Prisma Access-Expliziter Proxy. Hierzu wird ein XAU-Headereinschub (X-Authenticated-User) auf dem Blue Coat-Proxy verwendet.

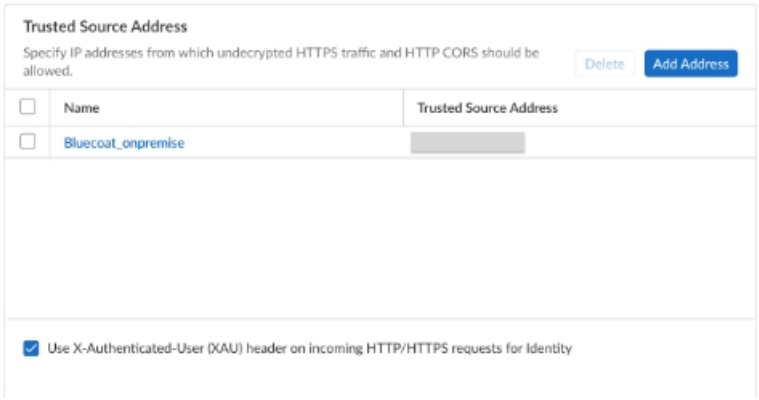
*Für IP-Adressen des expliziten Proxys sind die NAT für statische Routen und die Ziel-NAT in Netzwerken ohne Standardroute erforderlich.*

**STEP 1 |** Konfigurieren Sie Prisma Access.

1. Expliziten Proxy einrichten.
2. Fügen Sie Blue Coat Expliziter Proxy als vertrauenswürdige Quelladresse hinzu.
   1. Wählen Sie **Workflows** > **Einrichtung Prisma Access** > **Expliziter Proxy** > **Erweiterte Sicherheitseinstellungen** > **Adresse hinzufügen** aus.
   2. Geben Sie die IP-Adresse für den Blue Coat Expliziter Proxy ein.

      *Sie können entweder IP-Adressen oder Subnetze hinzufügen.*

   3. Wählen Sie den **XAU-Header (X-Authenticated-User) bei eingehenden HTTP-/HTTPS-Anfragen für die Identität aus**.

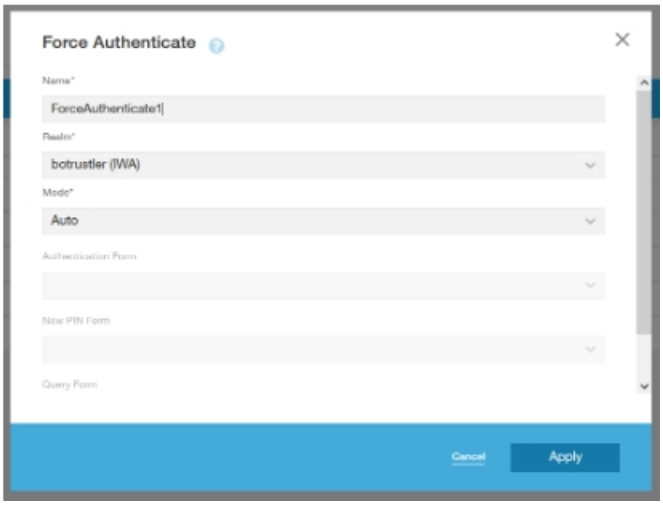



 ©2025 Palo Alto Networks, Inc.

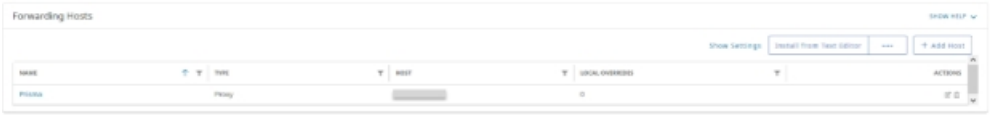
**STEP 2 |** Führen Sie die Konfiguration in Blue Coat Proxy durch.

1. Setzen Sie die Authentifizierung durch.

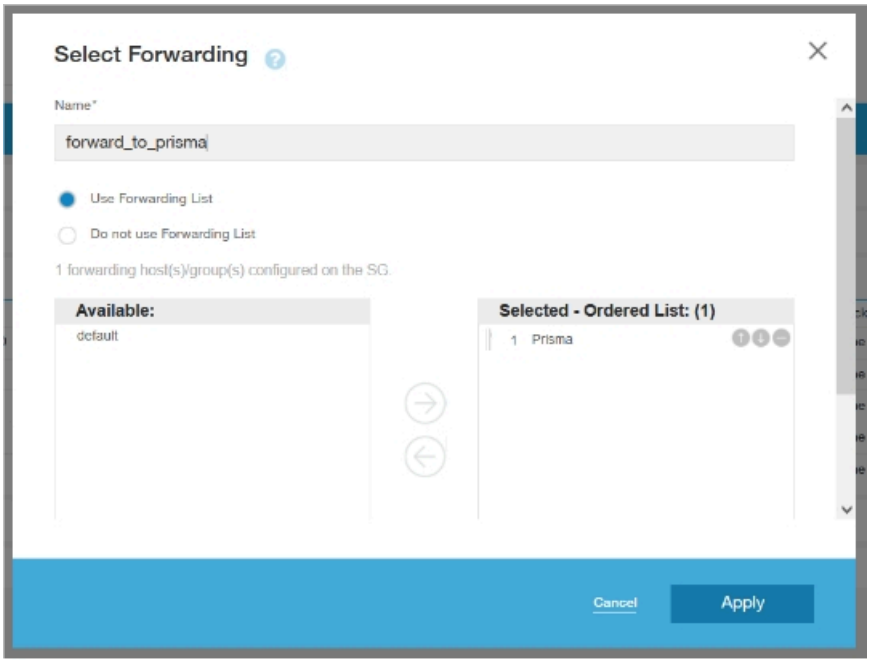





2. Konfigurieren Sie die Weiterleitungsebene.




1. Rufen Sie die IP-Adresse von Prisma Access-Expliziter Proxy
   1. im Strata Cloud Manager die Optionen **Workflows** > **Einrichtung Prisma Access** > **Expliziter Proxy** > **Infrastruktureinstellungen** aus.
   2. Kopieren Sie den Proxy-FQDN.

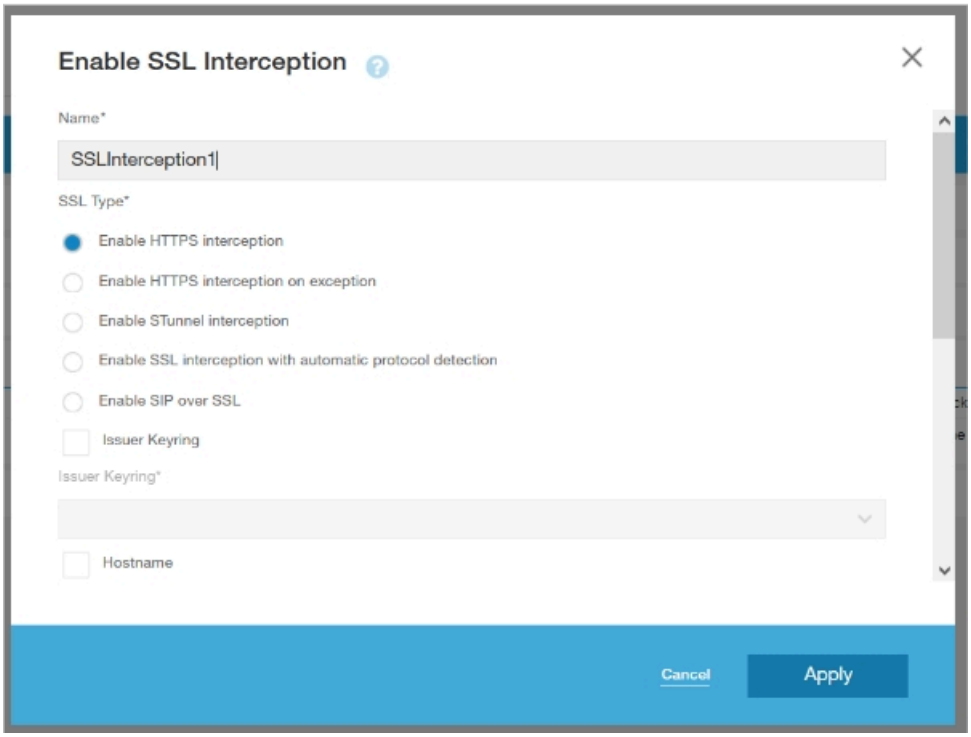



 ©2025 Palo Alto Networks, Inc.



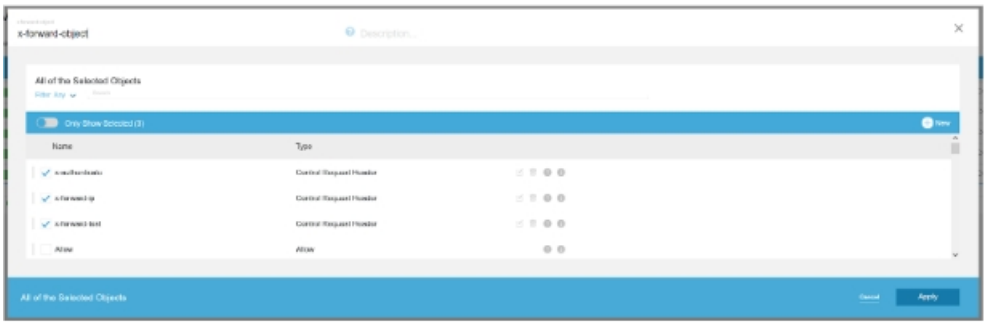
2. Aktivieren Sie die HTTPS-Entschlüsselung für das Einfügen von Headern.

   Die Entschlüsselung ist für das Einfügen von Headern obligatorisch.

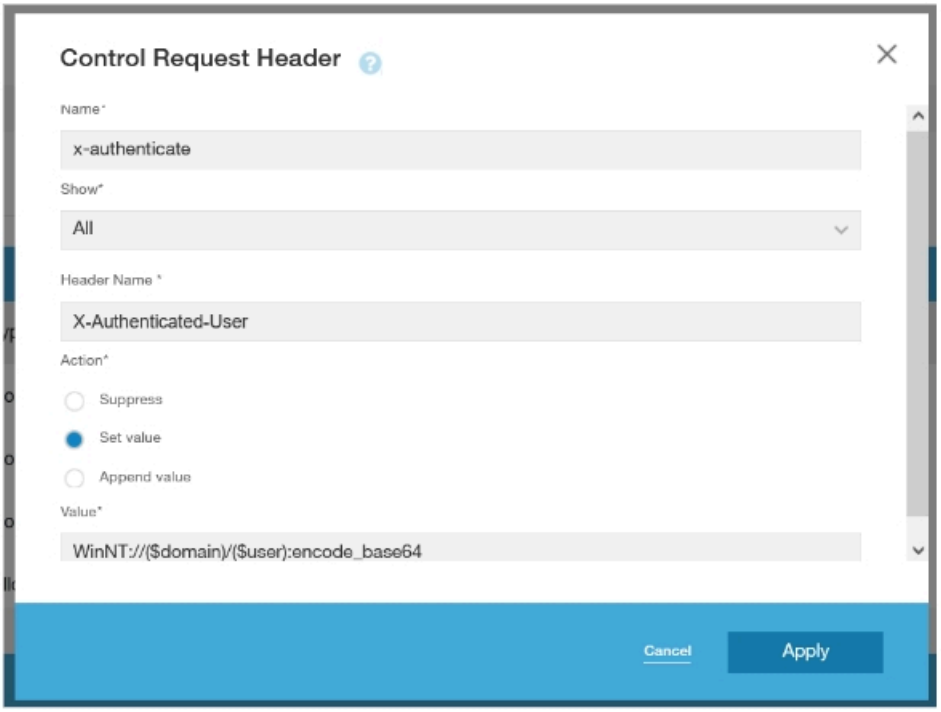


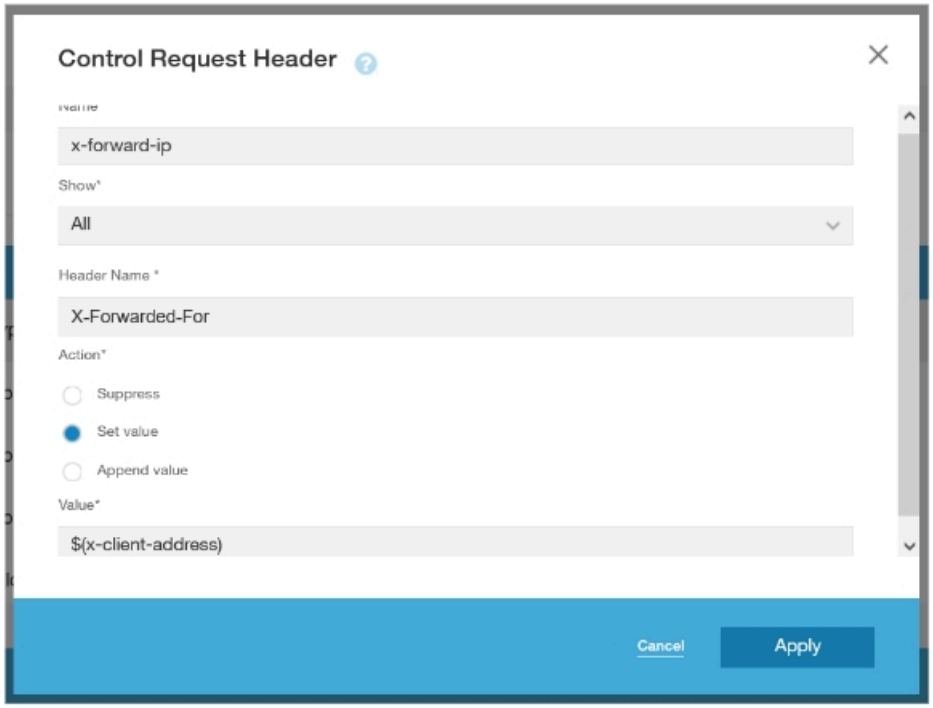



3. Konfigurieren der Headerweiterleitung.



 ©2025 Palo Alto Networks, Inc.




*Die über den XFF-Header empfangene Client-IP-Adresse wird einfach protokolliert und kann für Richtlinien nicht verwendet werden.*

4. Setzen Sie die Header-Wertcodierung auf base64:

```
define action Encode_All_XFF set( request.x_header.X-
Authenticated-User, "$(user:encode_base64)" ) end define action
```

 ©2025 Palo Alto Networks, Inc.

```
x-authenticate set( request.x_header.X-Authenticated-User,
"WinNT://($$domain)/($$user):encode_base64" ) end
```

**STEP 3 |** Überprüfen Sie die Konfiguration.

1. Wählen Sie in Strata Cloud Manager **Vorfälle und Benachrichtigungen** > **Protokoll-Viewer** aus.
2. Überprüfen Sie in den Spalten `X-Forwarded-For` und `Users`, ob die Benutzer- und IP-Adressinformationen in Prisma Access sichtbar sind.

**STEP 4 |** Beachten Sie die folgenden Punkte:

1. Der Blue Coat-Proxy erfordert die Authentifizierung und Entschlüsselung, um XAU-Headerinformationen einfügen zu können.
2. Der XAU-Headerwert (X-Authenticated-User) für die Authentifizierung sollte im Base64-Format vorliegen.
3. Prisma Access-Expliziter Proxy kann die Benutzeridentität für den entschlüsselten Datenverkehr erkennen.

# Einen expliziten Proxy mit GlobalProtect (oder einem VPN eines Drittanbieters) verwenden

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

Sie können einen expliziten Proxy mit GlobalProtect oder einem VPN von Drittanbietern kombinieren:

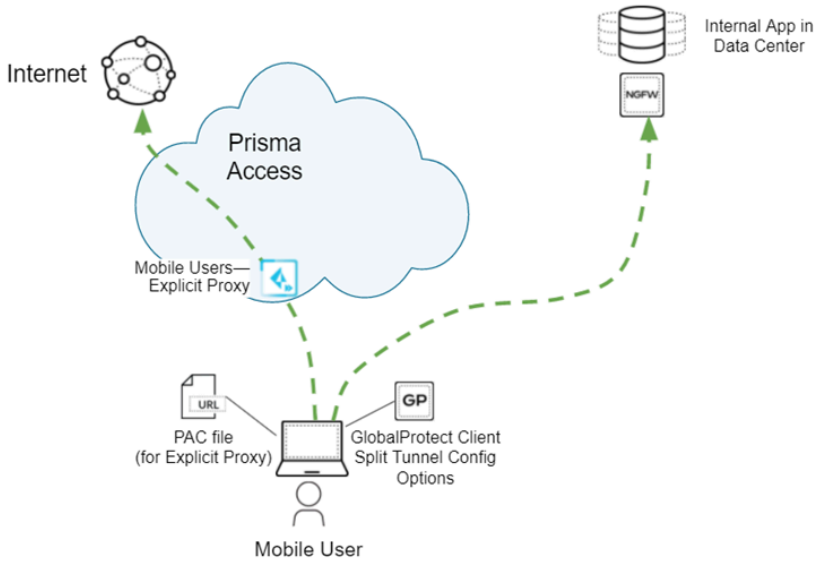
- **Expliziter Proxy und GlobalProtect**
  - Verwenden Sie GlobalProtect im Split-Tunnel-Modus, um nur privaten Apps sicheren Zugriff zu gewähren.
  - Verwenden Sie einen expliziten Proxy, um öffentliche Apps zu schützen, einschließlich Internetdatenverkehr und externer SaaS-Anwendungen.
- **Expliziter Proxy und ein VPN von Drittanbietern**

  Wenn Sie einen VPN-Client für den Zugriff auf Rechenzentrums- und private Anwendungen verwenden, können Sie ihn weiterhin für den sicheren Zugriff auf private Apps nutzen, während Sie mit dem expliziten Proxy und einer PAC-Datei den Zugriff auf öffentliche Apps sicherstellen. Sie können einen expliziten Proxy an einem Standort in der Nähe Ihrer mobilen Benutzer bereitstellen. Dadurch muss der Datenverkehr zur Wahrung der Websicherheit nicht mehr in Ihr Rechenzentrum zurückgeholt werden.

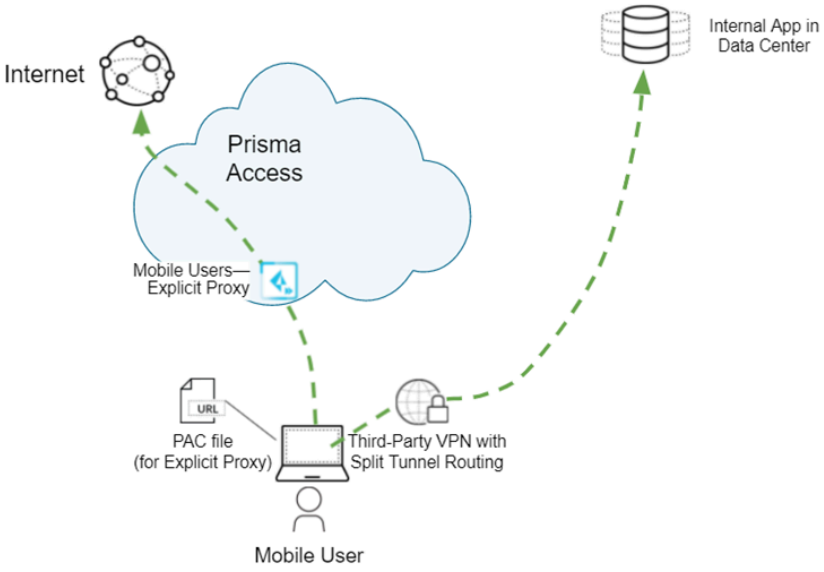
Die folgende Abbildung zeigt eine Bereitstellung mit einem GlobalProtect-Gateway zusammen mit einem expliziten Proxy. GlobalProtect leitet den Datenverkehr mit dem GlobalProtect-Client an die Firewall der nächsten Generation von Palo Alto Networks weiter. Erstellen Sie zum

 ©2025 Palo Alto Networks, Inc.

Konfigurieren dieser Bereitstellung eine aufgeteilte Tunnelkonfiguration in GlobalProtect, mit der private Apps mit GlobalProtect und öffentliche Apps mit explizitem Proxy gesichert werden können. Nach Abschluss der Konfiguration verbinden sich mobile Benutzer mittels GlobalProtect mit den privaten Apps im Rechenzentrum Ihres Unternehmens und stellen über den expliziten Proxy eine Verbindung zu privaten internetbasierten Apps her.




Wenn Sie über ein VPN eines Drittanbieters verfügen, können Sie damit eine Verbindung zu privaten Apps im Rechenzentrum herstellen und gleichzeitig öffentliche Apps mit dem expliziten Proxy sichern, wie in der folgenden Abbildung gezeigt.




**Erste Schritte:**

- Funktionsweise
- Expliziter Proxy – Richtlinien
- Expliziter Proxy und GlobalProtect: Einrichten


©2025 Palo Alto Networks, Inc.

- Expliziter Proxy mit VPNs von Drittanbietern

## Voraussetzungen für die Verwendung eines expliziten Proxy mit GlobalProtect oder einem VPN von Drittanbietern

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

Bevor Sie mit der Konfiguration beginnen, stellen Sie sicher, dass Sie die Anforderungen und Empfehlungen befolgen, die für die Bereitstellung eines expliziten Proxy mit GlobalProtect oder einem VPN eines Drittanbieters erforderlich sind:

- Für die Verwendung eines expliziten Proxy mit GlobalProtect müssen Sie GlobalProtect bereitstellen (entweder eine GlobalProtect-Bereitstellung für mobile Benutzer oder eine eigenständige GlobalProtect-Bereitstellung mit GlobalProtect-Gateways und -Portalen).

  Sie konfigurieren eine Split-Tunnel-Konfiguration in GlobalProtect. Die Beispiele in diesem Abschnitt zeigen, dass der Datenverkehr basierend auf einer Domäne (URL) oder Anwendung aufgeteilt wird. Sie können den Datenverkehr jedoch auch basierend auf der Zugriffsroute aufteilen.

  Sie können auch Split-DNS-Optionen in GlobalProtect konfigurieren, um zu konfigurieren, welche Domänen von den DNS-Servern, die über ein VPN zugewiesen werden, und welche Domänen von den lokalen DNS-Servern aufgelöst werden.
- Für die Verwendung eines expliziten Proxy mit einem VPN eines Drittanbieters müssen Sie die VPN-Lösung bereitstellen.
- Erstellen Sie eine Liste der Anwendungen, die Sie mit der GlobalProtect-Bereitstellung für mobile Benutzer oder mit einer VPN-Bereitstellung von Drittanbietern sichern möchten.

  Wenn Sie beispielsweise einen expliziten Proxy mit GlobalProtect konfigurieren, sollten Sie GlobalProtect so konfigurieren, dass der gesamte Zugriff auf private Apps oder Ressourcen gesichert ist, während Sie die PAC-Datei des expliziten Proxy so konfigurieren, dass öffentliche Apps oder SaaS-Anwendungen geschützt sind. Die Konfigurationsbeispiele in diesem Abschnitt enthalten GlobalProtect zur Auflösung der internen Domänen und den expliziten Proxy zur Auflösung externer Domänen.
- Konfigurieren Sie die Authentifizierung für den expliziten Proxy und GlobalProtect oder das VPN eines Drittanbieters.
  - Für den expliziten Proxy müssen Sie die SAML-Authentifizierung verwenden. Befolgen Sie die Richtlinien zum Konfigurieren von SAML in einer Bereitstellung mit explizitem Proxy, einschließlich der URLs für die SAML-Anmeldung.
  - Bei GlobalProtect-Bereitstellungen für mobile Benutzer: Wenn Sie die SAML-Authentifizierung mit Okta als Identitätsanbieter (IdP) verwenden, finden Sie im Prisma

 ©2025 Palo Alto Networks, Inc.

Access-Integrationshandbuch (von Panorama verwaltet) weitere Informationen zum Konfigurieren der SAML-Authentifizierung mit Okta.

- Für eigenständige GlobalProtect-Bereitstellungen können Sie die SAML-Authentifizierung in PAN-OS konfigurieren.
- Informationen zur Vorgehensweise beim VPN eines Drittanbieters finden Sie in der Produktdokumentation zum entsprechenden VPN.

Palo Alto Networks empfiehlt, für die SAML-Authentifizierung den Standardbrowser auf dem Endgerät des jeweiligen mobilen Benutzers zu verwenden, damit Sie die Vorteile von Single Sign-On (SSO) nutzen können, indem Sie die Portalkonfiguration wie unter „Expliziter Proxy“ einrichten beschrieben bearbeiten.

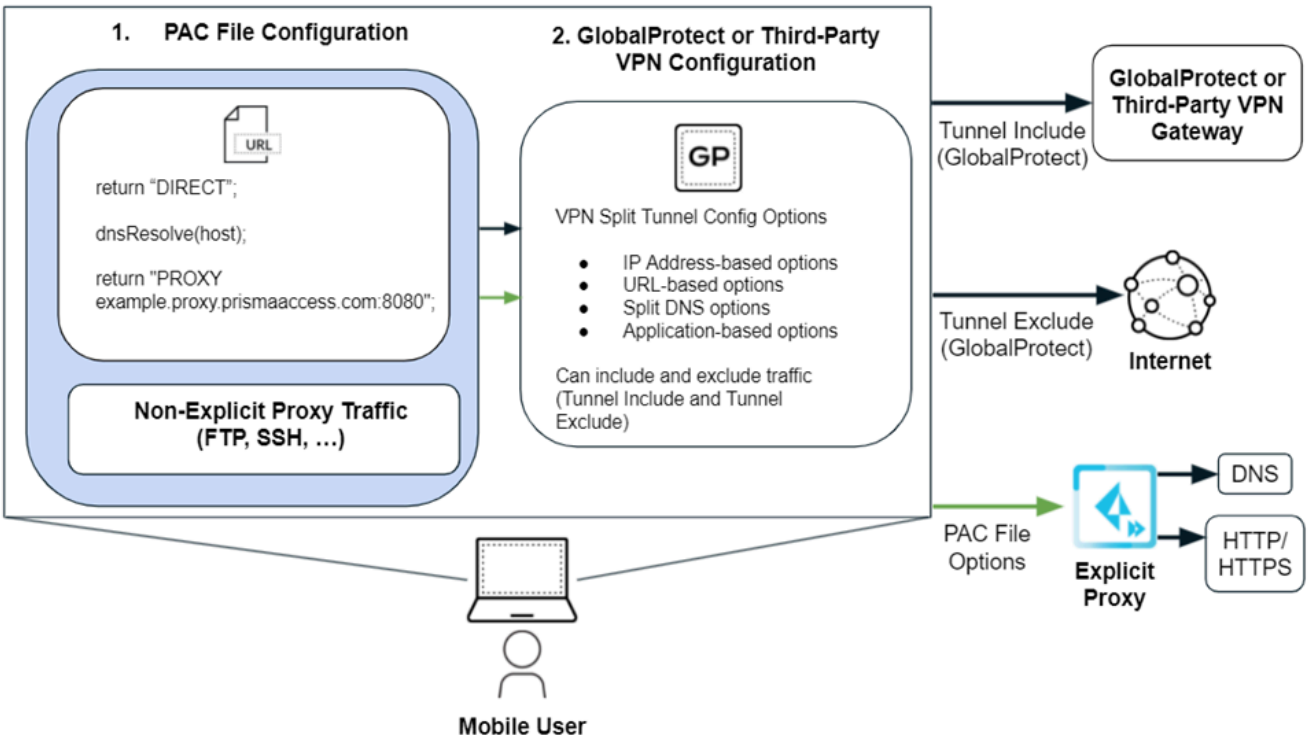
- Sie müssen sicherstellen, dass die von den mobilen Benutzern verwendeten Browser der Konfiguration in der PAC-Datei entsprechen.

## Expliziter Proxy und GlobalProtect: Funktionsweise

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

Bevor Sie entscheiden, welche Anwendungen oder welchen Datenverkehr Sie mit einem expliziten Proxy schützen sollten und welche Anwendungen Sie entweder mit GlobalProtect oder einem Drittanbieter-VPN schützen sollen, sollten Sie verstehen, wie GlobalProtect und Prisma Access ihre Weiterleitungsentscheidungen auf der Grundlage der Konfiguration des expliziten Proxy und des VPN treffen. Bei den Beispielen in diesem Abschnitt wird davon ausgegangen, dass Sie den expliziten Proxy und GlobalProtect bereits im Netzwerk Ihrer Organisation bereitgestellt und die Split-Tunnel-Optionen von GlobalProtect konfiguriert haben. Die folgende Abbildung zeigt den Vorgang.


©2025 Palo Alto Networks, Inc.




Wenn ein mobiler Benutzer eine private oder internetbasierte Ressource oder App anfordert, wird die Anfrage von der PAC-Datei des expliziten Proxy am Endpunkt ausgewertet.

- Die Funktion `return "DIRECT";` in der PAC-Datei bewirkt, dass der im Ausdruck angegebene Datenverkehr die Verarbeitung durch den expliziten Proxy umgeht.

  Der explizite Proxy stellt Ihnen eine PAC-Beispieldatei mit IP und URLs zur Verfügung, die die Funktion `return "DIRECT";` verwendet. Den Inhalt der PAC-Datei und eine Beschreibung ihrer Verwendung finden Sie unter PAC-Datei Ihres expliziten Proxy einrichten.
- Die Funktion `dnsresolve (host)` in der PAC-Datei zwingt den Endpunkt, eine DNS-Abfrage durchzuführen, um einen Hostnamen in eine IP aufzulösen. Diese Abfrage folgt dann der VPN-Richtlinie (z. B. Split-Tunnel oder Split-DNS) zur Weiterleitung der DNS-Anfrage an den Ziel-DNS-Server.

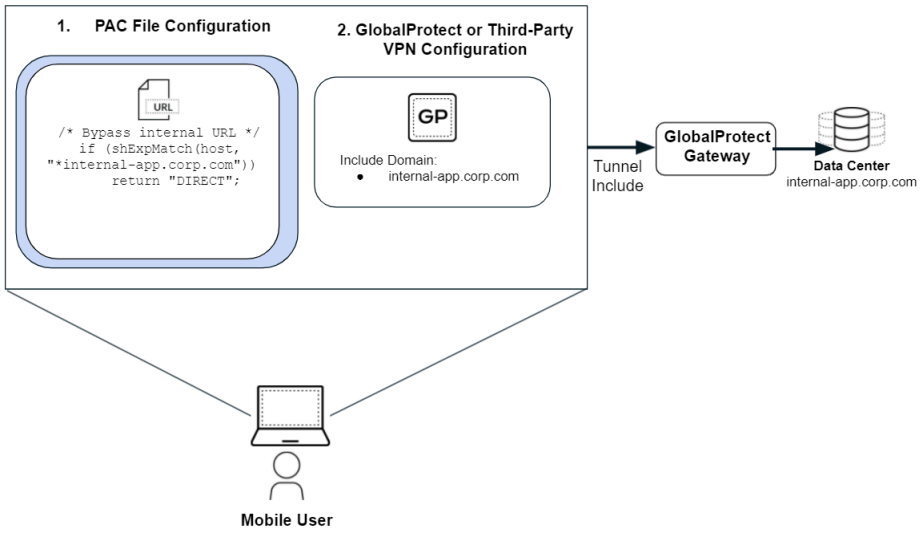
  Die mit dem expliziten Proxy bereitgestellte PAC-Datei verwendet `dnsresolve (host)`, `return "DIRECT";` und private IP-Adressen zusammen in einem Ausdruck. Wenn nach einer DNS-Suche die zurückgegebene IP-Adresse in den privaten IP-Adressen im Ausdruck enthalten ist, umgeht der mit der privaten IP-Adresse verknüpfte Datenverkehr die Verarbeitung durch den expliziten Proxy.
- Datenverkehr, der in der PAC-Datei als `return "PROXY` *`sitename`*`:8080";` angegeben ist, wird an den expliziten Proxy weitergeleitet.

Nachdem die Webanfrage anhand der Bedingungen in der PAC-Datei ausgewertet wurde, wird sie zur Verarbeitung an die GlobalProtect- oder Drittanbieter-VPN-Konfiguration am Endpunkt gesendet und der Datenverkehr wird in der GlobalProtect-App für Split-Tunnel-Konfigurationsoptionen ausgewertet. Sie können den Datenverkehr nach Domäne (URL) oder Anwendung oder Subnetz aufteilen. Wenn Sie Split-DNS-Optionen in GlobalProtect konfiguriert haben, wird der Datenverkehr auch auf der Grundlage dieser DNS-Optionen ausgewertet.

 ©2025 Palo Alto Networks, Inc.

Nachdem der Datenverkehr verarbeitet wurde, wird er basierend auf der PAC-Datei und der VPN-Verarbeitung an GlobalProtect, direkt an das Internet oder an den expliziten Proxy gesendet.

Die folgende Abbildung zeigt einen mobilen Benutzer, der versucht, über die URL **internal-app.corp.com** auf eine private Ressource zuzugreifen.



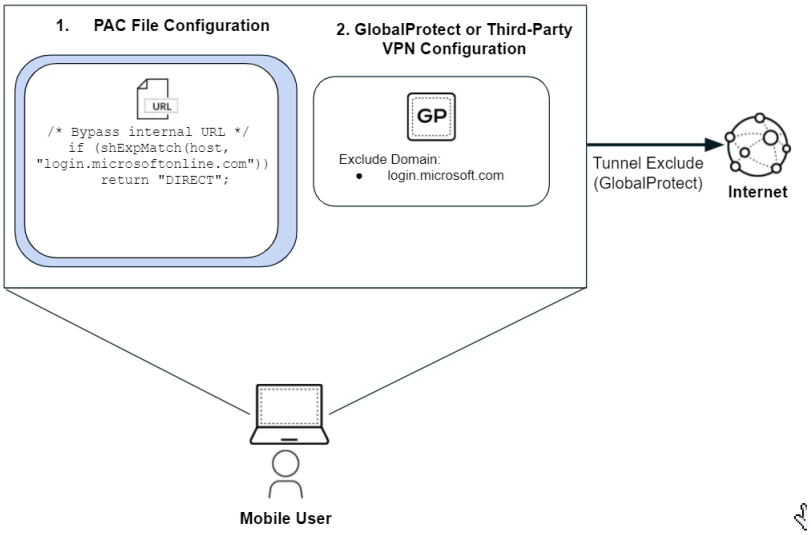

- Die PAC-Datei hat die folgende Konfiguration, damit **internal-app.corp.com** den expliziten Proxy umgehen kann.

```
    /* Bypass internal URL */ if (shExpMatch(host, "*internal-
app.corp.com")) return "DIRECT";
```

- Wenn der mobile Benutzer **internal-app.corp.com** von seinem Browser anfordert, wertet der Browser die Bedingungen in der PAC-Datei aus. Basierend auf dieser Auswertung leitet der Browser die Anfrage nicht an den Proxy weiter und sendet sie direkt an die GlobalProtect-App.
- GlobalProtect stellt fest, dass **internal-app.corp.com** in der **Include-Domäne** aufgeführt ist und sendet sie durch den VPN-Tunnel.
- GlobalProtect sendet die Anfrage basierend auf den Konfigurationsoptionen in GlobalProtect an die Ressource in **internal-app.corp.com**.

Möglicherweise möchten Sie einige Ressourcen, z. B. Anmelderessourcen, so konfigurieren, dass sie weder den expliziten Proxy noch das GlobalProtect- oder Drittanbieter-VPN für die Verarbeitung verwenden. Die folgende Abbildung zeigt einen Benutzer, der sich bei Microsoft Online anmeldet, indem er in seinem Browser **login.microsoftonline.com** eingibt.

 ©2025 Palo Alto Networks, Inc.




- Die PAC-Datei hat die folgende Konfiguration, damit **`internal-app.corp.com`** den Datenverkehr des expliziten Proxy umgehen kann.

```
   /* Bypass internal URL */ if (shExpMatch(host,
"login.microsoftonline.com")) return "DIRECT";
```

- Wenn der mobile Benutzer **`login.microsoftonline.com`** von seinem Browser anfordert, wertet die PAC-Datei die Anfrage aus der PAC-Datei am Endpunkt des mobilen Benutzers aus und sendet sie dann zur Verarbeitung an die GlobalProtect-VPN-Konfiguration (in diesem Fall GlobalProtect).
- Die GlobalProtect-App stellt fest, dass **`login.microsoftonline.com`** in der **Exclude-Domäne** aufgeführt ist.
- GlobalProtect umgeht das VPN und sendet die Anfrage basierend auf den Konfigurationsoptionen in GlobalProtect direkt an das Internet.

## Expliziter Proxy und GlobalProtect: Einrichten

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

Damit sich Ihre mobilen Benutzer sicher verbinden können, können Sie einen expliziten Proxy mit GlobalProtect oder einem VPN von Drittanbietern kombinieren.

 ©2025 Palo Alto Networks, Inc.

- Expliziter Proxy und GlobalProtect
  - Verwenden Sie GlobalProtect im Split-Tunnel-Modus, um nur privaten Apps sicheren Zugriff zu gewähren.
  - Verwenden Sie einen expliziten Proxy, um öffentliche Apps zu schützen, einschließlich Internetdatenverkehr und externer SaaS-Anwendungen.
- Expliziter Proxy und VPN von Drittanbietern
  - Verwenden Sie einen VPN-Client für den Zugriff auf Rechenzentrums- und private Anwendungen und für den sicheren Zugriff auf private Apps.
  - Verwenden Sie einen expliziten Proxy und eine PAC-Datei für den sicheren Zugriff auf öffentliche Apps.

Bevor Sie entscheiden, welche Anwendungen oder welchen Datenverkehr Sie mit einem expliziten Proxy und entweder mit GlobalProtect oder mit einem VPN von Drittanbietern schützen sollen, sollten Sie verstehen, wie GlobalProtect und Prisma Access ihre Weiterleitungsentscheidungen auf der Grundlage der Konfiguration des expliziten Proxys und des VPN treffen.

Wenn ein mobiler Benutzer eine private oder internetbasierte Ressource oder App anfordert, wird die Anforderung an die PAC-Datei des expliziten Proxys gesendet, die am Endpunkt installiert ist.

- Datenverkehr, der in der PAC-Datei als return "DIRECT"; angegeben wird, umgeht die Verarbeitung durch den expliziten Proxy. Die DNS-Auflösung (Host), die mit return "DIRECT"; verwendet wird, erlaubt, dass die angegebene IP-Adresse die Verarbeitung durch den expliziten Proxy umgeht.
- Datenverkehr, der in der PAC-Datei als return "PROXY sitename:8080"; angegeben wird, wird an einen expliziten Proxy weitergeleitet.

Nachdem der Datenverkehr verarbeitet wurde, wird er basierend auf der PAC-Datei- und VPN-Verarbeitung an GlobalProtect, direkt an das Internet oder an den expliziten Proxy gesendet.

Die PAC-Datei ist so konfiguriert, dass "internal-app.corp.com" den expliziten Proxy umgehen kann. Wenn der mobile Benutzer "internal-app.corp.com" von seinem Browser anfordert, wertet der Browser die Bedingungen in der PAC-Datei aus. GlobalProtect erkennt, dass "internal-app.corp.com" in der Include-Domäne enthalten ist und sendet sie durch den VPN-Tunnel. GlobalProtect sendet die Anforderung an die Ressource in "internal-app.corp.com" basierend auf den Konfigurationsoptionen in GlobalProtect.

- Strata Cloud Manager
- Panorama

### Expliziter Proxy und GlobalProtect: Einrichten (Strata Cloud Manager)

Führen Sie die folgenden Schritte aus, um GlobalProtect – Mobile Benutzer mit explizitem Proxy zu implementieren.

In diesen Konfigurationsschritten werden die folgenden Annahmen über Ihre Netzwerkumgebung getroffen (wenn sich Ihre Netzwerkumgebung unterscheidet, kann die Konfiguration davon abweichen):

 ©2025 Palo Alto Networks, Inc.

- Mobile Benutzer können den Hostnamen des GlobalProtect-Portals, die Gateway-FQDNs, die URL des expliziten Proxys und die URL der PAC-Datei erreichen und auflösen.

  Hier finden Sie diese Informationen:

  - **GlobalProtect-Gateway-FQDNs** und **Portal-Hostname**

    # Gehen Sie zu **Workflows** > **Einrichtung Prisma Access** > **GlobalProtect** > **Infrastruktur** und bearbeiten Sie die **Infrastruktureinstellungen**.
  - **URL des expliziten Proxys** und **URL der PAC-Datei**

    # Gehen Sie zu **Workflows** > **Einrichtung Prisma Access** > **Expliziter Proxy** > **Infrastruktur** und bearbeiten Sie die **Infrastruktureinstellungen**.
- Mobile Benutzer können interne Domänen von GlobalProtect aus auflösen.

**STEP 1 |** Entscheiden Sie, welche Anwendungen Sie an GlobalProtect senden möchten und welche an den expliziten Proxy.

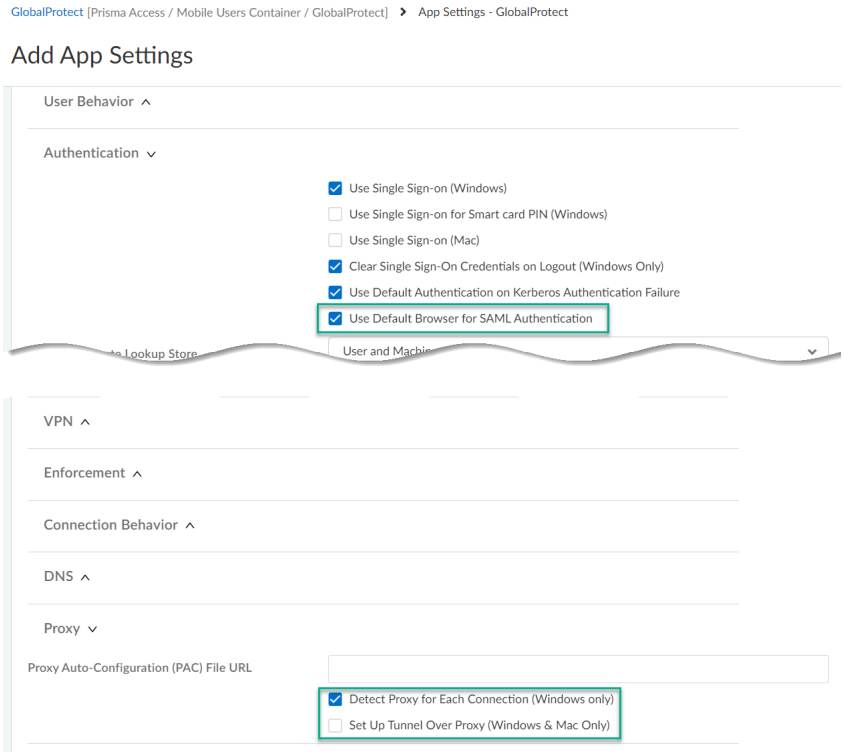
Die folgenden Schritte leiten private Anwendungen, die in Ihrem Rechenzentrum gehostet werden, an GlobalProtect und Anfragen an Internet- und öffentliche SaaS-Anwendungen an den expliziten Proxy.

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Bearbeiten Sie die Einstellungen des GlobalProtect-Portals.

Gehen Sie zu **GlobalProtect** > **App-Einstellungen** > **App-Konfiguration** > **Erweiterte Einstellungen**.

1. Führen Sie in den Einstellungen für den **Proxy** Folgendes aus:
   - Aktivieren Sie **Proxy für jede Verbindung erkennen**.
   - Deaktivieren Sie **Tunnel über Proxy einrichten (nur Windows und Mac)**.
2. Führen Sie in den Einstellungen für die **Authentifizierung** Folgendes aus:
   - Aktivieren Sie **Standardbrowser für SAML-Authentifizierung verwenden**.




**STEP 3 |** Erstellen Sie in GlobalProtect einen Split-Tunnel, mit dem Sie den internen Datenverkehr zu GlobalProtect leiten können.

Gehen Sie zu **GlobalProtect** > **Tunneleinstellungen** > **Split-Tunneling**. Konfigurieren Sie einen Split-Tunnel basierend auf Domäne (FQDN), Zugriffsrouten oder Anwendungen.

 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** Konfigurieren Sie die PAC-Datei, um die Domänen auszuschließen, die Sie für den GlobalProtect-Split-Tunnel angegeben haben.

Um die PAC-Datei herunterzuladen, damit Sie sie bearbeiten können, gehen Sie zu **Workflows** > **Einrichtung Prisma Access** > **Expliziter Proxy** > **Infrastruktur** > **Infrastruktureinstellungen** > **Proxy-Autokonfiguration**.

Das folgende Beispiel zeigt eine PAC-Datei mit der URL, die private Apps hostet (internal-app.corp.com), unter Umgehung des internen Proxys. Die Parameter in der folgenden PAC-Datei sind allesamt Beispielwerte:

- Der Hostname des Portals ist `splittunnel.gpcloudservice.com`.
- Die Gateways mobiler Benutzer sind im Platzhalter-FQDN `*examplegateways.gw.gpcloudservice.com` enthalten.
- Die PAC-Datei-URL lautet `https://pacfileurl.pac`.
- `internal-app.corp.com` hostet die privaten Apps, die von Mobile Benutzer – GlobalProtect geschützt werden.
- Okta wird für die SAML-Authentifizierung verwendet.
- Die URL des expliziten Proxys ist `example.proxy.prismaaccess.com`.

```
function FindProxyForURL(url, host) { /* Bypass FTP */ if
 (url.substring(0,4) == "ftp:") return "DIRECT"; /* Bypass
 the Prisma Access Portal Hostname */ if (shExpMatch(host,
 "*.splittunnel.gpcloudservice.com")) return "DIRECT"; /*
 Bypass the Prisma Access Gateway */ if (shExpMatch(host,
 "*examplegateways.gw.gpcloudservice.com")) return "DIRECT"; /*
 Bypass the Prisma Access PAC File URL */ if (shExpMatch(host,
 "https://pacfileurl.pac")) return "DIRECT"; /* Bypass the URLs
 Being Sent to the GlobalProtect Portal */ if (shExpMatch(host,
 "*.internal-app.corp.com")) return "DIRECT"; /* Bypass ACS
 */ if (shExpMatch(host, "*.acs.prismaaccess.com")) return
 "DIRECT"; /* Forward to Prisma Access */ return "PROXY
 example.proxy.prismaaccess.com:8080"; }
```

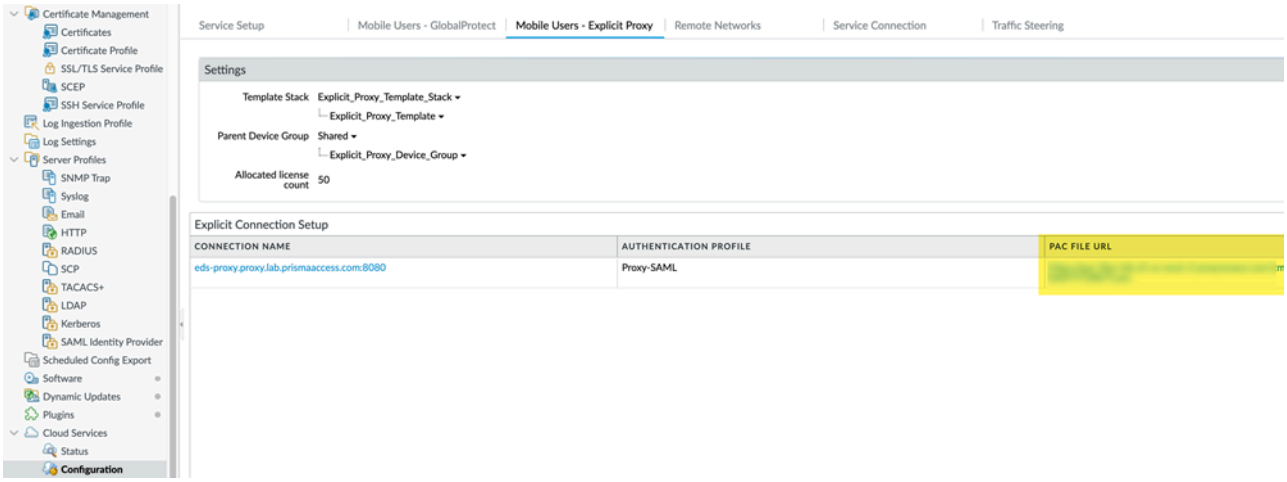
### Expliziter Proxy und GlobalProtect: Einrichten (Panorama)

Führen Sie die folgenden Schritte aus, um GlobalProtect – Mobile Benutzer mit explizitem Proxy zu implementieren.

In diesen Konfigurationsschritten werden die folgenden Annahmen über Ihre Netzwerkumgebung getroffen (wenn sich Ihre Netzwerkumgebung unterscheidet, kann die Konfiguration davon abweichen):

 ©2025 Palo Alto Networks, Inc.

- Mobile Benutzer können den Portal-Hostnamen von GlobalProtect, die Gateway-FQDNs, die URL des expliziten Proxys und die URL der PAC-Datei erreichen und auflösen.
  - Um die Gateway-FQDNs zu finden, wählen Sie **Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Mobile Benutzer – GlobalProtect** > **Gateways** aus.
  - Um die **URL der PAC-Datei** zu finden, wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Mobile Benutzer – Expliziter Proxy** > **URL der PAC-Datei** aus.




- Mobile Benutzer können interne Domänen von GlobalProtect aus auflösen.

**STEP 1 |** Planen Sie Ihre Bereitstellung für Mobile Benutzer – Expliziter Proxy und Ihre GlobalProtect-Bereitstellung (entweder Ihre Bereitstellung für Mobile Benutzer – GlobalProtect oder die alleinstehende GlobalProtect-Bereitstellung).

**STEP 2 |** Entscheiden Sie, welche Anwendungen Sie an GlobalProtect senden möchten und welche an den expliziten Proxy.

Die folgenden Schritte leiten private Anwendungen, die in Ihrem Rechenzentrum gehostet werden, an GlobalProtect und Anfragen an Internet- und öffentliche SaaS-Anwendungen an den expliziten Proxy.


©2025 Palo Alto Networks, Inc.

**STEP 3 |** Konfigurieren Sie im Panorama, das Prisma Access verwaltet, die Einstellungen des GlobalProtect-Portals.

1. Wählen Sie **Netzwerk** > **GlobalProtect** > **Portale** aus.

   Stellen Sie sicher, dass Sie sich in der Vorlage **Mobile_User_Template** aus dem Dropdown-Menü **Vorlage** befinden.
2. Wählen Sie **GlobalProtect_Portal** aus, um die Prisma Access-Portalkonfiguration zu bearbeiten.
3. Wählen Sie die Registerkarte **Agent** und dann die Konfiguration **STANDARD** aus. Alternativ können Sie eine neue Konfiguration **hinzufügen**.
4. Wählen Sie die Registerkarte **App** aus.
5. Nehmen Sie die folgenden App-Konfigurationsänderungen vor:
   - Wählen Sie für **Proxy für jede Verbindung erkennen** die Option **Ja** aus.
   - Wählen Sie für **Tunnel über Proxy einrichten (nur Windows und Mac)** die Option **Nein** aus.
   - Wählen Sie für **Standardbrowser für SAML-Authentifizierung verwenden** die Option **Ja** aus.

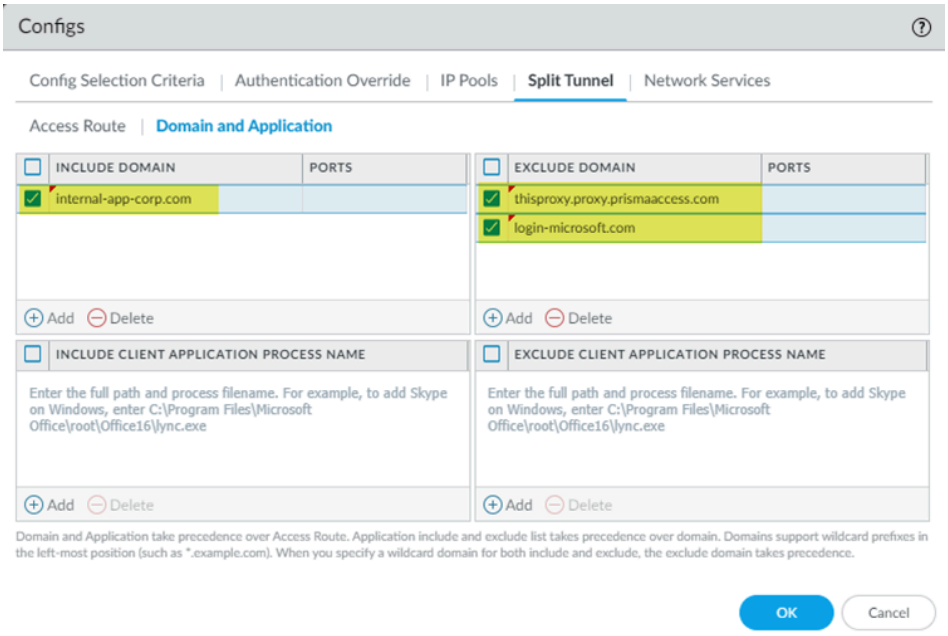
 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** Erstellen Sie in GlobalProtect einen Split-Tunnel, mit dem Sie den internen Datenverkehr zu GlobalProtect leiten können.

Im folgenden Beispiel wird ein Split-Tunnel verwendet, um Datenverkehr basierend auf der Domäne (FQDN) zu leiten. Sie können auch einen Split-Tunnel basierend auf der Zugriffsroute des Datenverkehrs konfigurieren.

1. Wählen Sie **Agent** > **Clienteinstellungen** aus, während Sie sich noch in der Konfiguration des GlobalProtect-Agenten (**Netzwerk** > **GlobalProtect** > **Gateways** > **Externes GlobalProtect-Gateway**) befinden.
2. Wählen Sie die Konfiguration **STANDARD** aus oder **fügen** Sie eine neue Konfiguration hinzu.
3. Wählen Sie **Split-Tunnel** > **Domäne und Anwendung** aus.
4. **Fügen** Sie die **Include-Domäne** und optional die **Ports** hinzu, die mit der Domäne verwendet werden sollen.

   Dieses Beispiel verwendet internal-app.corp.com als URL, mit der Sie Apps in Ihrem Rechenzentrum hosten. Sie fügen diese URL und die SAML-Authentifizierungs-URL in der **Exclude-Domäne** hinzu.




5. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.
6. Führen Sie für Ihre Änderungen die Aktion **Commit und Push** aus.

 ©2025 Palo Alto Networks, Inc.

**STEP 5 |** Konfigurieren Sie die PAC-Datei, um die Domänen auszuschließen, die Sie für den Split-Tunnel eingegeben haben.

Das folgende Beispiel zeigt eine PAC-Datei mit der URL, die private Apps hostet (internal-app.corp.com), unter Umgehung des internen Proxys. Die Parameter in der folgenden PAC-Datei sind allesamt Beispielwerte:

- Der Portal-Hostname ist `splittunnel.gpcloudservice.com`.
- Die Gateways für mobile Benutzer (**Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Mobile Benutzer – GlobalProtect** > **Gateways**) sind im Platzhalter-FQDN `*examplegateways.gw.gpcloudservice.com` enthalten.
- Die **URL der PAC-Datei** (**Panorama** > **Cloud Services** > **Konfiguration** > **Mobile Benutzer – Expliziter Proxy** > **URL der PAC-Datei**) lautet `https://pacfileurl.pac`.
- `internal-app.corp.com` hostet die privaten Apps, die von Mobile Benutzer – GlobalProtect geschützt werden.
- Okta wird für die SAML-Authentifizierung verwendet.
- Die URL des expliziten Proxys ist `example.proxy.prismaaccess.com`.

```
function FindProxyForURL(url, host) { /* Bypass FTP */ if
 (url.substring(0,4) == "ftp:") return "DIRECT"; /* Bypass
 the Prisma Access Portal Hostname */ if (shExpMatch(host,
 "*.splittunnel.gpcloudservice.com")) return "DIRECT"; /*
 Bypass the Prisma Access Gateway */ if (shExpMatch(host,
 "*examplegateways.gw.gpcloudservice.com")) return "DIRECT"; /*
 Bypass the Prisma Access PAC File URL */ if (shExpMatch(host,
 "https://pacfileurl.pac")) return "DIRECT"; /* Bypass the URLs
 Being Sent to the GlobalProtect Portal */ if (shExpMatch(host,
 "*.internal-app.corp.com")) return "DIRECT"; /* Bypass ACS
 */ if (shExpMatch(host, "*.acs.prismaaccess.com")) return
 "DIRECT"; /* Forward to Prisma Access */ return "PROXY
 example.proxy.prismaaccess.com:8080"; }
```

## Expliziter Proxy mit VPNs von Drittanbietern

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

Um VPNs von Drittanbietern mit dem expliziten Proxy zu verwenden, müssen Sie die folgenden Änderungen in Ihrem Netzwerk vornehmen können:

- Sie müssen Ihr VPN von Drittanbietern so konfigurieren, dass es Split-Tunneling durchführt, um Internetdatenverkehr an den expliziten Proxy weiterzuleiten.

  Wenden Sie sich für Unterstützung bei der Konfiguration Ihres VPN von Drittanbietern an Ihren VPN-Anbieter.

 ©2025 Palo Alto Networks, Inc.

- Ändern Sie die PAC-Datei so, dass der explizite Proxy die folgenden VPN-Komponenten umgeht:
  - Alle IP-Adressen, die mit dem VPN von Drittanbietern verknüpft sind
  - Alle für das VPN von Drittanbietern erforderlichen Login-URLs

Im folgenden Beispiel haben Sie die PAC-Datei so konfiguriert, dass der explizite Proxy interne Ressourcen mithilfe privater IP-Adressen sowie Authentifizierungsdatenverkehrsflüsse umgeht.

```
++++++++++++++++ function FindProxyForURL(url, host) { if
 (isPlainHostName(host) || shExpMatch(host, "*.local")
 || isInNet(dnsResolve(host), "10.0.0.0", "255.0.0.0") ||
 isInNet(dnsResolve(host), "127.0.0.0", "255.255.255.0"))
 return "DIRECT"; /* Bypass SAML for AnyConnect Azure */
 if (shExpMatch(host, "login.microsoftonline.com")) return
 "DIRECT"; if (shExpMatch(host, "login.windows.net")) return
 "DIRECT"; if (shExpMatch(host, "login.microsoft.com"))
 return "DIRECT"; /* Forward to Prisma Access */ return "PROXY
 example.proxy.prismaaccess.com:8080"; }
```

## IP-Adressoptimierung für Benutzer von explizitem Proxy – Proxy-Bereitstellungen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>Wenn Sie diese Funktion in Ihrer Prisma Access-Umgebung nutzen möchten, dann wenden Sie sich an Ihr Account-Team, um weiterführende Informationen zu erhalten. | • Prisma Access Version 5.2<br>• Prisma Access Dataplane Version 10.2.4<br>• Panorama-Plug-in Version 5.2.0 |

Bei der IP-Adressoptimierung handelt es sich um einen Satz von Architekturverbesserungen, die die Gesamtzahl der IP-Adressen in Ihrer Bereitstellung reduzieren, Ihre Workflows für Zulassungslisten vereinfachen und gleichzeitig die Ausfallsicherheit verbessern und ein schnelleres Onboarding von Prisma Access-Mandanten ermöglichen.

**IP-Adressaffinität**

Mithilfe der IP-Adressaffinität können Sie sicherstellen, dass SaaS-Apps und Websites, die Benutzersitzungen erfordern, während der gesamten Benutzersitzung dieselbe Ausgangs-IP-Adresse von Prisma Access beibehalten können.

**Vereinfachen Sie das Onboarding von SaaS-Anwendungen**

Das Hinzufügen eines Prisma Access-Standorts oder das Auftreten eines Skalierungsereignisses an einem bereits vorhandenen Prisma Access-Standort kann zur Zuweisung neuer IP-Adressen zu Ihren Bereitstellungen mit explizitem Proxy führen. Es empfiehlt sich, die neuen Ausgangs- und Gateway-IP-Adressen abzurufen und sie in eine Zulassungsliste der SaaS-Anwendungen

 ©2025 Palo Alto Networks, Inc.

aufzunehmen. Durch die IP-Adressoptimierung wird die Anzahl der IP-Adressen reduziert, die Sie in großen Bereitstellungen verwalten müssen.

**Fehlerbehebung**

Wenn Sie die IP-Adressoptimierung für bestimmte Anwendungen durchführen wollen, können Sie diese der URL-Kategorie oder der externen dynamischen Liste (EDL) hinzufügen. Nachdem Sie die speziellen Objekte konfiguriert haben, erhalten nur die Domänen, die in diesen Objekten enthalten sind, die IP-Adressoptimierung.

Panorama – Konfigurieren Sie die URL-Kategorie als **PANW EP URL-Liste für die IP-Affinität** oder die EDL als **PANW EP IP-Affinitätsliste**. Vermeiden Sie Platzhaltereinträge wie z. B. **.*** oder Top-Level-Domänen wie **.com**.

Strata Cloud Manager – Unterstützt die URL-Liste **PANW EP URL-Liste für die IP-Affinität**.

# DNS-Auflösung für Bereitstellungen für mobile Benutzer – Expliziter Proxy

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Wenn Sie diese Funktion in Ihrer Prisma Access-Umgebung nutzen möchten, wenden Sie sich an Ihr Kontoteam, um mehr zu erfahren. | ❑ Prisma Access-Lizenz<br>❑ Prisma Access-Version 5.2.0 |

Mit Prisma Access können Sie DNS-Server angeben, um sowohl unternehmensinterne als auch externe Domänen aufzulösen. Prisma Access leitet die DNS-Anfrage basierend auf der Konfiguration Ihrer DNS-Server weiter. Der explizite Proxy unterstützt die folgenden DNS-Funktionalitäten:

- Verwendung eines Drittanbieterbrowsers mit dem expliziten Proxy
- Verwendung eines regionenspezifischen DNS-Servers mit Prisma Access Browser

- *Die Konfiguration des DNS-Proxy für den expliziten Proxy hat Vorrang vor internen DNS-Servereinstellungen, die unter **Einrichtung Prisma Access** definiert sind.*
- *Nachdem Sie den DNS-Proxy für den expliziten Proxy aktiviert haben, müssen Sie die vorhandene DNS-Konfiguration von **Einrichtung Prisma Access** > **Interne DNS-Server** nach **Workflows** > **Einrichtung Prisma Access** > **Expliziter Proxy** > **Infrastruktureinstellungen** > **DNS-Proxy** migrieren.*

### DNS-Einstellungen konfigurieren

Führen Sie die folgenden Schritte aus, um DNS-Proxy-Einstellungen zu konfigurieren:

 ©2025 Palo Alto Networks, Inc.

1. Fügen Sie eine DNS-Serverregel des expliziten Proxy hinzu.
   1. Gehen Sie zu **Workflows** > **Einrichtung Prisma Access** > **Expliziter Proxy** > **Infrastruktureinstellungen**.
   2. Klicken Sie auf das Einstellungssymbol und gehen Sie zu **Client-DNS**.
   3. Klicken Sie auf **Region hinzufügen** und geben Sie einen eindeutigen Namen an.
   4. Wählen Sie eine Region oder einen Standort oder **Weltweit** aus.

      *Wenn Sie mehrere Proxy-Einstellungen mit einer Kombination aus „Weltweit“- und „Schauplatz“-Einstellungen angeben, verwendet Prisma Access die Einstellungen für die Standortgruppe, dann die für „Schauplatz“ und dann die für „Weltweit“. Prisma Access wertet die Regeln in der Liste von oben nach unten aus.*
   5. Fügen Sie die IP-Adresse des DNS-Servers hinzu.

2. Wählen Sie aus, ob Prisma Access **interne Domänen auflösen** soll oder nicht. Falls ja, müssen Sie eine oder mehrere **Interne Domänenauflösungsregeln hinzufügen**.

3. Sie können **Interne Domänenauflösungsregeln hinzufügen** und definieren.

   *Derzeit werden **Interne Domänenauflösungsregeln** nur für Prisma Access Browser und Agent-Proxy unterstützt.*
4. Fügen Sie unter **Primärer DNS** und **Sekundärer DNS** einen eindeutigen **Namen** für die Regel und eine benutzerdefinierte IP-Adresse hinzu.
5. Wählen Sie **Prisma Access-Standard** aus, um den standardmäßigen Prisma Access-DNS-Server zum Auflösen interner Domänen zu verwenden. Wenn Ihr interner DNS-Server nur die von Ihnen angegebenen Domänen auflösen soll, geben Sie die aufzulösenden Domänen in die **Domänenliste** ein.
6. Wenn Sie über einen **benutzerdefinierten** DNS-Server verfügen, der auf Ihre internen Domänen zugreifen kann, geben Sie die IP-Adressen vom **primären DNS-Server** und **sekundären DNS-Server** an.

7. Wenn Ihr interner DNS-Server nur die von Ihnen angegebenen Domänen auflösen soll, geben Sie die aufzulösenden Domänen in die **Domänenlisten** ein. Geben Sie vor der Domäne ein Sternchen an, z. B. *.acme.com. Klicken Sie auf **Speichern**.
8. Wählen Sie **Konfiguration übertragen** aus, um Ihre Konfigurationsänderungen zu speichern und übertragen.

 ©2025 Palo Alto Networks, Inc.

# Anzeigen von Zuordnungen von Benutzern zu IP-Adressen oder Benutzergruppen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Panorama Managed Prisma Access | • Prisma Access-Lizenz |

Mit Prisma Access Insights können Sie die Zuordnung von Benutzern zu IP-Adressen oder Benutzergruppen für mobile Benutzer in Echtzeit anzeigen. Für Remote-Netzwerke und Dienstverbindungen können Sie die Zuordnungen von Benutzern zu Benutzergruppen anzeigen.

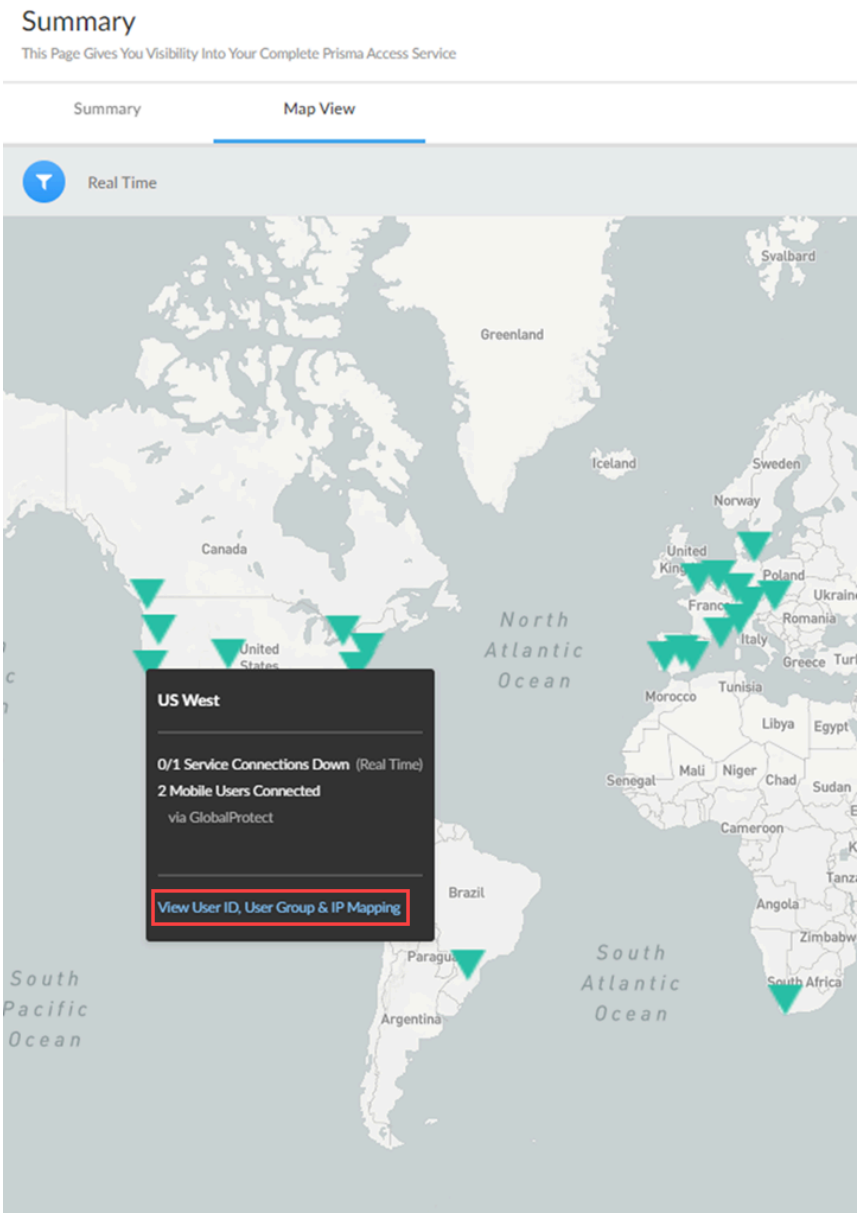
Die umgekehrten Dreiecke auf der Karte sind farblich gekennzeichnet, um den Prisma Access-Standortstatus anzuzeigen:

- Grün: Alle Instanzen sind aktiv.
- Rot: Alle Instanzen sind inaktiv.
- Gelb: Instanzen zeigen eine Kombination aus den Status „aktiv“, „inaktiv“ und „unbekannt“ und erfordern möglicherweise Ihre Aufmerksamkeit.
- Grau: Alle Instanzen haben den Status „unbekannt“.

**STEP 1 |** Wählen Sie im Dashboard **Zusammenfassung** die **Kartenansicht** aus.

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Bewegen Sie den Mauszeiger über einen Standort, bis ein Popup-Dialogfeld angezeigt wird.




**STEP 3 |** Wählen Sie im Dialogfeld die Option **Benutzer-ID, Benutzergruppen und IP-Zuordnung anzeigen** aus. Daraufhin wird das Dialogfeld **Prüfung der Benutzer-ID und Benutzergruppenverteilung** geöffnet.

**STEP 4 |** Wählen Sie den **Prisma AccessStandort** und den **Knotentyp** aus. Der **Prisma Access-Standortfilter** wird nicht berücksichtigt, wenn der **Knotentyp Mobile Benutzer (GlobalProtect)** lautet.

Für Remote-Netzwerke und Dienstverbindungen können Sie nur die Zuordnungen von Benutzer-ID zu Benutzergruppe anzeigen.

1. Wählen Sie einen **Prisma Access-Standort** aus. Wenn dem von Ihnen ausgewählten Prisma Access-Standort keine Remote-Netzwerke oder Dienstverbindungen zugeordnet sind, wird im Feld **Remote-Netzwerkstandort** oder im Feld **Dienstverbindungsstandort** die Meldung

 ©2025 Palo Alto Networks, Inc.

„Keine Daten verfügbar“ angezeigt, und die Schaltflächen **Benutzergruppen anzeigen** und **In CSV exportieren** sind deaktiviert.

2. Wählen Sie unter **Knotentyp** die Option „Remote-Netzwerke“ oder „Dienstverbindungen“ aus.
3. Wählen Sie im Feld **Remote-Netzwerkstandort** oder **Standort Dienstverbindungen** den Standort aus, von dem aus Sie die Daten abrufen möchten.
4. Wählen Sie unter „Ansicht“ aus, ob Sie sehen möchten, zu welchen Benutzergruppen eine Benutzer-ID gehört („Benutzer“) oder welche Benutzer zu einer bestimmten Gruppe („Gruppe“) gehören, die dem Standort zugeordnet ist.

   - Wenn Sie **Benutzer** auswählen, geben Sie die **Benutzer-ID des Benutzers** ein (z. B. saas\testuser3), um die Benutzer-ID der Benutzergruppe zuzuordnen. Wählen Sie anschließend die Option **Benutzergruppen anzeigen** aus. Unter **Benutzer-ID-IP-Zuordnungen** wird eine Liste aller Gruppen angezeigt, zu denen die Benutzer-ID gehört.

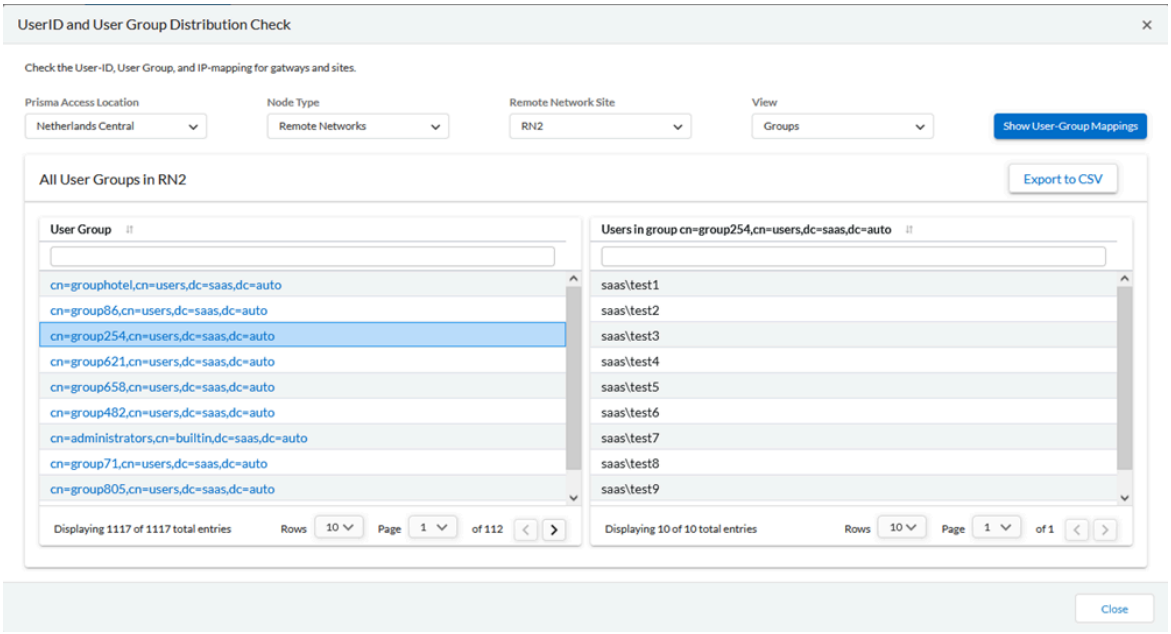
     Sie können nach einer bestimmten Gruppe suchen, indem Sie den Gruppennamen oder eine Zeichenfolge eingeben, die in dem gesuchten Gruppennamen enthalten ist. Geben Sie dazu den Namen oder die Zeichenfolge in das Textfeld **Benutzergruppe** ein. Wenn Sie nach einer Gruppe suchen, die nicht existiert, wird eine Fehlermeldung mit der Meldung „Keine Daten verfügbar“ angezeigt. Sie können die Liste der Gruppen auch sortieren, indem Sie zum Umschalten auf das Pfeilsymbol neben **Benutzergruppe** klicken. Durch Klicken auf die Vorwärts- und Rückwärtspfeile können Sie die Anzahl der Einträge auswählen, die Sie anzeigen möchten, und durch die Seiten blättern.

     Wenn Sie die Option **Gruppen** und anschließend **Benutzergruppenzuordnungen anzeigen** auswählen, werden unter **Alle Benutzergruppen*<selected_site> alle Gruppen angezeigt, die am Standort verfügbar sind.*** Wenn Sie eine Gruppe auswählen, werden rechts alle Benutzer angezeigt, die zu der Gruppe gehören. Die Schaltfläche **In CSV exportieren** wird aktiviert, und Sie können alle Benutzer, die zu dieser Gruppe gehören, in eine CSV-Datei exportieren. Die exportierte CSV-Datei enthält alle Einträge für die Gruppe, auch wenn sie zum Zeitpunkt des Exports nicht in der Benutzeroberfläche angezeigt werden.

     Sie können nach einer bestimmten Gruppe suchen, indem Sie den Gruppennamen oder eine Zeichenfolge eingeben, die in dem gesuchten Gruppennamen enthalten ist. Geben Sie dazu den Namen oder die Zeichenfolge in das Textfeld **Benutzergruppe** ein. Wenn Sie nach einer Gruppe suchen, die nicht existiert, wird eine Fehlermeldung mit der Meldung „Keine Daten verfügbar“ angezeigt. Sie können die Liste der Gruppen auch sortieren, indem Sie zum Umschalten auf das Pfeilsymbol neben **Benutzergruppe** klicken.

 ©2025 Palo Alto Networks, Inc.

Mit den Vorwärts- und Rückwärtspfeilen können Sie die Anzahl der Einträge auswählen, die Sie anzeigen möchten, und durch die Seiten blättern.




**Knotentyp**: **Mobile Benutzer (GlobalProtect)**

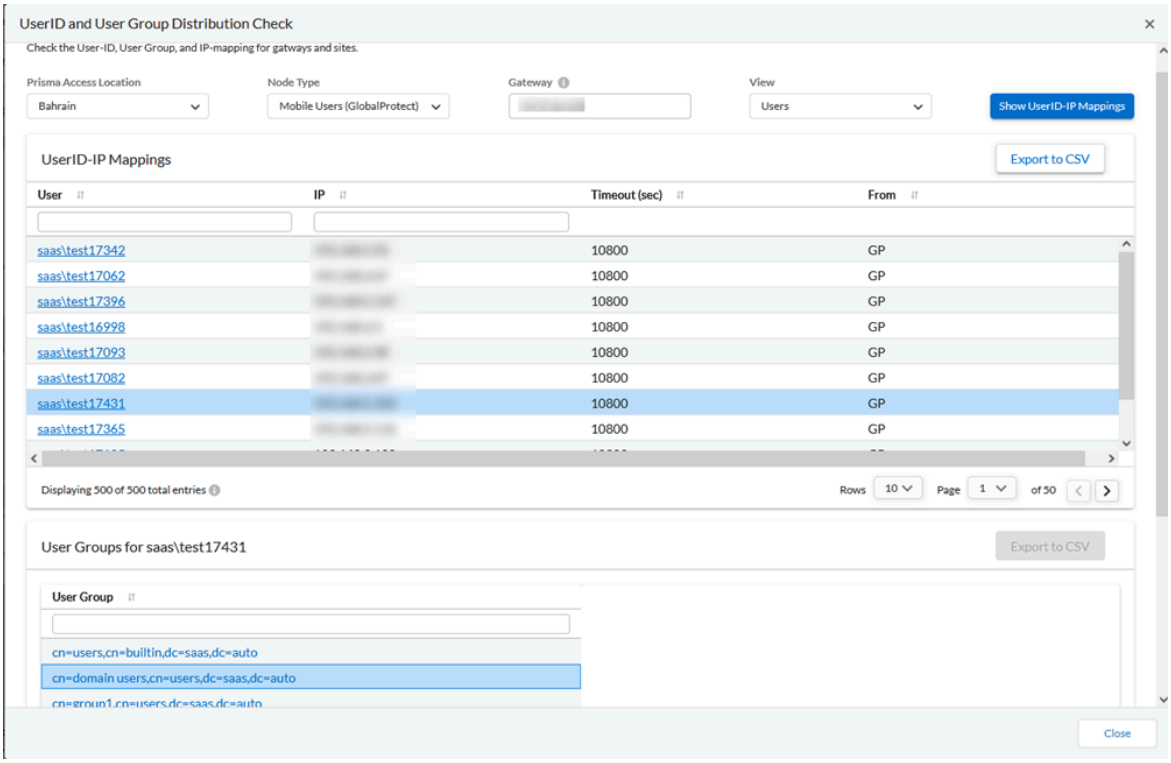
Sie können die Zuordnung von Benutzer-ID zu IP sowie die Zuordnung von Benutzer-ID zu Benutzergruppe sehen. Der Filter **Prisma Access-Standort** wird nicht berücksichtigt, wenn der gewählte **Knotentyp Mobile Users (GlobalProtect**) ist. Stattdessen verwendet Prisma Access Insights die GlobalProtect-Gateway-IP-Adresse, um nach den Daten zu suchen.

1. Geben Sie eine GlobalProtect IP-Gateway-Adresse in das Textfeld **Gateway** ein.
2. Wählen Sie unter **Ansicht** aus, ob Sie Daten für die Zuordnung von Benutzer-ID zu Benutzer-IP (Option **Benutzer**) oder von Benutzer-ID zu Benutzergruppen (Option **Gruppen**) für Benutzer anzeigen möchten, die mit Ihrem angegebenen GlobalProtect-Gateway verbunden sind.

   Wenn Sie **Benutzer** ausgewählt haben, wählen Sie **Benutzer-ID-IP-Zuordnungen anzeigen** aus. Daraufhin wird eine Tabelle mit der Zuordnung von Benutzer-ID zu Benutzer-IP zusammen mit dem **Timeout** angezeigt. Aus dieser Tabelle geht hervor, wie lange (in Sekunden) der Eintrag von Benutzer-ID zu Benutzer-IP gültig ist. Wenn Sie einen bestimmten Benutzer auswählen, werden die Gruppen angezeigt, zu denen der Benutzer gehört. Wenn Sie eine Gruppe auswählen, werden alle Benutzer angezeigt, die zu dieser Gruppe gehören. Außerdem wird die Schaltfläche **In CSV exportieren** angezeigt, mit der


©2025 Palo Alto Networks, Inc.

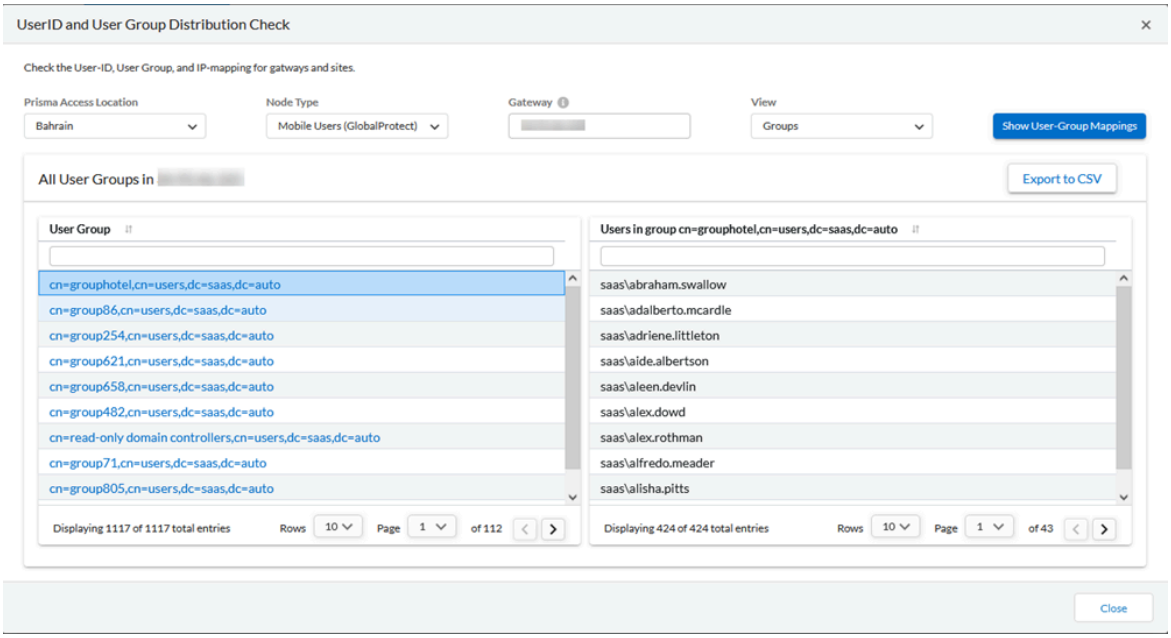
Sie alle Benutzer in dieser Gruppe exportieren können – unabhängig von der gefilterten Ansicht, die auf der Benutzeroberfläche angezeigt wird.




Wenn Sie **Gruppen** ausgewählt haben, wählen Sie die Option **Benutzergruppenzuordnungen anzeigen** aus. Daraufhin wird unter **Benutzergruppe** eine Liste aller Benutzergruppen angezeigt, die zu diesem GlobalProtect-Gateway gehören. Wenn Sie eine Benutzergruppe auswählen, werden rechts alle Benutzer angezeigt, die zu dieser Gruppe gehören. Außerdem wird die Schaltfläche **In CSV exportieren** angezeigt, mit

 ©2025 Palo Alto Networks, Inc.

der Sie alle Benutzer in dieser Gruppe exportieren können – unabhängig von der gefilterten Ansicht, die auf der Benutzeroberfläche angezeigt wird.



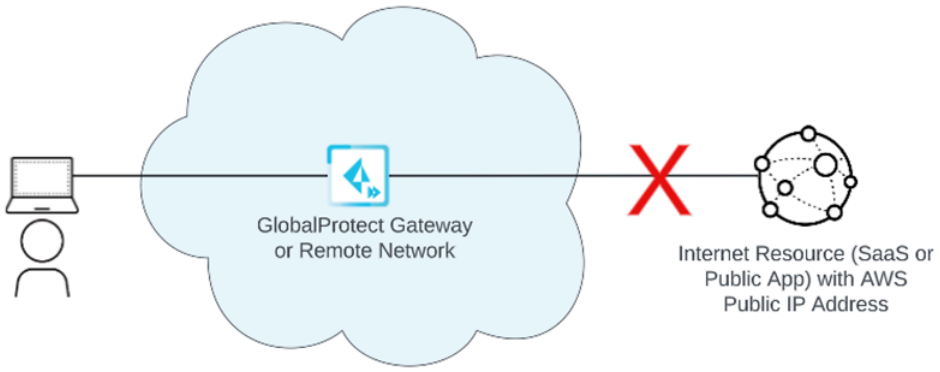

 ©2025 Palo Alto Networks, Inc.

# Probleme beim Zugriff auf Websites von mobilen Benutzern melden

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

Einige Websites wie stubhub.com, ticketmaster.com oder dollartree.com blockieren den Datenverkehr aus dem IP-Adressbereich von AWS Cloud. Wenn durch Prisma Access gesicherte Benutzer versuchen, auf diese Websites zuzugreifen, kann ihnen der Zugriff mit folgender Meldung im Webbrowser verweigert werden:

```
Zugriff verweigert. Sie haben keine Berechtigung, auf diesem
 Server auf „http://www.dollartree.com/“ zuzugreifen. Referenznr.
 18.7f955b8.1509600370.44eb7c8
```




Wenn Sie dieses Problem melden möchten, rufen Sie über einen Webbrowser https://reportasite.gpcloudservice.com/ auf und geben Sie dort die URL der Website an, auf die nicht zugegriffen werden kann. Nach 24–48 Stunden kehren Sie zu https://reportasite.gpcloudservice.com/ zurück und geben die gleiche URL erneut ein, um den Status anzuzeigen.

Palo Alto Networks stellt Ihnen die IP-Adresse zur Verfügung, die von der URL verwendet wird. In einigen Fällen müssen Sie diese IP-Adresse zu den Zulassungslisten Ihres Unternehmens hinzufügen, damit dieser Datenverkehr nicht ohne Rückmeldung verworfen wird. Wenn Sie URLs haben, die weitergeleitet werden, fügen Sie folgende IP-Adressen zu Ihren Zulassungslisten hinzu:

- 65.154.226.160
- 154.59.126.110
- 66.232.36.110

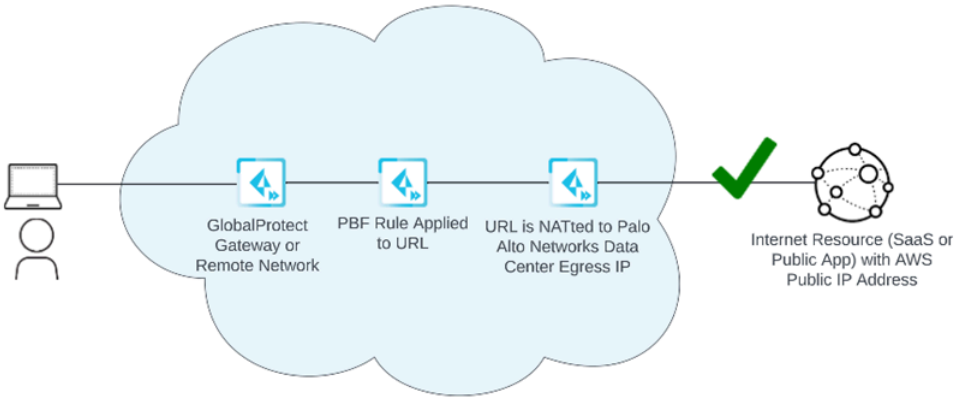

©2025 Palo Alto Networks, Inc.

### Prisma Access – URL-Weiterleitungsprozess

Einige Websites blockieren den Datenverkehr aus einem Cloud-IP-Adressbereich. Wenn durch Prisma Access gesicherte Benutzer versuchen, auf diese Websites zuzugreifen, kann ihnen der Zugriff verweigert werden. Palo Alto Networks überprüft alle diese gemeldeten Websites, um sicherzustellen, dass der Zugriff auf diese Websites wiederhergestellt wird. Wird ein Zugriffsproblem gefunden, kategorisiert es die Website und fügt eine Ausgangsrichtlinie hinzu, die durch eine Netzwerkadressübersetzung (Network Address Translation, kurz NAT) der IP-Adresse dafür sorgt, dass diese wieder zugänglich ist. Palo Alto Networks überprüft die Websites gründlich, um ihre Reputation zu ermitteln. Nur Websites mit einer makellosen Reputation werden der Ausgangsregel hinzugefügt, alle anderen werden abgelehnt. Dabei wird folgendes Verfahren verwendet:

1. Sie teilen uns unter https://reportasite.gpcloudservice.com/ die URL mit Zugriffsproblemen mit.
2. Site Reliability Engineering(SRE)-Automatisierung überprüft die URL.
3. Wenn SRE die URL als sicher bewertet, wird eine richtlinienbasierte Weiterleitungsregel (Policy-Based Forwarding, kurz PBF) auf die URL und ihre übergeordnete Domäne angewendet.
4. Der Datenverkehr wird über Prisma Access vom GlobalProtect-Gateway oder Remote-Netzwerk zu einem URL-Verarbeitungshub geleitet. Dort wird die PBF-Regel auf die Domäne angewendet und vom Hub zu einem Rechenzentrum von Palo Alto Networks.
5. Wenn der Datenverkehr vom Rechenzentrum ausgeht, wird die URL der Quelle per Source-NAT in die IP-Adresse des Rechenzentrums umgeschrieben.

Durch diese Maßnahmen wird der Datenverkehr zu und von den SaaS-Anwendungen nicht unterbrochen, da die IP-Adresse des Rechenzentrums eine tadellose Reputation hat.



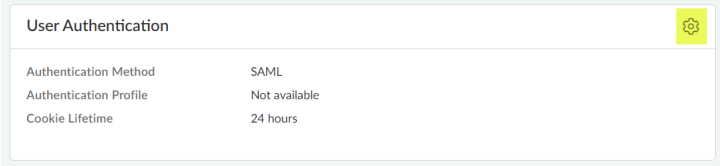

 ©2025 Palo Alto Networks, Inc.

# Mobilen Benutzern die Authentifizierung bei Prisma Access ermöglichen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

Sie können mobile Benutzer bei Prisma Access mit einem der unterstützten Authentifizierungstypen authentifizieren. Befolgen Sie diese Schritte, um die Authentifizierung für mobile Benutzer von GlobalProtect oder dem expliziten Proxy einzurichten.

**STEP 1 |** Gehen Sie zu **Workflows** > **Prisma Access-Einrichtung** und dann entweder zu Ihrer Konfiguration für Mobile Benutzer: GlobalProtect oder Expliziter Proxy und **richten Sie die Benutzerauthentifizierung ein**.




**STEP 2 |** Wählen Sie Ihre **Authentifizierungsmethode** aus den unterstützten Authentifizierungstypen aus.

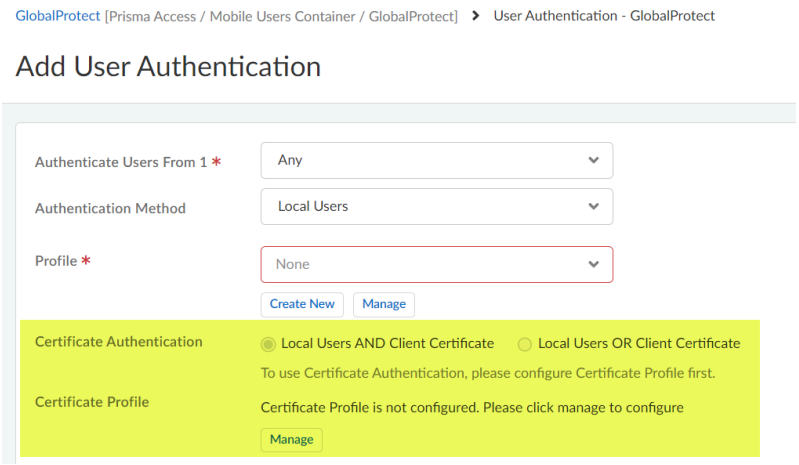
Wenn Sie Prisma Access noch nicht in Ihre Authentifizierungsdienste integriert haben, gehen Sie wie folgt vor:

**STEP 3 |** Wählen Sie das von Ihnen konfigurierte **Profil** für die Authentifizierung aus, damit Prisma Access sich mit dem Dienst verbinden kann, den Sie zur Authentifizierung von Benutzern verwenden möchten.

- Geben Sie das **Profil** für die SAML-Authentifizierung an, wenn Sie SAML in Schritt 2 verwendet haben, oder erstellen Sie ein neues SAML-Authentifizierungsprofil, das mit Prisma Access verwendet werden soll.
- Geben Sie das **Profil** für die CIE-Authentifizierung an, wenn Sie CIE in Schritt 2 verwendet haben, oder erstellen Sie ein neues CIE-Authentifizierungsprofil, das mit Prisma Access verwendet werden soll.
- Geben Sie das **Profil** für die Kerberos-Authentifizierung an, wenn Sie Kerberos in Schritt 2 verwendet haben, oder erstellen Sie ein neues Kerberos-Authentifizierungsprofil, das mit Prisma Access verwendet werden soll.

 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** Geben Sie Einstellungen für die Zertifikatauthentifizierung an:




- **Zertifikatauthentifizierung**

  Verwenden Sie für mehr Sicherheit ein Zertifikat (zusätzlich zu Ihrem Authentifizierungsdienst), um Benutzernamen zu erhalten und Benutzer bei Prisma Access zu authentifizieren. Um Benutzer auf der Grundlage eines Clientzertifikats zu authentifizieren, muss eines der Zertifikatfelder, wie z. B. das Feld „Name des Antragstellers“, den Benutzernamen identifizieren. Mobile Benutzer, die sich erfolgreich über die Clientzertifikatauthentifizierung authentifizieren, haben keine Möglichkeit, sich von der GlobalProtect-App abzumelden.

  Mit Prisma Access können Sie festlegen, dass mobile Benutzer sowohl die Zertifikatauthentifizierung als auch die Authentifizierung basierend auf dem Authentifizierungstyp bestehen müssen, oder dass mobilen Benutzern Zugriff gewährt wird, solange sie nur eine dieser Prüfungen erfolgreich bestanden haben.

- **Zertifikatprofil**

  Verwenden Sie ein optionales Zertifikatprofil, um die Zertifikate zu verifizieren, die mobile Benutzer Prisma Access mit einer Verbindungsanfrage vorlegen. Das Zertifikatprofil gibt den Inhalt der Felder „Benutzername“ und „Benutzerdomäne“ an, listet CA-Zertifikate sowie Kriterien für das Blockieren einer Sitzung auf und bietet Möglichkeiten, den Widerrufsstatus von CA-Zertifikaten zu ermitteln. Da das Zertifikat Teil der Authentifizierung für den mobilen Benutzer ist, müssen Sie Zertifikate, die in Zertifikatprofilen verwendet werden, für Ihre Benutzer vor deren Erstanmeldung bereitstellen. Das Zertifikatprofil gibt an, welches Zertifikatfeld den Benutzernamen („Antragsteller“ oder „Alternativer Antragsteller“) enthält. Wenn im Feld „Benutzername“ des Zertifikatprofils „Antragsteller“ angegeben ist, muss das vom Endpunkt präsentierte Zertifikat einen gemeinsamen Namen enthalten, damit der Endpunkt eine Verbindung herstellen kann. Wenn im Feld „Benutzername“ des Zertifikatprofils „Alternativer Antragsteller“ mit einer E-Mail-Adresse oder einem Principal-Name angegeben ist, muss das Zertifikat die entsprechenden Felder enthalten, die als Benutzername verwendet werden, wenn sich die GlobalProtect-App bei Prisma Access authentifiziert.

 ©2025 Palo Alto Networks, Inc.

**STEP 5 |** Geben Sie eine **Cookie-Lebensdauer** für das Cookie an, das die Authentifizierungsdaten der Benutzer speichert.

Nachdem der IdP den Benutzer authentifiziert hat, speichert Prisma Access den Authentifizierungsstatus des Benutzers im ACS (Authentication Cache Service). Die Gültigkeitsdauer der Authentifizierung basiert auf dem Wert für die **Cookie-Lebensdauer**, den Sie hier angeben.

Um zu verhindern, dass Benutzer Probleme mit dem Download großer Dateien vor Ablauf der Cookie-Lebensdauer haben oder das Cookie abläuft, wenn Benutzer über einen längeren Zeitraum auf eine einzelne Website zugreifen, empfiehlt Palo Alto Networks, eine Cookie-Lebensdauer von mindestens einem Tag zu konfigurieren. Wenn Benutzer des expliziten Proxy ein Problem mit dem Ablauf der Cookie-Lebensdauer haben, können sie zu einer anderen Website wechseln, um sich erneut bei ACS zu authentifizieren und das ACS-Cookie zu aktualisieren.

# Authentifizierungsunterstützung und -funktionen

Hier werden die Dienste aufgeführt, die mit Prisma Accessintegriert werden, um die Authentifizierung bereitzustellen, und außerdem auch die Funktionen, die Sie bei der Planung Ihrer Authentifizierungseinrichtung berücksichtigen sollten:

**Authentifizierungsunterstützung:**

- Cloud Identity Engine
- SAML
- TACACS+
- RADIUS
- LDAP
- Kerberos
- MFA
- Lokale Datenbankauthentifizierung

**Highlights der Authentifizierungsfunktion:**

- SSO
- Authentifizierungsportal
- Authentifizierungssequenz

## Authentifizierungsunterstützung

| | |
|---|---|
| **Cloud Identity Engine** | Sie stellen die Cloud Identity Engine für die Benutzerauthentifizierung bereit, indem Sie einen SAML-2.0-basierten Identitätsprovider (IdP), ein Clientzertifikat und eine Kette für die Zertifizierungsstelle (CA) oder beides konfigurieren. Nachdem Sie angegeben haben, wie Sie Ihre Benutzer authentifizieren möchten, richten Sie |

 ©2025 Palo Alto Networks, Inc.

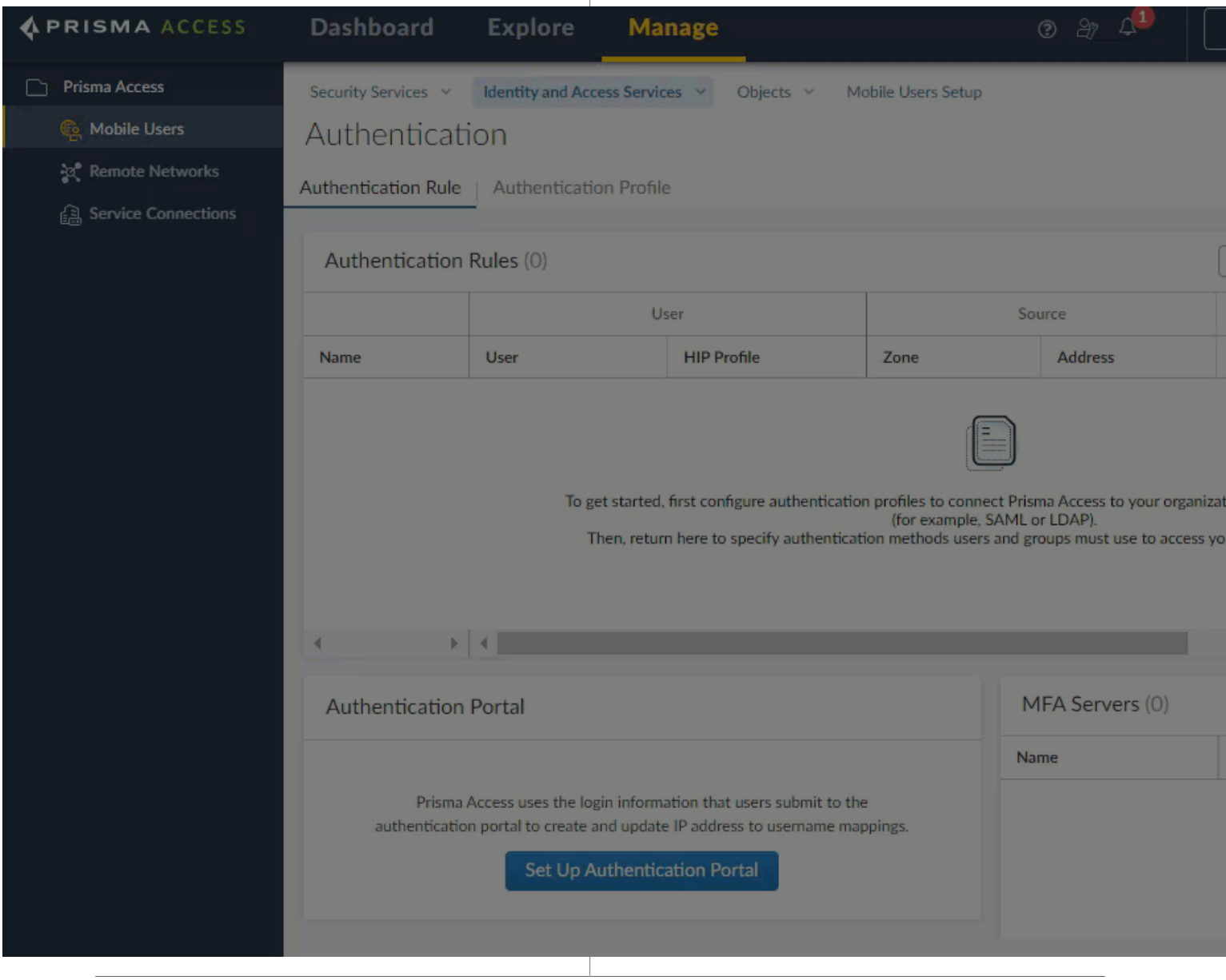
| | |
|---|---|
| | Ihr Authentifizierungsprofil ein, um Ihre Authentifizierungssicherheitsrichtlinie zu definieren und optional die Authentifizierungsrichtlinie auf Ihrer Firewall oder in Panorama zu konfigurieren. |
| **SAML** | Wenn Ihre Benutzer auf Dienste und Anwendungen zugreifen, die sich außerhalb Ihres Netzwerks befinden, können Sie SAML verwenden, um Prisma Access mit einem Identitätsprovider (Identity Provider – IdP) zu integrieren, der den Zugriff auf externe und interne Dienste und Anwendungen steuert. SAML Single Sign-on (SSO) ermöglicht eine einzige Anmeldung für den Zugriff auf mehrere Anwendungen. Das ist in Umgebungen hilfreich, in denen jeder Benutzer auf viele Anwendungen zugreifen muss, weil hier eine separate Authentifizierung pro Anwendung die Benutzerproduktivität beeinträchtigen würde. In diesem Fall ermöglicht SAML Single Sign-on (SSO) eine einzige Anmeldung für den Zugriff auf mehrere Anwendungen. Ebenso können Benutzer über SAML Single Logout (SLO) Sitzungen für mehrere Anwendungen beenden, indem sie sich von nur einer Sitzung abmelden. SSO funktioniert für mobile Benutzer, die über die GlobalProtect-App auf Anwendungen zugreifen, oder für Benutzer in Remote-Netzwerken, die über das Authentifizierungsportal auf Anwendungen zugreifen. SLO steht Benutzern der GlobalProtect-App zur Verfügung.<br><br>*SAML-Authentifizierungsprofile können nicht in Authentifizierungssequenzen verwendet werden.* |
| **TACACS+** | Terminal Access Controller Access-Control System Plus (TACACS+) ist eine Protokollfamilie, die die Authentifizierung und Autorisierung über einen zentralen Server ermöglicht. TACACS+ verschlüsselt Benutzernamen und Passwörter und ist damit sicherer als RADIUS, das nur Passwörter verschlüsselt. TACACS+ ist auch zuverlässiger, da es TCP verwendet, während RADIUS UDP verwendet. |


©2025 Palo Alto Networks, Inc.

| | |
|---|---|
| **RADIUS** | Der Remote Authentication Dial-In User Service (RADIUS) ist ein breit unterstütztes Netzwerkprotokoll, das eine zentrale Authentifizierung und Autorisierung ermöglicht. Sie können Prisma Access auch einen RADIUS-Server hinzufügen, um die Multi-Faktor-Authentifizierung zu implementieren. |
| **LDAP** | Lightweight Directory Access Protocol (LDAP) ist ein Standardprotokoll für den Zugriff auf Informationsverzeichnisse. Sie können LDAP verwenden, um Benutzer zu authentifizieren, die über das Authentifizierungsportal auf Anwendungen oder Dienste zugreifen. |
| **Kerberos** | Kerberos ist ein Authentifizierungsprotokoll, das einen sicheren Informationsaustausch zwischen Parteien ermöglicht, indem eindeutige Schlüssel (sogenannte Tickets) verwendet werden, um die Parteien zu identifizieren. Mit Kerberos können Sie Benutzer authentifizieren, die über das Authentifizierungsportal auf Anwendungen zugreifen. Wenn Kerberos SSO aktiviert ist, müssen sich Benutzer nur beim ersten Zugriff auf Ihr Netzwerk anmelden (z. B. eine Anmeldung bei Microsoft Windows). Nach dieser ersten Anmeldung können sie auf jeden browserbasierten Dienst im Netzwerk zugreifen, ohne sich erneut anmelden zu müssen, bis die SSO-Sitzung abläuft.<br><br>Um Kerberos verwenden zu können, benötigen Sie zunächst ein Kerberos-Konto für Prisma Access, das zur Authentifizierung von Benutzern eingesetzt wird. Ein Konto ist erforderlich, um ein Kerberos-Keytab zu erstellen. Dabei handelt es sich um eine Datei, die den Prinzipalnamen und das gehashte Passwort der Firewall bzw. von Panorama enthält. Für den SSO-Vorgang ist das Keytab erforderlich.<br><br>Kerberos SSO ist nur für Dienste und Anwendungen verfügbar, die in Ihrer Kerberos-Umgebung intern sind. Verwenden Sie SAML, um SSO für externe Dienste und Anwendungen zu aktivieren. |

 ©2025 Palo Alto Networks, Inc.

| | |
|---|---|
| **MFA** | Multi-Faktor-Authentifizierung (MFA) bietet Ihnen die Möglichkeit, mehrere Authentifizierungsmethoden verschiedener Art (sogenannte *Faktoren*) zu implementieren, um Ihre vertraulichsten Dienste und Anwendungen zu schützen. Beispielsweise möchten Sie möglicherweise für wichtige Finanzdokumente eine stärkere Authentifizierung als für Suchmaschinen.<br><br>Prisma Access verfügt über eine integrierte Liste mit den unterstützten MFA-Anbietern, die automatisch aktualisiert wird, wenn neue Anbieter hinzugefügt werden: |




 ©2025 Palo Alto Networks, Inc.

| | |
|---|---|
| **Lokale Datenbankauthentifizierung** | Erstellen Sie eine Datenbank, die lokal in Prisma Access ausgeführt wird und Benutzerkonten (Benutzernamen und Passwörter oder gehashte Passwörter) enthält. Diese Art der Authentifizierung ist nützlich, um in Fällen, in denen Sie nur die gehashten Passwörter, aber nicht die Klartext-Passwörter kennen, Benutzerkonten zu erstellen, die die Anmeldeinformationen vorhandener Unix-Konten wiederverwenden. Für Konten, die Klartext-Passwörter verwenden, können Sie auch Passwortkomplexität und Ablaufeinstellungen definieren. Diese Authentifizierungsmethode steht Benutzern zur Verfügung, die über das Authentifizierungsportal oder die GlobalProtect-App auf Dienste und Anwendungen zugreifen. |

## Highlights der Authentifizierungsfunktion

| | |
|---|---|
| **SSO** | Wenn Sie SAML oder Kerberos verwenden, können Sie Single Sign-on (SSO) implementieren, damit sich Benutzer nur einmal authentifizieren müssen, um auf mehrere Dienste und Anwendungen zuzugreifen. SAML und Kerberos unterstützen SSO. |
| **Authentifizierungsportal** | Leiten Sie Webanforderungen, die einer Authentifizierungsregel entsprechen, an eine Prisma Access-Anmeldeseite um, auf der sie zur Authentifizierung aufgefordert werden. Prisma Access verwendet die Informationen, die der Benutzer an dieses Authentifizierungsportal übermittelt, um Zuordnungen zwischen IP-Adressen und Benutzernamen zu erstellen oder zu aktualisieren.<br><br>Dies ist besonders für Remote-Netzwerke nützlich, wo Datenverkehrsüberwachung und Richtliniendurchsetzung weiterhin auf Grundlage eines Benutzers (oder einer Gruppe) durchgeführt werden müssen. Wenn ein Benutzer Web-Datenverkehr (HTTP oder HTTPS) initiiert, der einer Authentifizierungsregel entspricht, fordert |

 ©2025 Palo Alto Networks, Inc.

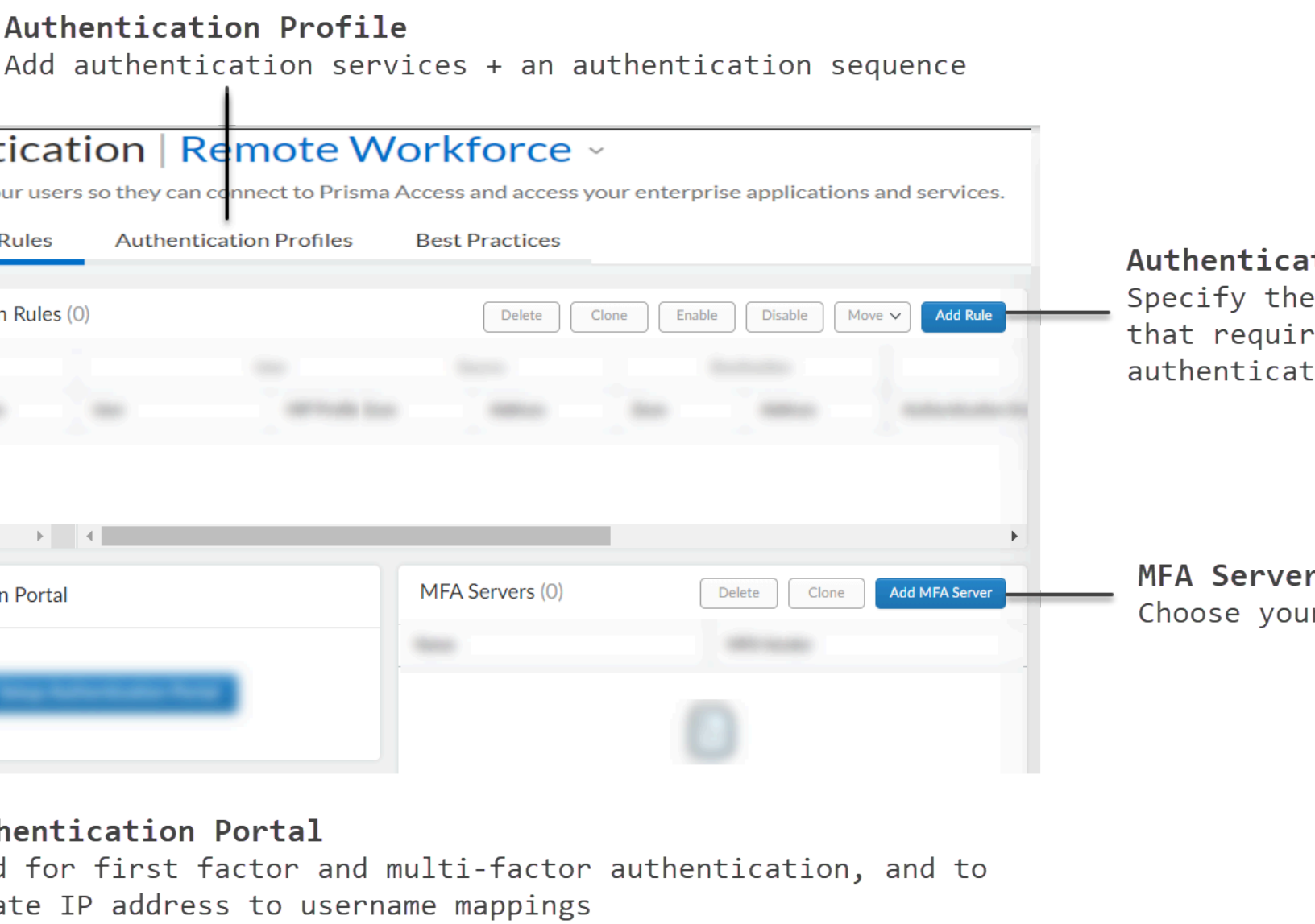
| | |
|---|---|
| | Prisma Access den Benutzer auf, sich über das Authentifizierungsportal zu authentifizieren. Prisma Access erstellt oder aktualisiert die Zuordnung zwischen IP-Adresse und Benutzername basierend auf den Informationen, die der Benutzer an das Portal übermittelt. Dies stellt sicher, dass Sie genau wissen, wer an einem Remote-Netzwerkstandort auf Ihre sensibelsten Anwendungen und Daten zugreift. |
| **Authentifizierungssequenz** | Wenn Sie mehrere Authentifizierungsarten für unterschiedliche Zwecke verwenden, können Sie eine Authentifizierungssequenz festlegen, um Ihre Profile zu bewerten. Prisma Access überprüft jedes Profil anhand Ihres Rankings, bis der Benutzer mit einem Profil erfolgreich authentifiziert werden kann. |

## Authentifizierung einrichten

Zum Einrichten der Authentifizierung mit Prisma Access fügen Sie zuerst Ihre Authentifizierungsdienste zu Prisma Access hinzu. Geben Sie dann den Datenverkehr an, für den eine Authentifizierung erforderlich sein soll. Bauen Sie auf diesen Einstellungen auf, um weitere Authentifizierungsfunktionen wie MFA und Authentifizierungssequenzen hinzuzufügen, oder richten Sie Prisma Access so ein, dass Zuordnungen von IP-Adressen zu Benutzernamen erstellt und aktualisiert werden.

So können Sie loslegen – alle Einstellungen, die Sie zum Aktivieren der Authentifizierung mit Prisma Access benötigen, befinden sich an einem Ort: **Verwalten** > **Konfiguration** > **NGFW- und Prisma Access** > **Identitätsdienste** > **Authentifizierung**. Wählen Sie den Konfigurationsumfang für **Prisma Access** aus.

 ©2025 Palo Alto Networks, Inc.




- **Authentifizierungsregeln:** Hier geben Sie den Datenverkehr an, für den eine Authentifizierung erforderlich sein soll.

  Zum Einrichten einer Authentifizierungsregel gehört auch das Hinzufügen eines Authentifizierungsprofils zur Regel. Wenn Prisma Access Datenverkehr erkennt, der einer Authentifizierungsregel entspricht, werden die im Authentifizierungsprofil definierten Authentifizierungsmethoden und -einstellungen auf den entsprechenden Datenverkehr angewandt. Das Profil definiert, wie sich die Benutzer authentifizieren müssen.

  1. Gehen Sie zu **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Identitätsdienste** > **Authentifizierung** > **Authentifizierungsregel** und **Authentifizierungsregel hinzufügen**. Wählen Sie den Konfigurationsumfang für **Prisma Access** aus.


©2025 Palo Alto Networks, Inc.

2. Definieren Sie die Benutzer, Dienste und URL-Kategorien, die eine Authentifizierung erfordern.
3. Legen Sie die Regelaktion auf **Authentifizieren** fest und wählen Sie das **Profil** aus, das die Authentifizierungsmethode für Datenverkehr definiert, der dieser Regel entspricht.




- **Authentifizierungsprofil:** Fügen Sie hier Ihre Authentifizierungsdienste hinzu und definieren Sie die Authentifizierungseinstellungen.

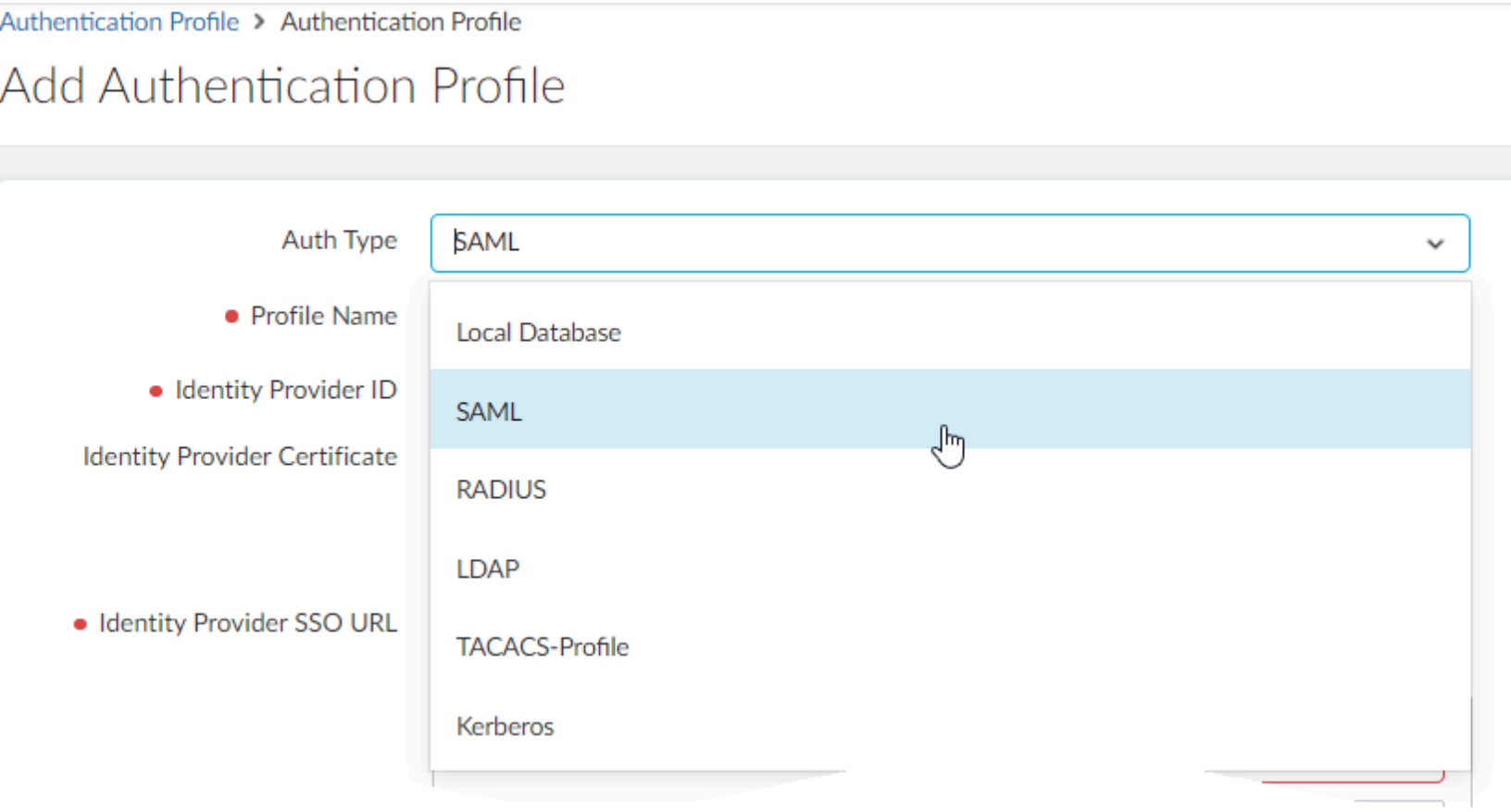
  Verbinden Sie Prisma Access mit den Diensten, die Sie zur Benutzerauthentifizierung verwenden möchten – SAML, TACACS+, RADIUS, LDAP oder Kerberos –, und definieren

 ©2025 Palo Alto Networks, Inc.

Sie Authentifizierungseinstellungen (legen Sie beispielsweise ein Limit für fehlgeschlagene Anmeldeversuche fest).

*Wenn Sie einen lokalen Authentifizierungsdienst verwenden, müssen Sie zuerst eine Dienstverbindung erstellen, um den lokalen Authentifizierungsdienst mit Prisma Access zu verbinden. Kehren Sie dann hierher zurück, um Ihr Authentifizierungsprofil einzurichten.*

Rufen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Identitätsdienste** > **Authentifizierung** > **Authentifizierungsprofil** > **Profil hinzufügen** auf und legen Sie zunächst den **Authentifizierungstyp** fest. Wählen Sie den Konfigurationsumfang für **Prisma Access** aus:



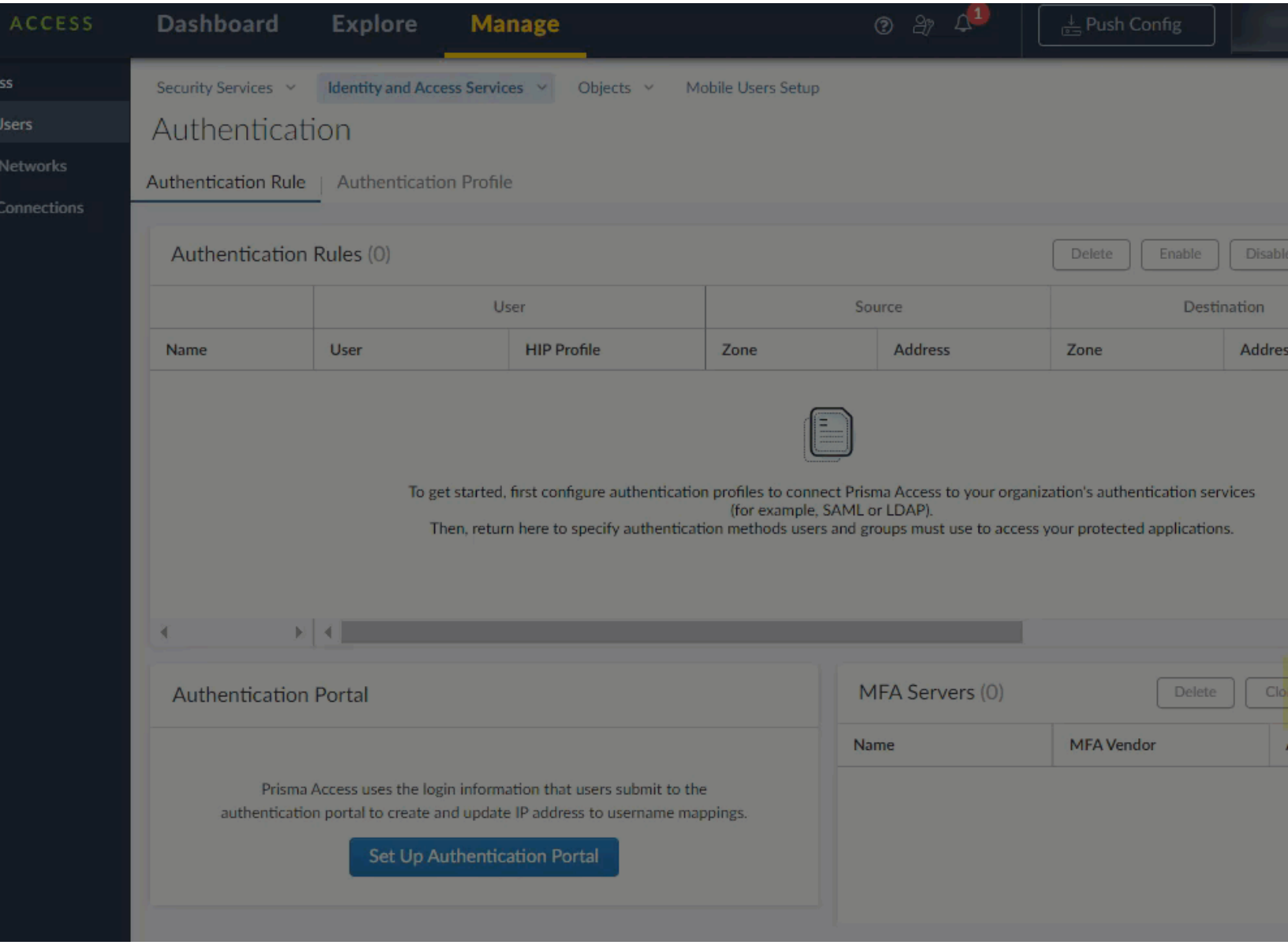

Sie werden aufgefordert, Details zu dem von Ihnen ausgewählten Authentifizierungsdienst hinzuzufügen, die es Prisma Access ermöglichen, eine Verbindung mit dem Dienst herzustellen und Benutzeranmeldedaten und Rollenberechtigungen zu lesen. Im Profil werden zusätzliche Einstellungen zum Anpassen der Authentifizierung bereitgestellt, die je nach Art der eingerichteten Authentifizierung variieren können.

- **MFA-Server:** Geben Sie den von Ihnen verwendeten MFA-Anbieter an.

  Um bei vertraulichen Anwendungen mehrere Methoden zur Benutzerauthentifizierung zu verwenden, fügen Sie zunächst die MFA-Anbieter hinzu, die Sie verwenden möchten (**MFA-**

 ©2025 Palo Alto Networks, Inc.

**Server hinzufügen**). Prisma Access stellt eine Liste zur Verfügung, aus der Sie den MFA-Anbieter auswählen können.



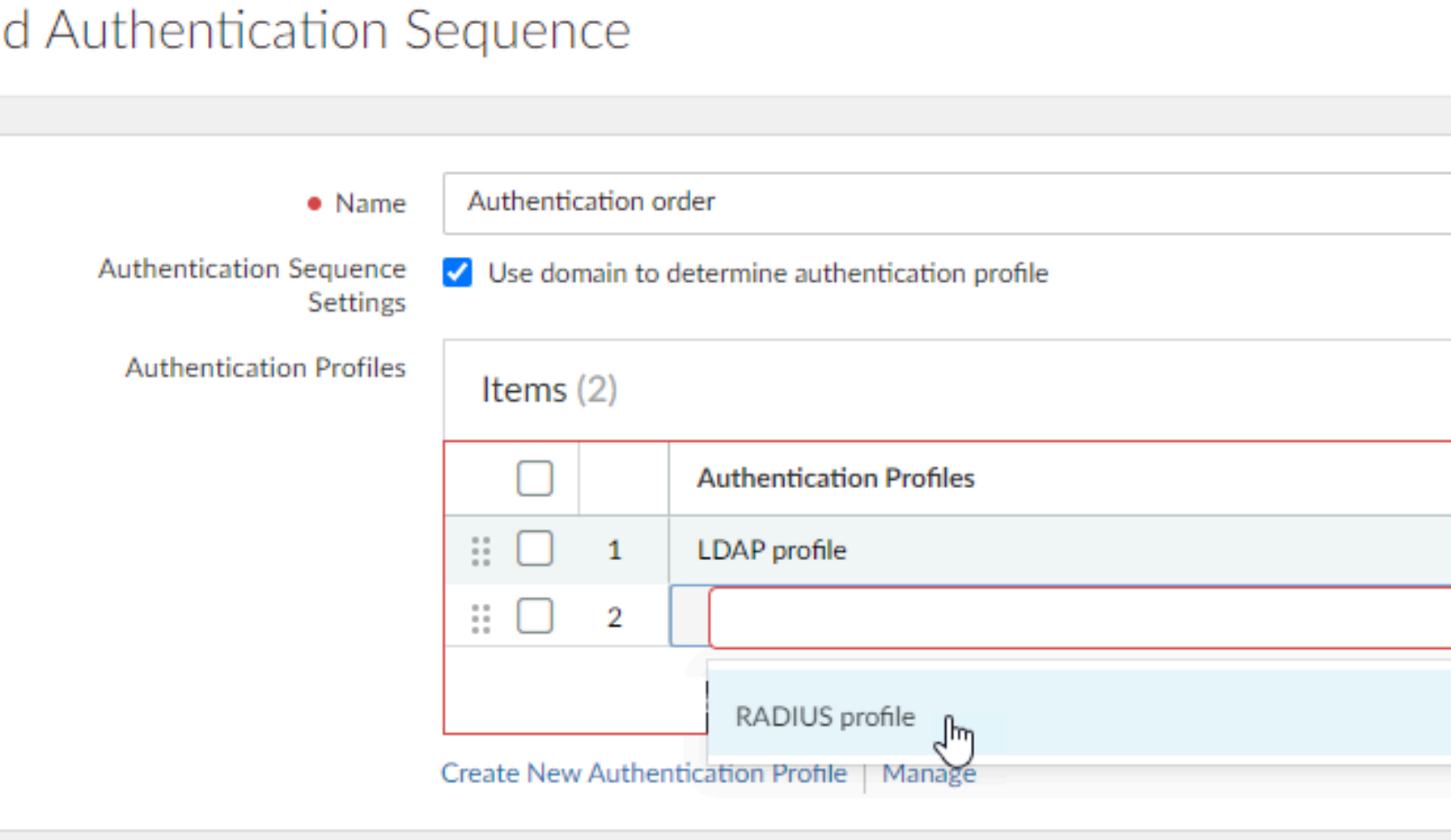

- **Authentifizierungsportal** Richten Sie das Authentifizierungsportal (früher *Captive Portal*) für Benutzer an Remote-Netzwerkstandorten ein und ermöglichen Sie es Prisma Access, Zuordnungen von IP-Adressen zu Benutzernamen zu erstellen.

  Bei der Authentifizierung mit dem ersten Faktor (Benutzername und Kennwort) müssen sich Benutzer an Remote-Netzwerkstandorten über das Authentifizierungsportal authentifizieren. Wenn die Authentifizierung erfolgreich ist, zeigt Prisma Access für jeden weiteren erforderlichen Authentifizierungsfaktor eine MFA-Anmeldeseite an. Prisma Access verwendet die Anmeldeinformationen, die Benutzer übermitteln, um Zuordnungen von IP-Adressen zu Benutzernamen zu erstellen und zu aktualisieren. Das bedeutet, dass Sie immer wissen, wer an einem Remote-Netzwerkstandort auf Webinhalte und Unternehmensanwendungen zugreift.


©2025 Palo Alto Networks, Inc.

- **Authentifizierungssequenz** Ordnen Sie die Authentifizierungsprofile in der Reihenfolge an, in der Prisma Access sie anwenden soll

  Wählen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Identitätsdienste** > **Authentifizierung** > **Authentifizierungsprofil** > **Authentifizierungssequenz hinzufügen** aus. Wählen Sie den Konfigurationsumfang für **Prisma Access** aus. Prisma Access überprüft alle Profile der Reihe nach, bis eines der Profile den Benutzer erfolgreich authentifiziert.




 ©2025 Palo Alto Networks, Inc.

# Mobilen Benutzern den Zugriff auf Unternehmensressourcen ermöglichen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Panorama Managed Prisma Access | • Prisma Access-Lizenz |

Um Prisma Access-Benutzern Internetzugriff zu ermöglichen, müssen Sie keine Netzwerkdienste einrichten, da Prisma Access einen Standard-IP-Adresspool und einen Cloud-Standard-DNS-Server bereitstellt.

Wenn Sie Ihren mobilen Benutzern jedoch Zugriff auf interne Ressourcen in Ihrem Hauptsitz, in Rechenzentren oder an Remote-Netzwerkstandorten ermöglichen möchten, an denen Sie Prisma Access integriert haben, müssen Sie wie folgt vorgehen:

- ❑ Definieren der IP-Adresspools, die Prisma Access verwendet, um Ihren mobilen Benutzern IP-Adressen zuzuweisen,
- ❑ Einrichten der Prisma Access-Dienstinfrastruktur,
- ❑ Integrieren der Dienstverbindungen, um den Zugang zu Ihrem Hauptsitz oder Ihren Rechenzentren zu ermöglichen.

Wenn Sie möchten, dass Ihre mobilen Benutzer eine Verbindung zu Remote-Netzwerkstandorten herstellen, müssen Sie mindestens eine Dienstverbindung konfigurieren, auch wenn Sie nicht vorhaben, die Verbindung zu verwenden, um Zugriff auf Ihre Rechenzentren oder Ihren Hauptsitz zu gewähren. Zwar sind alle Zweigstellen vollständig vermascht, dies gilt jedoch nicht für die Verbindungen mobiler Benutzer. Durch das Erstellen einer Dienstverbindung wird die Hub-and-Spoke-Architektur eingerichtet, die erforderlich ist, damit der Datenverkehr mobiler Benutzer an Ihre Zweigstellennetzwerke weitergeleitet werden kann. In diesem Fall können Sie die Dienstverbindung wie folgt minimal konfigurieren:

- Wenn Sie die Dienstverbindung integrieren, verwenden Sie einen Prisma Access-Standort, der sich in der Nähe Ihrer mobilen Benutzer befindet.
- Wenn Sie den primären IPSec-Tunnel für die Dienstverbindung einrichten, konfigurieren Sie die IPSec-Peer-Authentifizierung und die Tunneleinstellungen mithilfe von Platzhalterwerten.
- Wenn Sie Routing und QoS für die Dienstverbindung aktivieren, fügen Sie Platzhalter-IP-Subnetze hinzu.

  Da Prisma Access keinen Datenverkehr durch diesen Tunnel leitet, stellen Sie aber sicher, dass das von Ihnen verwendete IP-Subnetz nicht mit anderen konfigurierten Subnetzen in Konflikt steht oder sich mit anderen konfigurierten Subnetzen überschneidet, die mit Prisma Access verbunden sind.

**STEP 1 |** Gehen Sie zu **Verwalten** > **Mobile Benutzer** > **Einstellungen für mobile Benutzer** und bearbeiten Sie **Infrastruktureinstellungen**, um die Netzwerkeinstellungen für mobile Benutzer anzupassen.

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Überprüfen Sie oder passen Sie den **Client-IP-Pool** an, den Prisma Access verwendet, um mobilen Benutzern IP-Adressen zuzuweisen.

- Standardmäßig ist der IP-Pool **Weltweit** für alle mobilen Benutzer verfügbar.
- Sie können über **Für jede Region anpassen** einen eingerichteten IP-Pool verwenden, der Regionen oder Standorten zugeordnet ist. Für Regionen oder Standorte, für die Sie keinen IP-Pool angeben, verwendet Prisma Access den IP-Pool „Weltweit“.

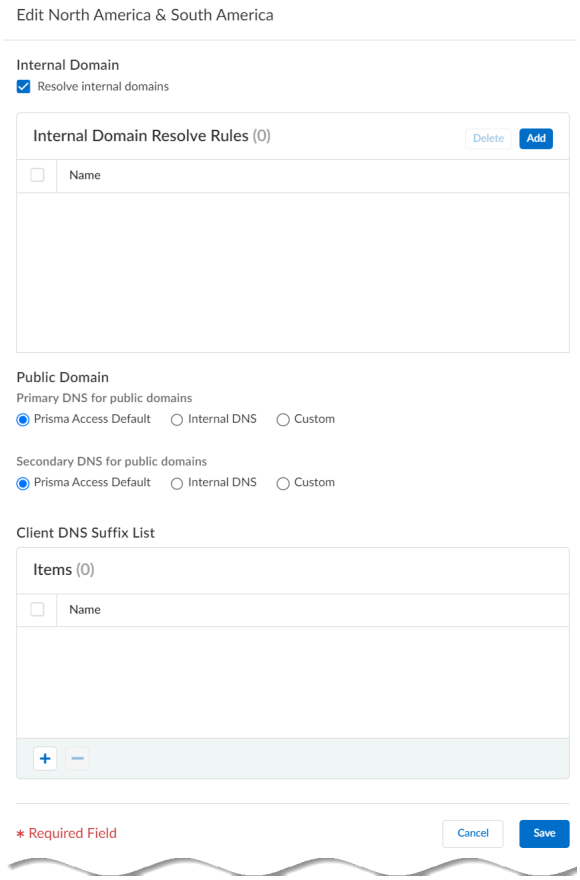
Die von Ihnen definierten IP-Adresspools müssen die folgenden Anforderungen erfüllen:

- ☐ Definieren Sie als Best Practice RFC 1918-kompatible IP-Adresspools, um IP-Adresskonflikte zu vermeiden.
- ☐ Stellen Sie sicher, dass sich die von Ihnen definierten IP-Adresspools nicht mit anderen IP-Adressen überschneiden, die Sie intern verwenden.
- ☐ Stellen Sie sicher, dass sich die von Ihnen definierten IP-Adresspools nicht mit dem Infrastruktur-IP-Adresspool überschneiden, den Sie für Prisma Access verwenden.
- ☐ Geben Sie keine Subnetze an, die sich mit 169.254.0.0/16 und dem Subnetzbereich 100.64.0.0/10 überschneiden, da Prisma Access diese IP-Adressen und Subnetze für den internen Gebrauch reserviert.
- ☐ Stellen Sie sicher, dass Sie einen IP-Adresspool festlegen, der eine ausreichende Abdeckung für alle mobilen Benutzer in Ihrer Organisation ermöglicht, basierend auf den folgenden Richtlinien:
- ☐ Wenn Sie einen weltweiten Adresspool verwenden möchten, der in einer oder zwei Regionen bereitgestellt wird, ist der minimal erforderliche IP-Adresspool /23 (512 IP-Adressen).
- ☐ Wenn Sie beabsichtigen, einen weltweiten Adresspool zu verwenden, der in drei oder mehr Regionen bereitgestellt wird, ist der minimal erforderliche IP-Adresspool /19 (8.192 IP-Adressen), entweder in einem einzelnen IP-Adresspool oder auf mehrere Pools verteilt.
- ☐ Wenn Sie IP-Adresspools pro Region definieren möchten, beträgt die minimale Poolgröße in jeder Region /23 (512 IP-Adressen).
- ☐ Sie müssen keinen IP-Adresspool in Regionen zuweisen, in denen Sie keine Prisma Access-Bereitstellung planen. Wählen Sie beispielsweise die Regionen „Osten der USA (Nord-Virginia)“, „Osten der USA (Ohio)“ und „Westen der USA (Nordkalifornien)“ nur aus, wenn Sie Prisma Access für Benutzer integrieren, für die Sie einen IP-Adresspool nur für die Region „Amerika“ angeben müssen. Beachten Sie jedoch, dass Benutzer in anderen Regionen keine Verbindung mit Prisma Access herstellen können.
- ☐ Wenn Sie eine Kombination aus weltweiten und regionalen Pools definieren möchten, stellen Sie sicher, dass Sie mindestens 512 IP-Adressen pro Region zuweisen. Für eine Bereitstellung in drei Regionen können Sie z. B. 1.024 Adressen in der Region „Europa“ und 512 Adressen „Weltweit“ angeben.
- ☐ Legen Sie als Best Practice IP-Adresspools so fest, dass Sie mindestens eine IP-Adresse für jeden einzelnen mobilen Benutzer in Ihrer Organisation haben, damit diese sich gleichzeitig anmelden können. Wenn Sie einen IP-Adressenpool festlegen, der über eine geringere Anzahl von IP-Adressen als die von Ihnen lizenzierte Anzahl von Benutzern verfügt, zeigt Prisma Access eine Warnmeldung an. Wenn Sie jedoch über einen begrenzten IP-Adresspool verfügen und nicht davon ausgehen, dass sich alle Benutzer gleichzeitig anmelden, können Sie die Meldung ignorieren und eine kleinere Poolgröße verwenden.

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Fügen Sie **Client-DNS**-Einstellungen hinzu: Sie können die Standardeinstellung **Weltweit** verwenden oder die Einstellungen je nach Region anpassen.

Wählen Sie die Region aus, für die Sie die DNS-Einstellungen anpassen möchten:




Aktivieren Sie die Option, diese DNS-Einstellungen zu verwenden, um **interne Domänen auflösen** zu können und optional **den internen DNS-Server auch für die Auflösung von öffentlichen Domänen zu verwenden**. Wenn Sie diese Option nicht auswählen, verwendet Prisma Access seine Cloud-Standard-DNS-Server, um Anfragen für öffentliche Domänen aufzulösen.

*Der DNS-Proxy in Prisma Access sendet die Anfragen an die von Ihnen angegebenen DNS-Server. Die Quelladresse in der DNS-Anfrage ist die erste IP-Adresse in dem IP-Pool, den Sie der Region zuweisen. Um zu gewährleisten, dass Ihre DNS-Anfragen die Server erreichen können, müssen Sie sicherstellen, dass Sie den Datenverkehr von allen Adressen im IP-Adresspool für Ihre mobile Benutzer zu Ihren DNS-Servern zulassen.*

**STEP 4 |** Wenn Sie möchten, dass Ihre mobilen Benutzer auf Ressourcen in Ihren Hauptsitz- oder Rechenzentrumsnetzwerken oder in anderen Zweigstellen zugreifen können, müssen Sie die Prisma Access-Infrastruktureinstellungen konfigurieren, um den Netzwerk-Backbone zu aktivieren.

Gehen Sie zu **Verwalten** > **Prisma Access** > **Einrichtung Prisma Access**.

 ©2025 Palo Alto Networks, Inc.

**STEP 5 |** Um mobilen Benutzern den Zugriff auf Ressourcen in Ihrem Hauptsitz oder Ihren Rechenzentren zu ermöglichen, erstellen Sie Dienstverbindungen, um diese Standorte mit Prisma Access zu verbinden.

Gehen Sie zu **Verwalten** > **Dienstverbindungen** > **Einrichtung von Dienstverbindungen**.

**STEP 6 |** Wenn Sie bereit sind, klicken Sie auf **Konfiguration übertragen**, damit Prisma Access die Einstellungen für Ihre mobilen Benutzer speichert.

 ©2025 Palo Alto Networks, Inc.

# Prisma Access-Remote-Netzwerke

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

Mit Prisma Access für Netzwerke können Sie Ihre Unternehmensskalen und Bürostandorte geografisch verteilen, Ihre Remote-Netzwerkstandorte schnell einbinden und Ihren Benutzern erstklassige Sicherheit bieten. Es bietet eine komfortable Option, durch welche die Komplexität bei der Konfiguration und Verwaltung von Geräten an jedem Remote-Standort beseitigt wird. Der Dienst bietet eine effiziente Möglichkeit, ohne großen Aufwand neue Remote-Netzwerkstandorte hinzuzufügen und die betrieblichen Herausforderungen zu minimieren, indem sichergestellt wird, dass Benutzer an diesen Standorten immer verbunden und sicher sind. Zudem können Sie Richtlinien zentral über Panorama verwalten, um eine konsistente und optimierte Sicherheit für Ihre Remote-Netzwerkstandorte zu gewährleisten.

Zum Verbinden Ihrer Remote-Netzwerkstandorte mit Prisma Access können Sie die Firewall der nächsten Generation von Palo Alto Networks oder ein IPSec-kompatibles Gerät eines Drittanbieters einschließlich SD-WAN verwenden, das einen IPSec-Tunnel zum Dienst aufbauen kann.

Zusätzlich zur IPSec-Tunnelkonnektivität können Sie mit Prisma SD-WAN ein CloudBlade verwenden, das Sie als Remote-Netzwerk einbinden, um den Prisma SD-WAN Controller und ION-Geräte in Prisma Access zu integrieren.

# Planungscheckliste für Remote-Netzwerke

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

**Bevor** Sie Remote-Netzwerke einbinden, stellen Sie sicher, dass Sie die folgenden Konfigurationselemente bereithalten, um sicherzustellen, dass Sie die Dienst- und Durchsetzungsrichtlinie für Benutzer an Ihren Remote-Netzwerkstandorten erfolgreich aktivieren können:

- **Benötigen Sie Zugriff auf Unternehmensressourcen?**

  Wenn Ihr Remote-Netzwerk Zugriff auf Infrastruktur oder Ressourcen in Ihrer Zentrale oder einem Rechenzentrum erfordert, erstellen Sie eine Prisma Access-Dienstverbindung zum Unternehmensstandort. Wenn der Remote-Netzwerkstandort autonom ist und nicht auf Infrastruktur an anderen Standorten zugreifen muss, ist dies nicht erforderlich.

- **Prisma Access Standorte**

  Wenn Benutzer in Ihrer Niederlassung eine Verbindung mit Prisma Access herstellen, bestimmt der von Ihnen gewählte Prisma Access-Standort, in welcher Sprache Inhalte aus dem Internet bereitgestellt werden. Wählen Sie für die beste Benutzererfahrung die Region und den Standort im selben Bezirk wie Ihre Niederlassung aus. Wenn ein Standort nicht im selben Land wie Ihre Niederlassung verfügbar ist, wählen Sie einen Standort, der dieselbe Sprache wie die Mehrheit der Benutzer auf der Website verwendet.

  Nur wenige Standorte sind als **lokale Zonen** gekennzeichnet. Diese Standorte bieten Prisma Access-Compute-Standorte in der Nähe großer Bevölkerungs- und Industriezentren.

- **IP-Subnetze**

  Damit Prisma Access den Datenverkehr zu Ihren Remote-Netzwerken weiterleiten kann, müssen Sie Routinginformationen für die Subnetze bereitstellen, die Prisma Access sichern soll. Hierfür stehen Ihnen verschiedene Möglichkeiten zur Verfügung: Sie können entweder eine statische Route zu jedem Subnetz am Remote-Netzwerkstandort definieren oder BGP zwischen Ihren Dienstverbindungsstandorten und Prisma Access konfigurieren oder eine Kombination beider Methoden verwenden. Wenn Sie sowohl statische Routen konfigurieren als auch BGP aktivieren, haben die statischen Routen Vorrang. Während es praktisch sein könnte, statische Routen zu verwenden, wenn nur wenige Subnetze an Ihren Remote-Netzwerkstandorten vorhanden sind, ermöglicht Ihnen BGP in einer großen Bereitstellung mit Remote-Netzwerken mit überlappenden Subnetzen eine einfachere Skalierung.

- **Modell mit aggregierter Bandbreite** – Die Bandbreite für Ihre Remote-Netzwerkstandorte wird auf aggregierter Ebene pro Compute-Standort zugewiesen. Jeder Standort, den Sie einbinden, hat einen entsprechenden Compute-Standort, für den Bandbreite zugewiesen wird. Sie weisen

 ©2025 Palo Alto Networks, Inc.

Bandbreite pro Compute-Standort und nicht pro Standort zu. Dieses Verfahren wird als *Modell mit aggregierter Bandbreite* bezeichnet.

Das Modell mit aggregierter Bandbreite ist für alle neuen Bereitstellungen verfügbar. Wenn Ihre vorhandene Bereitstellung Bandbreite nach Standort zuweist, können Sie von der Zuweisung von Bandbreite pro Standort zur Zuweisung von Bandbreite pro Compute-Standort migrieren.

*Bevor Sie zum Modell mit aggregierter Bandbreite migrieren, lesen Sie die Informationen unter* Migration zum neuen Modell planen.

Alle Standorte, die Sie einbinden, verwenden die zugewiesene Bandbreite für diesen Compute-Standort gemeinsam. Beispielsweise müssen Sie vier Niederlassungen mit Remote-Netzwerken an den Standorten Singapur, Thailand und Vietnam einbinden. Alle diese Standorte werden dem Compute-Standort „Asien (Südost)“ zugeordnet. Wenn Sie dem Compute-Standort „Asien (Südost)“ eine Bandbreite von 200 Mbit/s zuweisen, teilt Prisma Access diese Bandbreite von 200 Mbit/s auf die vier Niederlassungen auf, die Sie an diesem Standort eingebunden haben. Wenn Sie außerdem auch einen Standort in Hongkong hinzufügen, sollten Sie beachten, dass Hongkong dem Compute-Standort „Hongkong“ zugeordnet ist, sodass Sie die Bandbreite diesem Compute-Standort hinzufügen müssen. Geben Sie eine Mindestbandbreite von 50 Mbit/s pro Compute-Standort an.

Prisma Access ordnet die Bandbreite dynamisch nach Last oder Bedarf pro Standort zu. Im vorherigen Beispiel, bei dem die vier Standorte zusammen bis zu 200 Mbit/s nutzen, kann Prisma Access, wenn mindestens einer der Standorte weniger Bandbreite als die anderen Standorte nutzt, den anderen Standorten, die mehr Bedarf haben, mehr Bandbreite bereitstellen. Auf diese Weise kann die zugewiesene Bandbreite effizienter genutzt werden. Wenn außerdem einer der Standorte ausfällt, teilt Prisma Access die Bandbreite zwischen den verbleibenden Standorten, die am Compute-Standort weiterhin aktiv sind, neu auf.

Standorte, die als **lokale Zonen** gekennzeichnet sind, unterstützen eine maximale Bandbreite von 500 Mbit/s für Remote-Netzwerke. Um eine Bandbreite von 1 Gbit/s zu unterstützen, wenden Sie sich an den Support von Palo Alto Networks. Diese Standorte bieten Prisma Access-Compute-Standorte in der Nähe großer Bevölkerungs- und Industriezentren. Allerdings gelten für sie auch einige Einschränkungen. Um eine lokale Zone hinzuzufügen, wenden Sie sich an Ihren Palo Alto Networks Ansprechpartner.

- Wenn Sie Probleme beim Zugriff auf URLs haben, melden Sie das Websiteproblem dem Support von Palo Alto Networks.
- **Dimensionierungsrichtlinien und Überlegungen zur Bandbreitenzuweisung**

  Wenn Sie die Bandbreite berechnen, die Sie an einem Standort benötigen, berücksichtigen Sie, dass die Bandbreitennutzung sowohl ausgehenden als auch eingehenden Datenverkehr für die Remote-Netzwerkverbindung umfasst (d. h. die zugewiesene Bandbreite entspricht der Summe aus eingehendem und ausgehendem Datenverkehr). Außerdem verwenden alle Standorte, die Sie einbinden, die zugewiesene Bandbreite für diesen Compute-Standort gemeinsam. Um Ihnen die Ermittlung des Bandbreitenvolumens zu erleichtern, die ein bestimmter Standort benötigt, sollten Sie die Bandbreite überprüfen, die von Ihrem ISP an jedem Standort verfügbar ist.

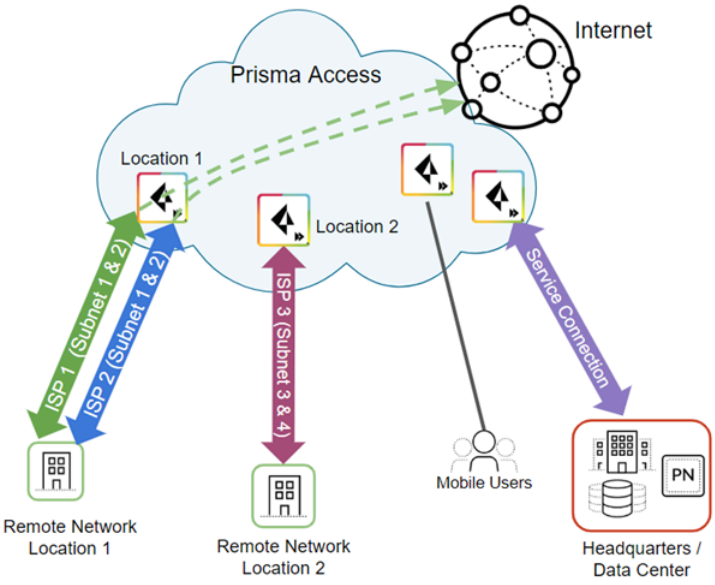
 ©2025 Palo Alto Networks, Inc.

## Überlappende Subnetze

Generell können keine überlappenden Subnetze innerhalb einer Prisma Access-Instanz vorhanden sein. Das heißt, die Subnetze für alle Remote-Netzwerkstandorte, Ihre Dienstverbindungen und Ihre IP-Adresspools für Prisma Access für mobile Benutzer dürfen sich nicht überlappen. Unter bestimmten Umständen können Sie jedoch nicht vermeiden, dass sich Subnetze überlappen, zum Beispiel wenn Sie ein Unternehmen übernommen haben, das Subnetze verwendet, die sich mit Ihren bestehenden Subnetzen überlappen. In einigen Fällen möchten Sie möglicherweise absichtlich zwei Regionen mit überlappenden Subnetzen konfigurieren, zum Beispiel wenn Sie ein separates Gastnetzwerk an einem Einzelhandelsstandort mit unterschiedlichen Richtlinienregeln erstellen möchten.

Mit Prisma Access können Sie Remote-Netzwerkstandorte mit überlappenden Subnetzen einbinden, wobei jedoch nur der internetgebundene Datenverkehrsfluss von Zweigstellen mit überlappenden Subnetzen unterstützt wird. Filialen ohne überlappende Subnetze im selben Mandanten erhalten volle Funktionalität von Prisma Access. Weitere Einzelheiten entnehmen Sie bitte der Tabelle in der folgenden Abbildung.

| Traffic Flow | Supported? |
|---|---|
| Remote Network to Internet | Yes |
| Remote Network to Remote Network (Overlapping Subnets) | No |
| Remote Network to Remote Network (No Overlapping Subnets) | Yes |
| Remote Network to HQ (Overlapping Subnets) | No |
| Remote Network to HQ (No Overlapping Subnets) | Yes |
| HQ to Remote Network (Overlapping Subnets) | No |
| Mobile Users to and from Remote Network (Overlapping Subnets) | No |
| Mobile Users to and from Remote Network (No Overlapping Subnets) | Yes |




Beachten Sie jedoch, dass die Standorte mit überlappenden Subnetzen folgenden Einschränkungen unterliegen:

- Es gibt keinen eingehenden Datenverkehr von Remote-Netzwerk zu Remote-Netzwerk. Die anderen Remote-Netzwerkstandorte wissen nicht, wohin der Datenverkehr geleitet wird, da mehrere Remote-Netzwerkstandorte zu denselben Subnetzen geleitet werden. Benutzer und Dienste an einem beliebigen Remote-Netzwerkstandort können jedoch auf Ressourcen an anderen Remote-Netzwerkstandorten zugreifen, sofern sich am Standort keine Subnetze überlappen und jeder Standort über die Prisma Access-Infrastruktur auf das Internet zugreifen kann.
- Datenverkehr von Ihren Dienstverbindungen kann an keinem Remote-Netzwerkstandort mit überlappenden Subnetzen auf Ressourcen zugreifen, da er über keine Informationen dazu verfügt, an welchen Remote-Netzwerkstandort der Datenverkehr geleitet werden soll. Die Remote-Netzwerkstandorte mit überlappenden Subnetzen können jedoch über Dienstverbindungen auf Ressourcen zugreifen.

 ©2025 Palo Alto Networks, Inc.

- Mobile Benutzer können an den Remote-Netzwerkstandorten mit überlappenden Subnetzen nicht auf Ressourcen zugreifen – auch dies liegt an den Einschränkungen für das eingehende Routing.

> *Wenn Sie Prisma Access mithilfe von Strata Cloud Manager verwalten, gehen Sie zu **Workflows** > **Einrichtung Prisma Access** > **Remote-Netzwerke** > **Erweiterte Einstellungen**. Bearbeiten Sie die Einstellungen für **Überlappende Subnetze**, um überlappende Subnetze zuzulassen. Wenn Sie Panorama zum Verwalten von Prisma Access verwenden, wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Remote-Netzwerke** aus und überprüfen Sie **Überlappende Subnetze**.*

- **IPSec-Terminierungsknoten** – Sie weisen dem Remote-Netzwerk während des Onboardings einen *IPSec-Terminierungsknoten* zu. Sie können maximal 500 Remote-Netzwerkstandorte (für Prisma Access 5.0 und höher) oder 400 Remote-Netzwerkstandorte (für Prisma Access-Releases vor 5.0) pro IPSec-Terminierungsknoten angeben. Weisen Sie dem Compute-Standort, der dem IPSec-Terminierungsknoten entspricht, mehr als 500 Mbit/s zu, um die maximale Anzahl zulässiger Remote-Netzwerke zu unterstützen.

  Es können maximal 200 IPSec-Terminierungsknoten an einem Compute-Standort vorhanden sein. Jeder IPSec-Terminierungsknoten kann Ihnen maximal 1.000 Mbit/s Bandbreite zur Verfügung stellen. Wenn Sie einem Compute-Standort mehr als 1.000 Mbit/s Bandbreite zuweisen, stellt Ihnen Prisma Access einen zusätzlichen IPSec-Terminierungsknoten zur Verfügung.

  - **IPSec-Terminierungsknoten und Upgrades von Releases vor 3.2** – Vor Release 3.2 wurde an einem Compute-Standort für je 500 Mbit/s zugewiesene Bandbreite ein IPSec-Terminierungsknoten zugewiesen. Wenn Sie mit einer Remote-Netzwerkbereitstellung vor 3.2 arbeiten und ein Upgrade auf eine Version 3.2.1 oder höher durchgeführt haben, und wenn Remote-Netzwerkstandorte mehr als 500 Mbit/s für ihren entsprechenden Compute-Standort zugewiesen haben, kann jedes Remote-Netzwerk, das mit dem IPSec-Terminierungsknoten verknüpft ist, bis zu 1.000 Mbit/s Bandbreite unterstützen. Nach dem Upgrade auf 3.2 oder höher stellt Prisma Access einen IPSec-Terminierungsknoten für je 1.000 Mbit/s zugewiesene Bandbreite bereit. Bei bestehenden Remote-Netzwerken kann Prisma Access die Bandbreite für ein Remote-Netzwerk mithilfe eines automatischen Skalierungsmechanismus erhöhen, der ausgelöst wird, wenn der Bandbreitenverbrauch im Remote-Netzwerk zusätzliche Kapazität erfordert. Weitere Informationen finden Sie unter Änderungen am Standardverhalten in den Versionshinweisen zu von Panorama verwaltetem Prisma Access .

    Die aktuelle Zuordnung von IPSec-Terminierungsknoten zu Remote-Netzwerkknoten nach dem Upgrade auf 3.2 bleibt unverändert und die Anzahl der IPSec-Terminierungsknoten bleibt gleich. IPSec-Terminierungsknoten werden nur hinzugefügt oder gelöscht, wenn Sie die Bandbreite für einen vorhandenen Compute-Standort erhöhen oder verringern oder wenn Sie neue Rechenstandorte für Remote-Netzwerke einbinden.

- **Dienstverbindung** – Wenn Ihre Remote-Netzwerkstandorte Zugriff auf die Infrastruktur in Ihrer Unternehmenszentrale benötigen, um Benutzer zu authentifizieren oder den Zugriff auf kritische Netzwerkressourcen zu ermöglichen, müssen Sie eine Dienstverbindung erstellen, damit Zentralen und Remote-Netzwerkstandorte verbunden werden. Wenn der Remote-Netzwerkstandort autonom ist und nicht auf Infrastruktur an anderen Standorten zugreifen muss, ist das Einrichten der Dienstverbindung nicht erforderlich (es sei denn, Ihre mobilen Benutzer benötigen Zugriff).

 ©2025 Palo Alto Networks, Inc.

- **Vorlage** –Prisma Access Erstellt automatisch einen Vorlagenstack (Remote_Network_Template_Stack) und eine Vorlage auf oberster Ebene (Remote_Network_Template) für Prisma Access für Netzwerke. Wenn Sie Remote-Netzwerke einbinden und konfigurieren möchten, müssen Sie entweder die Vorlage auf oberster Ebene von Grund auf konfigurieren oder Ihre bestehende Konfiguration nutzen, wenn Sie bereits eine Palo Alto Networks Firewall vor Ort ausführen. Die Vorlage erfordert, dass mit den Einstellungen die IPSec-Tunnel- und Internet Key Exchange(IKE)-Konfiguration für Protokollverhandlungen zwischen Ihrem Remote-Netzwerkstandort und Prisma Access für Netzwerke eingerichtet werden. Es sind Zonen erforderlich, auf die Sie in der Sicherheitsrichtlinie verweisen können, und ein Protokollweiterleitungsprofil, damit Sie Protokolle aus Prisma Access für Remote-Netzwerke an den Strata Logging Service weiterleiten können.
- **IPSec-Tunnelkonfigurationen** – Wenn Ihre vorhandene Vorlage Konfigurationen für IPSec-Tunnel, Tunnelüberwachung und IPSec-Verschlüsselungsprofil umfasst, können Sie diese Vorlage dem Vorlagenstack für Remote-Netzwerke (Remote_Network_Template_Stack) hinzufügen, um den Prozess zum Erstellen der IPSec-Tunnel zu vereinfachen. Alternativ hierzu können Sie auch die Vorlage „Remote_Network_Template“ bearbeiten, die automatisch erstellt wird, und die IPSec-Konfigurationen erstellen, die für die Erstellung des IPSec-Tunnels zum Unternehmensstandort erforderlich sind. Prisma Access stellt Ihnen außerdem einen Satz vordefinierter IPSec-Vorlagen für einige häufig verwendete Netzwerkgeräte und eine generische Vorlage für jedes Gerät zur Verfügung, das nicht in den vordefinierten Vorlagen enthalten ist. Beachten Sie bei der Konfiguration des Remote-Netzwerktunnels unbedingt die Empfehlungen für IPSec-Tunnel.
- **Bestimmen der Routingmethode (statisch oder dynamisch)** – Damit Prisma Access den Datenverkehr zu Ihren Remote-Netzwerken weiterleiten kann, müssen Sie Routinginformationen für die Subnetze bereitstellen, die Sie mit Prisma Access sichern möchten. Hierfür stehen Ihnen verschiedene Möglichkeiten zur Verfügung: Sie können entweder eine statische Route zu jedem Subnetz am Remote-Netzwerkstandort definieren oder BGP zwischen Ihren Dienstverbindungsstandorten und Prisma Access konfigurieren oder eine Kombination beider Methoden verwenden. Wenn Sie sowohl statische Routen konfigurieren als auch BGP aktivieren, haben die statischen Routen Vorrang. Während es praktisch sein könnte, statische Routen zu verwenden, wenn Sie nur über wenige Subnetze an Ihren Remote-Netzwerkstandorten verfügen, ermöglicht Ihnen BGP in einer großen Bereitstellung mit vielen Remote-Netzwerken mit überlappenden Subnetzen eine einfachere Skalierung.
- **Übergeordnete Gerätegruppe** – Prisma Access für Netzwerke erfordert die Angabe einer übergeordneten Gerätegruppe, die Ihre Sicherheitsrichtlinie, Sicherheitsprofile und andere Richtlinienobjekte (wie Anwendungsgruppen und -objekte sowie Adressgruppen) sowie Authentifizierungsrichtlinien umfasst. So kann Prisma Access für Netzwerke Richtlinien für Datenverkehr, der durch den IPSec-Tunnel zu Prisma Access für Netzwerke geleitet wird, konsequent durchsetzen. Sie müssen entweder Richtlinienregeln und Objekte in Panorama definieren oder eine vorhandene Gerätegruppe verwenden, um Benutzer am Remote-Netzwerkstandort zu schützen.

  *Wenn Sie eine vorhandene Gerätegruppe verwenden, die auf Zonen verweist, stellen Sie sicher, dass Sie die entsprechende Vorlage, die die Zonen definiert, zum Vorlagenstack für Remote-Netzwerke (Remote_Network_Template_Stack) hinzufügen. Auf diese Weise können Sie die Zonenzuordnung beim* Einbinden und Konfigurieren von Remote-Netzwerken *abschließen.*

 ©2025 Palo Alto Networks, Inc.

# Remote-Netzwerkbandbreite zuweisen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Remote-Netzwerke werden zur Sicherung von Remote-Netzwerkstandorten (z. B. Niederlassungen und Benutzer in diesen Niederlassungen) verwendet.

Für Remote-Netzwerke werden Messungen durchgeführt. Dies bedeutet, dass dem Compute-Standort ein bestimmtes Bandbreitenvolumen zugewiesen wird und dass mit dieser zugewiesenen Bandbreite Kosten verbunden sind.

Wenn Sie sich darauf vorbereiten, Remote-Netzwerke mit Prisma Access zu verbinden, müssen Sie wissen, wie viele Standorte Sie einbinden möchten und welche Bandbreitenanforderungen für jeden dieser Standorte bestehen.

Erfahren Sie hier, wie Sie Remote-Netzwerkbandbreite zuweisen können.

- Strata Cloud Manager
- Panorama

## Remote-Netzwerk-Bandbreite (Strata Cloud Manager) zuweisen

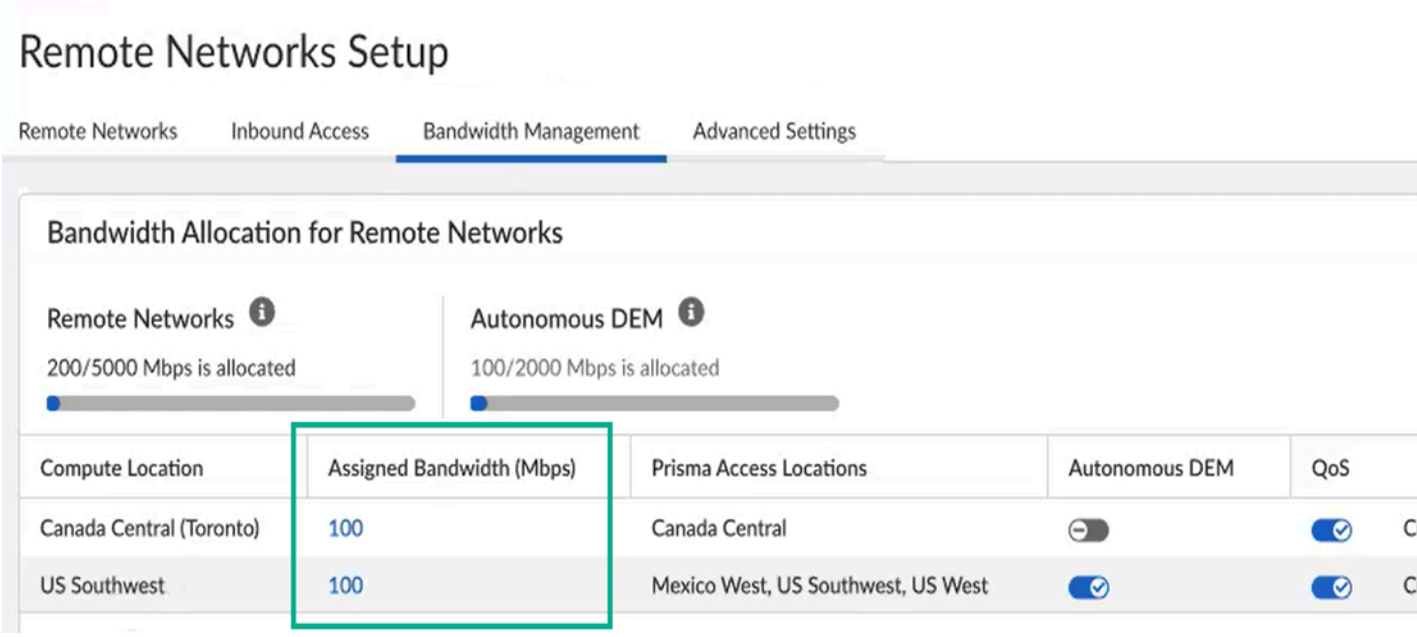
Mindestens zwei (und häufig weitere) geografisch nahe beieinander liegende Prisma Access-Standorte werden zu Gruppen von *Compute-Standorten* zusammengefasst. Hierbei handelt es sich um die Ebene, auf der Sie Bandbreite zuweisen, anstatt Bandbreite für einzelne Prisma Access-Standorte oder für bestimmte Remote-Netzwerk-Standorte zuzuweisen. Dies bedeutet, dass Prisma Access Standorten an einem Compute-Standort basierend auf Last oder Bedarf dynamisch Bandbreite zuweisen kann.

Beispiel: Sie müssen für vier Niederlassungen das Onboarding durchführen und dazu Remote-Netzwerke an Standorten in Singapur, Thailand und Vietnam verwenden. Alle diese Standorte werden dem Compute-Standort Südostasien zugeordnet. Wenn Sie dem Compute-Standort Südostasien eine Bandbreite von 200 Mbit/s zuweisen, teilt Prisma Access diese Bandbreite von 200 Mbit/s auf die vier Niederlassungen auf, für die Sie an diesem Standort das Onboarding durchgeführt haben. Wenn Sie außerdem auch einen Standort in Hongkong hinzufügen, sollten Sie beachten, dass Hongkong dem Compute-Standort Hongkong zugeordnet ist, sodass Sie die Bandbreite diesem Compute-Standort hinzufügen müssen. Geben Sie eine Mindestbandbreite von 50 Mbit/s pro Compute-Standort an.

Prisma Access ordnet die Bandbreite dynamisch nach Last oder Bedarf pro Standort zu. Im vorherigen Beispiel, bei dem die vier Standorte zusammen bis zu 200 Mbit/s nutzen, kann Prisma Access, wenn mindestens einer der Standorte weniger Bandbreite als die anderen Standorte nutzt, den anderen Standorten, die mehr Bedarf haben, mehr Bandbreite bereitstellen. Auf diese Weise kann die zugewiesene Bandbreite effizienter genutzt werden. Wenn außerdem einer der Standorte ausfällt, teilt Prisma Access die Bandbreite zwischen den verbleibenden Standorten, die am Compute-Standort weiterhin aktiv sind, neu auf.


©2025 Palo Alto Networks, Inc.

Rufen Sie zunächst **Workflows** > **Prisma Access-Einrichtung** > **Remote-Netzwerke** > **Bandbreitenverwaltung** auf.




**Berücksichtigen Sie trotzdem, wie viel Bandbreite jeder Standort benötigt, wenn Sie Bandbreite standortbasiert zuweisen**

Um Ihnen die Ermittlung des Bandbreitenvolumens zu erleichtern, die ein bestimmter Standort benötigt, sollten Sie die Bandbreite überprüfen, die von Ihrem ISP an jedem Standort verfügbar ist. Beachten Sie bei der Berechnung der Bandbreite, die an einem Standort benötigt wird, dass die Bandbreitennutzung sowohl ausgehenden als auch eingehenden Datenverkehr für die Remote-Netzwerkverbindung umfasst.

*Sicherer eingehender Zugriff für Remote-Netzwerkstandorte und Quality of Service (QoS) für Remote-Netzwerke werden nicht unterstützt, wenn Sie Bandbreite standortübergreifend zuweisen.*

## Remote-Netzwerk-Bandbreite (Panorama) zuweisen

Führen Sie die folgenden Schritte aus, um eine Remote-Netzwerk-Bereitstellung für Prisma Access zu konfigurieren, mit der Bandbreite nach Compute-Standort zugewiesen werden kann:

*Wenn Sie eine große Anzahl von Remote-Netzwerken (bis zu 1.000) einbinden müssen, können Sie dazu nach dem folgenden Verfahren das Onboarding eines Remote-Netzwerks durchführen. Anschließend können Sie die Remote-Netzwerk-Konfiguration in eine CSV-Datei exportieren, die anderen einzubindenden Remote-Netzwerke zur CSV-Datei hinzufügen und die CSV-Datei dann importieren, um die Konfiguration in Prisma Access zu speichern.*

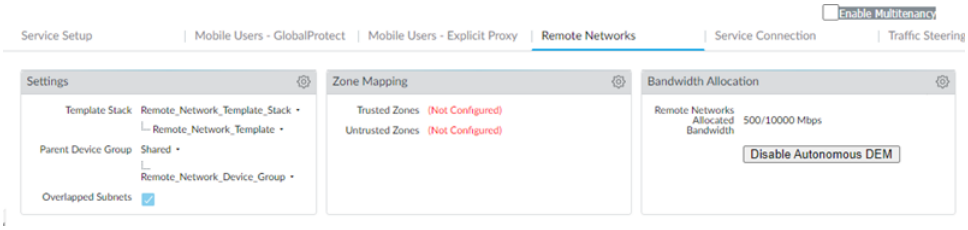
**STEP 1 |** Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Remote-Netzwerke** aus.

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Weisen Sie den Standorten, die Sie einbinden möchten, Bandbreite zu, indem Sie auf das Zahnradsymbol im Bereich **Bandbreitenzuweisung** klicken.

Sie weisen die Bandbreite auf aggregierter Ebene pro Compute-Standort zu. Weitere Einzelheiten finden Sie unter Prisma Access-Remote-Netzwerke.

*Wenn Sie Autonomous DEM als Add-on-Lizenz entfernt haben, oder wenn Sie Autonomous DEM für Remote-Netzwerke aus Ihrer Lizenz entfernen, wählen Sie **Autonomous DEM deaktivieren** aus. Wenn Sie Autonomous DEM für Remote-Netzwerke entfernen und Autonomous DEM nicht deaktivieren, erhalten Sie beim „Commit“ eine Fehlermeldung.*




Wenn Sie über eine vorhandene Remote-Netzwerk-Bereitstellung verfügen, für die momentan Remote-Netzwerke nach Standort eingebunden werden, wird ein Popupfenster angezeigt, in dem Sie gefragt werden, ob Sie eine Migration auf das aggregierte Bandbreitenmodell durchführen wollen. Klicken Sie auf **Migrieren**, um fortzufahren, oder auf **Abbrechen**, um die Migration abzubrechen.

*Die Migration auf das aggregierte Bandbreitenmodell ist dauerhaft und nicht reversibel. Überprüfen Sie vor der Migration die Checkliste zur Migrationsvorbereitung. Sie müssen Ihre Änderungen mit **Commit und Push** festschreiben und übertragen, damit sie wirksam werden.*

Die **Dienst-IP-Adresse** (der die öffentliche IP-Adresse, die auf der Prisma Access-Seite des IPSec-Tunnels für die Remote-Netzwerkverbindung verwendet wird) sollte nicht geändert werden, wenn Sie Ihre Bereitstellung auf das aggregierte Bandbreitenmodell migrieren. Dabei ist keine Neukonfiguration Ihres IPSec-Tunnels erforderlich.

**STEP 3 |** Geben Sie die **Bandbreitenzuweisung** an, die Sie für jeden **Compute-Standort** verwenden möchten, der den **Prisma Access-Standorten** zugeordnet ist, die Sie einbinden möchten.

Um die eingegebene Bandbreitenmenge zu überprüfen, aktivieren Sie das Häkchen neben der Bandbreitenmenge. Um den angezeigten Wert zu stornieren, wählen Sie **x** aus.

Geben Sie eine Mindestbandbreite von 50 Mbit/s und eine maximale Bandbreite an, die der maximal verbleibenden lizenzierten Bandbreite entspricht.

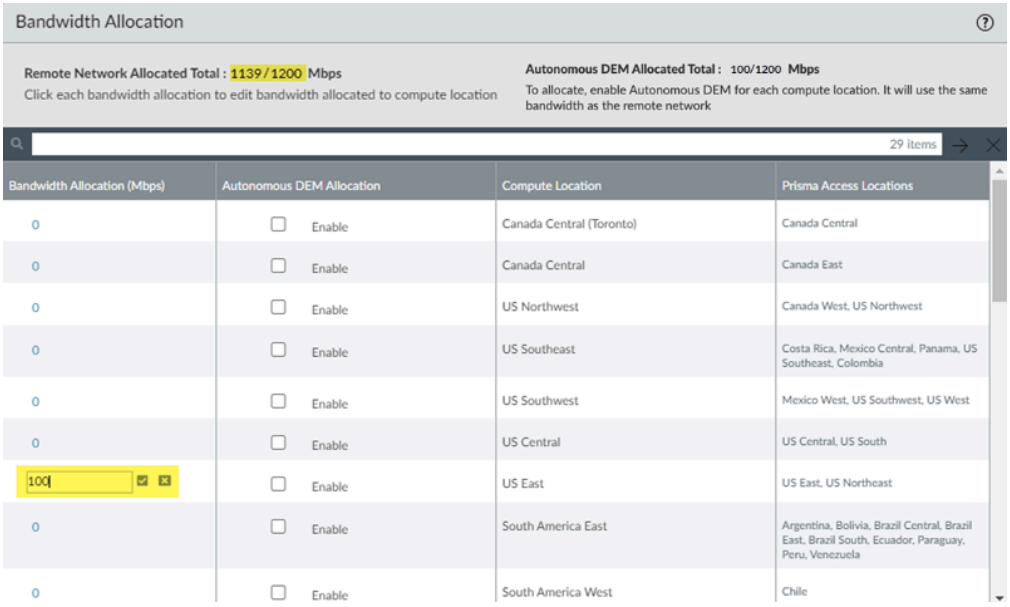
**STEP 4 |** (Optional, Bereitstellungen mit Autonomous DEM nur für Remote-Netzwerk-Lizenzen) **Aktivieren** Sie die **Autonomous DEM-Zuweisung** für den Compute-Standort, für den Sie Bandbreite zugewiesen haben.

Wenn Sie Autonomous DEM für den Compute-Standort aktivieren, ist die von der Autonomous DEM-Lizenz benutzte Bandbreite mit der Bandbreite identisch, die Sie für den Compute-Standort angeben. Der Wert für die **Gesamtzuweisung für Autonomous DEM** zeigt

 ©2025 Palo Alto Networks, Inc.

an, wie viel Bandbreite von Autonomous DEM verwendet wird und wie viel Bandbreite noch verbleibt. Weitere Informationen hierzu finden Sie im Leitfaden zu Autonomous DEM.

**STEP 5 |** Warten Sie, bis die Bandbreite im Feld **Gesamt zugewiesen** oben auf der Seite angezeigt wird, und klicken Sie dann auf **OK**.




**STEP 6 |** (Optional) Wenn Sie Ihr Remote-Netzwerk so konfigurieren möchten, dass ein sicherer Inbound Access auf Remote-Netzwerk-Standorte bereitgestellt werden kann, dann klicken Sie auf die Registerkarte **Remote-Netzwerke mit Inbound Access** und folgen Sie dem Workflow, um den sicheren Inbound Access für ein Remote-Netzwerk zu konfigurieren.

**STEP 7 |** Fügen Sie unter **Hinzufügen** ein Remote-Netzwerk hinzu und geben Sie dann im Feld **Name** einen Namen ein.

*Sie können den Namen des Remote-Netzwerk-Standorts nicht mehr ändern, nachdem Sie ihn eingegeben haben. Vergewissern Sie sich, dass Sie das Benennungsschema für Ihre Remote-Netzwerke kennen, bevor Sie mit dem Onboarding beginnen.*

**STEP 8 |** (Optional, nur für BGP-Bereitstellungen) Erstellen Sie eine Konfiguration, damit Ihre Remote-Netzwerkverbindung bis zu vier IPSec-Tunnel für den Datenverkehr verwenden kann (**ECMP-Lastausgleich**).

Statische Routen werden nicht unterstützt (BGP ist erforderlich). Wenn Sie QoS konfiguriert haben, können Sie das Zuweisungsverhältnis für ECMP-Links nicht ändern. Wenn Ihre Bereitstellung einen IPSec-Tunnel für die Remote-Netzwerkverbindung oder statische Routen verwendet, wählen Sie **Keine** für den **ECMP-Lastausgleich** aus und fahren Sie dann mit dem Schritt 11 fort.

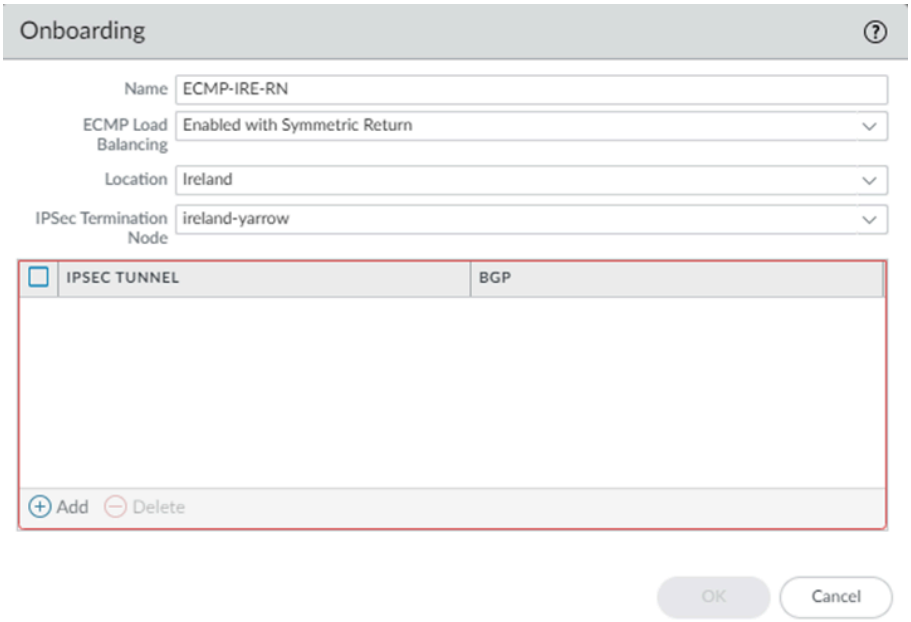
1. Wählen Sie eine der Optionen aus, um den ECMP-Lastausgleich zu aktivieren oder zu deaktivieren.
   - **Keine** – Verwenden Sie den ECMP-Lastausgleich nicht (verwenden Sie einen einzelnen Remote-Netzwerktunnel für diese Remote-Netzwerkverbindung). Dies ist

 ©2025 Palo Alto Networks, Inc.

die einzige Wahl, die Sie für statische Routen treffen können. BGP ist für den ECMP-Lastausgleich erforderlich.

- **Aktiviert mit symmetrischer Rückkehr** – Geben Sie bis zu vier IPSec-Tunnel für diese Remote-Netzwerkverbindung an und erzwingen Sie in Prisma Access die Verwendung desselben Links für den Rückkehrdatenverkehr, der auch zum Senden des Datenverkehrs benutzt wurde.

  Wählen Sie diese Option aus, wenn Sie mindestens einen Tunnel als Backup-Tunnel verwenden, der nur verwendet wird, wenn einer der primären Tunnel ausfällt. Wenn eine Verbindung ausfällt, verwendet Prisma Access einen der anderen Tunnel, um Datenverkehr symmetrisch zu senden und zu empfangen.




2. Mit **Hinzufügen** können Sie einen IPSec-Tunnel für die Remote-Netzwerkverbindung hinzufügen und die folgenden Werte angeben:

   - Mit **Aktivieren** wird BGP für den IPSec-Tunnel aktiviert.

     Diese Auswahl kann nicht konfiguriert werden. Sie müssen BGP aktivieren, um ECMP konfigurieren zu können.

   - Mit **Mobile Benutzerrouten vor dem Mitteilen zusammenfassen** kann die Anzahl der IP-Subnetzankündigungen mobiler Benutzer über BGP an CPE (Customer Premises Equipment) reduziert werden, indem die Ankündigungen zusammengefasst werden.

     Standardmäßig kündigt Prisma Access die IP-Adresspools der mobilen Benutzer in Blöcken von /24 Subnetzen an; wenn Sie sie zusammenfassen, kündigt Prisma Access den Pool basierend auf dem von Ihnen angegebenen Subnetz an. Beispiel: Prisma Access kündigt einen öffentlichen mobilen IP-Pool für Benutzer mit der Angabe 10.8.0.0/20 unter Verwendung des Subnetzes /20 an, anstatt den Pool in die Subnetze 10.8.1.0/24, 10.8.2.0/24, 10.8.3.0/24 usw. zu unterteilen, bevor sie angekündigt werden. Durch die Zusammenfassung dieser Ankündigungen kann die Anzahl der in den CPE-Routingtabellen gespeicherten Routen reduziert werden. Sie können z. B. die Zusammenfassung von IP-Pools mit Cloud-VPN-Gateways (Virtual

 ©2025 Palo Alto Networks, Inc.

Private Gateways (VGWs) oder Transit Gateways (TGWs)) verwenden, die eine begrenzte Anzahl von Routen akzeptieren können.

*Wenn Sie die Routenzusammenfassung für einen Standort aktivieren, der ECMP verwendet, müssen Sie die Routenzusammenfassung für alle Links zu diesem Standort aktivieren, da andernfalls während des Commits ein Fehler ausgegeben wird.*

Prisma Access legt den Community-String aggregierter Routen für mobile Benutzer auf `0xFFFE:0xFFF0` fest.

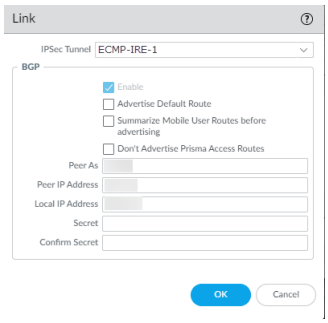
- **Standardroute ankündigen** – Prisma Access erstellt mit eBGP eine Standardroutenankündigung für das Remote-Netzwerk.

  *Vergewissern Sie sich, dass für Ihr Netzwerk keine andere Standardroute vorhanden ist, die von BGP angekündigt wurde, da es sonst zu Routingproblemen in Ihrem Netzwerk kommen kann.*

- **Prisma Access-Routen nicht ankündigen**– Verhindert, dass der Prisma Access-BGP-Peer Routen in das Netzwerk Ihrer Organisation weiterleitet.

  Standardmäßig teilt Prisma Access alle BGP-Routinginformationen einschließlich lokaler Routen und aller Präfixe mit, die von anderen Dienstverbindungen, Remote-Netzwerken und Subnetzen mobiler Benutzer empfangen werden. Aktivieren Sie dieses Kontrollkästchen, um Prisma Access daran zu hindern, BGP-Mitteilungen zu senden. Die empfangenen BGP-Informationen werden aber weiterhin verwendet, um Informationen zu Routen anderer BGP-Nachbarn zu erhalten.

  Da Prisma Access keine BGP-Mitteilungen sendet, wenn Sie diese Option auswählen, müssen Sie statische Routen auf dem lokalen Gerät konfigurieren, um Routen zurück zu Prisma Access einzurichten.




- **Peer-AS** – Geben Sie das autonome System (AS) an, zu dem die Firewall, der virtuelle Router oder der BGP-Router in Ihrem Remote-Netzwerk gehört.
- **Peer-IP-Adresse** – Geben Sie die IP-Adresse ein, die als Router-ID des eBGP-Routers im Remote-Netzwerk zugewiesen wurde, für das Sie diese Verbindung konfigurieren.
- **Lokale IP-Adresse** (Optional) – Geben Sie eine Adresse ein, die von Prisma Access als lokale IP-Adresse für BGP verwendet wird. Geben Sie die IP-Adresse an, die auf der Prisma Access-Seite des Tunnels verwendet werden soll.

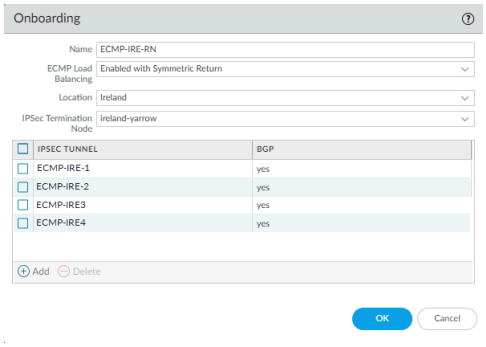
  Die Angabe eines Werts für **Lokale Adresse** ist nützlich, wenn das Gerät auf der anderen Seite der Verbindung (z. B. ein Amazon Web Service (AWS) Virtual Private Gateway) eine bestimmte lokale IP-Adresse benötigt, damit das BGP-Peering

 ©2025 Palo Alto Networks, Inc.

erfolgreich ist. Vergewissern Sie sich, dass die von Ihnen angegebene Adresse nicht mit IP-Adressen im Infrastruktursubnetz oder Subnetzen im Remote-Netzwerk in Konflikt steht oder sich mit diesen überschneidet.

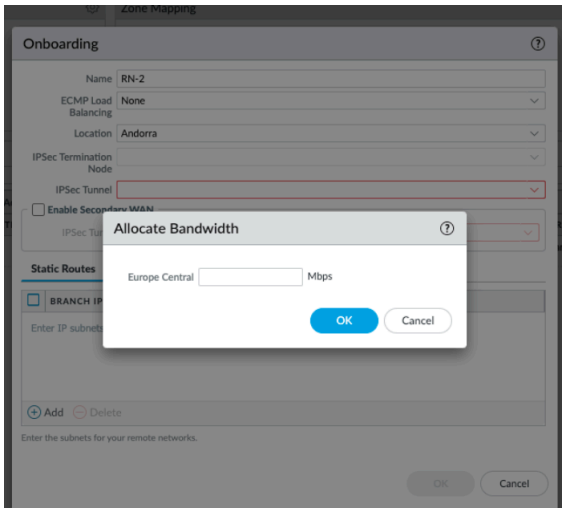
- **Geheimer Schlüssel** und **Geheimen Schlüssel bestätigen** (Optional) – Geben Sie eine Passphrase ein und bestätigen Sie diese, um die BGP-Peer-Kommunikation zu authentifizieren.

3. Wiederholen Sie den vorherigen Schritt, um bis zu vier Tunnel hinzuzufügen, die mit der Remote-Netzwerkverbindung verwendet werden sollen.




**STEP 9 |** Wählen Sie den **Standort** aus, an dem Prisma Access die Infrastruktur bereitstellt, die zum Sichern Ihres Remote-Netzwerkstandorts erforderlich ist. Diese Region sollte sich geografisch in der Nähe Ihres Remote-Netzwerkstandorts befinden.

Wenn Sie noch keine Bandbreite für den Compute-Standort zugeordnet haben, dem der Standort zugeordnet ist, werden Sie von Prisma Access aufgefordert, die Bandbreite für diesen Compute-Standort einzugeben.




**STEP 10 |** Wählen Sie den **IPSec-Terminierungsknoten** aus, den Sie für dieses Remote-Netzwerk verwenden möchten.

Prisma Access verwendet diesen Knoten, um Remote-Netzwerkstandorte mit den entsprechenden Compute-Standorten zu verknüpfen.

**STEP 11 |** (Nur statisches Routing oder Bereitstellungen mit nur einem Tunnel) Wählen Sie eine Konfigurationen für einen **IPSec-Tunnel** aus oder fügen Sie eine neue Konfiguration hinzu,

 ©2025 Palo Alto Networks, Inc.

mit der auf die Firewall, den Router oder das SD-WAN-Gerät am Unternehmensstandort zugegriffen werden kann:

- Wählen Sie eine der vordefinierten IPSec-Vorlagen im Remote_Network_Template aus. Wenn Sie eine Vorlage zum Remote_Network_Template_Stack hinzugefügt haben (oder das vordefinierte Remote_Network_Template geändert haben), die eine IPSec-Tunnelkonfiguration enthält, dann wählen Sie in der Dropdown-Liste den Eintrag **IPSec-Tunnel** aus. Beachten Sie, dass der Tunnel, den Sie für jede Remote-Netzwerkverbindung erstellen, Prisma Access mit dem IPSec-fähigen Gerät an jedem Niederlassungsstandort verbindet.

  Beachten Sie bei der Konfiguration eines IPSec-Tunnels die folgenden Richtlinien:

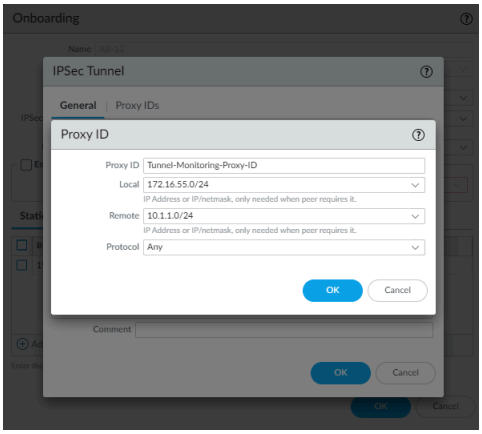
  - Die Peer-Adressen in der IKE-Gateway-Konfiguration müssen für jeden Tunnel eindeutig sein. Sie können jedoch einige der anderen allgemeinen Konfigurationselemente wie z. B. Verschlüsselungsprofile wiederverwenden.
  - Der IPSec-Tunnel, den Sie in einer Vorlage auswählen, darf nur den automatischen Schlüsselaustausch und IPv4 verwenden.
  - Die Namen des IPSec-Tunnels, des IKE-Gateways und der Verschlüsselungsprofile dürfen nicht mehr als 31 Zeichen umfassen.
  - Wenn Sie mehrere Remote-Netzwerke an demselben Standort mit dynamischen IKE-Peers einbinden, müssen Sie für alle Remote-Netzwerkkonfigurationen dasselbe IKE-Verschlüsselungsprofil verwenden.
- Zum Erstellen einer neuen Konfiguration für einen IPSec-Tunnel klicken Sie auf **Neuer IPSec-Tunnel**, ordnen dem neuen Element unter **Name** einen Namen zu und konfigurieren den IKE-Gateway, das IPSec-Verschlüsselungsprofilund die Einstellungen für die Tunnelüberwachung.
  - Wenn das IPSec-fähige Gerät an Ihrem Niederlassungsstandort ein richtlinienbasiertes VPN verwendet, müssen Sie auf der Registerkarte **Proxy-IDs** durch Auswahl von **Hinzufügen** eine Proxy-ID hinzufügen, die mit den auf Ihrem lokalen IPSec-Gerät konfigurierten Einstellungen übereinstimmt. Auf diese Weise können Sie sicherstellen, dass Prisma Access einen IPSec-Tunnel für Ihr lokales Gerät einrichten kann.
- Behalten Sie die Auswahl von **Replay-Schutz aktivieren** bei, um Replay-Angriffe zu erkennen und zu beseitigen.
- Wählen Sie **ToS-Header kopieren** aus, um den Header für ToS (Type of Service) aus dem inneren IP-Header in den äußeren IP-Header der gekapselten Pakete zu kopieren, damit die ursprünglichen ToS-Informationen erhalten bleiben.
- Um die Tunnelüberwachung für die Dienstverbindung zu aktivieren, wählen Sie **Tunnelüberwachung** aus.
  - Geben Sie eine **Ziel-IP**-Adresse ein.

    Geben Sie eine IP-Adresse an Ihrem Niederlassungsstandort an, an die Prisma Access ICMP-Ping-Anfragen für die IPSec-Tunnelüberwachung senden kann. Stellen Sie sicher, dass diese Adresse für ICMP im gesamten Prisma Access-Infrastruktursubnetz erreichbar ist.
  - Wenn Sie die Tunnelüberwachung mit einem Peergerät verwenden, das mehrere Proxy-IDs verwendet, geben Sie eine **Proxy-ID** an oder fügen Sie unter **Neue Proxy-**

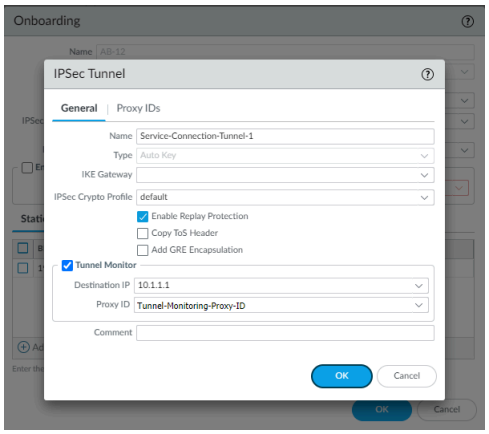
 ©2025 Palo Alto Networks, Inc.

**ID** eine neue Proxy-ID hinzu, die den Zugriff über das Infrastruktursubnetz auf Ihren Niederlassungsstandort ermöglicht.

Die folgende Abbildung zeigt eine Proxy-ID mit dem Infrastruktursubnetz des Dienstes (in diesem Beispiel 172.16.55.0/24) als **Lokales** IP-Subnetz und das Subnetz des Niederlassungsstandorts (in diesem Beispiel 10.1.1.0/24) als **Remote**-Subnetz.




Die folgende Abbildung zeigt, wie die von Ihnen erstellte Proxy-ID auf die Konfiguration der Tunnelüberwachung angewendet wird, indem sie im Feld **Proxy-ID** angegeben wird.




*Sie müssen auf Ihrem CPE eine statische Route zur IP-Adresse der Tunnelüberwachung konfigurieren, damit die Tunnelüberwachung fehlerfrei ausgeführt werden kann. Zum Suchen der Ziel-IP-Adresse, die für die Tunnelüberwachung von Ihrem Niederlassungsstandort zu Prisma Access benötigt wird, wählen Sie **Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** aus, klicken anschließend auf das Optionsfeld **Dienstinfrastruktur** und suchen dann die **IP-Adresse für Tunnelüberwachung**.*

 ©2025 Palo Alto Networks, Inc.

**STEP 12 |** Wenn Sie an diesem Standort über eine sekundäre WAN-Verbindung verfügen, wählen Sie **Sekundäres WAN aktivieren** aus.

*Stellen Sie sicher, dass für das sekundäre WAN jedes Remote-Netzwerks ein eindeutiger IPSec-Tunnel erstellt wird. Prisma Access bietet keine Unterstützung für die Wiederverwendung desselben IPSec-Tunnels für sekundäre WANs in mehreren Remote-Netzwerken.*

Die Konfiguration eines sekundären WAN wird in den folgenden Bereitstellungen nicht unterstützt:

- Wenn Ihr sekundäres WAN im Aktiv-Aktiv-Modus mit dem primären IPSec-Tunnel eingerichtet ist.
- Wenn Ihr Customer Premises Equipment (CPE) in einer ECMP-Konfiguration (Equal Cost Multipath) mit dem primären und sekundären IPSec-Tunnel eingerichtet ist.

Wenn Sie statische Routen verwenden, beträgt die Tunnel-Failover-Zeit abhängig von Ihrem WAN-Anbieter weniger als 15 Sekunden ab dem Zeitpunkt der Erkennung.

Wenn Sie das BGP-Routing konfigurieren und die Tunnelüberwachung aktiviert haben, besteht die kürzeste Standardhaltezeit zur Feststellung eines Fehlers bei einem Sicherheitsparameterindex (SPI) über die Tunnelüberwachung. Hierbei werden alle Routen zu einem Peer entfernt, wenn ein Tunnelfehler festgestellt wird, der länger als 15 aufeinanderfolgende Sekunden anhält. Auf diese Weise ermittelt die Tunnelüberwachung das Verhalten der BGP-Routen. Wenn Sie die Tunnelüberwachung nicht konfigurieren, bestimmt der Haltetimer die Zeitspanne, für die der Tunnel inaktiv sein darf, bevor die Route entfernt wird. Prisma Access verwendet den standardmäßigen BGP-HoldTime-Wert von 90 Sekunden, der in RFC 4271 definiert ist. Hierbei handelt es sich um die maximal zulässige Wartezeit, nach deren Ablauf Prisma Access eine Route für einen inaktiven SPI entfernt. Wenn das Peer-BGP-Gerät eine kürzere konfigurierte Haltezeit hat, verwendet der BGP-Haltetimer den niedrigeren Wert.

Nach der erfolgreichen Installation des sekundären Tunnels hat die sekundäre Route so lange Vorrang, bis der primäre Tunnel wieder einsatzbereit ist. Wenn sowohl die primäre als auch die sekundäre Route aktiv sind, hat die primäre Route Vorrang.

*Wenn Sie einen anderen BGP-Peer für die sekundäre (Backup-)Verbindung verwenden, berücksichtigt Prisma Access die vom CPE angekündigten MED-Attribute (Multi-Exit Discriminator) nicht. Diese Einschränkung gilt, wenn Sie mehrere BGP-Peers für Remote-Netzwerkverbindungen oder Dienstverbindungen verwenden.*

**STEP 13 |** Aktivieren Sie das Routing zu den Subnetzwerken oder einzelnen IP-Adressen am Remote-Netzwerkstandort, auf den die Benutzer Zugriff benötigen.

Prisma Access verwendet diese Informationen, um Anforderungen an den richtigen Standort weiterzuleiten. Die Netzwerke an den einzelnen Standorten dürfen sich nicht gegenseitig oder mit den IP-Adresspools überschneiden, die Sie für die Dienstinfrastruktur oder für Prisma

 ©2025 Palo Alto Networks, Inc.

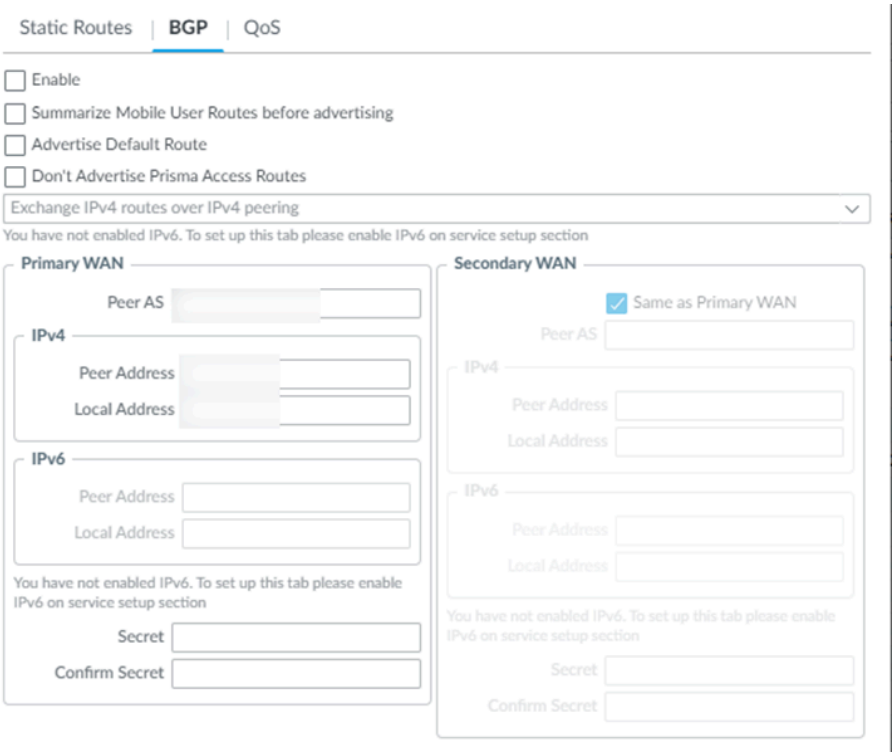
Access für IP-Pools der Benutzer bestimmt haben. Sie können **Statische Routen**, **BGP** oder eine Kombination dieser beiden Komponenten konfigurieren.

- So konfigurieren Sie **Statische Routen**:
  1. Klicken Sie auf der Registerkarte **Statische Routen** auf **Hinzufügen** und geben Sie dann die Subnetzadresse (z. B. 172.168.10.0/24) oder die individuelle IP-Adresse einer Ressource wie beispielsweise die IP-Adresse eines DNS-Servers (z. B. 10.32.5.1/32) ein, auf den Ihre Remote-Benutzer Zugriff benötigen.
  2. Wiederholen Sie diesen Vorgang für alle Subnetze oder IP-Adressen, auf die Prisma Access an diesem Standort Zugriff benötigt.




 ©2025 Palo Alto Networks, Inc.

- So konfigurieren Sie **BGP**:
  1. Wählen Sie die Registerkarte **BGP** aus.
  2. (Optional) Wählen Sie die Optionen für den **ECMP-Lastausgleich** aus. Siehe hierzu den Schritt 8.
  3. Wenn Sie **Keine** für den **ECMP-Lastausgleich** auswählen, dann geben Sie die BGP-Optionen ein.




  4. Um BGP für die Remote-Netzwerkverbindung zu aktivieren, wählen Sie **Aktivieren** aus.

     Wenn Sie BGP aktivieren, legt Prisma Access den TTL-Wert (Time to Live) für externes BGP (eBGP) auf 8 fest, um zusätzliche Hops zu berücksichtigen, die zwischen der Prisma Access-Infrastruktur und Ihrem Customer Premises Equipment (CPE) liegen können, das die eBGP-Verbindung abschließt.
  5. Um die Anzahl der IP-Subnetzankündigungen mobiler Benutzer über BGP zu Ihrem Customer Premises Equipment (CPE) durch Zusammenfassung zu reduzieren, wählen Sie **Mobile Benutzerrouten vor dem Mitteilen zusammenfassen** aus.

     Standardmäßig kündigt Prisma Access die IP-Adresspools der mobilen Benutzer in Blöcken von /24 Subnetzen an; wenn Sie sie zusammenfassen, kündigt Prisma Access den Pool basierend auf dem von Ihnen angegebenen Subnetz an. Beispiel: Prisma Access kündigt einen öffentlichen mobilen IP-Pool für Benutzer mit der Angabe 10.8.0.0/20 unter Verwendung des Subnetzes /20 an, anstatt den Pool in die Subnetze 10.8.1.0/24, 10.8.2.0/24, 10.8.3.0/24 usw. zu unterteilen, bevor sie angekündigt werden. Durch die Zusammenfassung dieser Ankündigungen kann die Anzahl der in den CPE-Routingtabellen gespeicherten Routen reduziert werden. Sie können z. B. die Zusammenfassung von IP-Pools mit Cloud-VPN-Gateways (Virtual Private Gateways

 ©2025 Palo Alto Networks, Inc.

(VGWs) oder Transit Gateways (TGWs)) verwenden, die eine begrenzte Anzahl von Routen akzeptieren können.

Prisma Access legt den Community-String aggregierter Routen für mobile Benutzer auf `0xFFFE:0xFFF0` fest.

6. Um zuzulassen, dass Prisma Access eine Standardroute für das Remote-Netzwerk mithilfe von eBGP ankündigt, wählen Sie **Standardroute mitteilen** aus.

   Wenn Sie **Standardroute mitteilen** auswählen, sollten Sie sicherstellen, dass in Ihrem Netzwerk keine andere Standardroute vorhanden ist, die von BGP mitgeteilt wird, da es sonst zu Routingproblemen in Ihrem Netzwerk kommen kann.

   *Sie müssen Ihre Standardrouten veröffentlichen, bevor Sie diese Auswahl treffen, um sie mitzuteilen. Darüber hinaus sollten Sie überprüfen, ob Ihr Netzwerk nicht über eine andere Standardroute verfügt, die von BGP mitgeteilt wird. Andernfalls kann es zu Routingproblemen in Ihrem Netzwerk kommen.*

7. Um zu verhindern, dass der BGP-Peer in der Prisma Access-Firewall Routen an das Netzwerk Ihrer Organisation weiterleitet, wählen Sie **Prisma Access-Routen nicht mitteilen** aus.

   Standardmäßig teilt Prisma Access alle BGP-Routinginformationen einschließlich lokaler Routen und aller Präfixe mit, die von anderen Dienstverbindungen, Remote-Netzwerken und Subnetzen mobiler Benutzer empfangen werden. Aktivieren Sie dieses Kontrollkästchen, um Prisma Access daran zu hindern, BGP-Mitteilungen zu senden. Die empfangenen BGP-Informationen werden aber weiterhin verwendet, um Informationen zu Routen anderer BGP-Nachbarn zu erhalten.

   Da Prisma Access keine BGP-Mitteilungen sendet, wenn Sie diese Option auswählen, müssen Sie statische Routen auf dem lokalen Gerät konfigurieren, um Routen zurück zu Prisma Access einzurichten.

8. Geben Sie im Feld **Peer-AS** einen Wert ein, der das autonome System (AS) festlegt, zu dem die Firewall, der virtuelle Router oder der BGP-Router Ihres Remote-Netzwerks gehört.

9. Geben Sie die IP-Adresse ein, die als Router-ID des eBGP-Routers in dem Remote-Netzwerk zugewiesen wurde, für das Sie diese Verbindung als **Peer-Adresse** konfigurieren.

10. (Optional) Geben Sie eine Adresse ein, die von Prisma Access als lokale IP-Adresse für BGP verwendet wird.

    Die Angabe eines Werts für **Lokale Adresse** ist nützlich, wenn das Gerät auf der anderen Seite der Verbindung (z. B. ein Amazon Web Service (AWS) Virtual Private Gateway) eine bestimmte lokale IP-Adresse benötigt, damit das BGP-Peering erfolgreich ist. Vergewissern Sie sich, dass die von Ihnen angegebene Adresse nicht mit IP-Adressen im

 ©2025 Palo Alto Networks, Inc.

Infrastruktursubnetz oder Subnetzen im Remote-Netzwerk in Konflikt steht oder sich mit diesen überschneidet.

*Im Feld **Lokale Adresse** müssen Sie eine statische Route auf Ihrem CPE (Customer Premises Equipment) zum BGP konfigurieren.*

11. (Optional) Geben Sie eine Passphrase ein und bestätigen Sie diese, um die BGP-Peer-Kommunikation zu authentifizieren.
12. (Optional) Wenn Sie ein **Sekundäres WAN** konfiguriert haben und die **Peer-Adresse** oder den Wert für **Lokale Adresse** für den sekundären (Backup-)BGP-Peer ändern müssen, dann nehmen Sie die Auswahl von **Identisch mit primärem WAN** zurück und geben Sie einen eindeutigen Peer und optional eine lokale IP-Adresse für das sekundäre WAN ein.

    Wenn Sie die IPv6-Vernetzung in Ihrer Remote-Netzwerkbereitstellung verwenden, können Sie **IPv6**-Adressen sowie **IPv4**-Adressen konfigurieren. Des Weiteren müssen Sie die IPv6-Vernetzung weltweit in Ihrer Prisma Access-Infrastruktur aktivieren, bevor Sie die IPv6-Adressierung verwenden können.

    In einigen Bereitstellungen (z. B. bei der Verwendung von BGP für das Peering mit einem AWS-VPN-Gateway) kann der BGP-Peer für das primäre und das sekundäre WAN unterschiedlich sein. In diesen Szenarien können Sie einen anderen BGP-Peer für das sekundäre WAN festlegen.

    *Für BGP-Bereitstellungen mit sekundären WANs legt Prisma Access sowohl den primären als auch den sekundären Tunnel im Status **AKTIV** fest, befolgt jedoch das normale BGP-Aktiv-Backup-Verhalten für den Netzwerkverkehr. Prisma Access setzt den primären Tunnel auf aktiv und sendet und empfängt Datenverkehr nur über diesen Tunnel. Wenn der primäre Tunnel ausfällt, erkennt Prisma Access den Fehler mithilfe von BGP-Regeln und legt den sekundären Tunnel als aktiv fest, um ausschließlich ihn zum Senden und Empfangen von Datenverkehr zu nutzen.*

**STEP 14 |** (Optional) Aktivieren Sie **QoS** für den Standort und geben Sie ein **QoS-Profil** an.

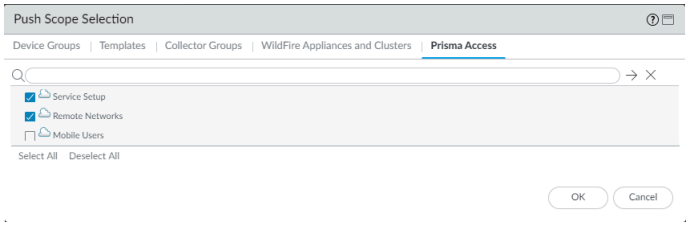
Sie legen QoS-Optionen und allgemeine Einstellungen separat für alle Compute-Standorte in den **Einstellungen** fest; allerdings können Sie QoS aktivieren oder deaktivieren oder das QoS-Profil für jeden Standort einzeln ändern.

**STEP 15 |** Schreiben Sie die Konfigurationsänderungen mit einer Commit-Aktion in Panorama fest und übertragen Sie die Konfiguration mit einer Push-Aktion an Prisma Access, um sie für Netzwerke bereitzustellen.

1. Klicken Sie auf **Commit** > **Commit in Panorama**.
2. Klicken Sie auf **Commit** > **Commit und Push**. Klicken Sie auf **Auswahlen bearbeiten** > **Prisma Access**und wählen Sie sowohl Prisma Access für Netzwerke als auch Prisma

 ©2025 Palo Alto Networks, Inc.

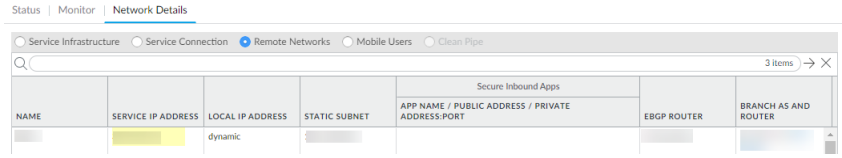
Access für die Diensteinrichtung aus, um die Konfiguration mit einer Push-Aktion an den Dienst zu übertragen.




3. Klicken Sie auf **OK** und dann auf **Push**.

**STEP 16 |** Konfigurieren Sie das IPSec-fähige Gerät am Remote-Netzwerkstandort, um eine IPSec-Verbindung mit Prisma Access für Netzwerke einzurichten.

1. Suchen Sie die **Dienst-IP-Adresse** für diese Remote-Netzwerkverbindung, indem Sie **Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** auswählen. Klicken Sie dann auf das Optionsfeld **Remote-Netzwerke** und zeigen Sie das Feld **Dienst-IP-Adresse** an. Prisma Access für die Netzwerkinfrastruktur hat diesen diese IP-Adresse für die Prisma Access-Remote-Netzwerkverbindung zugewiesen und Sie müssen diese als Peer-IP-Adresse konfigurieren, um den IPSec-Tunnel zwischen dem Remote-Netzwerkstandort und dem Prisma Access für Netzwerke einzurichten.




2. Aktivieren Sie die Option **Lokale IP-Adresse** für das Gerät am Remote-Netzwerkstandort auf der Seite **Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Remote-Netzwerke**. Wenn Sie die NAT am Remote-Netzwerkstandort ausführen, wird im Feld **Lokale IP-Adresse** die IP-Adresse des Geräts nach der NAT angezeigt.

**STEP 17 |** Um den Datenverkehr am Remote-Netzwerkstandort zu sichern, müssen Sie Sicherheitsrichtlinienregeln erstellen.

1. Wählen Sie **Richtlinien** aus.
2. Wählen Sie die **Gerätegruppe** aus, in der Richtlinienregeln hinzugefügt werden sollen. Sie können Remote_Network_Device_Group oder die übergeordnete Gerätegruppe auswählen, die Sie zum Definieren von Richtlinien ausgewählt haben, mit denen der Remote-Netzwerksstandort gesichert werden soll.
3. Erstellen Sie Sicherheitsrichtlinienregeln. Vergewissern Sie sich, dass keine Sicherheitsrichtlinienregeln definiert werden, mit denen Datenverkehr von einer Zone zu einer beliebigen anderen Zone zugelassen wird. Verwenden Sie in den Sicherheitsrichtlinienregeln die Zonen, die Sie in Ihrer Vorlage definiert haben.

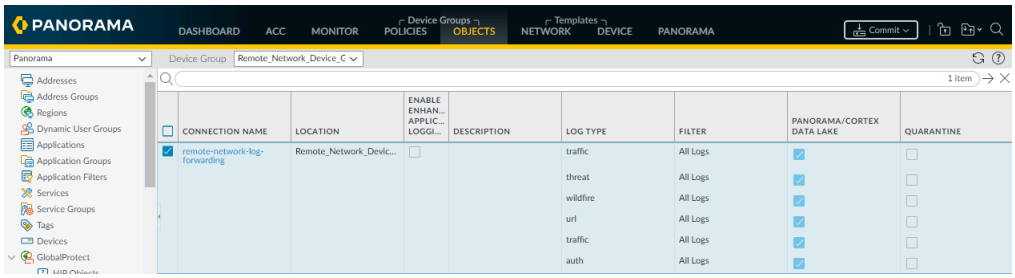
   Wenn einem Benutzer in Ihrem Netzwerk der Zugriff auf eine Website verweigert wird, dann melden Sie die Probleme beim Zugriff auf die Website, bevor Sie ein Ticket bei Palo Alto Networks eröffnen.

 ©2025 Palo Alto Networks, Inc.

**STEP 18 |** Aktivieren Sie die Protokollierung beim Strata Logging Service. Sie müssen ein Protokollweiterleitungsprofil erstellen und jeder Richtlinienregel hinzufügen, für die Sie Protokolle weiterleiten möchten.

1. Wählen Sie **Objekte > Protokollweiterleitung** aus.
2. Wählen Sie die **Gerätegruppe** aus, in der Sie die Richtlinienregeln hinzugefügt haben, z. B. Remote_Network_Device_Group.
3. **Hinzufügen** eines Protokollweiterleitungsprofils. Wählen Sie in der Übereinstimmungsliste des Protokollweiterleitungsprofils **Hinzufügen** und dann im Feld **Protokolltyp** jeden Protokolltyp aus, den Sie weiterleiten möchten.
4. Wählen Sie als Weiterleitungsmethode **Panorama/Strata-Protokollierungsdienst** aus, um für Prisma Access die Weiterleitung der Protokolle an Strata Logging Service zu aktivieren. Nun können Sie die Protokolle überwachen und Berichte über Panorama erstellen. Strata Logging Service bietet eine nahtlose Integration zum Speichern von Protokollen, ohne dass diese erneut an Panorama in der Unternehmenszentrale zurückgeleitet werden müssen. Panorama kann Abfragen im Strata Logging Service nach Bedarf durchführen.

   Im folgenden Beispiel wird die Weiterleitung von Datenverkehr, der Threat Prevention, WildFire-Übermittlung, URL-Filterung, Datenfilterung und Authentifizierungsprotokollen an Strata Logging Service aktiviert.




5. Wählen Sie **Richtlinien > Sicherheit** aus und bearbeiten Sie die Richtlinienregel. Wählen Sie unter **Aktionen** das von Ihnen erstellte Protokollweiterleitungsprofil aus.

**STEP 19 |** Schreiben Sie alle von Ihnen vorgenommenen Änderungen mit einer Commit-Aktion in Panorama fest und übertragen Sie die Konfigurationsänderungen mit einer Push-Aktion an Prisma Access.

1. Klicken Sie auf **Commit** > **Commit und Push**.
2. Wählen Sie **Auswahlen bearbeiten** aus und vergewissern Sie sich, dass auf der Registerkarte **Prisma Access** die Option **Prisma Access für Netzwerke** im Feld **Übertragungsumfang** ausgewählt wurde. Klicken Sie anschließend auf **OK**.
3. Führen Sie für Ihre Änderungen die Aktion **Commit und Push** aus.

**STEP 20 |** Überprüfen Sie den Status des Remote-Netzwerks.

Weitere Einzelheiten finden Sie unter Verbindung des Remote-Netzwerks mit Prisma Access prüfen.

 ©2025 Palo Alto Networks, Inc.

# Migration zum neuen Modell planen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Bandbreiten für neue Prisma Access-Remote-Netzwerkbereitstellungen werden auf aggregierter Ebene pro Compute-Standort zugewiesen. Diese wird auch als *Modell mit aggregierter Bandbreite* bezeichnet. Die Zuweisung von Bandbreite auf Compute-Standort-Ebene bietet Ihnen mehr Flexibilität, wenn Sie Ihre lizenzierte Remote-Netzwerkbandbreite zuweisen, da Prisma Access die Bandbreite für jeden Standort dynamisch basierend auf Last oder Bedarf zuweist.

Wenn Ihre vorhandene Bereitstellung Bandbreite nach Prisma Access-Standort zuweist, können Sie zum Modell mit aggregierter Bandbreite migrieren. Sie können auch Ihre Remote-Netzwerk-QoS-Bereitstellung migrieren. Bei der Migration verwenden alle Remote-Netzwerke das Modell mit der aggregierten Bandbreite.

Verwenden Sie die folgende Checkliste, um die Migration zum Modell mit aggregierter Bandbreite zu planen:

- ❑ Beachten Sie, dass die folgenden Remote-Netzwerkkomponenten nach der Migration unverändert bleiben:
  - Es gibt keine Änderungen an der Dataplane. Der Datenverkehr fließt weiterhin durch die Prisma Access-Dataplane, ohne dass Änderung an der bestehenden Konfiguration vorgenommen werden.
  - Die Migration wirkt sich nicht auf bestehende Tunnel aus.

    Eine Neukonfiguration Ihrer IPSec-Tunnelparameter ist nicht erforderlich. IKE-Gateways, IKE- und IPSec-Verschlüsselungsprofile sowie IPSec-Tunnelkonfigurationen bleiben unverändert.
  - Die **IP-Adresse des Dienstes** im Remote-Netzwerk (die öffentlichen IP-Adressen, die auf der Prisma Access-Seite des IPSec-Tunnels für die Remote-Netzwerkverbindung verwendet werden) ändert sich nicht für jedes Remote-Netzwerk, wenn Sie Ihre Bereitstellung auf das aggregierte Bandbreitenmodell migrieren.
- ❑ Prisma Access weist IPSec-Terminierungsknoten zu und sorgt für die Zuweisung von Bandbreite zu Remote-Netzwerken während einer Migration zum Modell mit aggregierter Bandbreite. Sie sollten vor der Migration verstanden haben, wie dieses Modell funktioniert.

  *Wenn Sie ein vorhandenes Remote-Netzwerk nach der Migration einem anderen IPSec-Terminierungsknoten neu zuweisen möchten, weist Prisma Access dem Remote-Netzwerk nach dem Festschreiben und Übertragen Ihrer Änderungen per Push eine andere **Dienst-IP-Adresse** zu. In diesem Fall müssen Sie Ihr CPE neu konfigurieren, um auf die neue IP-Adresse für den Remote-Netzwerktunnel zu verweisen.*
- ❑ Wenn eine nicht unterstützte Konfiguration vorliegt, wird die Registerkarte „Bandbreitenzuweisung“ oder das Banner zur Migration nicht angezeigt. Die folgenden

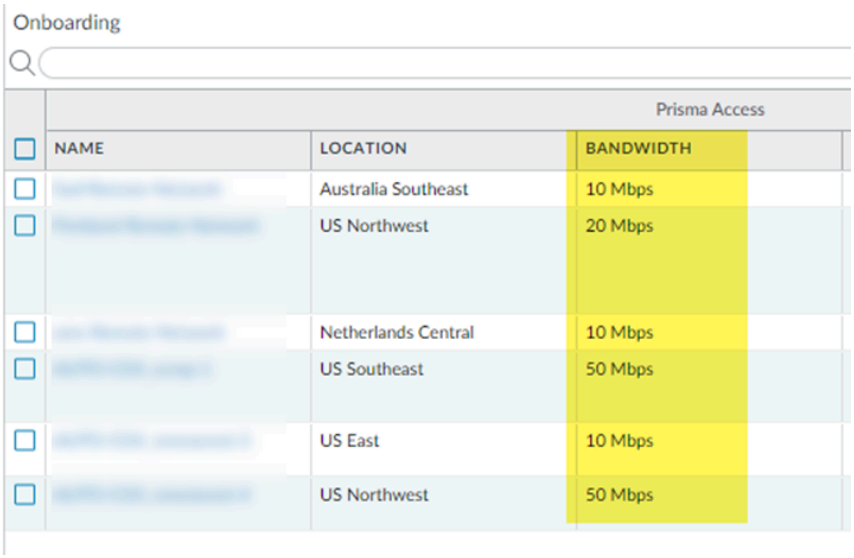
 ©2025 Palo Alto Networks, Inc.

Konfigurationen werden für die Migration zum Modell mit aggregierter Bandbreite nicht unterstützt:

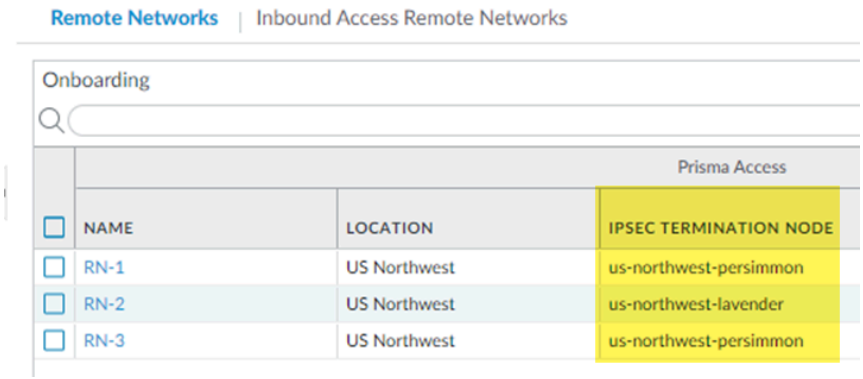
- Ein Remote-Netzwerk mit einer Bandbreite von **1.000 Mbit/s**.
- Eine Prisma SD-WAN-CloudBlade-Integration mit einer Prisma Access-Version vor 3.0.
- Eine Remote-Netzwerkkonfiguration, die sicheren eingehenden Zugriff auf Anwendungen an einem Remote-Netzwerkstandort vor 2.1 Innovation bietet.

Wenn Sie ein QoS mit Ihren Remote-Netzwerken verwenden, beachten Sie vor der Migration unbedingt die QoS-Migrationsrichtlinien.

- Wenn Sie nicht sicher sind, welches Modell Ihre Bereitstellung verwendet, wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Remote-Netzwerke** aus.
  - Wenn im Bereich „Remote-Netzwerke“ das Feld **Bandbreite** angezeigt wird, weisen Sie Bandbreite nach Prisma Access zu und können zum Modell mit aggregierter Bandbreite migrieren.



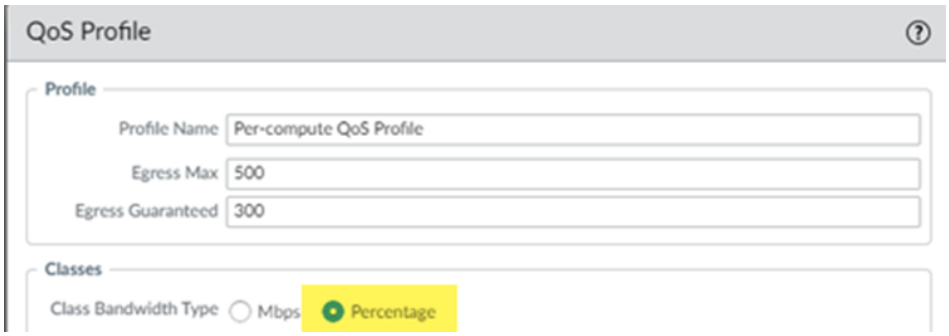

  - Wenn ein **IPSec-Terminierungsknoten** angezeigt wird, ist die Migration zum Modell mit aggregierter Bandbreite bereits abgeschlossen.




- Nach der Migration zum Modell mit aggregierter Bandbreite ist die Änderung dauerhaft und Sie können nicht zu einer Bereitstellung zurückkehren, die Bandbreite nach Prisma Access-Standort zuweist.

 ©2025 Palo Alto Networks, Inc.

- Ihnen muss eine Bandbreite von mindestens 50 Mbit/s zur Verfügung stehen, um zum Modell mit aggregierter Bandbreite zu migrieren.
- Wenn Sie QoS nach der Migration implementieren möchten, informieren Sie sich über die Unterschiede beim Konfigurieren von QoS für eine Bereitstellung mit aggregierter Bandbreite.
  - Stellen Sie sicher, dass Sie in Ihren QoS-Profilen den **Klassenbandbreitentyp Prozentsatz** anstelle von **Mbit/s** verwenden. Prisma Access unterstützt keine Bandbreitentypen von **Mbit/s** in QoS-Profilen für Bereitstellungen, die Bandbreite nach Compute-Standort zuweisen.




  - Erfahren Sie, wie Sie ein garantiertes Bandbreitenverhältnis angeben und die Bandbreite pro Standort anpassen.

    Mit einem garantierten Bandbreitenverhältnis können Sie einen Prozentsatz der gesamten zugewiesenen Bandbreite am Compute-Standort zuweisen. Prisma Access teilt die garantierte Bandbreite gleichmäßig durch die Anzahl der IPSec-Abschlussknoten am Compute-Standort.

    Durch Anpassen der Bandbreite pro Standort können Sie in den **Einstellungen** für das Remote-Netzwerk ein Zuordnungsverhältnis für die Standorte und einen einzelnen IPSec-Terminierungsknoten anwenden und QoS-Profile pro Standort angeben. Alternativ können Sie ein QoS-Profil während der Remote-Netzwerkkonfiguration angeben, indem Sie das Remote-Netzwerk auswählen und auf der Registerkarte **QoS** ein QoS-Profil angeben.
- Wenn Sie Ihre Remote-Netzwerke so konfiguriert haben, dass sie sicheren eingehenden Zugriff auf Ihre Remote-Netzwerkstandorte bieten, werden alle vorhandenen eingehenden Zugriffsfunktionen unterstützt, wie z. B. die Aktivierung einer sekundären WAN-Verbindung (**Sekundäres WAN aktivieren**) sowie BGP-, QoS- und Quell-NAT-Optionen. Es gibt auch keine Änderung an der verbrauchten Bandbreite durch öffentliche IP-Adressen, die Prisma Access zuweist (5 IP-Adressen verbrauchen 150 Mbit/s Ihrer Remote-Netzwerklizenzzuweisung und 10 IP-Adressen verbrauchen 300 Mbit/s).

  Wenn Sie nach der Migration eingehenden Zugriff konfigurieren müssen, verwenden Sie die für das Modell mit aggregierter Bandbreite spezifische Vorgehensweise für das Einrichten von eingehendem Zugriff.

 ©2025 Palo Alto Networks, Inc.

- Palo Alto Networks empfiehlt, sich vor der Migration die vorhandenen Bandbreiteneinstellungen und die gesamte lizenzierte Bandbreite zu notieren.

  *Obwohl Prisma Access Ihre Bandbreite während der Migration migriert, sollten Sie Ihre aktuellen Einstellungen als Best Practice notieren und nach der Migration Anpassungen an der Bandbreite des Compute-Standorts vornehmen.*

  - Überprüfen Sie Ihre vorhandenen Bandbreiteneinstellungen, indem Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Remote-Netzwerke** auswählen. Notieren Sie sich die vorhandene **Bandbreite**, die für jede Remote-Netzwerkverbindung verfügbar ist.
  - Navigieren Sie zu **Panorama** > **Lizenzen** und überprüfen Sie Ihre gesamte lizenzierte Bandbreite in Mbit/s für Remote-Netzwerke. Je nach Lizenztyp finden Sie diese Informationen unter **Prisma Access Nettokapazität** oder **GlobalProtect Cloud Service für mobile Benutzer**.

Beachten Sie nach der Migration die folgenden Unterschiede in Ihrer Bereitstellung:

- Sie nehmen alle neuen Remote-Netzwerke mit dem Onboarding-Verfahren für Remote-Netzwerke mit aggregierter Bandbreite auf.
- Wenn Sie Bandbreitennutzungsstatistiken anzeigen, sind diese nach den jeweiligen IPSec-Terminierungsknoten angeordnet.

## Bandbreitenzuweisung für eine migrierte Bereitstellung mit aggregierter Bandbreite.

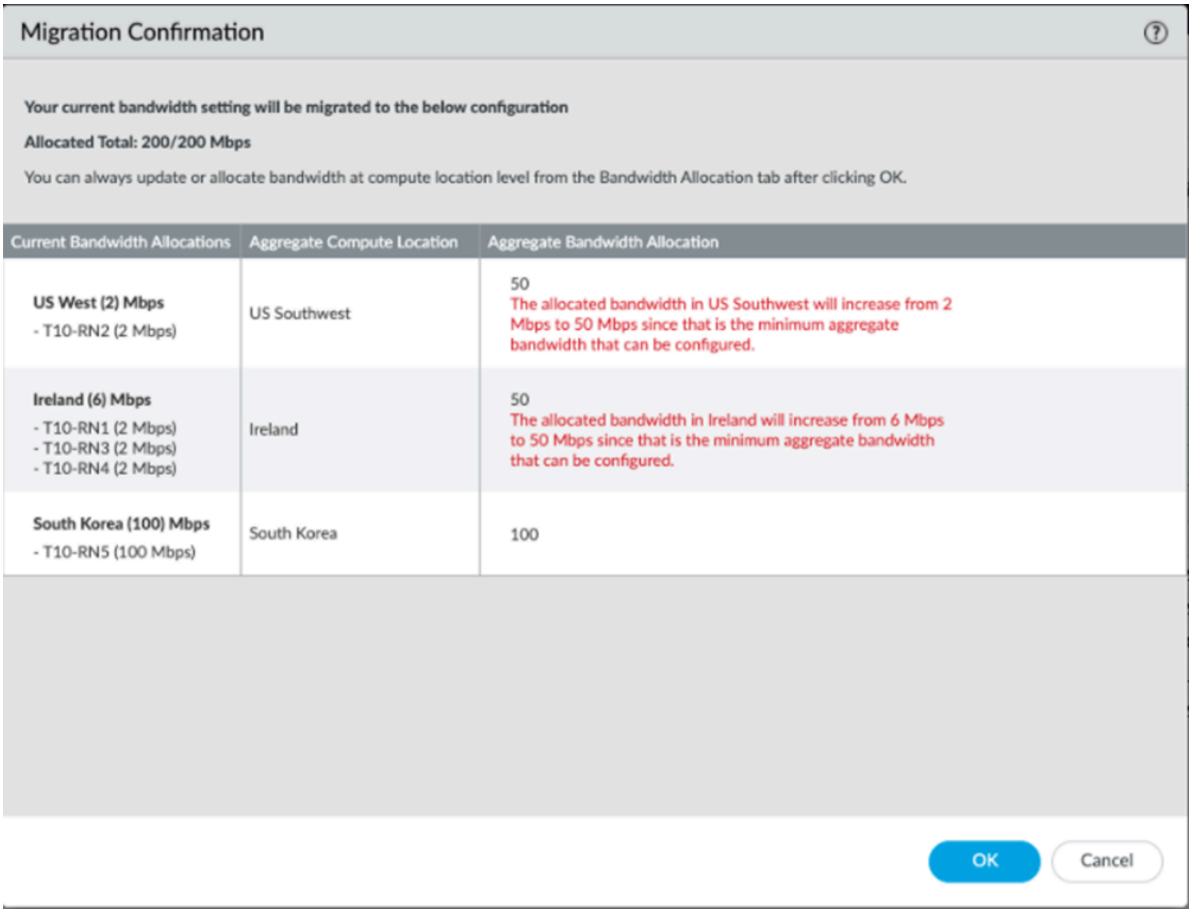
Wenn Ihre Bereitstellung die Bandbreite nach Prisma Access-Standort zuweist, nimmt Prisma Access folgende Änderungen vor, wenn Sie zum Modell mit aggregierter Bandbreite migrieren.

- Prisma Access summiert die Bandbreite für alle Standorte in einem bestimmten Compute-Standort und weist diesem Compute-Standort die summierte Bandbreite zu.

  Sie haben beispielsweise drei Standorte (**Standort 1**, **Standort 2** und **Standort 3**) in den Standorten „Mexiko (West)“, „USA (Südwest)“ und „USA (West)“, und jeder vorhandene Standort verfügt über eine Bandbreite von 50 Mbit/s. Da sich jeder Standort im Rechenstandort „USA (Südwest)“ befindet, summiert Prisma Access die Bandbreite der drei Standorte und weist dem Standort „USA (Südwest)“ 150 Mbit/s Bandbreite zu.
- Wenn alle Standorte an einem Rechenstandort eine Gesamtbandbreite von weniger als 50 Mbit/s aufweisen, erhöht Prisma Access die Bandbreite für diesen Rechenstandort auf

 ©2025 Palo Alto Networks, Inc.

50 Mbit/s. Prisma Access gibt die Standorte an, für die während des Migrationsprozesses eine Bandbreitenerhöhung erforderlich ist.




- Prisma Access verwendet IPSec-Terminierungsknoten in Bereitstellungen mit aggregierter Bandbreite. Während der Migration stellt Prisma Access einen IPSec-Terminierungsknoten pro Compute-Standort für 1.000 Mbit/s zugewiesene Bandbreite bereit. Wenn Sie beispielsweise 1.500 Mbit/s Bandbreite an einem Compute-Standort zuweisen, stellt Prisma Access diesem Standort zwei IPSec-Abschlussknoten zur Verfügung.

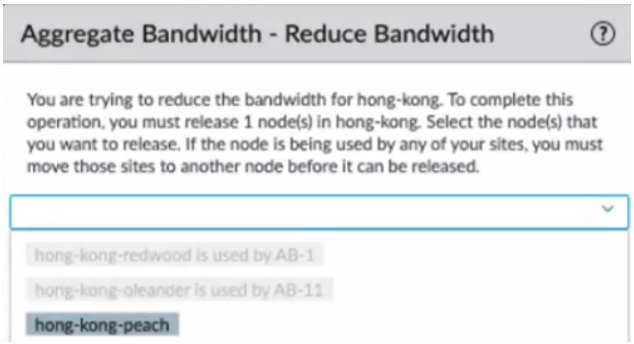
  Sie weisen einem Remote-Netzwerk während des Onboardings IPSec-Terminierungsknoten zu. Bei einer Migration mit aggregierter Bandbreite ordnet Prisma Access die IPSec-Terminierungsknoten während der Migration den Remote-Netzwerken zu. Die folgende Liste enthält einige Beispiele für die Zuordnung von IPSec-Terminierungsknoten für eine Migration:

  - Wenn Sie über vier Remote-Netzwerke verfügen, die sich am selben Compute-Standort befinden, und diese Standorte jeweils 50 Mbit/s Bandbreite aufweisen, weist Prisma Access diesem Compute-Standort 200 Mbit/s Bandbreite zu, stellt diesem Compute-Standort einen einzigen IPSec-Abschlussknoten zur Verfügung und ordnet diesen IPSec-Abschlussknoten allen vier Remote-Netzwerken zu.
  - Wenn Sie über drei Remote-Netzwerke mit jeweils 100 Mbit/s am selben Compute-Standort verfügen, weist Prisma Access diesem Compute-Standort 300 Mbit/s Bandbreite zu, stellt diesem Compute-Standort einen einzigen IPSec-Abschlussknoten zur Verfügung und ordnet diesen IPSec-Terminierungsknoten allen drei Remote-Netzwerken zu.

 ©2025 Palo Alto Networks, Inc.

- Wenn Sie sieben Remote-Netzwerke am selben Compute-Standort haben, davon zwei Remote-Netzwerke mit einer Bandbreite von jeweils 500 Mbit/s und fünf Remote-Netzwerke mit einer Bandbreite von jeweils 100 Mbit/s, weist Prisma Access diesem Compute-Standort 1.500 Mbit/s Bandbreite zu. Da die gesamte zugewiesene Bandbreite in diesem Compute-Standort größer als 1.000 Mbit/s ist, weist Prisma Access zwei IPSec-Terminierungsknoten zu und nimmt die folgenden Zuordnungen vor:
  - Den beiden Remote-Netzwerken mit je 500 Mbit/s ist ein IPSec-Terminierungsknoten (ein Knoten für jedes Remote-Netzwerk mit 1000 Mbit/s Bandbreite) zugeordnet.
  - Den fünf Remote-Netzwerken mit je 100 Mbit/s Bandbreite ist ein IPSec-Terminierungsknoten zugeordnet.

  Nach der Migration können Sie die IPSec-Terminierungsknotenzuordnung ändern, um die Bandbreite für einen Standort zu erhöhen. Wenn Sie beispielsweise einen Rechenstandort mit zwei IPSec-Terminierungsknoten verwenden, können Sie einen einzelnen IPSec-Terminierungsknoten einem einzelnen Standort neu zuweisen und den anderen IPSec-Terminierungsknoten den verbleibenden Standorten neu zuweisen, wodurch der Standort, an dem kein IPSec-Terminierungsknoten für die gemeinsame Verwendung vorhanden ist, effektiv mit mehr Bandbreite bereitgestellt wird.
- Wenn Sie die Bandbreite ausreichend reduzieren, müssen Sie möglicherweise einen IPSec-Terminierungsknoten freigeben. Wenn Sie beispielsweise die Bandbreite an einem Compute-Standort von 1.500 Mbit/s auf 800 Mbit/s reduzieren, müssten Sie einen der vorhandenen IPSec-Terminierungsknoten entfernen. Wenn einer dieser Knoten von vorhandenen Standorten verwendet wird, müssen Sie den IPSec-Terminierungsknoten neu zuweisen, bevor Sie den IPSec-Terminierungsknoten löschen.




## QoS-Migrationsrichtlinien

Wenn Sie QoS mit Ihrer aktuellen Prisma Access-Remote-Netzwerkbereitstellung verwenden und Bandbreite nach Standort zuweisen, können Sie zu einer Bereitstellung mit aggregierter Bandbreite migrieren, wobei Ihre vorhandenen QoS-Richtlinien und Profile beibehalten werden.

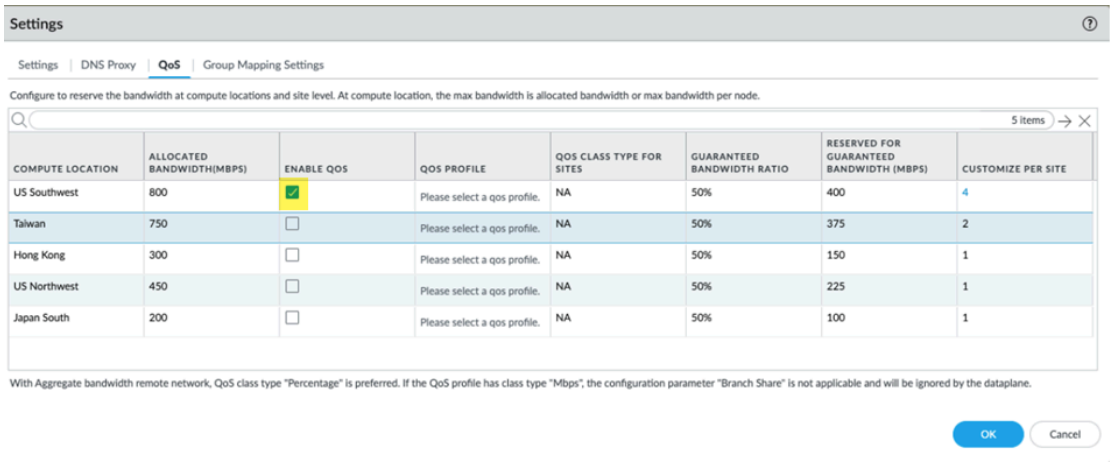
Mit dem Modell mit aggregierter Bandbreite weisen Sie Bandbreite auf aggregierter Ebene pro Compute-Standort zu, und Prisma Access weist die Bandbreite dynamisch basierend auf Last oder Bedarf pro Standort zu.

Nach der Migration wird auf der Registerkarte **QoS** die QoS-Konfiguration in den Remote-Netzwerkeinstellungen angezeigt (**Panorama** > **Cloud Services** > **Konfiguration** > **Remote-Netzwerke** > **Einstellungen**). An allen Compute-Standorte, die Standorten zugeordnet sind, für

 ©2025 Palo Alto Networks, Inc.

die QoS aktiviert wurde, ist **QoS aktivieren** ausgewählt. Alle Compute-Standorte, die Standorten zugeordnet sind, für die QoS nicht aktiviert wurde, ist **QoS aktivieren** deaktiviert.

Im folgenden Screenshot ist ein Beispiel für die Registerkarte „QoS“ nach der Migration dargestellt. Für ein Remote-Netzwerk am Standort „USA (West)“ ist QoS aktiviert, während QoS an keinem anderen Standort aktiviert ist. Da der Standort „USA (West) dem Compute-Standort „USA (Südwest)“ zugeordnet ist, wird auf der Registerkarte **QoS** für den Standort „USA (Südwest)“ angezeigt, dass QoS aktiviert ist.

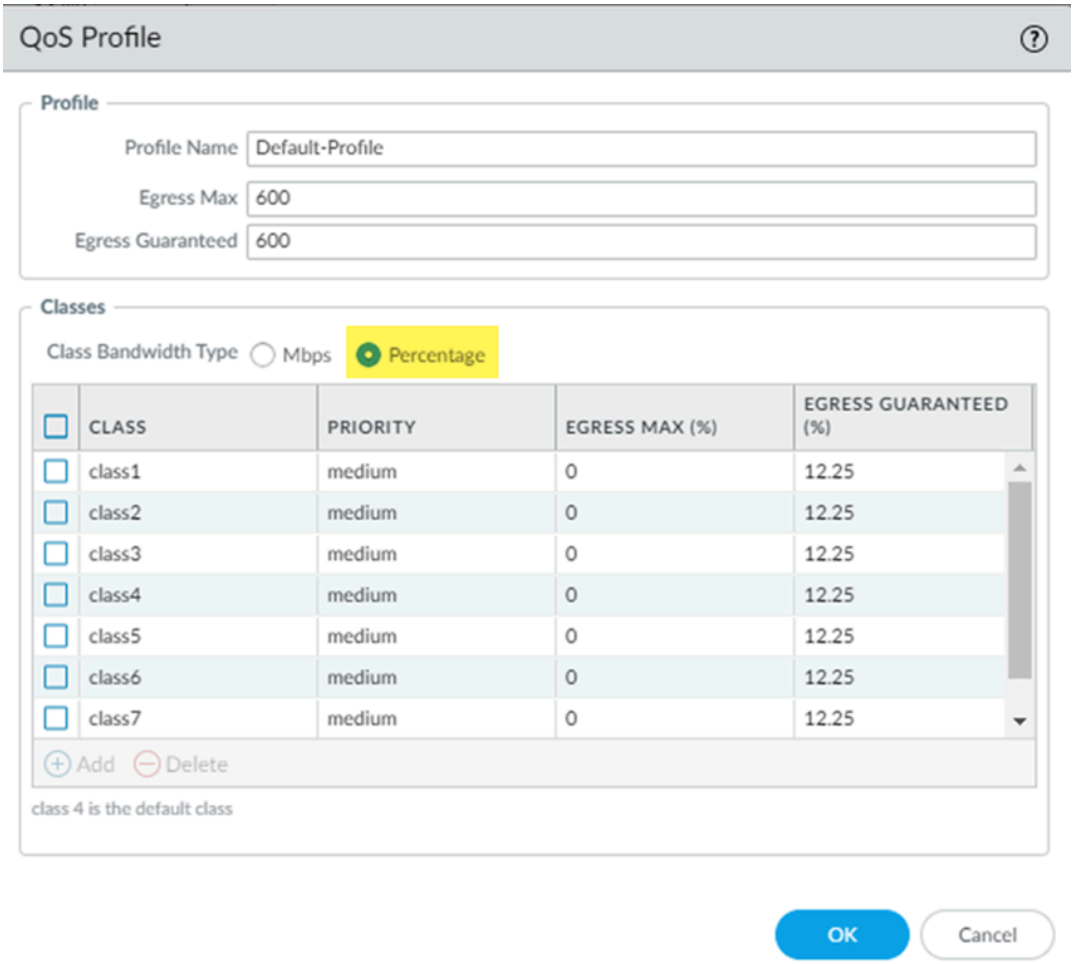



Palo Alto Networks hat die folgenden Empfehlungen und Anforderungen für QoS in einer Bereitstellung mit aggregierter Bandbreite festgelegt.

- Da die Bandbreite für alle Standorte an einem einzelnen Rechenstandort gemeinsam verwendet wird, sollten Sie den **Klassenbandbreitentyp** von **Mbit/s** in **Prozentsatz** ändern. Der Bandbreitentyp **Mbit/s** wird nur unterstützt, wenn Ihre vorhandene Bereitstellung Bandbreite

 ©2025 Palo Alto Networks, Inc.

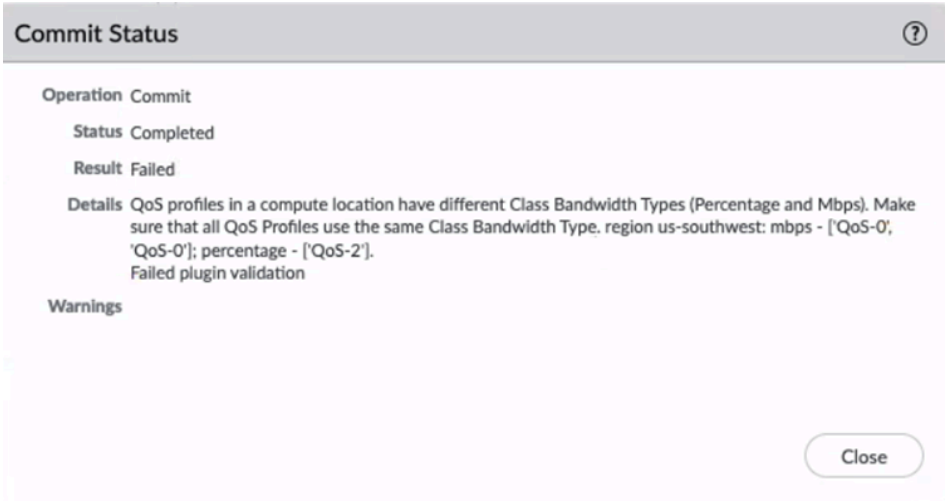
nach Standort zuweist, und Sie anschließend zu einer Bereitstellung mit aggregierter Bandbreite migrieren.




- Sie können die QoS-Bandbreitenzuweisung nicht basierend auf Mbit/s im Profil anpassen. Bei Profilen, die eine Bandbreite des Typs **Prozentsatz** verwenden, können Sie die QoS-Bandbreite pro Standort ändern, indem Sie das garantierte Bandbreitenverhältnis anpassen und das QoS-Profil pro Standort ändern.


©2025 Palo Alto Networks, Inc.

- Sie können an einem Compute-Standort nicht verschiedene Bandbreitentypen verwenden. Bei Nichtbeachtung wird beim Festschreiben eine Fehlermeldung angezeigt.

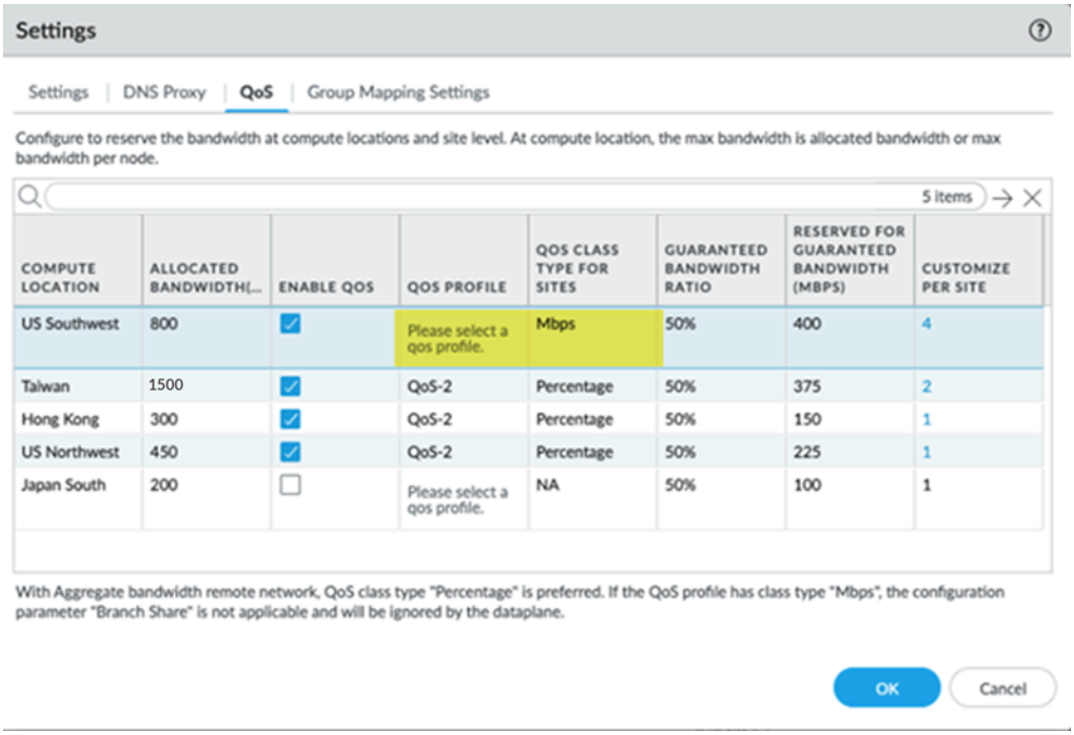



- Wenn Sie neue Standorte hinzufügen und diese Standorte zu einem neuen Compute-Standort gehören, können Sie nur Profile erstellen, die am neuen Compute-Standort den **Klassenbandbreitentyp Prozentsatz** aufweisen.
- Wenn Sie QoS-Profile mit dem **Klassenbandbreitentyp Mbit/s** beibehalten, werden alle Änderungen, die Sie am garantierten Bandbreitenverhältnis vornehmen, oder Anpassungen am QoS-Profil pro Standort, ignoriert.
- Nach der Migration zeigen alle Standorte, die QoS-Profile mit dem **Klassenbandbreitentyp Mbit/s** verwenden, auf der Registerkarte **QoS** für den jeweiligen Compute-Standort als **QoS-Klassentyp für Standorte Mbit/s** an. QoS-Profile mit dem **Klassenbandbreitentyp Prozentsatz** zeigen als **QoS-Klassentyp für Standorte** den Wert **Prozentsatz** an.

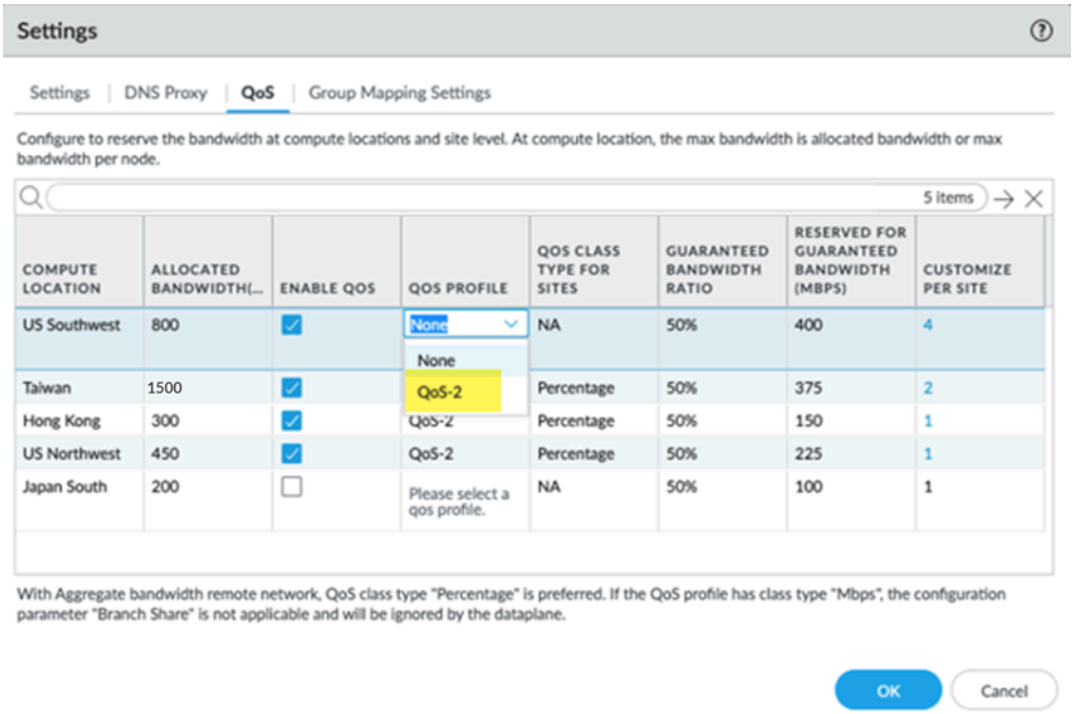
  Außerdem können Sie keine QoS-Profile auswählen, die den **Klassenbandbreitentyp Mbit/s** aufweisen. Der folgende Screenshot zeigt den Compute-Standort „USA (Südwest)“ an, der

 ©2025 Palo Alto Networks, Inc.

ein QoS-Profil mit dem **Klassenbandbreitentyp Mbit/s** verwendet. Diese Option kann im Dropdown-Menü im Bereich **QoS-Profil** nicht ausgewählt werden.



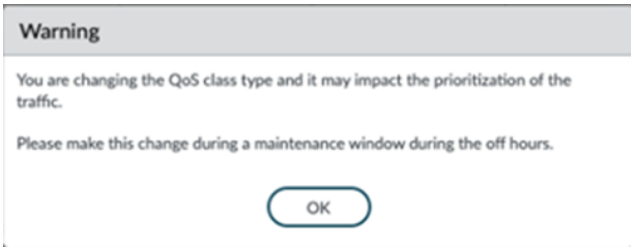

Sie können jedoch ein QoS-Profil auswählen, das den **Klassenbandbreitentyp Prozentsatz** verwendet (in diesem Beispiel „QoS-2“).



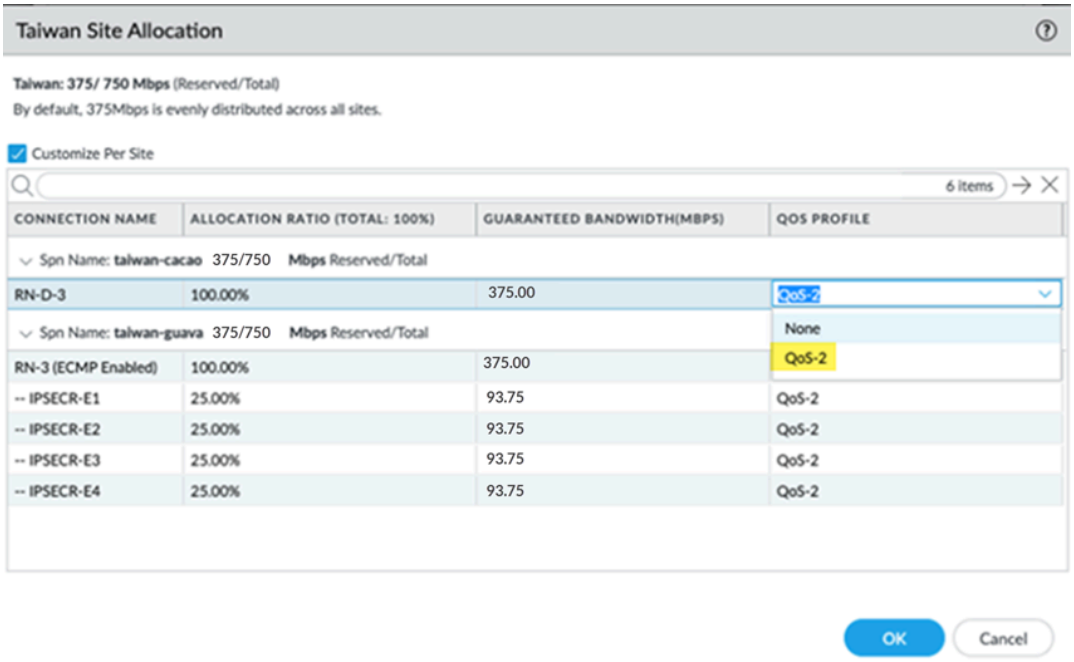

- Wenn Sie das QoS-Profil für einen Compute-Standort vom **Klassenbandbreitentyp Mbit/s** in **Prozentsatz** ändern, sollten Sie die Änderung während eines Wartungsfensters oder

 ©2025 Palo Alto Networks, Inc.

außerhalb der Spitzenzeiten vornehmen. Durch die Änderung des QoS-Profils könnte sich die Priorisierung des Datenverkehrs ändern.




- Sie können QoS-Profile mit dem **Klassenbandbreitentyp Prozentsatz** nur auswählen, wenn Sie das QoS-Profil für jeden Standort anpassen.




# Migration Ihrer Bandbreitenverwaltungseinstellungen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Erfahren Sie, wie Sie Ihre Bandbreitenverwaltungseinstellungen migrieren können.

Wenn Sie mit einer Prisma Access-Remote-Netzwerkbereitstellung arbeiten, die Bandbreite nach Standort zuweist, können Sie mit Prisma Access Ihre Bereitstellung flexibler und skalierbarer gestalten, indem Sie zu einer Bereitstellung migrieren, die Bandbreite nach Compute-Standort zuweist (das Modell mit aggregierter Bandbreite). Nachdem Sie die Checkliste für die Migrationsplanung überprüft haben, gehen Sie wie folgt vor, um zum Modell mit aggregierter

 ©2025 Palo Alto Networks, Inc.

Bandbreite zu migrieren. Sie können auch Ihre Remote-Netzwerk-QoS-Bereitstellung migrieren. Bei der Migration verwenden alle Remote-Netzwerke das Modell mit der aggregierten Bandbreite.

Verwenden Sie Folgendes, bevor Sie Ihre Bandbreiteneinstellungen migrieren:

- Die folgenden Remote-Netzwerkkomponenten, die nach der Migration unverändert bleiben:
  - Die Prisma Access-Dataplane.
  - Keine Auswirkungen auf bestehende Tunnel.
  - Keine Neukonfiguration Ihrer IPSec-Tunnelparameter.
  - IKE-Gateways, IKE- und IPSec-Verschlüsselungsprofile sowie IPSec-Tunnelkonfigurationen bleiben unverändert.
  - Die **IP-Adresse** ändert sich nicht für jedes Remote-Netzwerk.
- Prisma Access weist IPSec-Terminierungsknoten zu und sorgt für die Zuweisung von Bandbreite zu Remote-Netzwerken während einer Migration zum Modell mit aggregierter Bandbreite.
- Wenn eine nicht unterstützte Konfiguration vorliegt, wird die Registerkarte „Bandbreitenzuweisung“ oder das Banner zur Migration nicht angezeigt.
- Wenn Sie über ein QoS mit Ihren Remote-Netzwerken verfügen, beachten Sie vor der Migration unbedingt die QoS-Migrationsrichtlinien.
- Nach der Migration zum Modell mit aggregierter Bandbreite ist die Änderung dauerhaft und Sie können nicht zu einer Bereitstellung zurückkehren, die Bandbreite nach Prisma Access-Standort zuweist.
- Ihnen muss eine Bandbreite von mindestens 50 Mbit/s zur Verfügung stehen, um zum Modell mit aggregierter Bandbreite zu migrieren.
- Wenn Sie QoS nach der Migration implementieren möchten, informieren Sie sich über die Unterschiede beim Konfigurieren von QoS für eine Bereitstellung mit aggregierter Bandbreite.
- Nach der Migration werden alle neuen Remote-Netzwerke mit dem Onboarding-Verfahren für Remote-Netzwerke mit aggregierter Bandbreite eingebunden.
- Wenn Sie nach der Migration die Bandbreitennutzungsstatistiken anzeigen, sind diese nach den jeweiligen IPSec-Terminierungsknoten angeordnet.
- Verwenden Sie zum Ausführen der Migration nicht die CLI, sondern ausschließlich die Benutzeroberfläche.
- Strata Cloud Manager
- Panorama

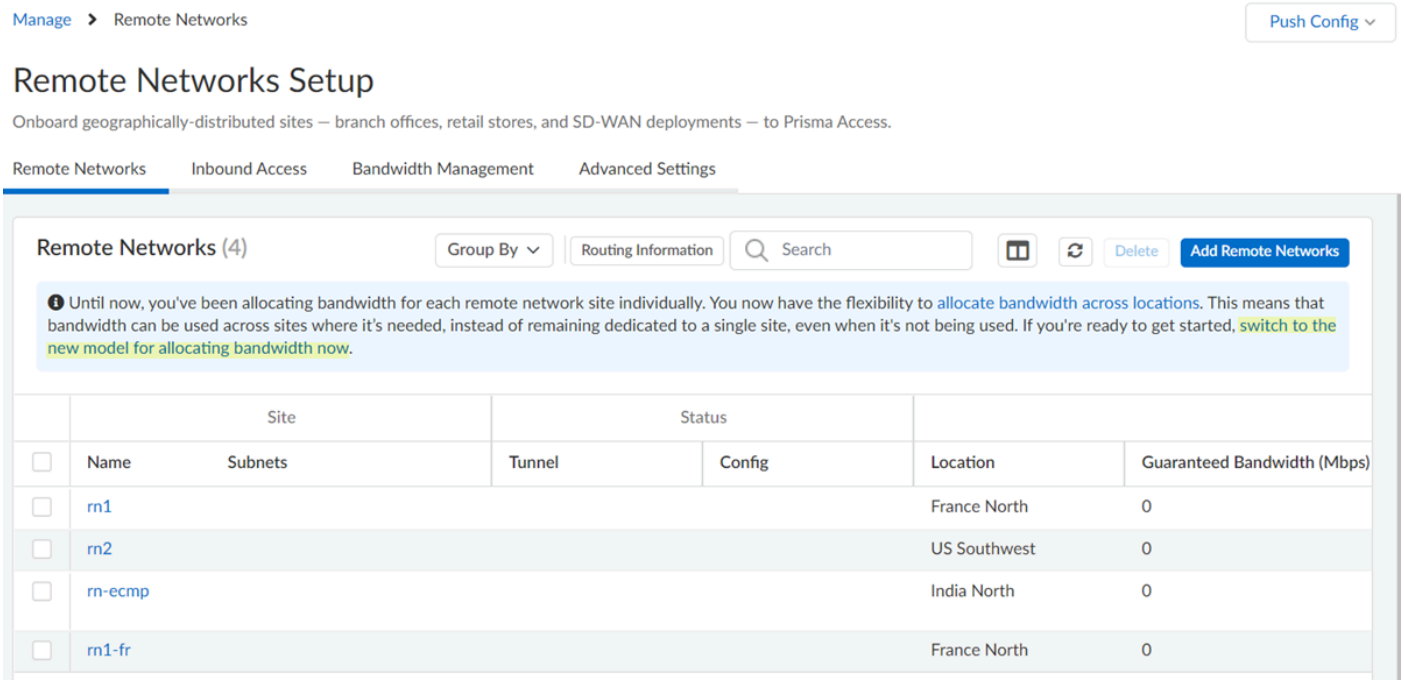
## Migration Ihrer Bandbreitenverwaltungseinstellungen (Strata Cloud Manager)

Wenn Sie mit einer Prisma Access-Remote-Netzwerkbereitstellung arbeiten, die Bandbreite nach Standort zuweist, können Sie mit Prisma Access Ihre Bereitstellung flexibler und skalierbarer gestalten, indem Sie zu einer Bereitstellung migrieren, die Bandbreite nach Compute-Standort zuweist (das Modell mit aggregierter Bandbreite). Nachdem Sie die Checkliste für die Migrationsplanung überprüft haben, gehen Sie wie folgt vor, um zum Modell mit aggregierter Bandbreite zu migrieren.

**STEP 1 |** Wählen Sie **Workflows** > **Einrichtung Prisma Access** > **Remote-Netzwerke** aus.

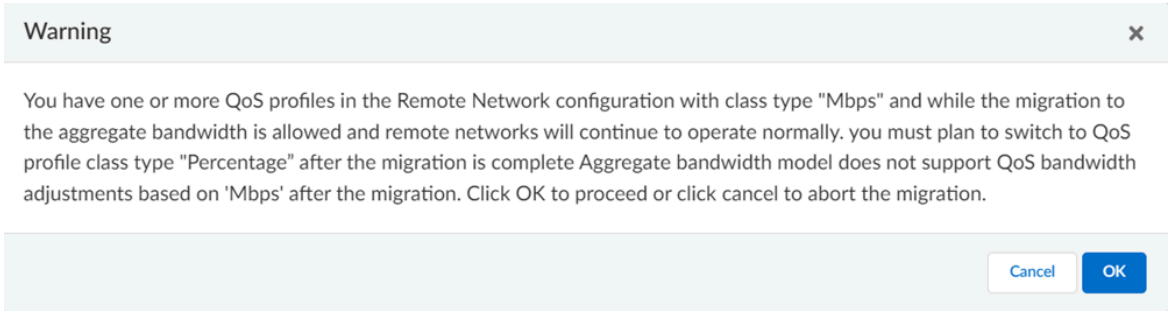
 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** **Wechseln Sie jetzt zum neuen Modell für die Zuweisung von Bandbreite.**

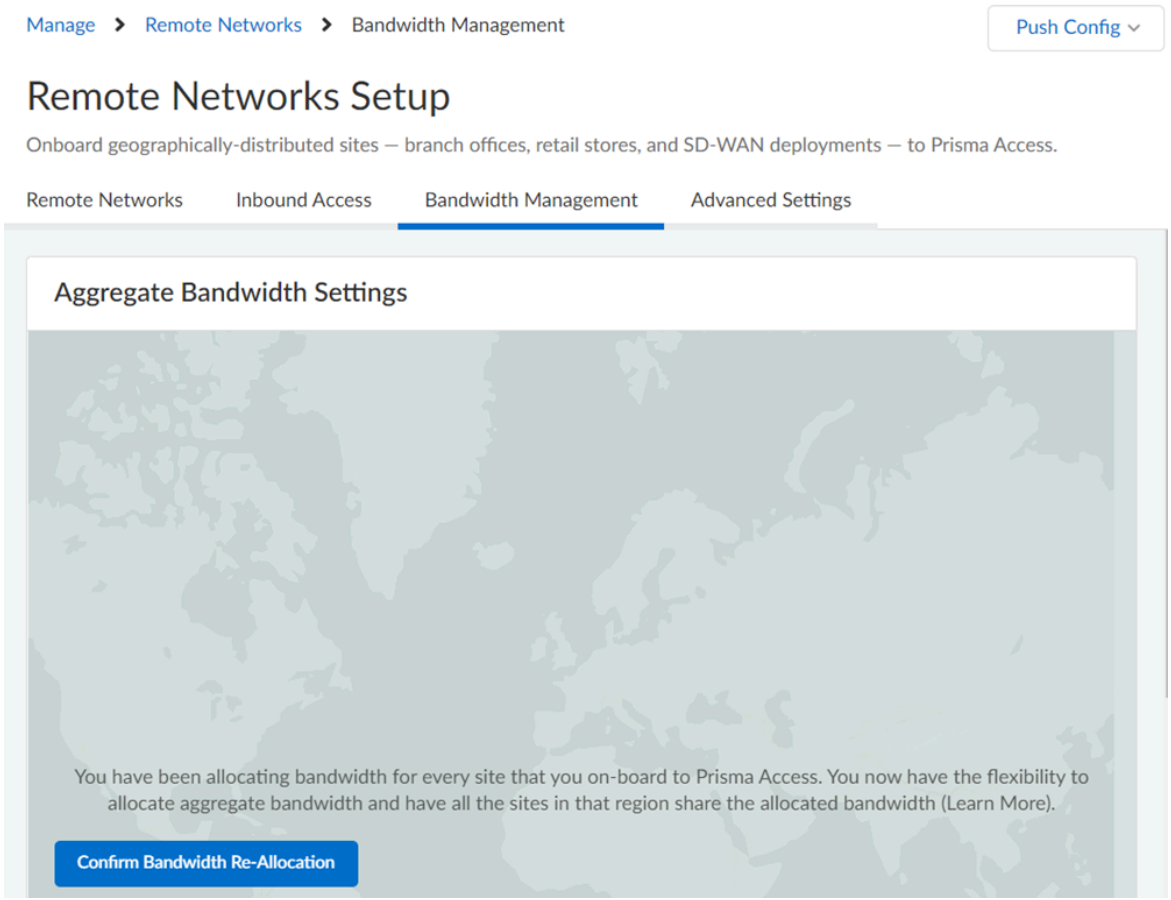



 ©2025 Palo Alto Networks, Inc.

- *Wenn Sie über QoS-Profile mit **Mbit/s** als **Klassenbandbreitentyp** verfügen, werden Sie von Prisma Access darauf hingewiesen, dass Sie die Änderung dieser Profile in einen **Klassenbandbreitentyp** von **Prozent** einplanen sollten.*



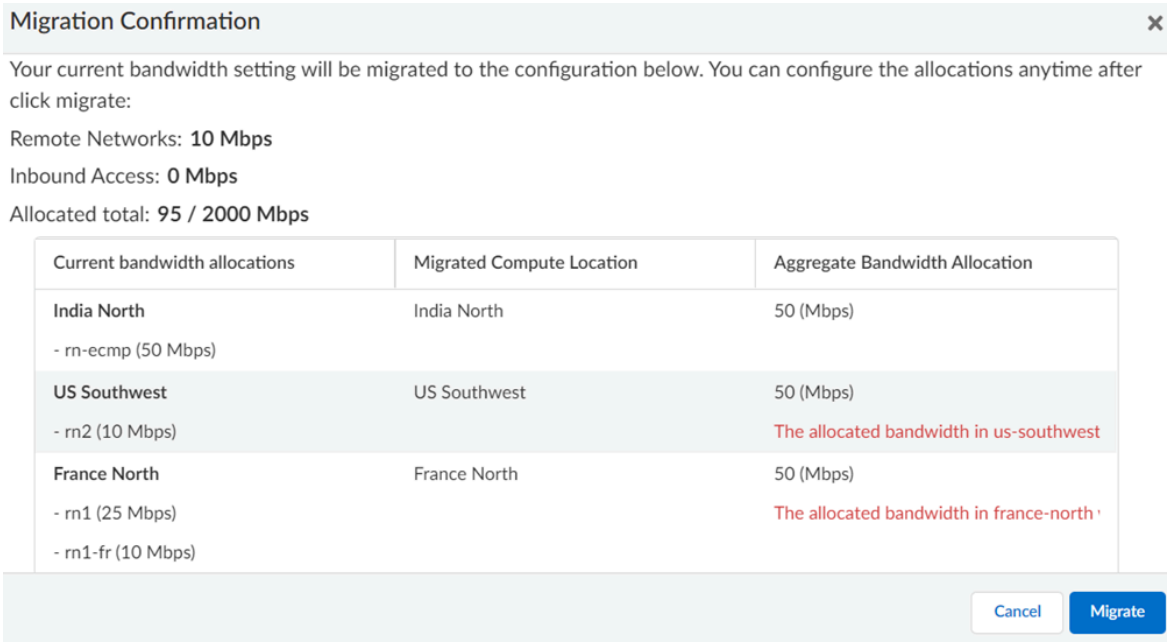

- *Alternativ wählen Sie auf der Registerkarte **Bandbreitenverwaltung** die Option **Bandbreitenneuzuweisung bestätigen** aus.*




 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Überprüfen Sie die Informationen und wählen Sie im angezeigten Popup-Fenster die Option **Migrieren** aus.

*Wenn alle Standorte an einem Rechenstandort eine Gesamtbandbreite von weniger als 50 Mbit/s aufweisen, erhöht Prisma Access die Bandbreite für diesen Rechenstandort auf 50 Mbit/s. Prisma Access gibt die Standorte an, für die während des Migrationsprozesses eine Bandbreitenerhöhung erforderlich ist.*




*Die Migration zum Modell mit aggregierter Bandbreite ist dauerhaft und nicht reversibel. Überprüfen Sie vor der Migration die Checkliste zur Migrationsvorbereitung. Damit Ihre Änderungen wirksam werden, müssen Sie **Commit und Push** auswählen.*

Prisma Access migriert Ihre zugewiesene Remote-Netzwerkbandbreite zum Modell mit aggregierter Bandbreite.

**STEP 4 |** Führen Sie für Ihre Änderungen die Aktion **Commit und Push** aus.

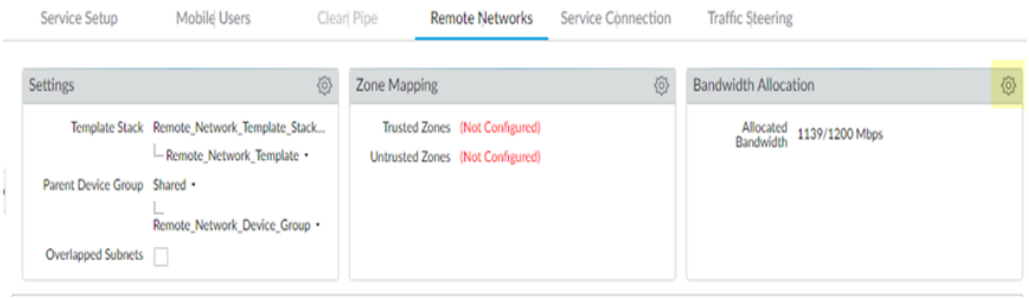
## Migration Ihrer Bandbreitenverwaltungseinstellungen (Panorama)

Wenn Sie mit einer Prisma Access-Remote-Netzwerkbereitstellung arbeiten, die Bandbreite nach Standort zuweist, können Sie mit Prisma Access Ihre Bereitstellung flexibler und skalierbarer gestalten, indem Sie zu einer Bereitstellung migrieren, die Bandbreite nach Compute-Standort zuweist (das Modell mit aggregierter Bandbreite). Nachdem Sie die Checkliste für die Migrationsplanung überprüft haben, gehen Sie wie folgt vor, um zum Modell mit aggregierter Bandbreite zu migrieren.

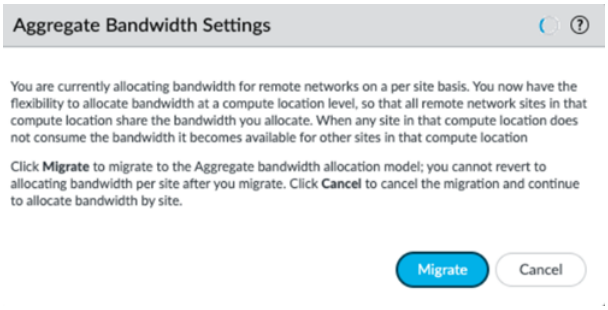
**STEP 1 |** Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Remote-Netzwerke** aus.

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Bearbeiten Sie die Einstellungen, indem Sie auf das Zahnradsymbol im Bereich **Bandbreitenzuweisung** klicken.

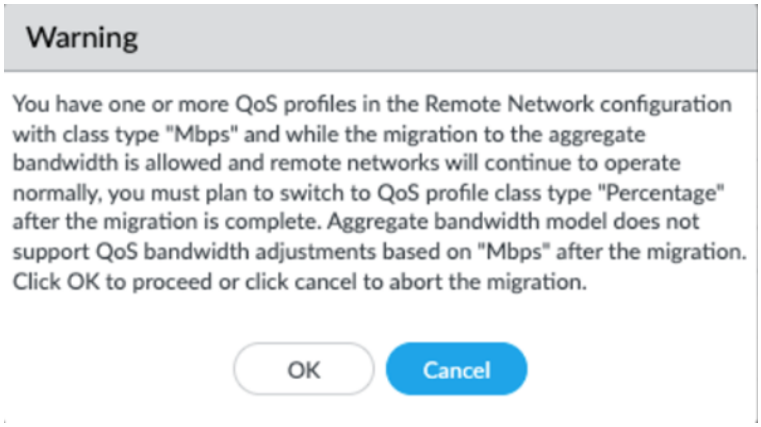



**STEP 3 |** Wählen Sie im Popup-Fenster, das angezeigt wird, **Migrieren** aus.




*Die Migration zum Modell mit aggregierter Bandbreite ist dauerhaft und nicht reversibel. Überprüfen Sie vor der Migration die Checkliste zur Migrationsvorbereitung. Damit Ihre Änderungen wirksam werden, müssen Sie* ***Commit und Push*** *auswählen.*

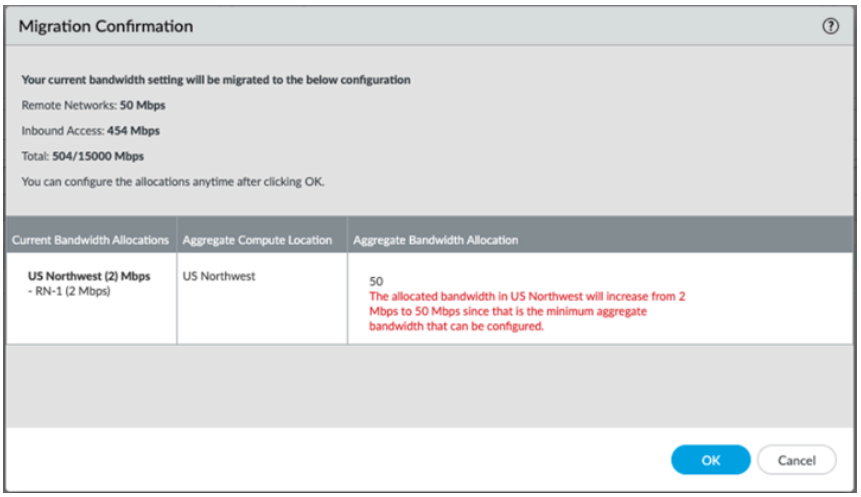
*Wenn Sie über QoS-Profile mit* ***Mbit/s*** *als* ***Klassenbandbreitentyp*** *verfügen, werden Sie von Prisma Access darauf hingewiesen, dass Sie die Änderung dieser Profile in einen* ***Klassenbandbreitentyp*** *von* ***Prozent*** *einplanen sollten.*



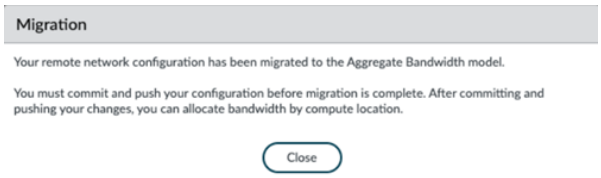

 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** Überprüfen Sie die Informationen im Fenster **Bestätigung der Migration** und klicken Sie dann auf **OK**.

*Wenn alle Standorte an einem Rechenstandort eine Gesamtbandbreite von weniger als 50 Mbit/s aufweisen, erhöht Prisma Access die Bandbreite für diesen Rechenstandort auf 50 Mbit/s. Prisma Access gibt die Standorte an, für die während des Migrationsprozesses eine Bandbreitenerhöhung erforderlich ist.*




Prisma Access migriert Ihre zugewiesene Remote-Netzwerkbandbreite zum Modell mit der aggregierten Bandbreite und zeigt ein Bestätigungsfenster an. Klicken Sie auf **Schließen**, um das Fenster zu schließen.




**STEP 5 |** Führen Sie für Ihre Änderungen die Aktion **Commit und Push** aus.

 ©2025 Palo Alto Networks, Inc.

# Remote-Netzwerk einbinden

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Sobald die Planung für Ihr Remote-Netzwerk abgeschlossen ist, können Sie mit der Konfiguration beginnen. Dazu gehören das Onboarding des Remote-Netzwerks, die Verbindung des Remote-Netzwerkstandorts mit Prisma Access und die Aktivierung von Routing und QoS für das Remote-Netzwerk. Für jedes Remote-Netzwerk, das Sie mit Prisma Access für Netzwerke sichern möchten, übertragen Sie die erforderliche Richtlinienkonfiguration per Push an Prisma Access und binden alle Remote-Netzwerke ein, damit Sie den Datenverkehr vom Remote-Standort durch den IPSec-Tunnel an Prisma Access senden können. Verwenden Sie eines der folgenden Verfahren, um Ihre Remote-Netzwerke abhängig von Ihrem Bandbreitenzuweisungstyp einzubinden:

Erfahren Sie, wie Sie ein Remote-Netzwerk einbinden.

- Strata Cloud Manager
- Panorama

## Remote-Netzwerk einbinden (Strata Cloud Manager)

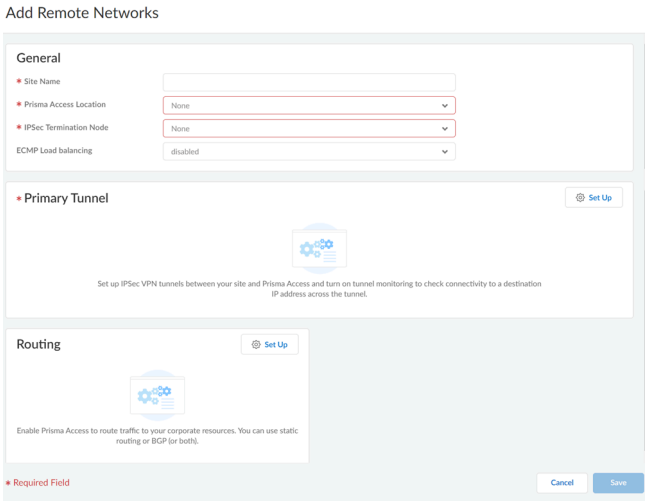
So fügen Sie Prisma Access einen neuen Remote-Netzwerkstandort hinzu. Sie beginnen mit der Angabe des Standorts und definieren, wie viel Bandbreite der Verbindung zugewiesen werden soll.

**STEP 1 |** Starten Sie Prisma Access (Managed by Strata Cloud Manager).

**STEP 2 |** Stellen Sie sicher, dass Sie dem Standort, an dem Sie das Remote-Netzwerk bereitstellen möchten, Bandbreite zugewiesen haben. Siehe Planungscheckliste für Remote-Netzwerke.


©2025 Palo Alto Networks, Inc.

**STEP 3 |** Gehen Sie zu **Workflows** > **Einrichtung Prisma Access** > **Remote-Netzwerke** > **Remote-Netzwerke hinzufügen**.




**STEP 4 |** Geben Sie dem Remote-Netzwerk einen aussagekräftigen **Standortnamen**.

**STEP 5 |** Wählen Sie neben der **Region**, in der sich der Standort befindet, auch den nächstgelegenen Prisma Access-**Standort** aus.

**STEP 6 |** (Nur wenn Sie planen, BGP für dynamisches Routing zu verwenden) Aktivieren Sie **ECMP-Lastausgleich**, damit der Remote-Netzwerkstandort bis zu vier IPSec-Tunnel verwenden kann.

BGP ist für ECMP-Lastausgleich erforderlich; QoS und statische Routen werden nicht unterstützt.

Wenn Sie ECMP aktivieren, erfolgt der Lastausgleich für den Remote-Netzwerkverkehr über die von Ihnen konfigurierten Tunnel.

**STEP 7 |** Konfigurieren Sie die **erweiterten Einstellungen**.

- (Optional) Verwenden Sie **Statische Einträge**, um FQDNs an bestimmte IP-Adressen aufzulösen.

  Diese Funktionalität kann nützlich sein, wenn in Ihrer Organisation Gast-Internetdienste vorhanden sind und Sie möchten, dass Ihre Gäste Suchmaschinen sicher verwenden, damit verhindert wird, dass diese nach potenziell unangemessenem oder anstößigem Material suchen, das gegen die Unternehmensrichtlinie verstoßen könnte. Geben Sie dazu einen eindeutigen **Namen** für die Regel für statische Einträge, einen **FQDN** und die IP-**Adresse** ein, an die die FQDN-Anforderung gerichtet werden soll.




 ©2025 Palo Alto Networks, Inc.

- Wenn Sie möchten, dass Prisma Access als Proxy für DNS-Anfragen fungiert, konfigurieren Sie Werte für **Wiederholung von UDP-Abfragen** (das **Intervall in Sek.)**, um die Abfrage nach einer bestimmten Anzahl von Sekunden zu wiederholen, sowie die Anzahl der durchzuführenden **Wiederholversuche**.

**STEP 8 |** Gehen Sie wie unter Verbinden eines Remote-Netzwerkstandorts mit Prisma Access beschrieben vor, um einen IPSec-VPN-Tunnel zu erstellen und den Remote-Netzwerkstandort mit Prisma Access zu verbinden.

**STEP 9 |** Konfigurieren Sie statisches Routing.

1. Wenn Sie statische Routen verwenden, um den Datenverkehr zu und von der Zentrale bzw. zum oder vom Rechenzentrum weiterzuleiten, wählen Sie **Hinzufügen** aus, um die IP-Subnetze oder IP-Adressen hinzuzufügen, die Sie am Standort der Zweigstelle sichern möchten.

   Wenn Sie Änderungen an den IP-Subnetzen im Netzwerk Ihrer Zentrale oder Ihres Rechenzentrums vornehmen, müssen Sie die statischen Routen manuell aktualisieren.

**STEP 10 |** Konfigurieren Sie das dynamische Routing.

1. Wenn beim dynamischen Routing der Zentrale oder dem Subnetz des Rechenzentrums die Informationen mitgeteilt werden sollen, wählen Sie die Option **BGP für dynamisches Routing aktivieren** aus.
2. (Optional) Wählen Sie einen Wert für **MRAI-Timer** aus.

   Das BGP-Routing bietet einen Timer namens *Minimum Route Advertisement Interval (MRAI)*, den Sie verwenden können, um die BGP-Routing-Konvergenz in Ihrem Netzwerk anzupassen. MRAI dient zur Ratenbegrenzung von Aktualisierungen auf Zielbasis und die BGP-Router warten mindestens die konfigurierte MRAI-Zeit ab, bevor sie eine Mitteilung für dasselbe Präfix senden. Eine kleinere Zahl ermöglicht eine schnellere Konvergenzzeit, erzeugt jedoch mehr Mitteilungen in Ihrem Netzwerk. Eine höhere Zahl verringert die Anzahl der Mitteilungen, die gesendet werden können, kann aber auch die Routing-Konvergenz verlangsamen. Sie entscheiden, welche Anzahl Sie in Ihr Netzwerk einfügen wollen, um das optimale Gleichgewicht zwischen schnellerer Routing-Konvergenz und weniger Mitteilungen zu erreichen.

   Konfigurieren Sie einen MRAI-Bereich zwischen 1 und 600 Sekunden, wobei der Standardwert 30 Sekunden beträgt.
3. Um die Anzahl der über BGP an Ihr Customer Premises Equipment (CPE) gesendeten IP-Subnetz-Mitteilungen für mobile Benutzer zu verringern, geben Sie an, dass Prisma Access die Subnetze vor der Mitteilung zusammenzufassen soll. Wählen Sie hierzu **Mobile Benutzerrouten vor dem Mitteilen zusammenfassen** aus.

   Standardmäßig teilt Prisma Access die IP-Adresspools der mobilen Benutzer in Blöcken von /24-Subnetzen mit. Wenn Sie sie zusammenfassen, teilt Prisma Access den Pool basierend auf dem von Ihnen angegebenen Subnetz mit. Beispiel: Prisma Access teilt einen öffentlichen, mobilen IP-Pool für Benutzer mit der Angabe 10.8.0.0/20 unter Verwendung des /20-Subnetzes mit, anstatt den Pool in die Subnetze 10.8.1.0/24, 10.8.2.0/24, 10.8.3.0/24 usw. zu unterteilen, bevor sie mitgeteilt werden. Durch die Zusammenfassung dieser Mitteilungen kann die Anzahl der in den CPE-Routingtabellen gespeicherten Routen reduziert werden. Sie können die Zusammenfassung von IP-Pools

 ©2025 Palo Alto Networks, Inc.

z. B. mit Cloud-VPN-Gateways (Virtual Private Gateways (VGWs) oder Transit Gateways (TGWs)) verwenden, die eine begrenzte Anzahl von Routen akzeptieren können.

4. (Optional) Damit Prisma Access eine Mitteilung für das Remote-Netzwerk über die Standardroute mithilfe von eBGP erstellt, wählen Sie **Standardroute mitteilen** aus. Vergewissern Sie sich, dass für Ihr Netzwerk keine andere Standardroute vorhanden ist, die von BGP mitgeteilt wird, da es sonst zu Routing-Problemen in Ihrem Netzwerk kommen kann.
5. (Optional) Wenn Sie ein sekundäres WAN konfiguriert haben und die Peer-Adresse für den sekundären (Backup-)BGP-Peer ändern müssen, wählen Sie **Anderen BGP-Peer für sekundären Tunnel verwenden** aus und geben Sie einen eindeutigen Peer und optional eine lokale IP-Adresse für das sekundäre WAN ein.
6. (Optional) Wählen Sie **Routen nicht exportieren** aus, um zu verhindern, dass Prisma Access Routen an die Zentrale oder das Rechenzentrum weiterleitet.

   Standardmäßig teilt Prisma Access alle BGP-Routinginformationen einschließlich lokaler Routen und aller Präfixe mit, die von anderen Dienstverbindungen, Remote-Netzwerken und Subnetzen mobiler Benutzer empfangen werden. Aktivieren Sie dieses Kontrollkästchen, um Prisma Access daran zu hindern, BGP-Mitteilungen zu senden. Die empfangenen BGP-Informationen werden aber weiterhin verwendet, um Informationen zu Routen anderer BGP-Nachbarn zu erhalten.

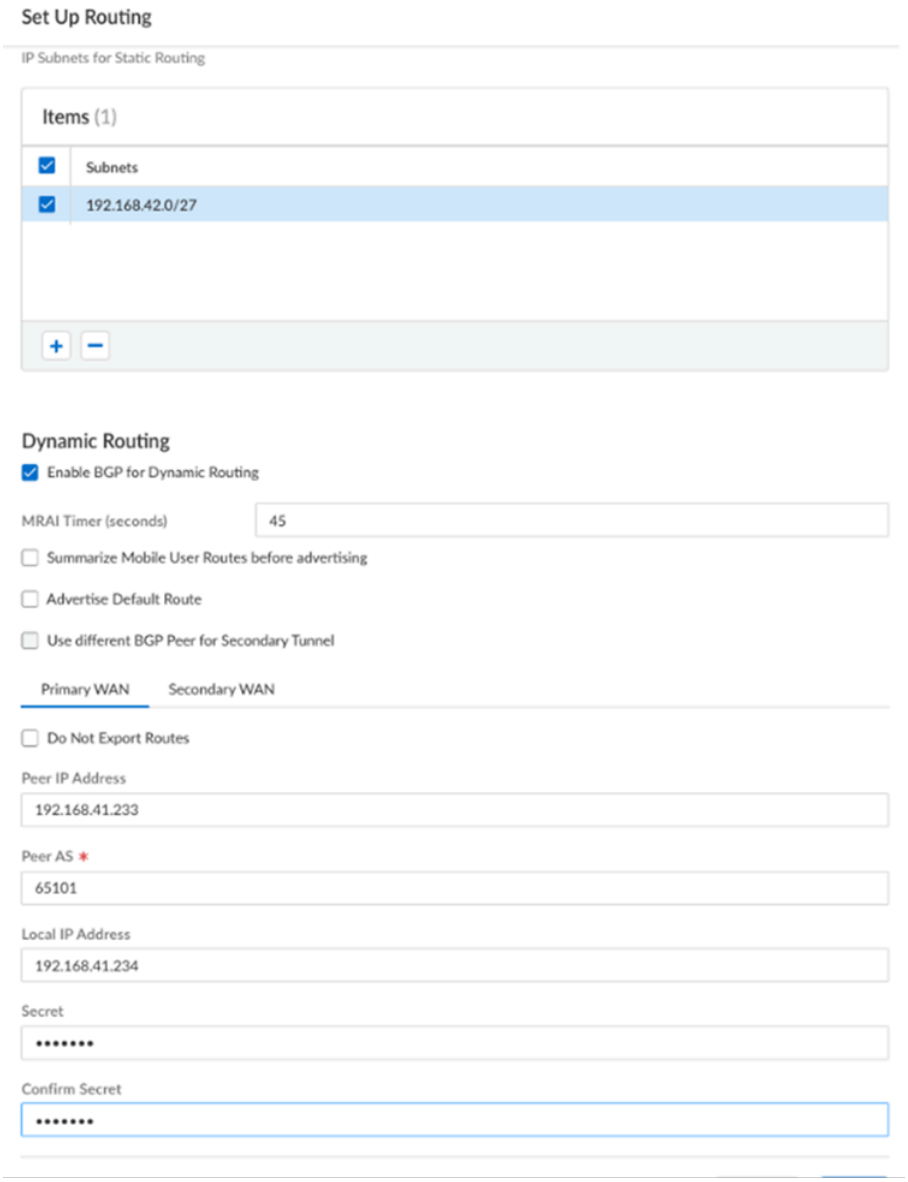
   *Da Prisma Access keine BGP-Mitteilungen sendet, müssen Sie, wenn Sie diese Option auswählen, statische Routen auf dem lokalen Gerät konfigurieren, um Routen zurück zu Prisma Access einzurichten.*
7. Geben Sie die **Peer-IP-Adresse** ein, die als Router-ID des eBGP-Routers im Netzwerk der Zentrale oder des Rechenzentrums zugewiesen wurde.
8. Geben Sie das **Peer-AS** ein, also das autonome System (AS) für Ihr Netzwerk.

   Verwenden Sie eine RFC 6996-konforme private BGP-AS-Nummer.
9. Geben Sie die **lokale IP-Adresse** ein, die Prisma Access als lokale IP-Adresse für BGP verwendet.

   Eine lokale Adresse ist nur erforderlich, wenn Ihr Gerät in der Zentrale oder im Rechenzentrum diese Adresse für ein erfolgreiches BGP-Peering benötigt. Stellen Sie sicher, dass die angegebene Adresse nicht mit IP-Adressen im Infrastruktursubnetz oder in den Subnetzen des Remote-Netzwerks in Konflikt steht oder sich mit diesen überschneidet.
10. Geben Sie einen Wert für **Geheimer Schlüssel** ein, um die BGP-Peer-Kommunikation zu authentifizieren.

 ©2025 Palo Alto Networks, Inc.

11. Wählen Sie **Geheimen Schlüssel bestätigen** aus.




*Ausgehend von Prisma Access 5.2 können Sie maximal 25.000 Remote-Netzwerke und 50.000 IKE-Gateways pro Mandant in eine Prisma Access-Bereitstellung integrieren. Um dieser Verbesserung Rechnung zu tragen, wurden die folgenden Änderungen an der Weboberfläche von Strata Cloud Manager vorgenommen:*

- Die Paginierung wurde ergänzt, damit Sie auswählen können, wie viele Zeilen auf einer bestimmten Seite angezeigt werden sollen.

- Die Filterung ist für Remote-Netzwerke aktiviert.

  Nachdem Sie die Filterung angewendet haben, können Sie die resultierende Ausgabe nach Namen sortieren.

 ©2025 Palo Alto Networks, Inc.

- Das Feld **Gruppieren nach** wurde hinzugefügt. Wenn Sie eine Gruppe nach **Compute-Standort** auswählen, werden alle Gruppen zusammengefasst (ausgeblendet) angezeigt und die ausgewählte Seitengröße wird auf die Gruppen angewendet. Wenn Sie einen Compute-Standort zum Erweitern auswählen, werden die Zeilen basierend auf der ausgewählten Seitengröße angezeigt.

- Wenn Remote-Netzwerke in einer Dropdown-Liste angezeigt werden, zeigt die Weboberfläche die ersten 500 Elemente an. Sie finden das gewünschte Remote-Netzwerk in der Liste, indem Sie den Namen in das Textfeld eingeben.

  Zusätzlich wird die Gesamtzahl der Remote-Netzwerke angezeigt.

- Auf die folgenden zusätzlichen Seiten wurde die Paginierung angewendet:
  - IPSec-Tunnel:
  - QoS:
  - QoS-Statistiken:
  - **Fehlerbehebung – Remote-Netzwerke** unter **Externe dynamischen Listen**:

## Remote-Netzwerk einbinden (Panorama)

Gehen Sie wie folgt vor, um eine Remote-Netzwerkbereitstellung für Prisma Access zu konfigurieren, mit der Bandbreite nach Compute-Standort zugewiesen werden kann:

*Wenn Sie eine große Anzahl von Remote-Netzwerken (bis zu 1.000) einbinden müssen, können Sie dazu nach dem folgenden Verfahren das Onboarding eines Remote-Netzwerks durchführen. Anschließend können Sie* die Remote-Netzwerk-Konfiguration in eine CSV-Datei exportieren*, die anderen einzubindenden Remote-Netzwerke zur CSV-Datei hinzufügen und die CSV-Datei dann importieren, um die Konfiguration in Prisma Access zu speichern.*

**STEP 1 |** Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Remote-Netzwerke** aus und bearbeiten Sie die Einstellungen, indem Sie auf das Zahnradsymbol im Bereich **Einstellungen** klicken.

1. Im Abschnitt „Vorlagen“ können Sie alle Vorlagen **hinzufügen**, die Konfigurationen enthalten, die Sie an Prisma Access für Netzwerke per Push übertragen möchten. Wenn z. B. Vorlagen vorhanden sind, die Ihre Zonenkonfigurationen oder die Einstellungen für IPSec-Tunnel, IKE-Gateways oder das Verschlüsselungsprofil enthalten, können Sie diese dem vordefinierten Vorlagenstack für Remote-Netzwerke (Remote_Network_Template_Stack) hinzufügen, um den Onboarding-Prozess zu vereinfachen.

   Sie können mehrere Vorlagen zum Stack **hinzufügen** und diese dann mithilfe der Funktionen **Nach oben verschieben** bzw. **Nach unten verschieben** entsprechend

 ©2025 Palo Alto Networks, Inc.

anordnen. Dies ist wichtig, da Panorama die Vorlagen im Stack von oben nach unten auswertet, wobei Einstellungen in Vorlagen, die sich weiter oben im Stack befinden, Vorrang vor den gleichen Einstellungen haben, die sich in Vorlagen weiter unten im Stack befinden. Beachten Sie, dass Sie die Standardvorlage nicht von der obersten Position im Stack verschieben können.



*Sie können zwar vorhandene Vorlagen aus dem Plug-in zum Stack hinzufügen, aber keine neue Vorlage aus dem Plug-in erstellen. Verwenden Sie stattdessen den Workflow zum Hinzufügen einer neuen Vorlage.*

2. Wählen Sie die **übergeordnete Gerätegruppe** für Prisma Access für Remote-Netzwerke aus. Sie können eine vorhandene Gerätegruppe auswählen oder die Option **Freigegeben** verwenden.

   Sie werden die gesamte Konfiguration per Push übertragen – dazu gehören die Sicherheitsrichtlinie, Sicherheitsprofile und andere Richtlinienobjekte (z. B. Anwendungsgruppen und -objekte sowie Adressgruppen), HIP-Objekte und -profile sowie die Authentifizierungsrichtlinie –, die Prisma Access für Netzwerke benötigt, um eine konsistente Richtlinie für Ihre Remote-Netzwerkbenutzer mithilfe der hier angegebenen Gerätegruppenhierarchie durchzusetzen.

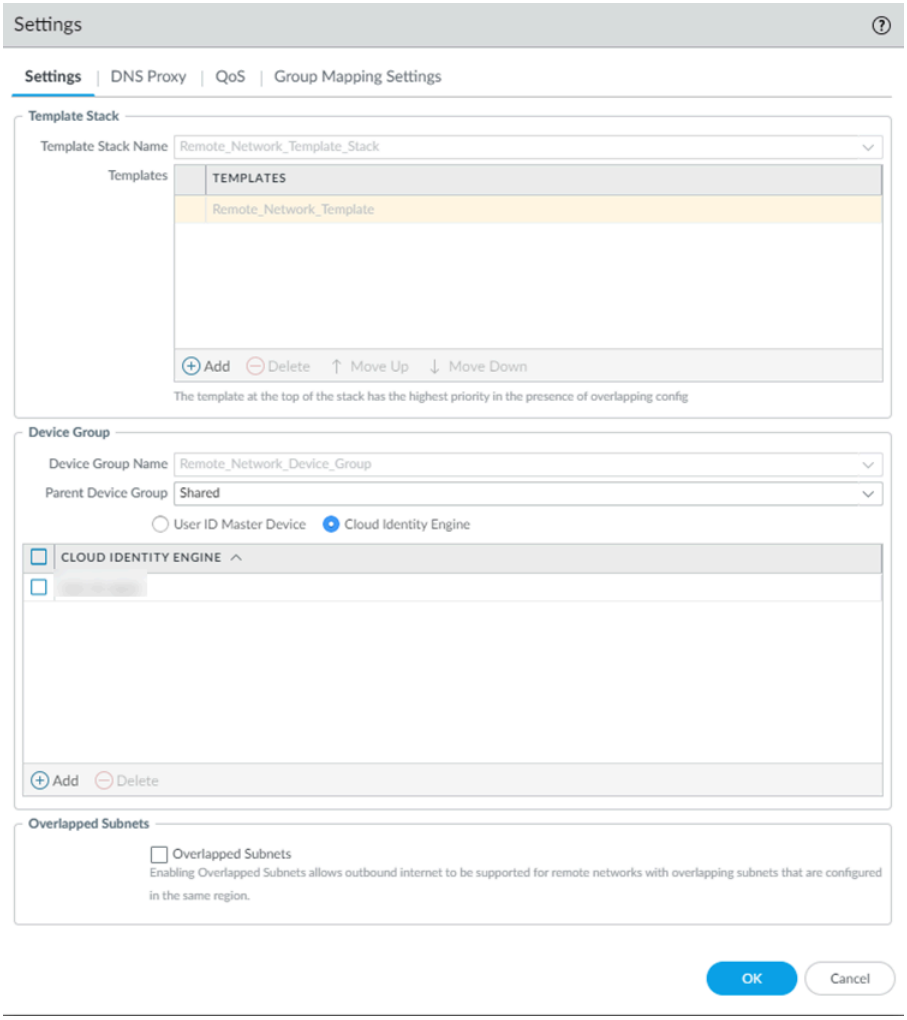
   *Sie müssen noch nicht die gesamte Richtlinie definieren, die Sie per Push in das Remote-Netzwerk übertragen. Konfigurieren Sie stattdessen die Einstellungen, um den Remote-Standort einzubinden. Sie können dann zurückgehen und die Vorlagen sowie Gerätegruppen mit den vollständigen Konfigurationen hinzufügen, um konsistente Richtlinien per Push an Ihre Remote-Netzwerke zu übertragen.*

3. (Optional) Wenn Sie eine Firewall der nächsten Generation als Mastergerät konfiguriert oder ein Cloud Identity Engine-Profil hinzugefügt haben, um Benutzer- und Gruppeninformationen in Sicherheitsrichtlinien auswählbar zu machen, wählen Sie **Benutzer-ID-Mastergerät** oder **Cloud Identity Engine** aus. Anschließend wählen Sie entweder das Mastergerät oder das Cloud Identity Engine-Profil aus, das Sie erstellt haben.

 ©2025 Palo Alto Networks, Inc.

4. Wenn Sie Remote-Netzwerke mit überlappenden Subnetzen konfigurieren möchten, aktivieren Sie das Kontrollkästchen **Überlappende Subnetze**, um den ausgehenden Internetzugang für diese Standorte zu aktivieren.

   Zwar bringt die Konfiguration von Remote-Netzwerkstandorten mit überlappenden Subnetzen einige Einschränkungen mit sich, doch dies ist in einigen Fällen akzeptabel (z. B., wenn Sie ein Gastnetzwerk an einem Einzelhandelsstandort hinzufügen möchten).




**STEP 2 |** (Optional) Konfigurieren Sie **DNS-Proxy**-Einstellungen für Ihr Remote-Netzwerk.

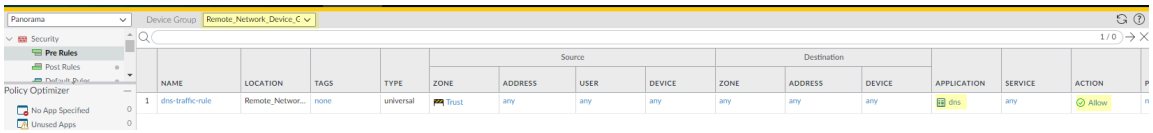
Mit Prisma Access können Sie DNS-Server angeben, um sowohl unternehmensinterne als auch externe Domänen aufzulösen. Wenn Sie keine Einstellungen angeben, leitet Prisma Access DNS-Anfragen für Remote-Netzwerke nicht weiter.

1. Wählen Sie in der Gerätegruppe **Remote_Network_Device_Group** die Optionen **Richtlinien** > **Sicherheit** aus, um eine Sicherheitsrichtlinienregel **hinzuzufügen**. Geben Sie

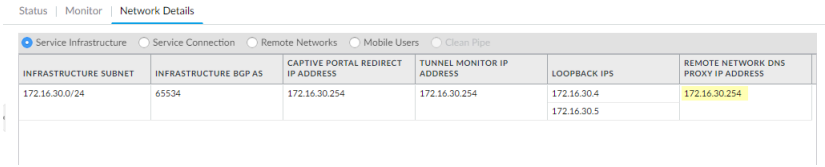
 ©2025 Palo Alto Networks, Inc.

dabei für **Anwendung** den Wert **DNS** und für **Aktion** den Wert **Zulassen** an, um DNS-Datenverkehr zuzulassen.

Wenn keine Sicherheitsrichtlinienregel vorliegt, die DNS-Datenverkehr zulässt, ist eine DNS-Auflösung nicht möglich.




2. Wenn Sie Prisma Access für die Weiterleitung der DNS-Anforderungen aus Ihren Remote-Netzwerken konfigurieren, aktualisieren Sie die DNS-Einstellungen für alle Endpunkte in diesem Netzwerk, sodass die Prisma Access **IP-Adresse des DNS-Proxy im Remote-Netzwerk** als primärer DNS-Server und Ihr DNS-Server als sekundärer DNS-Server verwendet wird. Sie können diese DNS-Proxy-IP über **Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Dienstinfrastruktur** abrufen.




3. Sie können mindestens eine **DNS-Proxy**-Einstellung **hinzufügen** oder folgende Werte eingeben:

   - Wählen Sie aus dem Dropdown-Menü am oberen Rand des Fensters eine **Region** aus.

     Wählen Sie **Weltweit** aus, um die DNS-Einstellungen global anzuwenden, einen bestimmten Schauplatz oder Einstellungen pro Standortgruppe auszuwählen (eine Standortgruppe, die kleiner als der Schauplatz ist). Wenn Sie mehrere Einstellungen hinzufügen, werden zuerst die Standortgruppeneinstellungen verwendet, dann die Schauplatzeinstellungen und schließlich die weltweiten Einstellungen. Prisma Access wertet die Regeln in der Liste von oben nach unten aus.

   - Sie können eine oder mehrere Regeln **hinzufügen**, um die DNS-Einstellungen für **Interne Domänen** zu konfigurieren.

     - Geben Sie einen eindeutigen **Regelnamen** ein.
     - Wenn Ihr interner DNS-Server nur die von Ihnen angegebenen Domänen auflösen soll, geben Sie die aufzulösenden Domänen in die **Domänenliste** ein. Geben Sie vor der Domäne ein Sternchen an, z. B. *.acme.com. Sie können maximal 1.024 Domäneneinträge angeben.
     - Wenn Sie über einen **benutzerdefinierten DNS-Server** verfügen, der auf Ihre internen Domänen zugreifen kann, geben Sie die IP-Adressen des primären und des sekundären DNS-Servers an (**Primärer DNS** und **Sekundärer DNS**) oder wählen Sie **Cloud-Standard verwenden** aus, um den Standard-DNS-Server von Prisma Access zu verwenden.

 ©2025 Palo Alto Networks, Inc.

- Geben Sie die DNS-Einstellungen für **Öffentliche Domänen** an.
  - **Cloud-Standard verwenden** – Verwenden Sie den Standard-DNS-Server von Prisma Access.
  - **Wie interne Domänen** – Verwenden Sie denselben Server, den Sie zum Auflösen interner Domänen verwenden. Wenn Sie diese Option aktivieren, entspricht der DNS-Server, der zur Auflösung öffentlicher Domänen verwendet wird, dem Server, der für die erste Regel im Abschnitt **Interne Domänen** konfiguriert ist.
  - **Benutzerdefinierter DNS-Server** – Wenn Sie über einen DNS-Server verfügen, der auf Ihre öffentlichen (externen) Domänen zugreifen kann, geben Sie in dieses Feld die Adresse des primären DNS-Servers ein.

  (Optional) Sie können ein **DNS-Suffix hinzufügen**, um das Suffix anzugeben, das der Client lokal verwenden soll, wenn ein nicht qualifizierter Hostname eingegeben wird, den er nicht auflösen kann, z. B. acme.local. Geben Sie vor dem Domänensuffix (z. B. acme.com) kein Platzhalterzeichen (*) ein. Sie können mehrere Suffixe hinzufügen.
- Wenn Sie möchten, dass Prisma Access als Proxy für DNS-Anfragen fungiert, konfigurieren Sie Werte für die Wiederholung von UDP-Abfragen (das **Intervall** in Sek.), um die Abfrage nach einer bestimmten Anzahl von Sekunden zu wiederholen, sowie die Anzahl der durchzuführenden **Wiederholversuche**.

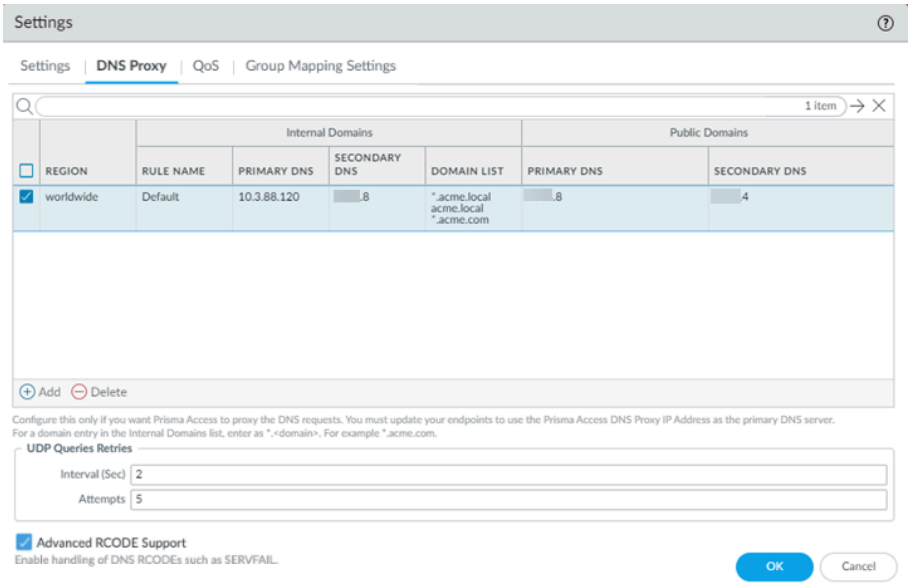
  Wenn Sie möchten, dass Prisma Access als Proxy für DNS-Anfragen fungiert, müssen Sie Ihre Endpunkte aktualisieren, um die **IP-Adresse des DNS-Proxy im Remote-Netzwerk** als primären DNS-Server zu verwenden (**Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Dienstinfrastruktur**).

4. (Optional) Wählen Sie die erweiterte RCODE-Unterstützung aus, um ein Failover des primären DNS-Servers auf den sekundären DNS-Server zuzulassen, wenn ein DNS-Rückgabecode vom Typ RCODE 2 (SERVFAIL) oder RCODE 5 (REFUSED) empfangen wird.

   Der DNS-Antwortcode SERVFAIL weist auf einen Kommunikationsfehler mit dem primären DNS-Server hin, und der DNS-Antwortcode REFUSED bedeutet, dass sich der primäre DNS-Server geweigert hat, die angeforderten Informationen bereitzustellen.

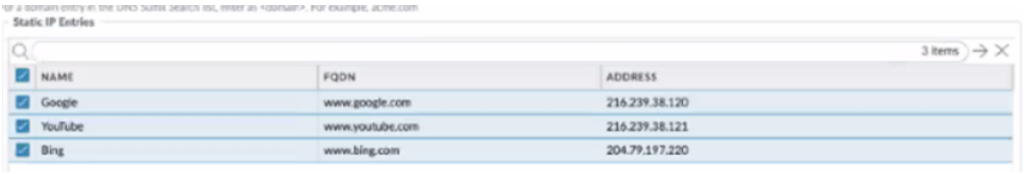
 ©2025 Palo Alto Networks, Inc.

In beiden Fällen wird für den Dienst ein Failover auf den sekundären DNS-Server durchgeführt.




5. (Optional) Verwenden Sie **Statische IP-Einträge**, um FQDNs in bestimmte IP-Adressen aufzulösen.

   Diese Funktionalität kann nützlich sein, wenn es in Ihrer Organisation Gast-Internetdienste gibt und Sie möchten, dass Ihre Gäste Suchmaschinen sicher verwenden, um zu verhindern, dass sie nach potenziell unangemessenem oder anstößigem Material suchen, das gegen die Unternehmensrichtlinie verstoßen könnte. Geben Sie dazu einen eindeutigen **Namen** für die Regel für statische Einträge, einen **FQDN** und die IP-**Adresse** ein, an die die FQDN-Anforderung gerichtet werden soll.




**STEP 3 |** (Optional) Aktivieren Sie **QoS** für Ihre Remote-Netzwerkbereitstellung und geben Sie ein **QoS-Profil**, das **garantierte Bandbreitenverhältnis** und die **Größenordnung der garantierten Bandbreite (Mbit/s)** ein. Optional können Sie die Standortoptionen für jeden Standort anpassen (**Für jeden Standort anpassen**).

Sie aktivieren QoS auf Compute-Standort-Ebene. Allerdings können Sie angeben, ob QoS für jeden Standort einzeln aktiviert oder deaktiviert werden soll, und ein standortbasiertes QoS-Profil angeben, wenn Sie Ihr Remote-Netzwerk in einem späteren Schritt hinzufügen. Bevor Sie QoS konfigurieren, sollten Sie verstehen, wie QoS für Remote-Netzwerke funktioniert, die Bandbreite nach Compute-Standort zuweisen, einschließlich der garantierten Bandbreite und der Anpassung der Bandbreite pro Standort.

 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** (Optional) Konfigurieren Sie **Einstellungen für die Gruppenzuordnung**, damit Prisma Access die Komponente „Verzeichnissynchronisierung“ der Cloud Identity Engine zum Abrufen von Benutzer- und Gruppeninformationen verwenden kann.

Sie müssen die Cloud Identity Engine zum Abrufen von Benutzer- und Gruppeninformationen aus Ihrem Active Directory (AD) konfigurieren, bevor Sie die Gruppenzuordnung in Prisma Access mithilfe der **Einstellungen für die Gruppenzuordnung** aktivieren.

**STEP 5 |** Erstellen Sie neue Zonen in einer der Vorlagen im Stack (**Netzwerk > Zonen> Hinzufügen**) oder ordnen Sie die Zonen zu, auf die in vorhandenen Vorlagen, die Sie dem Stack als vertrauenswürdig oder nicht vertrauenswürdig hinzugefügt haben, verwiesen wird. In Panorama werden Richtlinienregeln in Gerätegruppen und Zonen in Vorlagen definiert. Daher müssen Sie sicherstellen, dass Sie dem Vorlagenstack die Vorlagen hinzufügen, die auf die in Ihren Richtlinienregeln enthaltenen Zonen verweisen.

Auf einer Palo Alto Networks® Firewall der nächsten Generation wird die Sicherheitsrichtlinie zwischen Zonen durchgesetzt, die physischen oder virtuellen Schnittstellen auf der Firewall zugeordnet sind. Da in Prisma Access für Netzwerke jedoch nur zwei Zonen vorgesehen sind, vertrauenswürdig und nicht vertrauenswürdig, müssen Sie jede Zone mit an das Internet gebundenem Datenverkehr (einschließlich Ihrer sanktionierten SaaS-Anwendungen) als nicht vertrauenswürdig und alle internen Zonen als vertrauenswürdig zuordnen.

1. (Optional) Bearbeiten Sie die Einstellungen für die Zonenzuordnung.

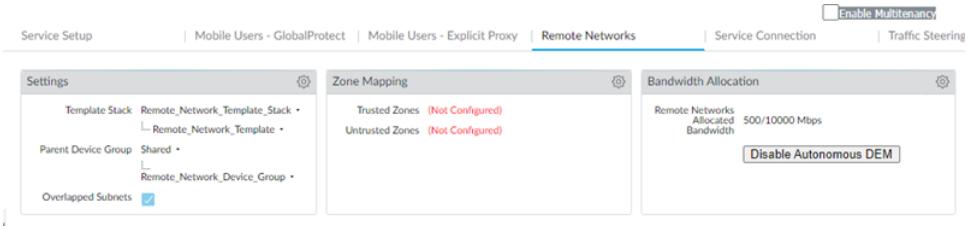
   Standardmäßig sind alle Zonen in Prisma Access für Netzwerkvorlagenstacks als nicht vertrauenswürdige Zonen klassifiziert. Wenn Sie noch keine Zonen definiert haben oder die Vorlagen im Vorlagenstack für Remote-Netzwerke (Remote_Network_Template_Stack) keine Zonenkonfigurationen enthalten, können Sie diese hier später hinzufügen, wenn Sie Richtlinien per Push an Prisma Access für Netzwerke übertragen.
2. Wählen Sie jede Zone aus, die Sie als vertrauenswürdig festlegen möchten, und klicken Sie auf **Hinzufügen**, um sie in die Liste der **vertrauenswürdigen Zonen** zu verschieben.
3. Klicken Sie auf **OK**, um die Zuordnungen zu speichern.

 ©2025 Palo Alto Networks, Inc.

**STEP 6 |** Weisen Sie den Standorten, die Sie einbinden möchten, Bandbreite zu, indem Sie auf das Zahnradsymbol im Bereich **Bandbreitenzuweisung** klicken.

Sie weisen Bandbreite auf aggregierter Ebene pro Compute-Standort zu. Weitere Einzelheiten finden Sie unter Prisma Access-Remote-Netzwerke.

*Wenn Sie Autonomous DEM als Add-on-Lizenz entfernt haben, oder wenn Sie Autonomous DEM für Remote-Netzwerke aus Ihrer Lizenz entfernen, wählen Sie **Autonomous DEM deaktivieren** aus. Wenn Sie Autonomous DEM für Remote-Netzwerke entfernen und Autonomous DEM nicht deaktivieren, wird beim Festschreiben (Commit) eine Fehlermeldung angezeigt.*




Wenn für Ihre vorhandene Remote-Netzwerkbereitstellung derzeit Remote-Netzwerke nach Standort eingebunden werden, wird ein Popup-Fenster angezeigt, in dem Sie gefragt werden, ob Sie eine Migration zum aggregierten Bandbreitenmodell durchführen möchten. Klicken Sie auf **Migrieren**, um fortzufahren, oder auf **Abbrechen**, um die Migration abzubrechen.

*Die Migration zum Modell mit aggregierter Bandbreite ist dauerhaft und nicht reversibel. Überprüfen Sie vor der Migration die Checkliste zur Migrationsvorbereitung. Damit Ihre Änderungen wirksam werden, müssen Sie **Commit und Push** auswählen.*

Die **IP-Adresse des Dienstes** (die öffentlichen IP-Adressen, die auf der Prisma Access-Seite des IPSec-Tunnels für die Remote-Netzwerkverbindung verwendet werden) sollte nicht geändert werden, wenn Sie Ihre Bereitstellung auf das aggregierte Bandbreitenmodell migrieren. Dabei ist keine Neukonfiguration Ihres IPSec-Tunnels erforderlich.

**STEP 7 |** Geben Sie die **Bandbreitenzuweisung** an, die Sie für jeden **Compute-Standort** verwenden möchten, der den **Prisma Access-Standorten** zugeordnet ist, die Sie einbinden möchten.

Um die eingegebene Größenordnung der Bandbreite zu überprüfen, aktivieren Sie das Häkchen neben der Bandbreitenangabe. Um den angezeigten Wert zu stornieren, wählen Sie **x** aus.

Geben Sie eine Mindestbandbreite von 50 Mbit/s und eine maximale Bandbreite an, die der maximal verbleibenden lizenzierten Bandbreite entspricht.

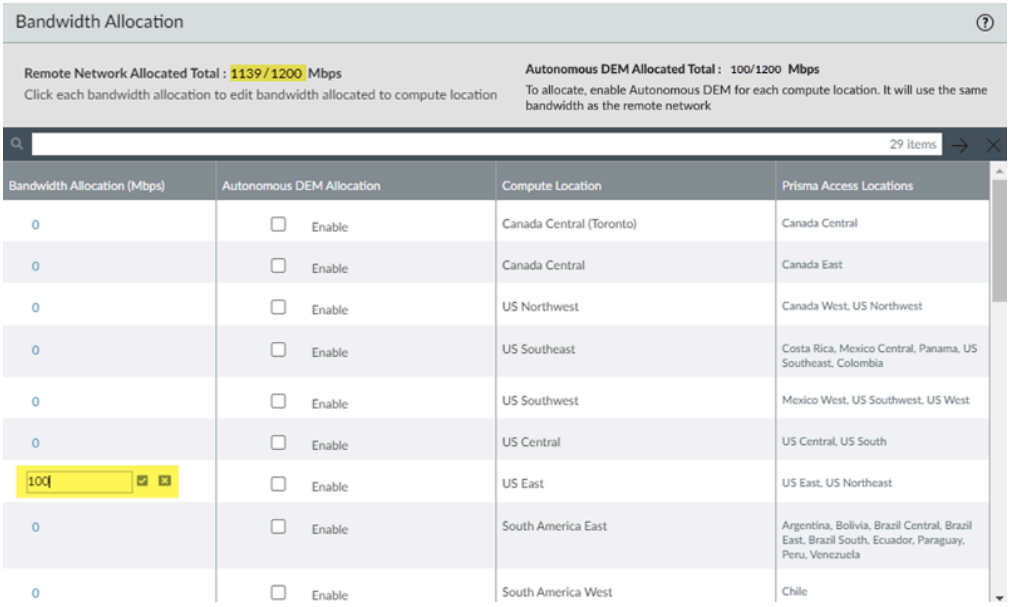
**STEP 8 |** (Optional, Bereitstellungen mit Autonomous DEM nur für Remote-Netzwerk-Lizenzen) **Aktivieren** Sie die **Autonomous DEM-Zuweisung** für den Compute-Standort, für den Sie Bandbreite zugewiesen haben.

Wenn Sie Autonomous DEM für den Compute-Standort aktivieren, ist die von der Autonomous DEM-Lizenz verwendete Bandbreite mit der Bandbreite identisch, die Sie für den Compute-Standort angeben. Der Wert für die **Gesamtzuweisung für Autonomous DEM** zeigt

 ©2025 Palo Alto Networks, Inc.

an, wie viel Bandbreite von Autonomous DEM verwendet wird und wie viel Bandbreite noch verbleibt. Weitere Informationen hierzu finden Sie im Leitfaden zu Autonomous DEM.

**STEP 9 |** Warten Sie, bis die Bandbreite im Feld **Gesamt zugewiesen** oben auf der Seite angezeigt wird und klicken Sie dann auf **OK**.




**STEP 10 |** (Optional) Wenn Sie Ihr Remote-Netzwerk so konfigurieren möchten, dass ein sicherer eingehender Zugriff auf Remote-Netzwerkstandorte bereitgestellt werden kann, dann klicken Sie auf die Registerkarte **Remote-Netzwerke mit Inbound Access** und folgen Sie dem Workflow, um den sicheren eingehenden Zugriff für ein Remote-Netzwerk zu konfigurieren.

**STEP 11 |** Fügen Sie unter **Hinzufügen** ein Remote-Netzwerk hinzu und geben Sie dann im Feld **Name** einen Namen ein.

*Sie können den Namen des Remote-Netzwerkstandorts nicht mehr ändern, nachdem Sie ihn eingegeben haben. Vergewissern Sie sich, dass Sie das Benennungsschema für Ihre Remote-Netzwerke kennen, bevor Sie mit dem Onboarding beginnen.*

**STEP 12 |** (Optional, nur für BGP-Bereitstellungen) Erstellen Sie eine Konfiguration, damit Ihre Remote-Netzwerkverbindung bis zu vier IPSec-Tunnel für den Datenverkehr verwenden kann (**ECMP-Lastausgleich**).

Statische Routen werden nicht unterstützt (BGP ist erforderlich). Wenn Sie QoS konfiguriert haben, können Sie das Zuweisungsverhältnis für ECMP-Links nicht ändern. Wenn Ihre Bereitstellung einen IPSec-Tunnel für die Remote-Netzwerkverbindung oder statische Routen verwendet, wählen Sie **Keine** für den **ECMP-Lastausgleich** aus und fahren Sie dann mit Schritt 15 fort.

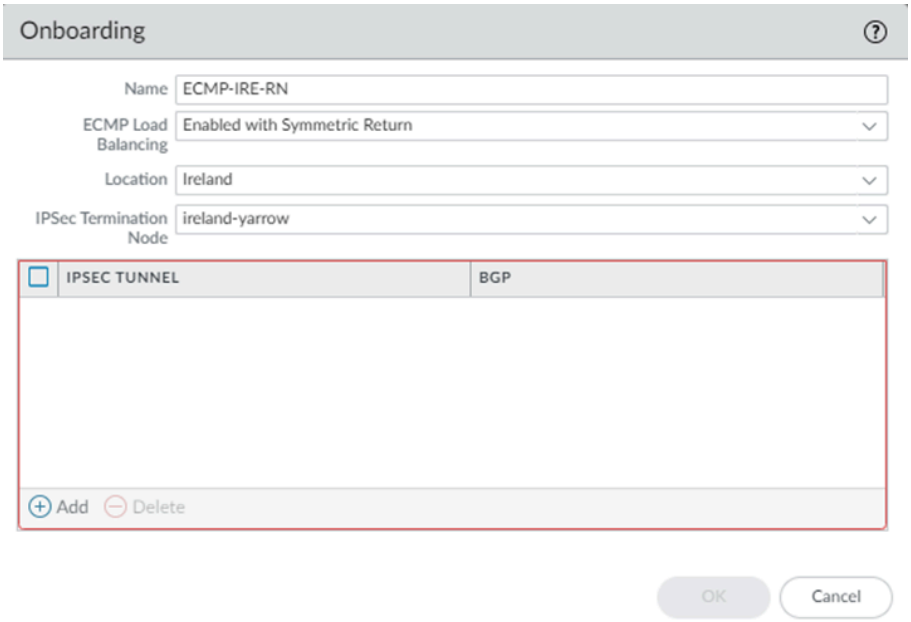
1. Wählen Sie eine der Optionen aus, um den ECMP-Lastausgleich zu aktivieren oder zu deaktivieren.
   - **Keine** – Verwenden Sie den ECMP-Lastausgleich nicht (verwenden Sie einen einzelnen Remote-Netzwerktunnel für diese Remote-Netzwerkverbindung). Dies ist

 ©2025 Palo Alto Networks, Inc.

die einzige Wahl, die Sie für statische Routen treffen können. BGP ist für den ECMP-Lastausgleich erforderlich.

- **Aktiviert mit symmetrischer Rückkehr** – Geben Sie bis zu vier IPSec-Tunnel für diese Remote-Netzwerkverbindung an und erzwingen Sie in Prisma Access die Verwendung desselben Links für den Rückkehrdatenverkehr, der auch zum Senden des Datenverkehrs benutzt wurde.

  Wählen Sie diese Option aus, wenn Sie mindestens einen Tunnel als Backup-Tunnel verwenden, der nur verwendet wird, wenn einer der primären Tunnel ausfällt. Wenn eine Verbindung ausfällt, verwendet Prisma Access einen der anderen Tunnel, um Datenverkehr symmetrisch zu senden und zu empfangen.




2. Mit **Hinzufügen** können Sie einen IPSec-Tunnel für die Remote-Netzwerkverbindung hinzufügen und die folgenden Werte angeben:

   - Mit **Aktivieren** wird BGP für den IPSec-Tunnel aktiviert.

     Diese Auswahl kann nicht konfiguriert werden. Sie müssen BGP aktivieren, um ECMP konfigurieren zu können.

   - Mit **Mobile Benutzerrouten vor dem Mitteilen zusammenfassen** kann die Anzahl der IP-Subnetzankündigungen mobiler Benutzer über BGP an CPE (Customer Premises Equipment) durch Zusammenfassung der Ankündigungen reduziert werden.

     Standardmäßig teilt Prisma Access die IP-Adresspools der mobilen Benutzer in Blöcken von /24-Subnetzen mit. Wenn Sie sie zusammenfassen, teilt Prisma Access den Pool basierend auf dem von Ihnen angegebenen Subnetz mit. Beispiel: Prisma Access kündigt einen öffentlichen mobilen IP-Pool für Benutzer mit der Angabe 10.8.0.0/20 unter Verwendung des Subnetzes /20 an, anstatt den Pool in die Subnetze 10.8.1.0/24, 10.8.2.0/24, 10.8.3.0/24 usw. zu unterteilen, bevor sie angekündigt werden. Durch die Zusammenfassung dieser Mitteilungen kann die Anzahl der in den CPE-Routingtabellen gespeicherten Routen reduziert werden. Sie können die Zusammenfassung von IP-Pools z. B. mit Cloud-VPN-Gateways (Virtual

 ©2025 Palo Alto Networks, Inc.

Private Gateways (VGWs) oder Transit Gateways (TGWs)) verwenden, die eine begrenzte Anzahl von Routen akzeptieren können.

*Wenn Sie die Routenzusammenfassung für einen Standort aktivieren, der ECMP verwendet, müssen Sie die Routenzusammenfassung für alle Links zu diesem Standort aktivieren, da andernfalls während des Commits ein Fehler ausgegeben wird.*

Prisma Access legt die Community-Zeichenfolge aggregierter Routen für mobile Benutzer auf `0xFFFE:0xFFF0` fest.

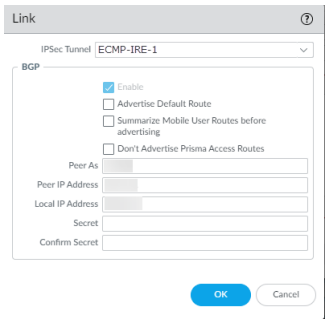
- **Standardroute ankündigen** – Prisma Access erstellt mithilfe von eBGP eine Standardroutenankündigung für das Remote-Netzwerk.

  *Vergewissern Sie sich, dass für Ihr Netzwerk keine andere Standardroute vorhanden ist, die von BGP mitgeteilt wird, da es sonst zu Routingproblemen in Ihrem Netzwerk kommen kann.*

- **Prisma Access-Routen nicht ankündigen**– Verhindert, dass der Prisma Access-BGP-Peer Routen in das Netzwerk Ihrer Organisation weiterleitet.

  Standardmäßig teilt Prisma Access alle BGP-Routinginformationen einschließlich lokaler Routen und aller Präfixe mit, die von anderen Dienstverbindungen, Remote-Netzwerken und Subnetzen mobiler Benutzer empfangen werden. Aktivieren Sie dieses Kontrollkästchen, um Prisma Access daran zu hindern, BGP-Mitteilungen zu senden. Die empfangenen BGP-Informationen werden aber weiterhin verwendet, um Informationen zu Routen anderer BGP-Nachbarn zu erhalten.

  Da Prisma Access keine BGP-Ankündigungen sendet, wenn Sie diese Option auswählen, müssen Sie statische Routen auf dem lokalen Gerät konfigurieren, um Routen zurück zu Prisma Access einzurichten.




- (Optional) Wählen Sie einen Wert für **MRAI**-Timer aus.

  Das BGP-Routing bietet einen Timer namens *Minimum Route Advertisement Interval (MRAI)*, den Sie verwenden können, um die BGP-Routing-Konvergenz in Ihrem Netzwerk anzupassen. MRAI dient zur Ratenbegrenzung von Aktualisierungen auf Zielbasis und die BGP-Router warten mindestens die konfigurierte MRAI-Zeit ab, bevor sie eine Mitteilung für dasselbe Präfix senden. Eine kleinere Zahl ermöglicht eine schnellere Konvergenzzeit, erzeugt jedoch mehr Mitteilungen in Ihrem Netzwerk. Eine höhere Zahl verringert die Anzahl der Mitteilungen, die gesendet werden können, kann aber auch die Routingkonvergenz verlangsamen. Sie bestimmen die

 ©2025 Palo Alto Networks, Inc.

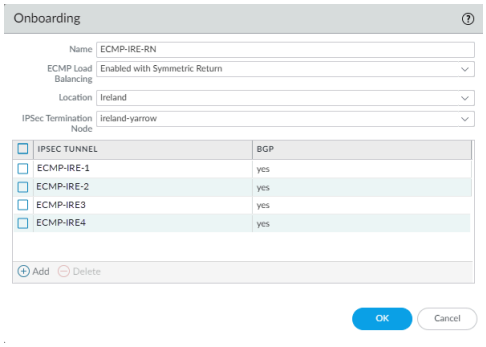
Anzahl, die Sie in Ihr Netzwerk einfügen möchten, um die beste Balance zwischen schnellerer Routingkonvergenz und weniger Ankündigungen zu erzielen.

Konfigurieren Sie einen MRAI-Bereich zwischen 1 und 600 Sekunden mit einem Standardwert von 30 Sekunden.

- **Peer-AS** – Geben Sie das autonome System (AS) an, zu dem die Firewall, der virtuelle Router oder der BGP-Router in Ihrem Remote-Netzwerk gehört.
- **Peer-IP-Adresse** – Geben Sie die IP-Adresse ein, die als Router-ID des eBGP-Routers im Remote-Netzwerk zugewiesen wurde, für das Sie diese Verbindung konfigurieren.
- **Lokale IP-Adresse** (Optional) – Geben Sie eine Adresse ein, die von Prisma Access als lokale IP-Adresse für BGP verwendet wird. Geben Sie die IP-Adresse an, die auf der Prisma Access-Seite des Tunnels verwendet werden soll.

  Die Angabe eines Werts für **Lokale Adresse** ist hilfreich, wenn das Gerät auf der anderen Seite der Verbindung (z. B. ein Amazon Web Service (AWS) Virtual Private Gateway) eine bestimmte lokale IP-Adresse benötigt, damit das BGP-Peering erfolgreich ist. Stellen Sie sicher, dass die angegebene Adresse nicht mit IP-Adressen im Infrastruktursubnetz oder in den Subnetzen des Remote-Netzwerks in Konflikt steht oder diese überlappt.
- **Geheimer Schlüssel** und **Geheimen Schlüssel bestätigen** (Optional) – Geben Sie eine Passphrase ein und bestätigen Sie diese, um die BGP-Peer-Kommunikation zu authentifizieren.

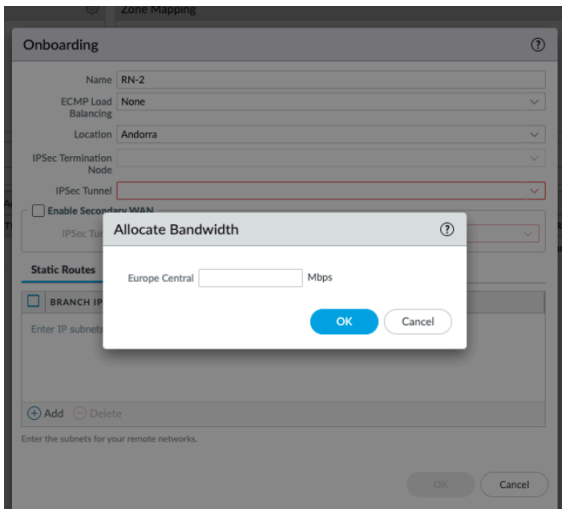
3. Wiederholen Sie den vorherigen Schritt, um bis zu vier Tunnel hinzuzufügen, die mit der Remote-Netzwerkverbindung verwendet werden sollen.




 ©2025 Palo Alto Networks, Inc.

**STEP 13 |** Wählen Sie den **Standort** aus, an dem Prisma Access die Infrastruktur bereitstellt, die zum Sichern Ihres Remote-Netzwerkstandorts erforderlich ist. Diese Region sollte sich geografisch in der Nähe Ihres Remote-Netzwerkstandorts befinden.

Wenn Sie noch keine Bandbreite für den Compute-Standort zugewiesen haben, dem der Standort zugeordnet ist, werden Sie von Prisma Access aufgefordert, die Bandbreite für diesen Compute-Standort einzugeben.




Standorte, die mit zwei Sternchen angegeben werden, sind **lokale Zonen**. Diese Standorte platzieren Rechen-, Speicher-, Datenbank- und Infrastrukturdienste in der Nähe großer Bevölkerungs- und Industriezentren; sie haben jedoch auch einige Einschränkungen. Um eine lokale Zone hinzuzufügen, wenden Sie sich an Ihren Palo Alto Networks Ansprechpartner.

**STEP 14 |** Wählen Sie den **IPSec-Terminierungsknoten** aus, den Sie für dieses Remote-Netzwerk verwenden möchten.

Prisma Access verwendet diesen Knoten, um Remote-Netzwerkstandorte mit den entsprechenden Compute-Standorten zu verknüpfen.

**STEP 15 |** (Nur statisches Routing oder Bereitstellungen mit nur einem Tunnel) Wählen Sie eine Konfiguration für einen **IPSec-Tunnel** aus oder fügen Sie eine neue Konfiguration hinzu, mit der auf die Firewall, den Router oder das SD-WAN-Gerät am Unternehmensstandort zugegriffen werden kann:

- Wählen Sie eine der vordefinierten IPSec-Vorlagen in der Remote-Netzwerk-Vorlage (Remote_Network_Template) aus. Wenn Sie eine Vorlage zum Vorlagenstack für Remote-Netzwerke (Remote_Network_Template_Stack) hinzugefügt haben (oder die vordefinierte Vorlage „Remote_Network_Template“ geändert haben), die eine IPSec-Tunnelkonfiguration enthält, dann wählen Sie in der Dropdown-Liste den Eintrag **IPSec-Tunnel** aus. Beachten Sie, dass der Tunnel, den Sie für jede Remote-Netzwerkverbindung erstellen, Prisma Access mit dem IPSec-fähigen Gerät an jedem Niederlassungsstandort verbindet.

  Beachten Sie bei der Konfiguration eines IPSec-Tunnels die folgenden Richtlinien:

  - Die Peer-Adressen in der IKE-Gateway-Konfiguration müssen für jeden Tunnel eindeutig sein. Sie können jedoch einige der anderen allgemeinen Konfigurationselemente wie z. B. Verschlüsselungsprofile wiederverwenden.

 ©2025 Palo Alto Networks, Inc.

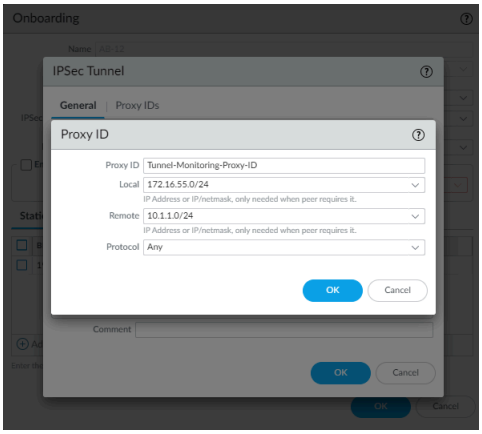
  - Der IPSec-Tunnel, den Sie in einer Vorlage auswählen, darf nur den automatischen Schlüsselaustausch und IPv4 verwenden.
  - Die Namen des IPSec-Tunnels, des IKE-Gateways und der Verschlüsselungsprofile dürfen nicht mehr als 31 Zeichen umfassen.
  - Wenn Sie mehrere Remote-Netzwerke an demselben Standort mit dynamischen IKE-Peers einbinden, müssen Sie für alle Remote-Netzwerkkonfigurationen dasselbe IKE-Verschlüsselungsprofil verwenden.
- Zum Erstellen einer neuen Konfiguration für einen IPSec-Tunnel klicken Sie auf **Neuer IPSec-Tunnel**, ordnen dem neuen Element unter **Name** einen Namen zu und konfigurieren den IKE-Gateway, das IPSec-Verschlüsselungsprofil und die Einstellungen für die Tunnelüberwachung.
  - Wenn das IPSec-fähige Gerät an Ihrem Niederlassungsstandort ein richtlinienbasiertes VPN verwendet, müssen Sie auf der Registerkarte **Proxy-IDs** durch Auswahl von **Hinzufügen** eine Proxy-ID hinzufügen, die mit den auf Ihrem lokalen IPSec-Gerät konfigurierten Einstellungen übereinstimmt. Auf diese Weise können Sie sicherstellen, dass Prisma Access einen IPSec-Tunnel für Ihr lokales Gerät einrichten kann.
- Behalten Sie die Auswahl von **Replay-Schutz aktivieren** bei, um Replay-Angriffe zu erkennen und zu beseitigen.
- Wählen Sie **ToS-Header kopieren** aus, um den Header für ToS (Type of Service) aus dem inneren IP-Header in den äußeren IP-Header der gekapselten Pakete zu kopieren, damit die ursprünglichen ToS-Informationen erhalten bleiben.
- Um die Tunnelüberwachung für die Dienstverbindung zu aktivieren, wählen Sie **Tunnelüberwachung** aus.
  - Geben Sie eine **Ziel-IP**-Adresse ein.

    Geben Sie eine IP-Adresse an Ihrem Niederlassungsstandort an, an die Prisma Access ICMP-Ping-Anfragen für die IPSec-Tunnelüberwachung senden kann. Stellen Sie sicher, dass diese Adresse für ICMP im gesamten Prisma Access-Infrastruktursubnetz erreichbar ist.
  - Wenn Sie die Tunnelüberwachung mit einem Peer-Gerät verwenden, das mehrere Proxy-IDs verwendet, geben Sie eine **Proxy-ID** an oder fügen Sie unter **Neue Proxy-ID** eine neue Proxy-ID hinzu, die den Zugriff über das Infrastruktursubnetz auf Ihren Niederlassungsstandort ermöglicht.

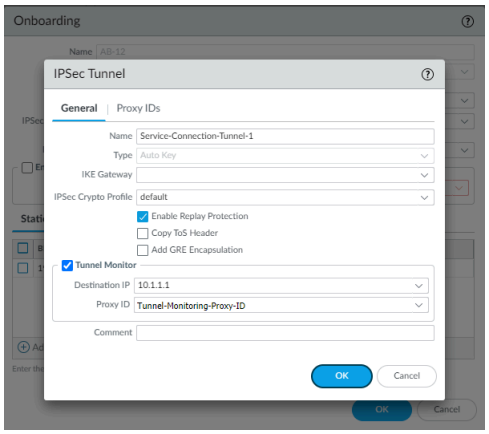
    In der folgenden Abbildung ist eine Proxy-ID mit dem Infrastruktursubnetz des Dienstes (in diesem Beispiel 172.16.55.0/24) als **lokales** IP-Subnetz und das Subnetz

 ©2025 Palo Alto Networks, Inc.

des Niederlassungsstandorts (in diesem Beispiel 10.1.1.0/24) als **Remote**-Subnetz dargestellt.




Die folgende Abbildung veranschaulicht, wie die von Ihnen erstellte Proxy-ID auf die Konfiguration der Tunnelüberwachung angewendet wird, indem sie im Feld **Proxy-ID** angegeben wird.




*Sie müssen auf Ihrem CPE eine statische Route zur IP-Adresse der Tunnelüberwachung konfigurieren, damit die Tunnelüberwachung fehlerfrei ausgeführt werden kann. Zum Suchen der Ziel-IP-Adresse, die für die Tunnelüberwachung von Ihrem Niederlassungsstandort zu Prisma Access benötigt wird, wählen Sie **Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** aus, klicken Sie auf das Optionsfeld **Dienstinfrastruktur** und suchen Sie anschließend die **IP-Adresse für Tunnelüberwachung**.*

 ©2025 Palo Alto Networks, Inc.

**STEP 16 |** Wenn Sie an diesem Standort über eine sekundäre WAN-Verbindung verfügen, wählen Sie **Sekundäres WAN aktivieren** aus.

*Stellen Sie sicher, dass für das sekundäre WAN jedes Remote-Netzwerks ein eindeutiger IPSec-Tunnel erstellt wird. Prisma Access bietet keine Unterstützung für die Wiederverwendung desselben IPSec-Tunnels für sekundäre WANs in mehreren Remote-Netzwerken.*

Die Konfiguration eines sekundären WAN wird in den folgenden Bereitstellungen nicht unterstützt:

- Wenn Ihr sekundäres WAN im Aktiv-Aktiv-Modus mit dem primären IPSec-Tunnel eingerichtet ist.
- Wenn Ihre Kundenendgeräte (Customer Premises Equipment, CPE) in einer Equal Cost Multipath(ECMP)-Konfiguration mit dem primären und sekundären IPSec-Tunnel eingerichtet sind.

Wenn Sie statische Routen verwenden, beträgt die Tunnel-Failover-Zeit abhängig von Ihrem WAN-Anbieter weniger als 15 Sekunden ab dem Zeitpunkt der Erkennung.

Wenn Sie das BGP-Routing konfigurieren und die Tunnelüberwachung aktiviert haben, entspricht die kürzeste Standardhaltezeit, um Festzustellen, dass ein Sicherheitsparameterindex (SPI) ausfällt, der Tunnelüberwachung. Hierbei werden alle Routen zu einem Peer entfernt, wenn ein Tunnelfehler festgestellt wird, der länger als 15 aufeinanderfolgende Sekunden anhält. Auf diese Weise ermittelt die Tunnelüberwachung das Verhalten der BGP-Routen. Wenn Sie die Tunnelüberwachung nicht konfigurieren, bestimmt der Haltetimer, wie lange der Tunnel inaktiv sein darf, bevor die Route entfernt wird. Prisma Access verwendet den Standardwert für die BGP-Haltezeit (90 Sekunden), der in RFC 4271 definiert ist. Hierbei handelt es sich um die maximal zulässige Wartezeit, nach deren Ablauf Prisma Access eine Route für einen inaktiven SPI entfernt. Wenn für das Peer-BGP-Gerät eine kürzere konfigurierte Haltezeit festgelegt wurde, verwendet der BGP-Haltetimer den niedrigeren Wert.

Nach der erfolgreichen Installation des sekundären Tunnels hat die sekundäre Route so lange Vorrang, bis der primäre Tunnel wieder einsatzbereit ist. Wenn sowohl die primäre als auch die sekundäre Route aktiv ist, hat die primäre Route Vorrang.

*Wenn Sie einen anderen BGP-Peer für die sekundäre (Backup-)Verbindung verwenden, berücksichtigt Prisma Access die vom CPE angekündigten MED-Attribute (Multi-Exit Discriminator) nicht. Diese Einschränkung gilt, wenn Sie mehrere BGP-Peers für Remote-Netzwerkverbindungen oder Dienstverbindungen verwenden.*

**STEP 17 |** Aktivieren Sie das Routing zu den Subnetzen oder einzelnen IP-Adressen am Remote-Netzwerkstandort, auf den die Benutzer Zugriff benötigen.

Prisma Access verwendet diese Informationen, um Anforderungen an den richtigen Standort weiterzuleiten. Die Netzwerke an den einzelnen Standorten dürfen sich nicht gegenseitig und auch nicht die IP-Adresspools überlappen, die Sie für die Dienstinfrastruktur oder für Prisma

 ©2025 Palo Alto Networks, Inc.

Access für IP-Pools der Benutzer bestimmt haben. Sie können **Statische Routen**, **BGP** oder eine Kombination dieser beiden Komponenten konfigurieren.

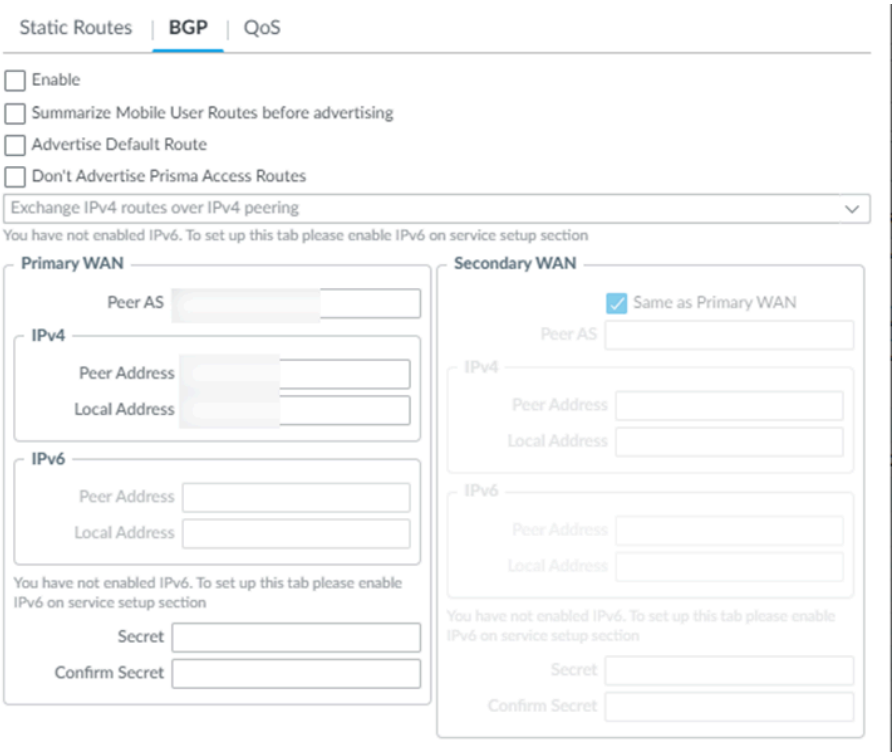
- So konfigurieren Sie **Statische Routen**:

  1. Klicken Sie auf der Registerkarte **Statische Routen** auf **Hinzufügen** und geben Sie dann die Subnetzadresse (z. B. 172.168.10.0/24) oder die individuelle IP-Adresse einer Ressource ein, beispielsweise die IP-Adresse eines DNS-Servers (z. B. 10.32.5.1/32), auf die Ihre Remote-Benutzer Zugriff benötigen.
  2. Wiederholen Sie diesen Vorgang für alle Subnetze oder IP-Adressen, auf die Prisma Access an diesem Standort Zugriff benötigt.




 ©2025 Palo Alto Networks, Inc.

- So konfigurieren Sie **BGP**:
  1. Wählen Sie die Registerkarte **BGP** aus.
  2. (Optional) Wählen Sie die Optionen für den **ECMP-Lastausgleich** aus. Siehe hierzu den Schritt 12.
  3. Wenn Sie **Keine** für den **ECMP-Lastausgleich** auswählen, dann geben Sie die BGP-Optionen ein.




  4. Um BGP für die Remote-Netzwerkverbindung zu aktivieren, wählen Sie **Aktivieren** aus.

     Wenn Sie BGP aktivieren, legt Prisma Access den TTL-Wert (Time to Live) für externes BGP (eBGP) auf 8 fest, um zusätzliche Hops zu berücksichtigen, die zwischen der Prisma Access-Infrastruktur und Ihrem Customer Premises Equipment (CPE) liegen können, das die eBGP-Verbindung abschließt.
  5. Um die Anzahl der IP-Subnetzankündigungen mobiler Benutzer über BGP zu Ihrem Customer Premises Equipment (CPE) durch Zusammenfassung zu reduzieren, wählen Sie **Mobile Benutzerrouten vor dem Mitteilen zusammenfassen** aus.

     Standardmäßig teilt Prisma Access die IP-Adresspools der mobilen Benutzer in Blöcken von /24-Subnetzen mit. Wenn Sie sie zusammenfassen, teilt Prisma Access den Pool basierend auf dem von Ihnen angegebenen Subnetz mit. Beispiel: Prisma Access kündigt einen öffentlichen mobilen IP-Pool für Benutzer mit der Angabe 10.8.0.0/20 unter Verwendung des Subnetzes /20 an, anstatt den Pool in die Subnetze 10.8.1.0/24, 10.8.2.0/24, 10.8.3.0/24 usw. zu unterteilen, bevor sie angekündigt werden. Durch die Zusammenfassung dieser Mitteilungen kann die Anzahl der in den CPE-Routingtabellen gespeicherten Routen reduziert werden. Sie können die Zusammenfassung von IP-Pools

 ©2025 Palo Alto Networks, Inc.

z. B. mit Cloud-VPN-Gateways (Virtual Private Gateways (VGWs) oder Transit Gateways (TGWs)) verwenden, die eine begrenzte Anzahl von Routen akzeptieren können.

Prisma Access legt die Community-Zeichenfolge aggregierter Routen für mobile Benutzer auf `0xFFFE:0xFFF0` fest.

6. Um zuzulassen, dass Prisma Access eine Standardroute für das Remote-Netzwerk mithilfe von eBGP ankündigt, wählen Sie **Standardroute mitteilen** aus.

   Wenn Sie **Standardroute mitteilen** auswählen, sollten Sie sicherstellen, dass in Ihrem Netzwerk keine andere Standardroute vorhanden ist, die von BGP angekündigt wird, da es sonst zu Routingproblemen in Ihrem Netzwerk kommen kann.

   *Sie müssen Ihre Standardrouten veröffentlichen, bevor Sie diese Auswahl treffen, um sie mitzuteilen. Darüber hinaus sollten Sie überprüfen, ob Ihr Netzwerk nicht über eine andere Standardroute verfügt, die von BGP angekündigt wird. Andernfalls kann es zu Routingproblemen in Ihrem Netzwerk kommen.*

7. Um zu verhindern, dass der BGP-Peer in der Prisma Access-Firewall Routen an das Netzwerk Ihrer Organisation weiterleitet, wählen Sie **Prisma Access-Routen nicht ankündigen** aus.

   Standardmäßig teilt Prisma Access alle BGP-Routinginformationen einschließlich lokaler Routen und aller Präfixe mit, die von anderen Dienstverbindungen, Remote-Netzwerken und Subnetzen mobiler Benutzer empfangen werden. Aktivieren Sie dieses Kontrollkästchen, um Prisma Access daran zu hindern, BGP-Mitteilungen zu senden. Die empfangenen BGP-Informationen werden aber weiterhin verwendet, um Informationen zu Routen anderer BGP-Nachbarn zu erhalten.

   Da Prisma Access keine BGP-Ankündigungen sendet, wenn Sie diese Option auswählen, müssen Sie statische Routen auf dem lokalen Gerät konfigurieren, um Routen zurück zu Prisma Access einzurichten.

8. Geben Sie in das Feld **Peer-AS** einen Wert ein, der das autonome System (AS) festlegt, zu dem die Firewall, der virtuelle Router oder der BGP-Router Ihres Remote-Netzwerks gehört.

9. Geben Sie die IP-Adresse ein, die als Router-ID des eBGP-Routers in dem Remote-Netzwerk zugewiesen wurde, für das Sie diese Verbindung als **Peer-Adresse** konfigurieren.

10. (Optional) Geben Sie eine Adresse ein, die von Prisma Access als lokale IP-Adresse für BGP verwendet wird.

    Die Angabe eines Werts für **Lokale Adresse** ist hilfreich, wenn das Gerät auf der anderen Seite der Verbindung (z. B. ein Amazon Web Service (AWS) Virtual Private Gateway) eine bestimmte lokale IP-Adresse benötigt, damit das BGP-Peering erfolgreich ist. Stellen Sie

 ©2025 Palo Alto Networks, Inc.

sicher, dass die angegebene Adresse nicht mit IP-Adressen im Infrastruktursubnetz oder in den Subnetzen des Remote-Netzwerks in Konflikt steht oder diese überlappt.

*Im Feld **Lokale Adresse** müssen Sie eine statische Route auf Ihrem CPE (Customer Premises Equipment) zum BGP konfigurieren.*

11. (Optional) Geben Sie eine Passphrase ein und bestätigen Sie diese, um die BGP-Peer-Kommunikation zu authentifizieren.
12. (Optional) Wenn Sie ein **Sekundäres WAN** konfiguriert haben und die **Peer-Adresse** oder den Wert für **Lokale Adresse** für den sekundären (Backup-)BGP-Peer ändern müssen, dann nehmen Sie die Auswahl von **Identisch mit primärem WAN** zurück und geben Sie einen eindeutigen Peer und optional eine lokale IP-Adresse für das sekundäre WAN ein.

    Wenn Sie die IPv6-Vernetzung in Ihrer Remote-Netzwerkbereitstellung verwenden, können Sie **IPv6**-Adressen sowie **IPv4**-Adressen konfigurieren. Des Weiteren müssen Sie die IPv6-Vernetzung weltweit in Ihrer Prisma Access-Infrastruktur aktivieren, bevor Sie die IPv6-Adressierung verwenden können.

    In einigen Bereitstellungen (z. B. bei der Verwendung von BGP für das Peering mit einem AWS-VPN-Gateway) kann der BGP-Peer für das primäre und das sekundäre WAN unterschiedlich sein. In diesen Szenarien können Sie einen anderen BGP-Peer für das sekundäre WAN festlegen.

    *Für BGP-Bereitstellungen mit sekundären WANs legt Prisma Access sowohl den primären als auch den sekundären Tunnel im Status **AKTIV** fest, befolgt jedoch das normale BGP-Aktiv-Backup-Verhalten für den Netzwerkverkehr. Prisma Access setzt den primären Tunnel auf aktiv und sendet und empfängt Datenverkehr nur über diesen Tunnel. Wenn der primäre Tunnel ausfällt, erkennt Prisma Access den Fehler mithilfe von BGP-Regeln und legt den sekundären Tunnel als aktiv fest, um ausschließlich diesen Tunnel zum Senden und Empfangen von Datenverkehr zu nutzen.*

**STEP 18 |** (Optional) Aktivieren Sie **QoS** für den Standort und geben Sie ein **QoS-Profil** an.

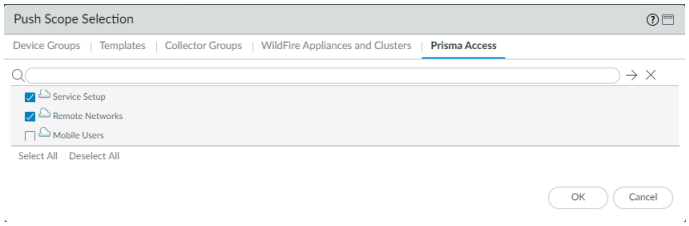
Sie legen QoS-Optionen und allgemeine Einstellungen separat für alle Compute-Standorte in den **Einstellungen** fest; allerdings können Sie QoS aktivieren oder deaktivieren oder das QoS-Profil für jeden Standort einzeln ändern.

**STEP 19 |** Schreiben Sie die Konfigurationsänderungen mit einer Commit-Aktion in Panorama fest und übertragen Sie die Konfiguration mit einer Push-Aktion an Prisma Access, um sie für Netzwerke bereitzustellen.

1. Klicken Sie auf **Commit** > **Commit in Panorama**.
2. Klicken Sie auf **Commit** > **Commit und Push**. Klicken Sie auf **Auswahl bearbeiten** > **Prisma Access**und wählen Sie sowohl Prisma Access für Netzwerke als auch Prisma

 ©2025 Palo Alto Networks, Inc.

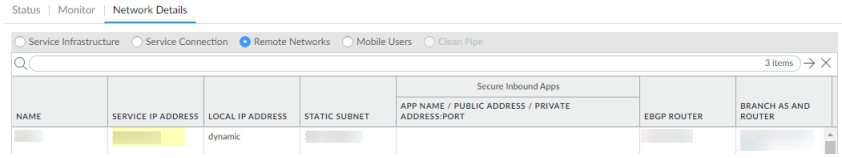
Access für die Diensteinrichtung aus, um die Konfiguration mit einer Push-Aktion an den Dienst zu übertragen.




3. Klicken Sie auf **OK** und **Push**.

**STEP 20 |** Konfigurieren Sie das IPSec-fähige Gerät am Remote-Netzwerkstandort, um eine IPSec-Verbindung mit Prisma Access für Netzwerke einzurichten.

1. Suchen Sie die **IP-Adresse des Dienstes** für diese Remote-Netzwerkverbindung, indem Sie **Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** auswählen. Klicken Sie dann auf das Optionsfeld **Remote-Netzwerke** und zeigen Sie das Feld **IP-Adresse des Dienstes** an. Prisma Access für die Netzwerkinfrastruktur hat diese IP-Adresse für die Prisma Access-Remote-Netzwerkverbindung zugewiesen und Sie müssen diese als Peer-IP-Adresse konfigurieren, um den IPSec-Tunnel zwischen dem Remote-Netzwerkstandort und dem Prisma Access für Netzwerke einzurichten.




2. Aktivieren Sie die Option **Lokale IP-Adresse** für das Gerät am Remote-Netzwerkstandort auf der Seite **Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Remote-Netzwerke**. Wenn Sie die NAT am Remote-Netzwerkstandort ausführen, wird im Feld **Lokale IP-Adresse** die IP-Adresse des Geräts nach der NAT angezeigt.

**STEP 21 |** Um den Datenverkehr am Remote-Netzwerkstandort zu sichern, müssen Sie Sicherheitsrichtlinienregeln erstellen.

1. Wählen Sie **Policies (Richtlinien)** aus.
2. Wählen Sie die **Gerätegruppe** aus, in der Richtlinienregeln hinzugefügt werden sollen. Sie können Remote_Network_Device_Group oder die übergeordnete Gerätegruppe auswählen, die Sie zum Definieren von Richtlinien ausgewählt haben, mit denen der Remote-Netzwerksstandort gesichert werden soll.
3. Erstellen Sie Sicherheitsrichtlinienregeln. Vergewissern Sie sich, dass keine Sicherheitsrichtlinienregeln definiert werden, mit denen Datenverkehr von einer Zone zu einer beliebigen anderen Zone zugelassen wird. Verwenden Sie in den Sicherheitsrichtlinienregeln die Zonen, die Sie in Ihrer Vorlage definiert haben.

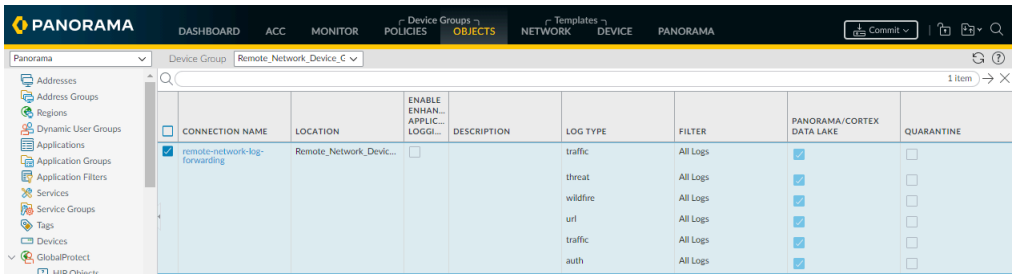
   Wenn einem Benutzer in Ihrem Netzwerk der Zugriff auf eine Website verweigert wird, melden Sie die Probleme beim Zugriff auf die Website, bevor Sie ein Ticket bei Palo Alto Networks eröffnen.


©2025 Palo Alto Networks, Inc.

**STEP 22 |** Aktivieren Sie die Protokollierung beim Strata Logging Service. Sie müssen ein Protokollweiterleitungsprofil erstellen und jeder Richtlinienregel hinzufügen, für die Sie Protokolle weiterleiten möchten.

1. Wählen Sie **Objekte > Protokollweiterleitung** aus.
2. Wählen Sie die **Gerätegruppe** aus, in der Sie die Richtlinienregeln hinzugefügt haben, z. B. Remote_Network_Device_Group.
3. **Hinzufügen** eines Protokollweiterleitungsprofils. Wählen Sie in der Übereinstimmungsliste des Protokollweiterleitungsprofils **Hinzufügen** und dann im Feld **Protokolltyp** jeden Protokolltyp aus, den Sie weiterleiten möchten.
4. Wählen Sie als Weiterleitungsmethode **Panorama/Strata-Protokollierungsdienst** aus, um für Prisma Access die Weiterleitung der Protokolle an Strata Logging Service zu aktivieren. Nun können Sie in Panorama die Protokolle überwachen und Berichte erstellen. Strata Logging Service bietet eine nahtlose Integration zum Speichern von Protokollen, ohne dass diese erneut an Panorama in der Unternehmenszentrale zurückgeleitet werden müssen. Panorama kann Abfragen im Strata Logging Service nach Bedarf durchführen.

   Im folgenden Beispiel wird die Weiterleitung von Datenverkehr, der Threat Prevention, WildFire-Übermittlung, URL-Filterung, Datenfilterung und Authentifizierungsprotokollen an Strata Logging Service aktiviert.




5. Wählen Sie **Richtlinien > Sicherheit** aus und bearbeiten Sie die Richtlinienregel. Wählen Sie unter **Aktionen** das von Ihnen erstellte Protokollweiterleitungsprofil aus.

**STEP 23 |** Übertragen Sie alle Änderungen an Panorama und übertragen Sie die Konfigurationsänderungen per Push an Prisma Access.

1. Klicken Sie auf **Commit** > **Commit und Push**.
2. Wählen Sie **Auswahl bearbeiten** aus und vergewissern Sie sich, dass auf der Registerkarte **Prisma Access** die Option **Prisma Access für Netzwerke** im Feld **Übertragungsumfang** ausgewählt wurde. Klicken Sie anschließend auf **OK**.
3. Führen Sie für Ihre Änderungen die Aktion **Commit und Push** aus.

**STEP 24 |** Überprüfen Sie den Status des Remote-Netzwerks.

Weitere Informationen finden Sie im Abschnitt Status der Remote-Netzwerkverbindung prüfen.

 ©2025 Palo Alto Networks, Inc.

# Verbinden eines Remote-Netzwerkstandorts mit Prisma Access

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access-Lizenz |

Richten Sie IPSec-VPN-Tunnel ein, um Ihre Remote-Netzwerkstandorte mit Prisma Access zu verbinden. Sie müssen einen IPSec-Tunnel von Ihrem Zweig-IPSec-Gerät zu Prisma Access erstellen.

Der erste Tunnel, den Sie erstellen, ist der primäre Tunnel für den Remote-Netzwerkstandort. Anschließend können Sie diesen Workflow wiederholen, um optional einen sekundären Tunnel einzurichten. Wenn beide Tunnel aktiv sind, hat der primäre Tunnel Vorrang vor dem sekundären Tunnel. Fällt der primäre Tunnel für einen Remote-Netzwerkstandort aus, greift das Remote-Netzwerk auf den sekundären Tunnel zurück, bis der primäre Tunnel wieder verfügbar ist.

Abhängig vom IPSec-Gerät, das Sie zum Einrichten des Tunnels verwenden, bietet Prisma Access integrierte, empfohlene IKE- und IPSec-Sicherheitseinstellungen. Sie können die empfohlenen Einstellungen für den schnellen Einstieg verwenden oder sie nach Bedarf an Ihre Umgebung anpassen.

- Hinzufügen primärer und sekundärer IPSec-VPN-Tunnel
- Weitere IKE Optionen
- Weitere IPSec-Optionen

## Hinzufügen primärer und sekundärer IPSec-VPN-Tunnel

**STEP 1 |** Starten Sie Prisma Access.

**STEP 2 |** Wählen Sie **Workflows** > **Einrichtung Prisma Access** > **Remote-Netzwerke** > **Remote-Netzwerke hinzufügen** und **Einrichten** aus, um den primären Tunnel einzurichten. Wenn Sie bereits einen primären Tunnel eingerichtet haben, können Sie hier fortfahren, um auch einen sekundären Tunnel hinzuzufügen.

1. Geben Sie dem Tunnel einen beschreibenden **Namen**.
2. Wählen Sie den **Zweiggerätetyp** für das IPSec-Gerät am Remote-Netzwerkstandort aus, den Sie zum Einrichten des Tunnels mit Prisma Access verwenden.
3. Wählen Sie für die **IP-Adresse des Zweiggeräts** entweder eine **statische** IP-Adresse aus, die den Tunnelendpunkt identifiziert, oder eine **dynamische** IP-Adresse.

   Wenn Sie die **IP-Adresse des Zweiggeräts** auf **Dynamisch** setzen, müssen Sie auch die IKE-ID für den entfernten Netzwerkstandort (**IKE Lokale Identifikation**) oder für Prisma

 ©2025 Palo Alto Networks, Inc.

Access (**IKE Peer-Identifikation**) hinzufügen, damit sich die IPSec-Peers authentifizieren können.

Da Sie die Werte für die Prisma Access-IKE-ID (**IKE Peer-Identifikation**) erst verwenden können, wenn das Remote-Netzwerk vollständig bereitgestellt ist, sollten Sie in der Regel die IKE-ID für den Remote-Netzwerkstandort (**IKE Lokale Identifikation**) anstelle der Prisma Access-IKE-ID festlegen.

**STEP 3 |** **Aktivieren Sie die Tunnelüberwachung**.

Geben Sie eine **Ziel-IP**-Adresse für die Tunnelüberwachung im Remote-Netzwerk ein, damit Prisma Access feststellen kann, ob der Tunnel aktiv ist, und geben Sie, falls Ihr Zweig-IPSec-Gerät richtlinienbasiertes VPN verwendet, die zugehörige **Proxy-ID** ein.

Die eingegebene IP-Adresse für die Tunnelüberwachung wird automatisch zur Liste der Zweigstellensubnetze hinzugefügt.

**STEP 4 |** **Speichern** Sie die Tunneleinstellungen.

Fortfahren:

- Richten Sie erweiterte Verschlüsselungseinstellungen für IKE und IPSec ein und passen Sie diese an. Siehe Weitere IKE Optionen und Weitere IPSec-Optionen.
- Routing für Ihr Remote-Netzwerk aktivieren.

## Weitere IKE Optionen

Basierend auf dem von Ihnen ausgewählten IPSec-Gerätetyp bietet Prisma Access einen empfohlenen Satz von Verschlüsselungen und eine Schlüssellebensdauer für den Schlüsselaustausch in IKE-Phase 1 zwischen dem Gerät am Remote-Netzwerkstandort und Prisma Access. Sie können die empfohlenen Einstellungen verwenden oder sie nach Bedarf an Ihre Umgebung anpassen.

- Wählen Sie eine **IKE-Protokollversion** für Ihr Zweiggerät und Prisma Access zur Verwendung für IKE-Verhandlungen aus.

  Wenn Sie **Nur-IKEv1-Modus** auswählen, kann Prisma Access für die Verhandlung nur das IKEv1-Protokoll verwenden. Wenn Sie **Nur-IKEv2-Modus** auswählen, kann Prisma Access für die Verhandlung nur das Protokoll IKEv2 verwenden. Wenn Sie **IKEv2-bevorzugt-Modus** auswählen, verwendet Prisma Access das IKEv2-Protokoll nur, wenn Ihr IPSec-Zweiggerät auch IKEv2 unterstützt. Wenn Ihr IPSec-Zweiggerät IKEv2 nicht unterstützt, greift Prisma Access auf das IKEv1-Protokoll zurück.

 ©2025 Palo Alto Networks, Inc.

- Fügen Sie ein **IKEv1-Verschlüsselungsprofil** hinzu, um die IKE-Verschlüsselungseinstellungen anzupassen, die die Verschlüsselungs- und Authentifizierungsalgorithmen definieren, die für den Schlüsselaustauschprozess in IKE-Phase 1 verwendet werden.

  Prisma Access verwendet automatisch ein standardmäßiges IKE-Verschlüsselungsprofil, das auf dem **Zweiggerätetyp** basiert, der für die Einrichtung dieses Tunnels verwendet wird.

  - **Verschlüsselung** – Geben Sie den Verschlüsselungsalgorithmus an, der in der IKE-SA-Verhandlung verwendet wird.

    Prisma Access unterstützt die folgenden Verschlüsselungsalgorithmen: 3des (168 Bit), aes-128-cbc (128 Bit), aes-192-cbc (192 Bit), aes-256-cbc (256 Bit) und des (56 Bit). Sie können auch null (keine Verschlüsselung) auswählen.
  - **Authentifizierung** – Geben Sie den Authentifizierungsalgorithmus an, der in der IKE-SA-Verhandlung verwendet wird.

    Prisma Access unterstützt die folgenden Authentifizierungsalgorithmen: sha1 (160 Bit), sha256 (256 Bit), sha384 (384 Bit), sha512 (512 Bit) und md5 (128 Bit). Sie können auch null (keine Authentifizierung) auswählen.
  - **DH-Gruppe** – Geben Sie die Diffie-Hellman-(DH-)Gruppen an, die zum Generieren symmetrischer Schlüssel für IKE in der IKE-SA-Verhandlung verwendet werden. Der Diffie-Hellman-Algorithmus verwendet den privaten Schlüssel einer Partei und den öffentlichen Schlüssel der anderen, um ein geteiltes Geheimnis zu erstellen, also einen verschlüsselten Schlüssel, den beide VPN-Tunnel-Peers gemeinsam verwenden.

    Prisma Access unterstützt folgende DH-Gruppen: Gruppe 1 (768 Bit), Gruppe 2 (1024 Bit – Standard), Gruppe 5 (1536 Bit), Gruppe 14 (2048 Bit), Gruppe 19 (256 Bit, Gruppe elliptischer Kurven) und Gruppe 20 (384 Bit, Gruppe elliptischer Kurven). Für die stärkste Sicherheit wählen Sie die Gruppe mit der höchsten Zahl aus.
  - **Lebensdauer** – Geben Sie die Einheit und die Dauer an, für die der IKE-Phase-1-Schlüssel gültig ist (der Standardwert ist 8 Stunden). Bei IKEv1 wird die Sicherheitszuordnung (Security Association, SA) nicht aktiv neu verschlüsselt, bevor die Schlüssellebensdauer abläuft. Die IKEv1 Phase 1-Neuverschlüsselung löst nur aus, wenn die SA abläuft. Bei IKEv2 muss die SA vor Ablauf der Schlüssellebensdauer neu verschlüsselt werden. Wenn die SA nach Ablauf nicht neu verschlüsselt wird, muss die SA mit dem Erstellen eines neuen Phase-1-Schlüssels beginnen.
  - **IKEv2-Authentifizierung mehrfach** – Geben Sie den Wert an, der mit der Schlüssellebensdauer multipliziert wird, um die Authentifizierungsanzahl zu bestimmen (Bereich ist 0 bis 50, der Standardwert ist 0). Die Authentifizierungsanzahl gibt an, wie oft der Sicherheitsverarbeitungsknoten die IKEv2-IKE-SA-Neuverschlüsselung durchführen kann, bevor mit der erneuten IKEv2-Authentifizierung begonnen werden muss. Mit dem Standardwert 0 wird die Funktion zur erneuten Authentifizierung deaktiviert.

- Aktivieren Sie den **IKE Passivmodus**, damit Prisma Access nur auf IKE-Verbindungen reagiert und diese nicht initiiert.

- **IKE NAT-Traversal** ist standardmäßig aktiviert.

  Dies bedeutet, dass die UDP-Kapselung in IKE- und UDP-Protokollen verwendet wird, sodass sie Netzwerkadressübersetzungsgeräte (NAT-Geräte) passieren können, die sich zwischen den IPSec-VPN-Tunnelendpunkten befinden.

 ©2025 Palo Alto Networks, Inc.

# Weitere IPSec-Optionen

Basierend auf dem von Ihnen ausgewählten IPSec-Gerätetyp bietet Prisma Access einen empfohlenen Satz von Einstellungen für IPSec-Protokoll und Schlüssellebensdauer zum Sichern von Daten innerhalb des IPSec-Tunnels zwischen Ihrem Zweiggerät und Prisma Access in IKE-Phase 2 für die Sicherheitszuordnung Security Association (SA). Sie können die empfohlenen Einstellungen verwenden oder sie nach Bedarf an Ihre Umgebung anpassen.

- Passen Sie das **IPSec-Verschlüsselungsprofil** an, um zu definieren, wie Daten innerhalb des Tunnels gesichert werden, wenn Auto Key IKE während IKE- Phase 2 automatisch Schlüssel für die IKE-SAs generiert.

  Prisma Access konfiguriert automatisch ein IPSec-Standardverschlüsselungsprofil basierend auf dem Anbieter des **Zweiggerätetyps**. Sie können entweder das Standardprofil verwenden oder ein benutzerdefiniertes Profil erstellen.

  - **IPSec-Protokoll** – Sichern Sie die Daten, die den VPN-Tunnel durchqueren. Das Encapsulating Security Payload-(**ESP**-)Protokoll verschlüsselt die Daten, authentifiziert die Quelle und überprüft die Datenintegrität. Das Authentication Header-(**AH**-)Protokoll authentifiziert die Quelle und überprüft die Datenintegrität.

    Wenn Sie **ESP** als IPSec-Protokoll verwenden, geben Sie auch den **Verschlüsselungsalgorithmus** an, der in der IPSec-SA-Verhandlung verwendet wird.

    Prisma Access unterstützt die folgenden Verschlüsselungsalgorithmen: aes-256-gcm (256 Bit), aes-256-cbc (256 Bit), aes-192-cbc (192 Bit), aes-128-gcm (128 Bit), aes-128-cbc (128 Bit), 3des (168 Bit) und des (56 Bit). Sie können auch null (keine Verschlüsselung) auswählen.

- **Authentifizierung** – Geben Sie den Authentifizierungsalgorithmus an, der in der IPSec-SA-Verhandlung verwendet wird.

  Prisma Access unterstützt die folgenden Authentifizierungsalgorithmen: sha1 (160 Bit), sha256 (256 Bit), sha384 (384 Bit), sha512 (512 Bit) und md5 (128 Bit). Wenn Sie das IPSec-Protokoll auf „ESP“ setzen, können Sie auch „Keine“ (keine Authentifizierung) auswählen.

- **DH-Gruppe** – Geben Sie die Diffie-Hellman-(DH-)Gruppen für IKE in der IPSec-Security Association (SA-)Verhandlung an.

  Prisma Access unterstützt folgende DH-Gruppen: Gruppe 1 (768 Bit), Gruppe 2 (1024 Bit – Standard), Gruppe 5 (1536 Bit), Gruppe 14 (2048 Bit), Gruppe 19 (256 Bit, Gruppe elliptischer Kurven) und Gruppe 20 (384 Bit, Gruppe elliptischer Kurven). Für die stärkste Sicherheit wählen Sie die Gruppe mit der höchsten Zahl aus. Wenn Sie den Schlüssel, den Prisma Access während der IKE-Phase 1 erstellt, nicht erneuern möchten, wählen Sie **no-pfs** (kein perfektes Weiterleitungs-Geheimnis) aus. Wenn Sie diese Option auswählen, wird Prisma Access den aktuellen Schlüssel für die IPSec-SA-Verhandlung wiederverwenden.

- **Lebensdauer** – Geben Sie die Einheit und die Dauer an, während der der verhandelte Schlüssel gültig ist (Standard ist eine Stunde).

- **Lebensgroß** – Geben Sie die Einheit und Datenmenge an, die der Schlüssel zur Verschlüsselung verwenden kann.

 ©2025 Palo Alto Networks, Inc.

# Routing für Ihr Remote-Netzwerk aktivieren

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access-Lizenz |

Damit Prisma Access den Datenverkehr zu Ihren Remote-Netzwerken weiterleiten kann, müssen Sie Routinginformationen für die Subnetzwerke bereitstellen, die Sie mit Prisma Access sichern möchten. Hierfür stehen Ihnen verschiedene Möglichkeiten zur Verfügung: Sie können entweder eine statische Route zu jedem Subnetz am Remote-Netzwerkstandort definieren oder BGP zwischen Ihren Dienstverbindungsstandorten und Prisma Access konfigurieren oder eine Kombination beider Methoden verwenden.

Wenn Sie sowohl statischen Routen konfigurieren als auch BGP aktivieren, haben die statischen Routen Vorrang. Während es praktisch sein könnte, statische Routen zu verwenden, wenn Sie nur wenige Subnetze an Ihren Remote-Netzwerkstandorten haben, ermöglicht BGP Ihnen in einer großen Bereitstellung mit vielen Remote-Netzwerken mit überlappenden Subnetzen eine einfachere Skalierung.

- **Statische Routen** – Um statische Routen zu und von Ihrem Remote-Standort zu Prisma Access zu aktivieren, identifizieren Sie die Subnetzwerke oder einzelnen IP-Adressen am Remote-Standort, die Prisma Access sichern soll (sowohl für eingehenden als auch ausgehenden Datenverkehr). Die Subnetze an jedem Standort dürfen sich nicht untereinander, mit den IP-Pools, die Sie für Prisma Access für Benutzer bestimmt haben, oder mit dem Infrastruktursubnetz überlappen.
- **BGP** – Wenn Sie BGP die dynamische Weiterleitung von Datenverkehr zu und von Ihrem Remote-Netzwerk ermöglichen möchten, müssen Sie die BGP-Informationen für den eBGP-Router in Ihrer Zweigstelle angeben:
  - **AS (Autonomes System)-Nummer des Zweigstellenrouters** – Die AS-Nummer, zu der der eBGP-Router im Remote-Netzwerk gehört. Diese wird als **Peer-AS** bezeichnet.
  - **Router-ID** – Die IP-Adresse, die als Router-ID des eBGP-Routers im Remote-Netzwerk zugewiesen wird. Diese wird als **Peer-Adresse** bezeichnet.

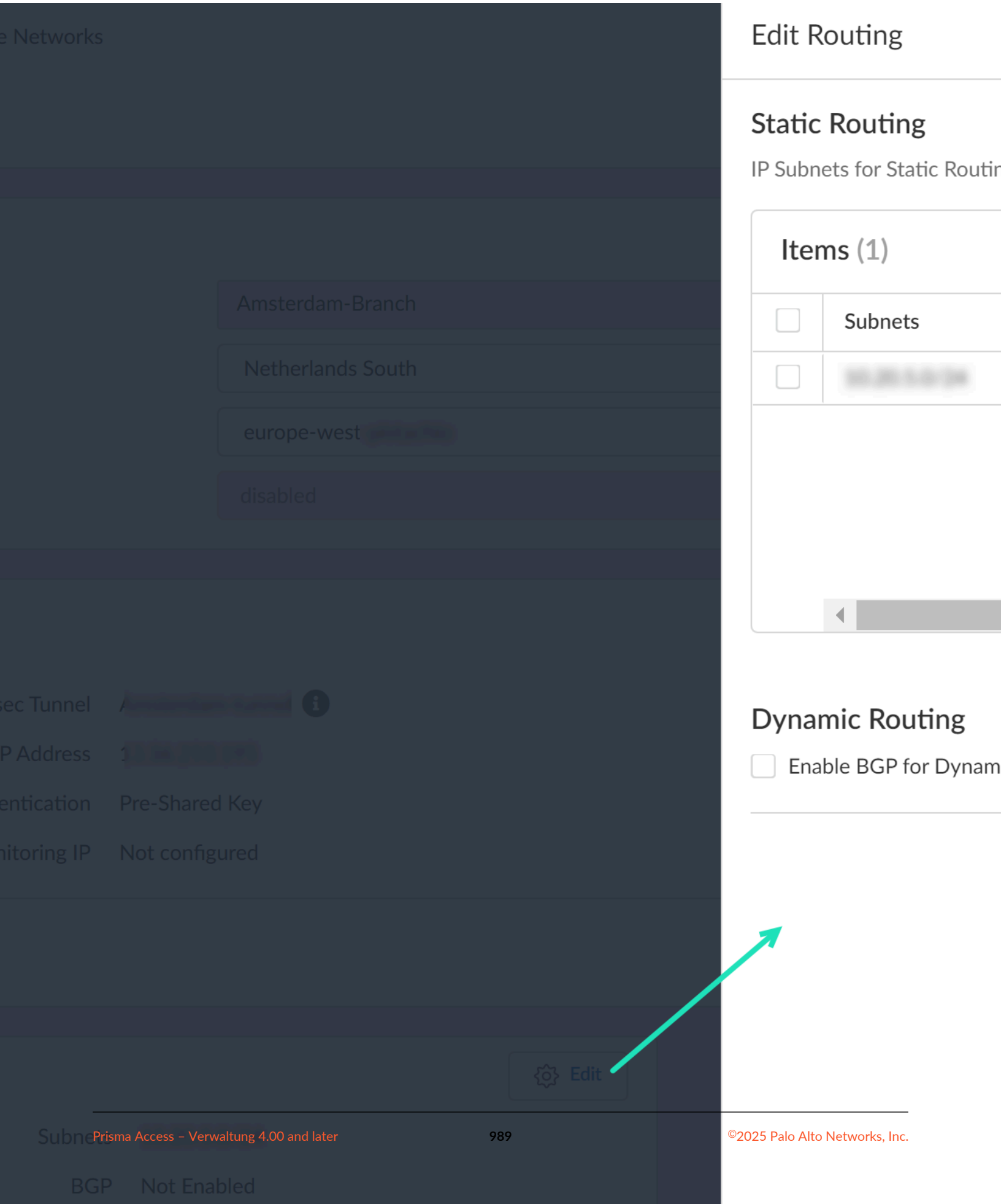
  Wenn Sie sowohl statische Routen als auch BGP-Routing konfigurieren, haben die statischen Routen Vorrang.

So konfigurieren Sie Routingeinstellungen für Ihren Remote-Netzwerkstandort.

 ©2025 Palo Alto Networks, Inc.

- Um Routingeinstellungen hinzuzufügen oder anzupassen, gehen Sie zu **Workflows** > **Prisma Access-Einrichtung** > **Remote-Netzwerke** und fügen Sie einen Remote-Netzwerkstandort hinzu bzw. bearbeiten Sie ihn.


©2025 Palo Alto Networks, Inc.





©2025 Palo Alto Networks, Inc.

- Konfigurieren Sie statische Routen.

  Wenn Sie statische Routen verwenden, um den Datenverkehr zu und von Remote-Netzwerkstandorten zu leiten, **fügen** Sie die IP-Subnetze oder IP-Adressen hinzu, die Sie in der Zweigstelle sichern möchten. Beachten Sie, dass Sie die statischen Routen manuell aktualisieren müssen, wenn Sie Änderungen an den IP-Subnetzen in Ihrer Zweigstelle vornehmen.

- Konfigurieren Sie das dynamische Routing.

  Um dynamisches Routing für Ihre Zweigstellensubnetze zu verwenden, **aktivieren Sie BGP für dynamisches Routing** und konfigurieren Sie dann die folgenden Einstellungen:

  - **Routen nicht exportieren** – Verhindern Sie, dass Prisma Access Routen in Ihr Remote-Netzwerk weiterleitet.

    Standardmäßig teilt Prisma Access alle BGP-Routinginformationen mit, einschließlich lokaler Routen und aller Präfixe, die von anderen Dienstverbindungen, Remote-Netzwerken und den Subnetzen mobiler Benutzer empfangen werden. Aktivieren Sie dieses Kontrollkästchen, um Prisma Access daran zu hindern, BGP-Mitteilungen zu senden. Die empfangenen BGP-Informationen werden aber weiterhin verwendet, um Informationen zu Routen anderer BGP-Nachbarn zu erhalten.

    *Da Prisma Access keine BGP-Mitteilungen sendet, müssen Sie, wenn Sie diese Option auswählen, statische Routen auf dem lokalen Gerät konfigurieren, um Routen zurück zu Prisma Access einzurichten.*
  - **Peer-IP-Adresse** – Geben Sie die Peer-IP-Adresse ein, die als Router-ID des eBGP-Routers im Remote-Netzwerk zugewiesen ist.
  - **Peer-AS** – Geben Sie die Peer-AS-Nummer ein, also das autonome System (AS) für Ihr Netzwerk.

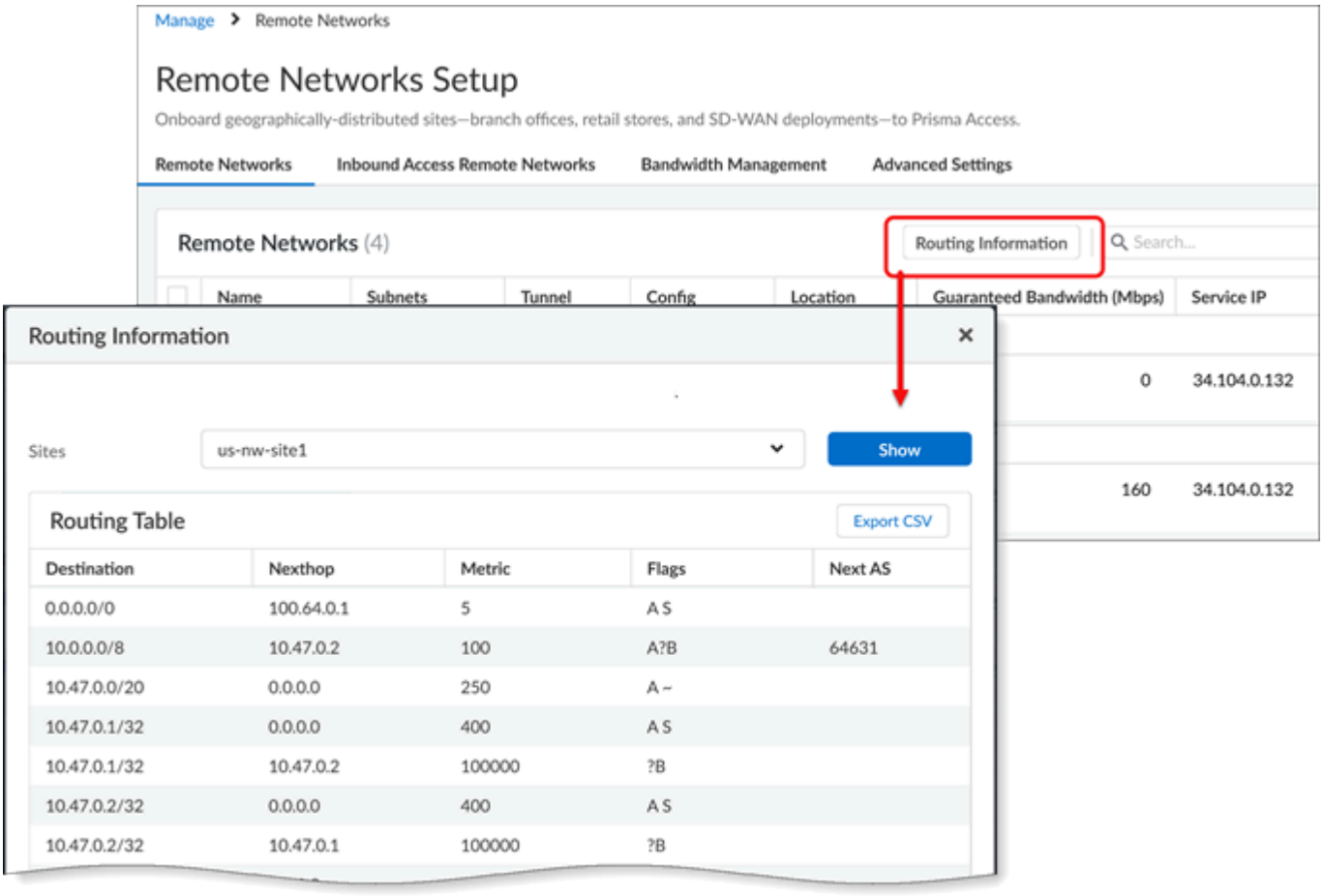
    Sie müssen eine RFC 6996-konforme BGP private AS-Nummer verwenden.
  - **Lokale IP-Adresse** – Geben Sie die IP-Adresse ein, die Prisma Access als lokale IP-Adresse für BGP verwendet.

    Eine lokale Adresse ist nur erforderlich, wenn Ihr Gerät am Remote-Standort sie für das erfolgreiche BGP-Peering benötigt. Stellen Sie sicher, dass die angegebene Adresse nicht mit IP-Adressen im Infrastruktursubnetz oder in den Subnetzen des Remote-Netzwerks in Konflikt steht oder sich mit diesen überschneidet.
  - **Geheimer Schlüssel** – Geben Sie einen geheimen Schlüssel ein, um die BGP-Peer-Kommunikation zu authentifizieren, und **bestätigen Sie den geheimen Schlüssel**.

## Fehlerbehebung bei Standortverbindungen

Zur Fehlerbehebung können Sie nun die Routingtabelle für einen Remote-Netzwerkstandort oder einen Dienstverbindungsstandort anzeigen. Suchen Sie die Schaltfläche **Routinginformationen** im Dashboard für Remote-Netzwerke oder die Dienstverbindung.

 ©2025 Palo Alto Networks, Inc.




 ©2025 Palo Alto Networks, Inc.

# Mehrere Remote-Netzwerke einbinden

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

Zur Optimierung des Prozesses für das Onboarding und die Konfiguration von Remote-Netzwerken haben Sie die Möglichkeit, mindestens ein Remote-Netzwerk einzubinden und diese Einstellungen dann in eine Textdatei mit durch Komma getrennten Werten (Comma Separated Value, CSV) zu exportieren. Die CSV-Datei enthält die Werte der IPSec-Tunnel- und IKE-Gateway-Einstellungen für das Netzwerk, das Sie für den Export ausgewählt haben. Anschließend können Sie diese Einstellungen bearbeiten und für jedes neue Netzwerk, das Sie möglicherweise einbinden möchten, eindeutig festlegen. Sie können die CSV-Datei so anpassen, dass 100 neue Remote-Netzwerke aufgenommen werden, und dann die CSV-Datei erneut importieren, um den Prozess des Onboardings neuer Remote-Netzwerke zu beschleunigen.

Die CSV-Datei enthält keine Schlüssel oder Passwörter, wie z. B. den gemeinsam genutzten geheimen BGP-Schlüssel, den vorab gemeinsam genutzten IKE-Schlüssel, die Proxy-ID, das IKE-Verschlüsselungsprofil, das IPSec-Verschlüsselungsprofil. Daher werden alle Schlüssel und Passwörter, die für die IPSec-Tunnel- und IKE-Gateway-Einstellungen erforderlich sind, von dem Netzwerk geerbt, das Sie beim Starten des CSV-Dateiimports auswählen.

Wenn Sie diesen Massenimportvorgang verwenden, müssen Sie warten, bis Prisma Access die Infrastruktur zum Sichern dieser Standorte bereitstellt.

**STEP 1 |** Wählen Sie (im Abschnitt „Einbinden“) die Optionen **Panorama** > **Cloud Services** > **Konfiguration** > **Remote-Netzwerke** aus.

**STEP 2 |** Wählen Sie einen Standort aus und **exportieren** Sie dann die Konfiguration eines Remote-Netzwerks, das Sie zuvor eingebunden haben.

Wenn Sie noch keine Standorte hinzugefügt haben, müssen Sie einen Standort **hinzufügen** und dann seine Konfiguration herunterladen. Sie müssen ein Remote-Netzwerk auswählen und auf **Export** klicken. Es wird eine CSV-Datei mit den Einstellungen auf Ihren Computer heruntergeladen.

**STEP 3 |** (Bereitstellungen, die Bandbreite nur nach Compute-Standort zuweisen) Vergewissern Sie sich, dass Sie Bandbreite für die einzubindenden Standorte zugewiesen haben.

Jeder Standort, den Sie einbinden, hat einen entsprechenden Compute-Standort, für den Bandbreite zugewiesen wird.

1. Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Remote-Netzwerke** aus und klicken Sie im Bereich **Bandbreitenzuweisung** auf das Zahnrad.
2. Aktivieren Sie das Feld **Bandbreitenzuweisung** in der angezeigten Tabelle.

   Der Tabelle in diesem Bereich kann die Zuordnung zwischen Compute-Standort und Prisma Access-Standort entnommen werden. Sie müssen Bandbreite für die Compute-Standorte zugewiesen haben, die den einzubindenden Standorten zugeordnet sind.

 ©2025 Palo Alto Networks, Inc.

Wenn Sie beispielsweise den Standort „Japan (Mitte)“ einbinden möchten, vergewissern Sie sich, dass Sie Bandbreite im Compute-Standort „Asien (Nordost)“ zugewiesen haben.

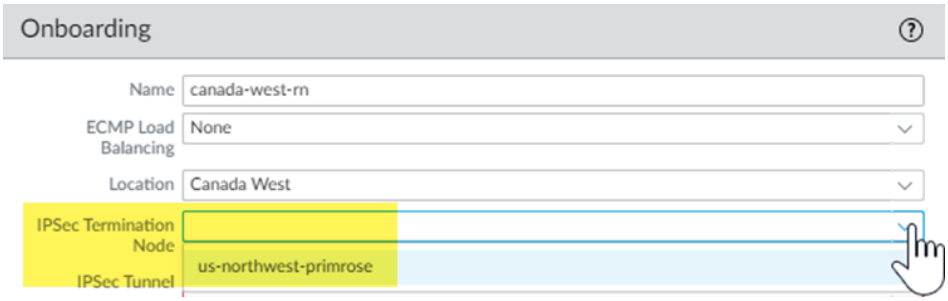
3. Wenn Sie noch keine Bandbreite für die Compute-Standorte zugewiesen haben, die den einzubindenden Standorten zugeordnet sind, fügen Sie sie jetzt hinzu.

**STEP 4 |** (Bereitstellungen, die Bandbreite nur nach Compute-Standort zuweisen) Suchen Sie den **IPSec-Terminierungsknoten**, der dem oder den Standorten zugeordnet ist, die Sie einbinden möchten.

Sie weisen dem Remote-Netzwerk beim Einbinden einen *IPSec-Terminierungsknoten* zu und geben diesen Wert in die Spalte **spn-name** der CSV-Datei ein. Jeder IPSec-Terminierungsknoten kann bis zu 1.000 Mbit/s Bandbreite bereitstellen.

Führen Sie eine der folgenden Aktionen aus, um den IPSec-Terminierungsknoten zu finden:

- Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Remote-Netzwerke** aus, um ein Remote-Netzwerk **hinzuzufügen**, und wählen Sie den einzubindenden Standort aus. Notieren Sie sich den IPSec-Terminierungsknoten im Bereich „Onboarding“.




- Öffnen Sie eine CLI-Sitzung (Command-Line Interface) mit der Panorama-Instanz, von der Prisma Access verwaltet wird, und geben Sie den Befehl `show plugins cloud_services remote-networks agg-bandwidth region` *Compute-Standort-Name* ein, wobei *Compute-Standort-Name* der Compute-Standort ist, der mit dem einzubindenden Standort verknüpft ist. Der IPSec-Terminierungsknoten wird im Feld `spn-name-list` angezeigt.

**STEP 5 |** Ändern Sie die CSV-Datei, um die Konfiguration für Remote-Netzwerke hinzuzufügen.

Eine Beschreibung der Felder und der möglichen Werte in dieser Datei finden Sie unter Felder in der Remote-Netzwerk-Tabelle.

Sie müssen die in der exportierten Datei aufgeführten Netzwerke umbenennen. Wenn die Datei doppelte Namen enthält, schlägt der Import fehl.

**STEP 6 |** **Importieren** Sie die CSV-Datei.

Die Konfiguration aus der Datei wird auf dem Bildschirm angezeigt. Das Remote-Netzwerk, das Sie zum Importieren der Datei ausgewählt haben, dient als Modellkonfiguration, und die Remote-Netzwerke, die in der Datei aufgeführt sind, erben von dort die Schlüssel und alle fehlenden Werte, die nicht eindeutig sein müssen.

 ©2025 Palo Alto Networks, Inc.

**STEP 7 |** Führen Sie einen Commit aus und übertragen Sie die Änderung per Push.

1. Wählen Sie **Commit** > **Commit und Push** aus, um Ihre Änderung festzuschreiben und per Push zu übertragen.
2. Klicken Sie auf **OK** und **Push**.

## Felder in der Remote-Netzwerk-Tabelle

Die folgende Tabelle enthält eine Beschreibung der Felder in der Remote-Netzwerk-Tabelle. Mit **J** gekennzeichnete Felder in der Zeile **Erforderlich** sind erforderliche Felder und mit **N** gekennzeichnete Felder sind optional.

| Feld | Beschreibung | Erforderlich (J/N) |
|---|---|---|
| name | Der Name des Remote-Netzwerks. | J |
| bandwidth | (Nur Bereitstellungen, die Bandbreite nach Standort zuweisen) Die zugewiesene Bandbreite des Remote-Netzwerks. Zulässige Werte sind:<br>• 2 Mbit/s<br>• 5 Mbit/s<br>• 10 Mbit/s<br>• 20 Mbit/s<br>• 25 Mbit/s<br>• 50 Mbit/s<br>• 100 Mbit/s<br>• 150 Mbit/s<br>• 300 Mbit/s<br>• 500 Mbit/s<br>• 1.000 Mbit/s<br>*Die Bandbreitenoption von 1.000 Mbit/s befindet sich im Vorschaumodus. Der Durchsatz während der Vorschau wird nach bestem Wissen und Gewissen bereitgestellt. Die tatsächliche Leistung variiert je nach Datenverkehrsmix.* | J |
| region | Standort des Remote-Netzwerks. | J |

 ©2025 Palo Alto Networks, Inc.

| Feld | Beschreibung | Erforderlich (J/N) |
|---|---|---|
| | Geben Sie die Standorte genau so ein, wie sie in diesem Dokument angegeben sind (z. B. **USA (West)** oder **Japan (Süd)**). | |
| subnets | Statisch geroutete Subnetze auf der LAN-Seite des Remote-Netzwerks. Trennen Sie mehrere Subnetze mit Kommas. | N |
| bgp_peer_as | Die BGP-ASN (Autonomous System Number) des Remote-Netzwerk-Peer-Geräts. | N |
| bgp_peer_address | Die BGP-Peer-Adresse des Remote-Netzwerk-Peer-Geräts. | N |
| tunnel_name | Der Name der IPSec-Tunnelkonfiguration. Es ist ein eindeutiger Wert erforderlich. | J |
| gateway_name | Der Name der IKE-Gateway-Konfiguration. Es ist ein eindeutiger Wert erforderlich. | J |
| peer_ip_address | Die IP-Adresse des Prisma Access-Peer-Geräts. | N |
| local_id_type | Der Typ der IKE-ID, die Prisma Access dem Peer-Gerät präsentiert. Wenn Sie Zertifikate in dem Remote-Netzwerk verwenden, in das Sie diese Datei importieren, verweisen alle angegebenen importierten Typen auf die Werte des konfigurierten Zertifikats. | N |
| local_id_value | Der Wert der IKE-ID, die Prisma Access dem Peer-Gerät präsentiert. Wenn Sie Zertifikate in dem Remote-Netzwerk verwenden, in das Sie diese Datei importieren, verweisen alle angegebenen importierten Typen auf die Werte des konfigurierten Zertifikats. | N |
| peer_id_type | Der Wert der IKE-ID, die der Peer Prisma Access präsentiert. Wenn Sie Zertifikate in dem Remote-Netzwerk verwenden, in das Sie diese Datei importieren, verweisen alle angegebenen importierten Typen auf die Peer-Zertifikat-Werte. | N |
| peer_id_value | Der Wert der IKE-ID, die Prisma Access dem Peer-Gerät präsentiert. Wenn Sie Zertifikate in dem Remote-Netzwerk verwenden, in das Sie diese Datei importieren, verweisen alle | N |

 ©2025 Palo Alto Networks, Inc.

| Feld | Beschreibung | Erforderlich (J/N) |
|---|---|---|
| | angegebenen importierten Typen auf die Peer-Zertifikat-Werte. | |
| monitor_ip | Die IP-Adresse der Tunnelüberwachung, anhand der die Cloud ermittelt, ob der IPSec-Tunnel aktiv ist und das Peer-Netzwerk erreichbar ist.<br><br>*Sie können einen Proxy-ID-Wert für den Tunnelmonitor nicht exportieren.* | N |
| proxy_ids | Die Proxy-IDs, die für den Peer konfiguriert sind. Bei routenbasierten VPNs lassen Sie dieses Feld leer. Geben Sie die Proxy-ID im folgenden CSV-Konfigurationsformat an:<br><br>[{"name":"*proxyidname*", "local":"*1.2.3.4/32*", "remote":"*4.3.2.1/32*", "protocol":{"udp": {"local-port":*123*, "remote-port":*234*}}}, {"name":"*proxyidname2*", "local":"*2.3.4.5/32*", "remote":"*3.4.5.6/32*", "protocol":{"tcp": {"local-port":*234*,"remote-port":*345*}}}] | N |
| sec_wan_enabled | Gibt an, ob Sie einen sekundären IPSec-Tunnel aktivieren oder nicht. Zulässige Werte sind `yes` und `no`. | N |
| sec_tunnel_name | Der Name der sekundären IPSec-Tunnelkonfiguration. Wenn Sie einen sekundären Tunnel angeben, ist ein eindeutiger Wert erforderlich. | N |
| sec_gateway_name | Der Name der sekundären IKE-Gateway-Konfiguration. Wenn Sie einen sekundären Tunnel angeben, ist ein eindeutiger Wert erforderlich. | N |
| sec_peer_ip_address | Die IP-Adresse des Prisma Access-Peer-Geräts für den sekundären IPSec-Tunnel. | N |
| sec_local_id_type | Der Typ der IKE-ID, die Prisma Access dem Peer-Gerät für den sekundären IPSec-Tunnel präsentiert. Wenn Sie Zertifikate in dem Remote-Netzwerk verwenden, in das Sie diese Datei importieren, verweisen alle angegebenen importierten Typen auf die Werte des konfigurierten Zertifikats. | N |

 ©2025 Palo Alto Networks, Inc.

| Feld | Beschreibung | Erforderlich (J/N) |
|---|---|---|
| sec_local_id_value | Der Wert der IKE-ID, die Prisma Access dem Peer-Gerät für den sekundären IPSec-Tunnel präsentiert. Wenn Sie Zertifikate in dem Remote-Netzwerk verwenden, in das Sie diese Datei importieren, verweisen alle angegebenen importierten Typen auf die Werte des konfigurierten Zertifikats. | N |
| sec_peer_id_type | Der Wert der IKE-ID, die der Peer Prisma Access für den sekundären IPSec-Tunnel präsentiert. Wenn Sie Zertifikate in dem Remote-Netzwerk verwenden, in das Sie diese Datei importieren, verweisen alle angegebenen importierten Typen auf die Peer-Zertifikat-Werte. | N |
| sec_peer_id_value | Der Wert der IKE-ID, die Prisma Access dem Peer-Gerät für den sekundären IPSec-Tunnel präsentiert. Wenn Sie Zertifikate in dem Remote-Netzwerk verwenden, in das Sie diese Datei importieren, verweisen alle angegebenen importierten Typen auf die Peer-Zertifikat-Werte. | N |
| sec_monitor_ip | Die IP-Adresse der Tunnelüberwachung, die die Cloud für den sekundären IPSec-Tunnel verwendet, um festzustellen, ob der IPSec-Tunnel aktiv ist und das Peer-Netzwerk erreichbar ist.<br><br>*Sie können einen Proxy-ID-Wert für den Tunnelmonitor nicht exportieren.* | N |
| sec_proxy_ids | Die Proxy-IDs, die für den Peer für den sekundären IPSec-Tunnel konfiguriert sind. Bei routenbasierten VPNs lassen Sie dieses Feld leer. Geben Sie die Proxy-ID im folgenden CSV-Konfigurationsformat an:<br><br>[{"name":"*proxyidname*", "local":"*1.2.3.4/32*", "remote":"*4.3.2.1/32*", "protocol":{"udp": {"local-port":*123*, "remote-port":*234*}}}, {"name":"*proxyidname2*", "local":"*2.3.4.5/32*", "remote":"*3.4.5.6/32*", "protocol":{"tcp": {"local-port":*234*,"remote-port":*345*}}}] | N |

 ©2025 Palo Alto Networks, Inc.

| Feld | Beschreibung | Erforderlich (J/N) |
|---|---|---|
| ecmp_link_1_tunnel_name | (Nur ECMP-Bereitstellungen) Der Name der IPSec-Tunnelkonfiguration für ECMP-Tunnel 1. Es ist ein eindeutiger Wert erforderlich. | |
| ecmp_link_1_gateway_name | (Nur ECMP-Bereitstellungen) Der Name der IKE-Gateway-Konfiguration für ECMP-Tunnel 1. Es ist ein eindeutiger Wert erforderlich. | |
| ecmp_link_1_peer_ip_address | (Nur ECMP-Bereitstellungen) Die IP-Adresse des Prisma Access-Peer-Geräts für ECMP-Tunnel 1. | |
| ecmp_link_1_local_id_type | (Nur ECMP-Bereitstellungen) Der Typ der IKE-ID, die Prisma Access dem Peer-Gerät für ECMP-Tunnel 1 präsentiert. Wenn Sie Zertifikate in dem Remote-Netzwerk verwenden, in das Sie diese Datei importieren, verweisen alle angegebenen importierten Typen auf die Werte des konfigurierten Zertifikats. | |
| ecmp_link_1_local_id_value | (Nur ECMP-Bereitstellungen) Der Wert der IKE-ID, die Prisma Access dem Peer-Gerät für ECMP-Tunnel 1 präsentiert. Wenn Sie Zertifikate in dem Remote-Netzwerk verwenden, in das Sie diese Datei importieren, verweisen alle angegebenen importierten Typen auf die Werte des konfigurierten Zertifikats. | |
| ecmp_link_1_peer_id_type | (Nur ECMP-Bereitstellungen) Der Wert der IKE-ID, die der Peer Prisma Access für ECMP-Tunnel 1 präsentiert. Wenn Sie Zertifikate in dem Remote-Netzwerk verwenden, in das Sie diese Datei importieren, verweisen alle angegebenen importierten Typen auf die Peer-Zertifikat-Werte. | |
| ecmp_link_1_peer_id_value | (Nur ECMP-Bereitstellungen) Der Wert der IKE-ID, die Prisma Access dem Peer-Gerät für ECMP-Tunnel 1 präsentiert. Wenn Sie Zertifikate in dem Remote-Netzwerk verwenden, in das Sie diese Datei importieren, verweisen alle angegebenen importierten Typen auf die Peer-Zertifikat-Werte. | |
| ecmp_link_1_monitor_ip | (Nur ECMP-Bereitstellungen) Die IP-Adresse der Tunnelüberwachung, anhand der die Cloud ermittelt, ob der IPSec-Tunnel aktiv ist und das | |

 ©2025 Palo Alto Networks, Inc.

| Feld | Beschreibung | Erforderlich (J/N) |
|---|---|---|
| | Peer-Netzwerk für ECMP-Tunnel 1 erreichbar ist.<br><br>*Sie können einen Proxy-ID-Wert für die Tunnelmonitore nicht exportieren.* | |
| ecmp_link_1_proxy_ids | (Nur ECMP-Bereitstellungen) Die Proxy-IDs, die für den Peer für ECMP-Tunnel 1 konfiguriert sind. Bei routenbasierten VPNs lassen Sie dieses Feld leer. Geben Sie die Proxy-ID im folgenden CSV-Konfigurationsformat an:<br><br>[{"name":"*proxyidname*", "local":"*1.2.3.4/32*", "remote":"*4.3.2.1/32*", "protocol":{"udp": {"local-port":*123*, "remote-port":*234*}}}, {"name":"*proxyidname2*", "local":"*2.3.4.5/32*", "remote":"*3.4.5.6/32*", "protocol":{"tcp": {"local-port":*234*,"remote-port":*345*}}}] | |
| ecmp_link_1_bgp_peer_as | (Nur ECMP-Bereitstellungen) Die BGP-ASN (Autonomous System Number) des Remote-Netzwerk-Peer-Geräts für ECMP-Tunnel 1. | |
| ecmp_link_1_bgp_peer_address | (Nur ECMP-Bereitstellungen) Die BGP-Peer-Adresse des Remote-Netzwerk-Peer-Geräts für ECMP-Tunnel 1. | |
| ecmp_link_2_tunnel_name | (Nur ECMP-Bereitstellungen) Der Name der IPSec-Tunnelkonfiguration für ECMP-Tunnel 2. Es ist ein eindeutiger Wert erforderlich. | |
| ecmp_link_2_gateway_name | (Nur ECMP-Bereitstellungen) Der Name der IKE-Gateway-Konfiguration für ECMP-Tunnel 2. Es ist ein eindeutiger Wert erforderlich. | |
| ecmp_link_2_peer_ip_address | (Nur ECMP-Bereitstellungen) Die IP-Adresse des Prisma Access-Peer-Geräts für ECMP-Tunnel 2. | |
| ecmp_link_2_local_id_type | (Nur ECMP-Bereitstellungen) Der Typ der IKE-ID, die Prisma Access dem Peer-Gerät für ECMP-Tunnel 2 präsentiert. Wenn Sie Zertifikate in dem Remote-Netzwerk verwenden, in das Sie diese Datei importieren, verweisen alle angegebenen importierten Typen auf die Werte des konfigurierten Zertifikats. | |

 ©2025 Palo Alto Networks, Inc.

| Feld | Beschreibung | Erforderlich (J/N) |
|---|---|---|
| ecmp_link_2_local_id_value | (Nur ECMP-Bereitstellungen) Der Wert der IKE-ID, die Prisma Access dem Peer-Gerät für ECMP-Tunnel 2 präsentiert. Wenn Sie Zertifikate in dem Remote-Netzwerk verwenden, in das Sie diese Datei importieren, verweisen alle angegebenen importierten Typen auf die Werte des konfigurierten Zertifikats. | |
| ecmp_link_2_peer_id_type | (Nur ECMP-Bereitstellungen) Der Wert der IKE-ID, die der Peer dem Prisma Access für ECMP-Tunnel 2 präsentiert. Wenn Sie Zertifikate in dem Remote-Netzwerk verwenden, in das Sie diese Datei importieren, verweisen alle angegebenen importierten Typen auf die Peer-Zertifikat-Werte. | |
| ecmp_link_2_peer_id_value | (Nur ECMP-Bereitstellungen) Der Wert der IKE-ID, die Prisma Access dem Peer-Gerät für ECMP-Tunnel 2 präsentiert. Wenn Sie Zertifikate in dem Remote-Netzwerk verwenden, in das Sie diese Datei importieren, verweisen alle angegebenen importierten Typen auf die Peer-Zertifikat-Werte. | |
| ecmp_link_2_monitor_ip | (Nur ECMP-Bereitstellungen) Die IP-Adresse der Tunnelüberwachung, anhand der die Cloud ermittelt, ob der IPSec-Tunnel aktiv ist und das Peer-Netzwerk für ECMP-Tunnel 2 erreichbar ist.<br><br>*Sie können einen Proxy-ID-Wert für die Tunnelmonitore nicht exportieren.* | |
| ecmp_link_2_proxy_ids | (Nur ECMP-Bereitstellungen) Die Proxy-IDs, die für den Peer für ECMP-Tunnel 2 konfiguriert sind. Bei routenbasierten VPNs lassen Sie dieses Feld leer. Geben Sie die Proxy-ID im folgenden CSV-Konfigurationsformat an:<br><br>[{"name":"*proxyidname*", "local":"*1.2.3.4/32*", "remote":"*4.3.2.1/32*", "protocol":{"udp": {"local-port":*123*, "remote-port":*234*}}}, {"name":"*proxyidname2*", "local":"*2.3.4.5/32*", "remote":"*3.4.5.6/32*", "protocol":{"tcp": {"local-port":*234*,"remote-port":*345*}}}] | |

 ©2025 Palo Alto Networks, Inc.

| Feld | Beschreibung | Erforderlich (J/N) |
|---|---|---|
| ecmp_link_2_bgp_peer_as | (Nur ECMP-Bereitstellungen) Die BGP-ASN (Autonomous System Number) des Remote-Netzwerk-Peer-Geräts für den ECMP-Tunnel 2. | |
| ecmp_link_2_bgp_peer_address | (Nur ECMP-Bereitstellungen) Die BGP-Peer-Adresse des Remote-Netzwerk-Peer-Geräts für ECMP-Tunnel 2. | |
| ecmp_link_3_tunnel_name | (Nur ECMP-Bereitstellungen) Der Name der IPSec-Tunnelkonfiguration für ECMP-Tunnel 3. Es ist ein eindeutiger Wert erforderlich. | |
| ecmp_link_3_gateway_name | (Nur ECMP-Bereitstellungen) Der Name der IKE-Gateway-Konfiguration für ECMP-Tunnel 3. Es ist ein eindeutiger Wert erforderlich. | |
| ecmp_link_3_peer_ip_address | (Nur ECMP-Bereitstellungen) Die IP-Adresse des Prisma Access-Peer-Geräts für ECMP-Tunnel 3. | |
| ecmp_link_3_local_id_type | (Nur ECMP-Bereitstellungen) Die Art der IKE-ID, die Prisma Access dem Peer-Gerät für ECMP-Tunnel 3 präsentiert. Wenn Sie Zertifikate in dem Remote-Netzwerk verwenden, in das Sie diese Datei importieren, verweisen alle angegebenen importierten Typen auf die Werte des konfigurierten Zertifikats. | |
| ecmp_link_3_local_id_value | (Nur ECMP-Bereitstellungen) Der Wert der IKE-ID, die Prisma Access dem Peer-Gerät für ECMP-Tunnel 3 präsentiert. Wenn Sie Zertifikate in dem Remote-Netzwerk verwenden, in das Sie diese Datei importieren, verweisen alle angegebenen importierten Typen auf die Werte des konfigurierten Zertifikats. | |
| ecmp_link_3_peer_id_type | (Nur ECMP-Bereitstellungen) Der Wert der IKE-ID, die der Peer Prisma Access für ECMP-Tunnel 3 präsentiert. Wenn Sie Zertifikate in dem Remote-Netzwerk verwenden, in das Sie diese Datei importieren, verweisen alle angegebenen importierten Typen auf die Peer-Zertifikat-Werte. | |
| ecmp_link_3_peer_id_value | (Nur ECMP-Bereitstellungen) Der Wert der IKE-ID, die Prisma Access dem Peer-Gerät für ECMP-Tunnel 3 präsentiert. Wenn Sie Zertifikate in dem Remote-Netzwerk verwenden, in das | |

 ©2025 Palo Alto Networks, Inc.

| Feld | Beschreibung | Erforderlich (J/N) |
|---|---|---|
| | Sie diese Datei importieren, verweisen alle angegebenen importierten Typen auf die Peer-Zertifikat-Werte. | |
| ecmp_link_3_monitor_ip | (Nur ECMP-Bereitstellungen) Die IP-Adresse der Tunnelüberwachung, anhand der die Cloud ermittelt, ob der IPSec-Tunnel aktiv ist und das Peer-Netzwerk für ECMP-Tunnel 3 erreichbar ist.<br><br>*Sie können einen Proxy-ID-Wert für die Tunnelmonitore nicht exportieren.* | |
| ecmp_link_3_proxy_ids | (Nur ECMP-Bereitstellungen) Die Proxy-IDs, die für den Peer für ECMP-Tunnel 3 konfiguriert sind. Bei routenbasierten VPNs lassen Sie dieses Feld leer. Geben Sie die Proxy-ID im folgenden CSV-Konfigurationsformat an:<br><br>[{"name":"*proxyidname*", "local":"*1.2.3.4/32*", "remote":"*4.3.2.1/32*", "protocol":{"udp": {"local-port":*123*, "remote-port":*234*}}}, {"name":"*proxyidname2*", "local":"*2.3.4.5/32*", "remote":"*3.4.5.6/32*", "protocol":{"tcp": {"local-port":*234*,"remote-port":*345*}}}] | |
| ecmp_link_3_bgp_peer_as | (Nur ECMP-Bereitstellungen) Die BGP-ASN (Autonomous System Number) des Remote-Netzwerk-Peer-Geräts für ECMP-Tunnel 3. | |
| ecmp_link_3_bgp_peer_address | (Nur ECMP-Bereitstellungen) Die BGP-Peer-Adresse des Remote-Netzwerk-Peer-Geräts für ECMP-Tunnel 3. | |
| ecmp_link_4_tunnel_name | (Nur ECMP-Bereitstellungen) Der Name der IPSec-Tunnelkonfiguration für ECMP-Tunnel 4. Es ist ein eindeutiger Wert erforderlich. | |
| ecmp_link_4_gateway_name | (Nur ECMP-Bereitstellungen) Der Name der IKE-Gateway-Konfiguration für ECMP-Tunnel 4. Es ist ein eindeutiger Wert erforderlich. | |
| ecmp_link_4_peer_ip_address | (Nur ECMP-Bereitstellungen) Die IP-Adresse des Prisma Access-Peer-Geräts für ECMP-Tunnel 4. | |

 ©2025 Palo Alto Networks, Inc.

| Feld | Beschreibung | Erforderlich (J/N) |
|---|---|---|
| ecmp_link_4_local_id_type | (Nur ECMP-Bereitstellungen) Die Art der IKE-ID, die Prisma Access dem Peer-Gerät für ECMP-Tunnel 4 präsentiert. Wenn Sie Zertifikate in dem Remote-Netzwerk verwenden, in das Sie diese Datei importieren, verweisen alle angegebenen importierten Typen auf die Werte des konfigurierten Zertifikats. | |
| ecmp_link_4_local_id_value | (Nur ECMP-Bereitstellungen) Der Wert der IKE-ID, die Prisma Access dem Peer-Gerät für ECMP-Tunnel 4 präsentiert. Wenn Sie Zertifikate in dem Remote-Netzwerk verwenden, in das Sie diese Datei importieren, verweisen alle angegebenen importierten Typen auf die Werte des konfigurierten Zertifikats. | |
| ecmp_link_4_peer_id_type | (Nur ECMP-Bereitstellungen) Der Wert der IKE-ID, die der Peer Prisma Access für ECMP-Tunnel 4 präsentiert. Wenn Sie Zertifikate in dem Remote-Netzwerk verwenden, in das Sie diese Datei importieren, verweisen alle angegebenen importierten Typen auf die Peer-Zertifikat-Werte. | |
| ecmp_link_4_peer_id_value | (Nur ECMP-Bereitstellungen) Der Wert der IKE-ID, die Prisma Access dem Peer-Gerät für ECMP-Tunnel 4 präsentiert. Wenn Sie Zertifikate in dem Remote-Netzwerk verwenden, in das Sie diese Datei importieren, verweisen alle angegebenen importierten Typen auf die Peer-Zertifikat-Werte. | |
| ecmp_link_4_monitor_ip | (Nur ECMP-Bereitstellungen) Die IP-Adresse der Tunnelüberwachung, anhand der die Cloud ermittelt, ob der IPSec-Tunnel aktiv ist und das Peer-Netzwerk für ECMP-Tunnel 4 erreichbar ist.<br><br>*Sie können einen Proxy-ID-Wert für die Tunnelmonitore nicht exportieren.* | |
| ecmp_link_4_proxy_ids | (Nur ECMP-Bereitstellungen) Die Proxy-IDs, die für den Peer für ECMP-Tunnel 4 konfiguriert sind. Bei routenbasierten VPNs lassen Sie dieses Feld leer. Geben Sie die Proxy-ID im folgenden CSV-Konfigurationsformat an: | |

 ©2025 Palo Alto Networks, Inc.

| Feld | Beschreibung | Erforderlich (J/N) |
|---|---|---|
| | [{"name":"*proxyidname*", "local":"*1.2.3.4/32*", "remote":"*4.3.2.1/32*", "protocol":{"udp": {"local-port":*123*, "remote-port":*234*}}}, {"name":"*proxyidname2*", "local":"*2.3.4.5/32*", "remote":"*3.4.5.6/32*", "protocol":{"tcp": {"local-port":*234*,"remote-port":*345*}}}] | |
| ecmp_link_4_bgp_peer_as | (Nur ECMP-Bereitstellungen) Die BGP-ASN (Autonomous System Number) des Remote-Netzwerk-Peer-Geräts für den ECMP-Tunnel 4. | |
| ecmp_link_4_bgp_peer_address | (Nur ECMP-Bereitstellungen) Die BGP-Peer-Adresse des Remote-Netzwerk-Peer-Geräts für ECMP-Tunnel 4. | |
| spn-name | (Bereitstellungen, die Bandbreite nur nach Compute-Standort zuweisen) Der Name des IPSec-Terminierungsknotens. Dieses Feld wird für Bereitstellungen benötigt, die Bandbreite nach Compute-Standort zuweisen. | |

 ©2025 Palo Alto Networks, Inc.

# Verbindung des Remote-Netzwerks mit Prisma Access prüfen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

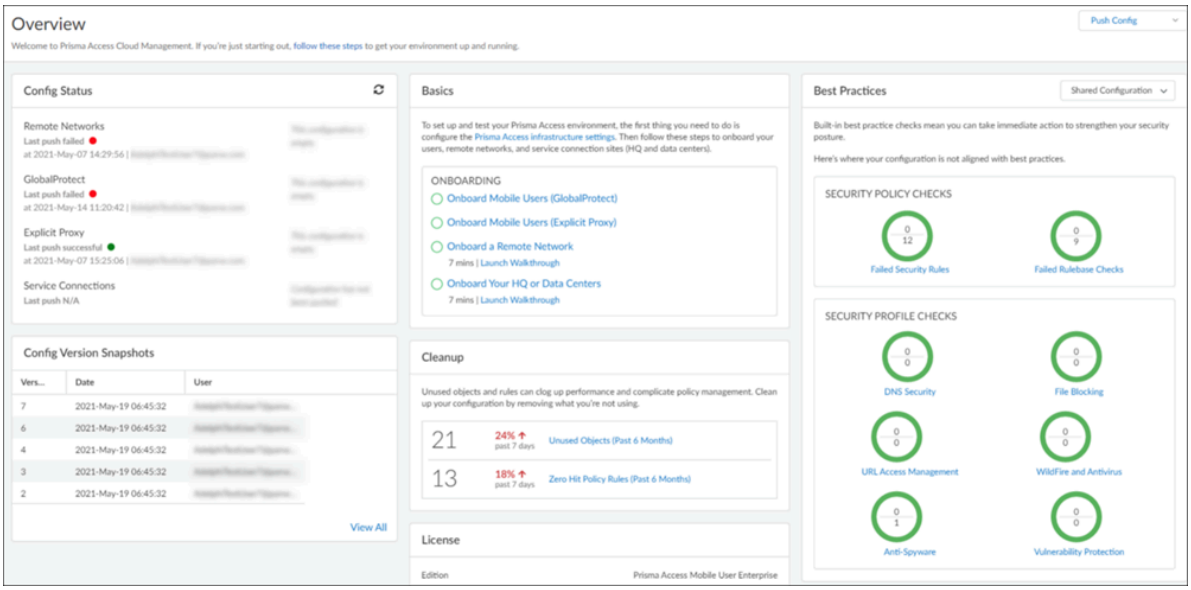
Überprüfen Sie nach der Konfiguration des IPSec-VPN-Geräts im Remote-Netzwerk den Tunnelstatus. Beachten Sie beim Überprüfen von Remote-Netzwerken Folgendes:

- Überprüfen Sie den Status des IPSec-Tunnels zu Ihrem Remote-Netzwerk.
- Der letzte Schritt bei der Überprüfung von Remote-Netzwerken besteht darin, die Protokolle zu überprüfen und sicherzustellen, dass der Datenverkehr durch Prisma Access fließt. Wenn Fehler oder Warnungen auftreten, überprüfen Sie die Systemprotokolle in Prisma Access und in lokalen Protokollen auf dem Remote-Netzwerkgerät. Beheben Sie alle Fehler oder Warnungen, bevor Sie mit der Konfiguration fortfahren.
- Fügen Sie weitere Remote-Netzwerke nach Bedarf hinzu.
- Strata Cloud Manager
- Panorama

## Überprüfen der Verbindung des Remote-Netzwerks zu Prisma Access (Strata Cloud Manager)

Wählen Sie die Optionen **Verwalten** > **Konfiguration** > **NGFW und Prisma Access**aus, und ändern Sie den **Konfigurationsumfang** in **Prisma Access**. Wählen Sie dann die Optionen **Prisma Access-Synchronisierungsstatus** > **Remote-Netzwerke**.


©2025 Palo Alto Networks, Inc.




# Überprüfen der Verbindung des Remote-Netzwerks zu Prisma Access (Panorama)

**STEP 1 |** Wählen Sie **Panorama** > **Cloud-Dienste** > **Status** > **Status**aus, um zu überprüfen, ob die Remote-Netzwerkverbindungen erfolgreich bereitgestellt wurden.

Im Bereich **Bereitstellungsstatus** können Sie den Fortschritt von Onboarding- und Bereitstellungsaufträgen anzeigen, bevor diese abgeschlossen sind. Außerdem können Sie dort weiterführende Informationen zum Status abgeschlossener Aufträge einsehen.

**STEP 2 |** Wenn Sie eine Karte anzeigen möchten, die die Standorte der Remote-Netzwerke in den von Ihnen ausgewählten Regionen anzeigt, wählen Sie **Panorama** > **Cloud-Dienste** > **Status** > **Überwachen** und klicken anschließend auf die Registerkarte **Remote-Netzwerke**.

**STEP 3 |** Wählen Sie eine Region aus, um weiterführende Details zu dieser Region abzufragen.

**STEP 4 |** Klicken Sie auf die Registerkarten unter der Karte, um zusätzliche Remote-Netzwerkstatistiken anzuzeigen.

Registerkarte **Status**:

- **Standort** – Der Standort, an dem Ihr Remote-Netzwerk bereitgestellt wird.
- **Remote Peer** – Der Peer, zu dem das Remote-Netzwerk eine IPSec-Tunnelverbindung hat.
- **IPSec-Terminierungsknoten** – Der IPSec-Terminierungsknoten, der dem Remote-Netzwerk zugeordnet ist. Dieses Feld wird nur angezeigt, wenn Sie Bandbreite nach Compute-Standort zuweisen.
- **ECMP** – Gibt an, ob Sie **ECMP-Lastausgleich** für diese Remote-Netzwerkverbindung aktiviert haben.
- **Konfigurationsstatus** – Der Status Ihrer letzten Konfigurationsübertragung an den Dienst. Wenn Sie lokal eine Änderung vorgenommen und die Konfiguration noch nicht in die Cloud übertragen haben, lautet der Status **Nicht synchron**. Bewegen Sie den Mauszeiger über die Statusanzeige, um detailliertere Informationen zu erhalten. Nach dem Festschreiben und

 ©2025 Palo Alto Networks, Inc.

Übertragen der Konfiguration auf Prisma Accessändert sich der Konfigurationsstatus in **Synchron**.

- **BGP-Status** – Zeigt Informationen zum BGP-Status zwischen Firewall oder Router am Remote-Netzwerkstandort und Prisma Access an. Obwohl der Status beim Durchlaufen der verschiedenen BGP-Status nur kurz angezeigt wird (**Inaktiv**, **Aktiv**, **Offen Senden**, **Offen Anstehend**, **Offen Bestätigen**), wird der BGP-Status meist wie folgt angezeigt:
  - **Verbinden** – Der Router am Standort des Remote-Netzwerks versucht, die BGP-Peer-Beziehung mit Prisma Access herzustellen.
  - **Eingerichtet** – Die BGP-Peer-Beziehung wurde eingerichtet.

    In diesem Feld wird auch angezeigt, ob sich die BGP-Verbindung in einem Fehlerzustand befindet:
  - **Warnung** – Seit mehr als acht Minuten wurde der BGP-Status nicht aktualisiert. Dies kann auf einen Ausfall der Firewall hindeuten.
  - **Fehler** – Der BGP-Status ist unbekannt.
- **Tunnelstatus** – Der Betriebsstatus der Verbindung zwischen Prisma Access und dem Remote-Netzwerk.

Registerkarte **Statistiken**:

- **Standort** – Der Standort, an dem Ihr Remote-Netzwerk bereitgestellt wird.
- **Remote Peer** – Der Unternehmensstandort, zu dem dieses Remote-Netzwerk einen IPSec-Tunnel einrichtet.
- **Eingangsbandbreite (Mbit/s)** – Die Bandbreite vom Remote-Netzwerkstandort bis zu Prisma Access.

  *Für die Felder „Eingangsbandbreite“, „Höchste Eingangsbandbreite“, „Ausgangsbandbreite“ und „Höchste Ausgangsbandbreite“ werden die Zahlen rot angezeigt, wenn der Bandbreitenverbrauch in einem Remote-Netzwerk 80 % der zugewiesenen Bandbreite überschreitet.*
- **Höchste Eingangsbandbreite (Mbit/s)** – Die Spitzenlast vom Remote-Netzwerkstandort in den Cloud-Dienst.
- **Ausgangsbandbreite (Mbit/s)** – Die Bandbreite von Prisma Access in den Remote-Netzwerkstandort.
- **Höchste Ausgangsbandbreite (Mbit/s)** – Die Spitzenlast von Prisma Access in den Remote-Netzwerkstandort.

Wenn Sie Statistiken zu Standorten in der Region abrufen möchten, wählen Sie die Option **Bandbreitennutzung** aus.

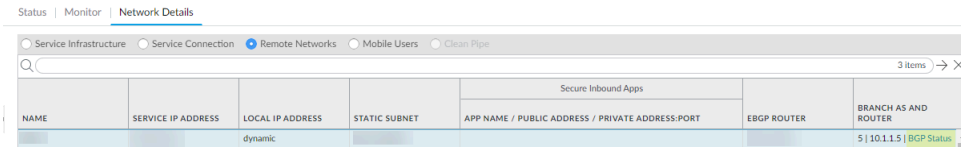
Aktivieren Sie das Häkchen für einen gewünschten Standort, um die ausführliche Bandbreitennutzung anzuzeigen. Wählen Sie bei Bereitstellungen, die Bandbreite nach Compute-Standort zuweisen, einen IPSec-Terminierungsknoten aus, um Statistiken zu diesem Knoten anzuzeigen. Prisma Access verwendet standardmäßig das 95. Perzentil zum Sammeln von Statistiken. Es verfolgt die Bandbreite bei Spitzenauslastung und ignoriert die oberen 5 Prozent der Auslastungsspitzen und großer Bursts.

 ©2025 Palo Alto Networks, Inc.

# Überprüfen des BGP-Status einer Remote-Verbindung

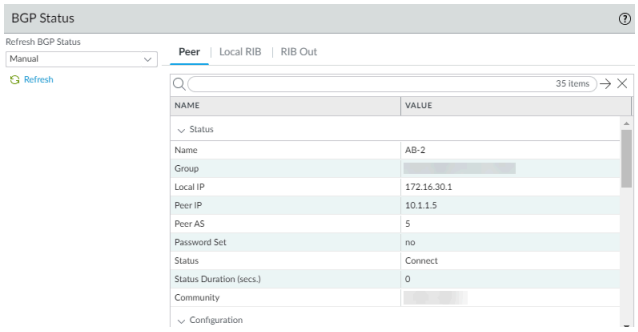
| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Wenn Sie BGP konfiguriert haben, können Sie dessen Status überprüfen, indem Sie die Optionen **Panorama** > **Cloud-Dienste** > **Status** > **Netzwerkdetails** > **Remote-Netzwerke** > **BGP-Status**auswählen.

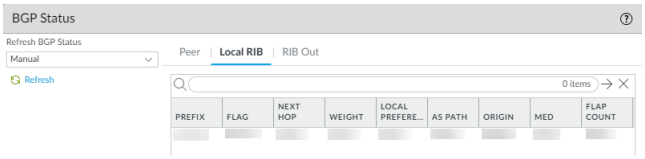



Daraufhin wird der Dialog für den BGP-Status angezeigt. Diese Tabelle enthält folgende Informationen:

- **Peer** – Routinginformationen für den BGP-Peer, einschließlich Status, Gesamtzahl der Routen, Konfigurations- und Laufzeitstatistiken sowie Zähler. Die Gesamtzahl der Routen wird im Bereich **bgpAfiIpv4-unicast Counters** in den Feldern **Gesamtwert eingehend** und **Gesamtwert ausgehend** angezeigt.




- **Lokale RIB** – Routinginformationen, die von verschiedenen Peers empfangen und in der Routing Information Base (RIB) gespeichert wurden.




- **RIB Out** – Routinginformationen, die Prisma Access über BGP-Aktualisierungsnachrichten an seine Peers mitteilt. Ein Beispiel dieser Tabelle und Informationen dazu, wie BGP den von Ihnen erstellten IP-Adresspool für mobile Benutzer nutzt, finden Sie in Wie BGP IP-Adresspools mobiler Benutzer für Dienstverbindungen und Remote-Netzwerkverbindungen ankündigt.

 ©2025 Palo Alto Networks, Inc.

# Konfigurieren eines über WAN-Link verbundenen Remote-Netzwerks und einer Serviceverbindung

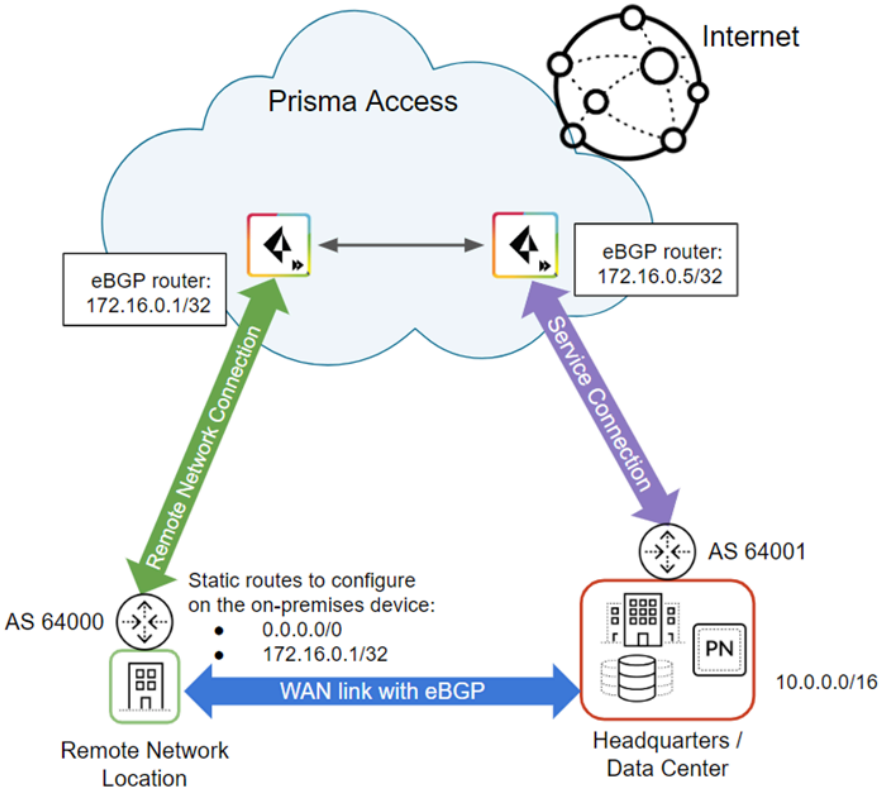
| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Wenn Sie über eine Bereitstellung verfügen, in der ein Remote-Netzwerkstandort und eine Zentrale oder ein Rechenzentrum direkt über einen WAN-Link mit einer Dienstverbindung verbunden sind, müssen Sie Folgendes berücksichtigen, um ein optimales Routing (mit eBGP) sicherzustellen:

- Fügen Sie der eBGP-Routeradresse eine statische Route hinzu. Zusätzlich zur Standardroute, die den gesamten Datenverkehr an Prisma Access sendet, müssen Sie lokal auf dem IPSec-fähigen Gerät oder Router im Remote-Netzwerk eine statische Route hinzufügen.
- Filtern Sie die Routen, die vom IPSec-fähigen Gerät oder Router in der Zentrale an die eBGP-Peers an anderen direkt verbundenen Standorten mitgeteilt werden. Es hat sich bewährt, den BGP-Router in der Zentrale so zu konfigurieren, dass er nur Routen mitteilt, die Sie über den WAN-Link zulassen möchten. Sie stellen sicher, dass der eBGP-Router in der Zentrale keine Routen mitteilt, die von Prisma Access zu anderen Remote-Netzwerkstandorten bestehen, die durch Prisma Access gesichert werden. In diesem Beispiel teilt der eBGP-Router in der Zentrale nur Routen mit, die Mitarbeiter aus der Zweigstelle benötigen, um eine Verbindung zu den Servern (Subnetzen) in der Zentrale herzustellen.

Die folgende Abbildung zeigt ein Einzelhandelsgeschäft mit zwei Pfaden zu den Servern am Standort der Zentrale. Bei einem der Pfade handelt es sich um einen WAN-Link, der Mitarbeitern, die auf Server in der Zentrale zugreifen, direkte Konnektivität bietet, der andere Pfad sichert den von anderen Benutzern an diesem Standort generierten Datenverkehr. Der Datenverkehr, der durch Kunden generiert wird, die über WLAN auf die Website des Händlers zugreifen oder den Kiosk in der Filiale nutzen, um den Bestand zu überprüfen. Dieser Datenverkehr wird durch den Tunnel an das Remote-Netzwerk und weiter an die Zentrale gesendet.

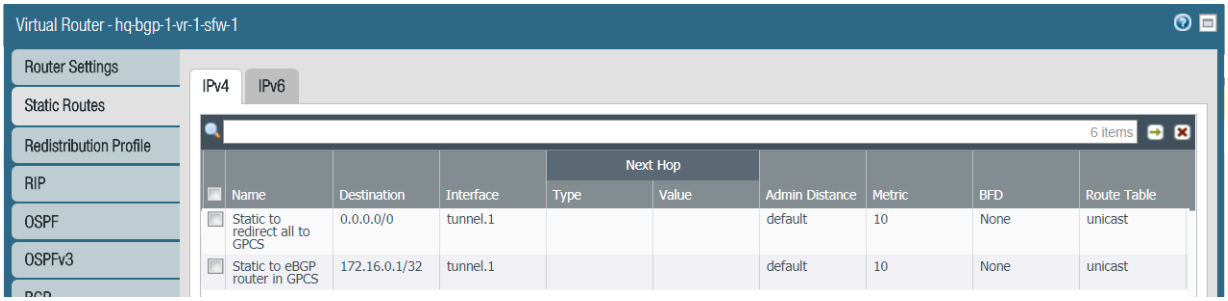
 ©2025 Palo Alto Networks, Inc.




Erstellen Sie zum Einrichten dieser Konfiguration eine Remote-Netzwerkverbindung und eine Dienstverbindung, um die Standorte des Remote-Netzwerks und der Zentrale einzubinden. Die folgenden Details zeigen, wie Sie die Routerkonfiguration an jedem Standort so einrichten können, um ein optimales Routing zu gewährleisten:

**STEP 1 |** Fügen Sie die statischen Routen auf Ihrem Router oder lokalen IPSec-fähigen Gerät am Remote-Netzwerkstandort hinzu.

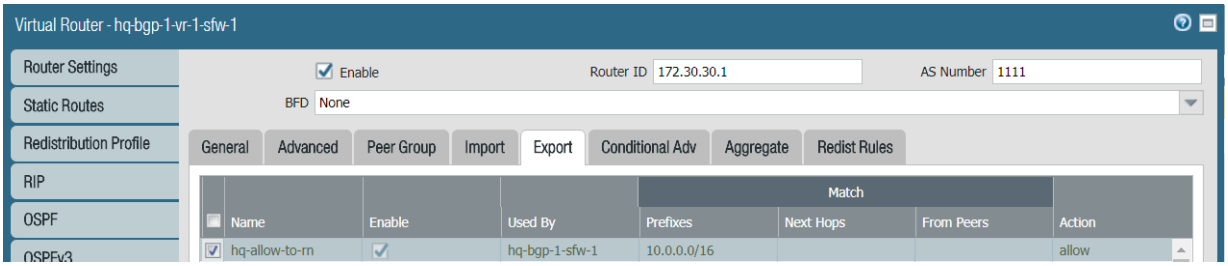
Wenn Sie über eine Palo Alto Networks-Firewall im Edge-Bereich des WAN-Links verfügen, dann wählen Sie**Netzwerk** > **Virtuelle Router** > **Statische Routen** und **Hinzufügen** aus, um die statischen Routen hinzuzufügen:




 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Konfigurieren Sie die Routen, die Sie über den WAN-Link an einen anderen, direkt verbundenen Standort mitteilen möchten.

In diesem Beispiel müssen Sie diesen Arbeitsschritt am Standort der Zentrale konfigurieren. Wenn Sie über eine lokale Palo Alto Networks-Firewall im Edge-Bereich des WAN-Links verfügen, können Sie die Routenumverteilung einrichten und konfigurieren, welche BGP-Routen über **Netzwerk** > **Virtuelle Router** > **BGP** exportiert werden sollen.




 ©2025 Palo Alto Networks, Inc.

# QoS für Remote-Netzwerke

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz<br>❑ Minimum Required Prisma Access Version: 3.0 Bevorzugt |

Neue Prisma Access-Bereitstellungen binden die Bandbreite für Remote-Netzwerke nach Compute-Standort ein. Wenn Sie QoS mit Remote-Netzwerken verwenden möchten, aktivieren oder deaktivieren Sie QoS und geben Sie die garantierte Bandbreite auf der Ebene des Compute-Standorts an. Dennoch können Sie QoS und die garantierte Bandbreite auf Standortebene weiterhin anpassen, indem Sie die Bandbreite pro Standort anpassen.

Prisma Access teilt die Bandbreite des Compute-Standorts mit *IPSec-Terminierungsknoten* auf. Jeder IPSec-Terminierungsknoten kann Ihnen maximal 1.000 Mbit/s Bandbreite zur Verfügung stellen. Wenn Sie einem Compute-Standort mehr als 1.000 Mbit/s Bandbreite zuweisen, stellt Ihnen Prisma Access zusätzliche IPSec-Terminierungsknoten zur Verfügung.

- Strata Cloud Manager
- Panorama

## QoS für Remote-Netzwerke (Strata Cloud Manager)

Verwenden Sie QoS, um den kritischen Datenverkehr in Ihren Remote-Netzwerken mit Priorität zu übertragen und die maximalen und garantierten Bandbreiten für Remote-Netzwerkstandorte an einem Compute-Standort festzulegen.

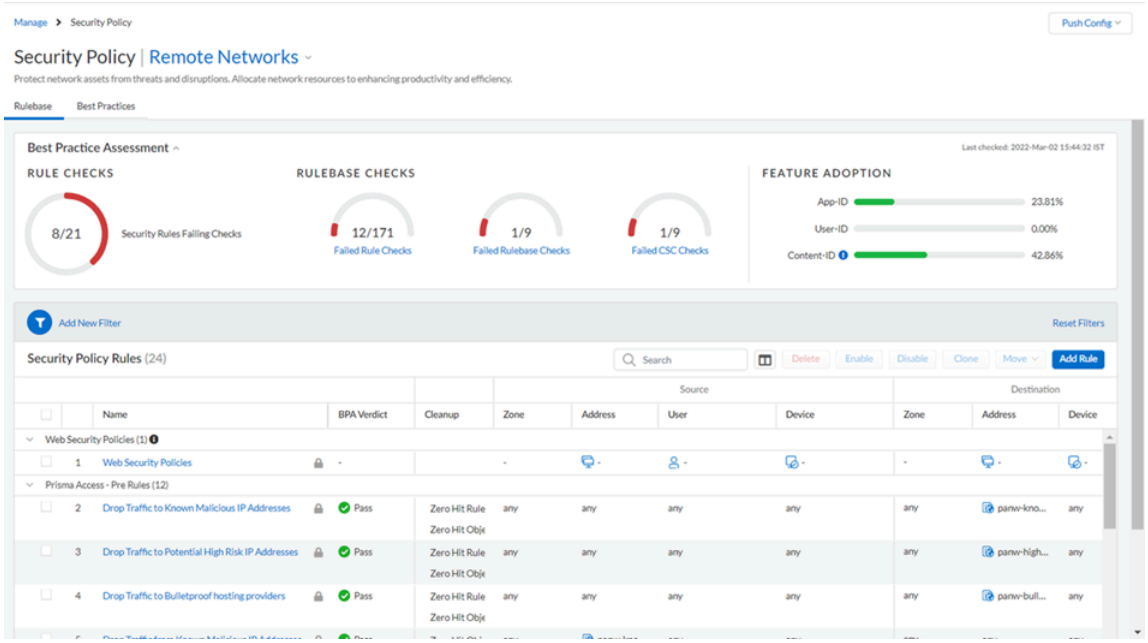
 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** Markieren Sie den Datenverkehr, für den Sie QoS-Behandlung erhalten möchten.

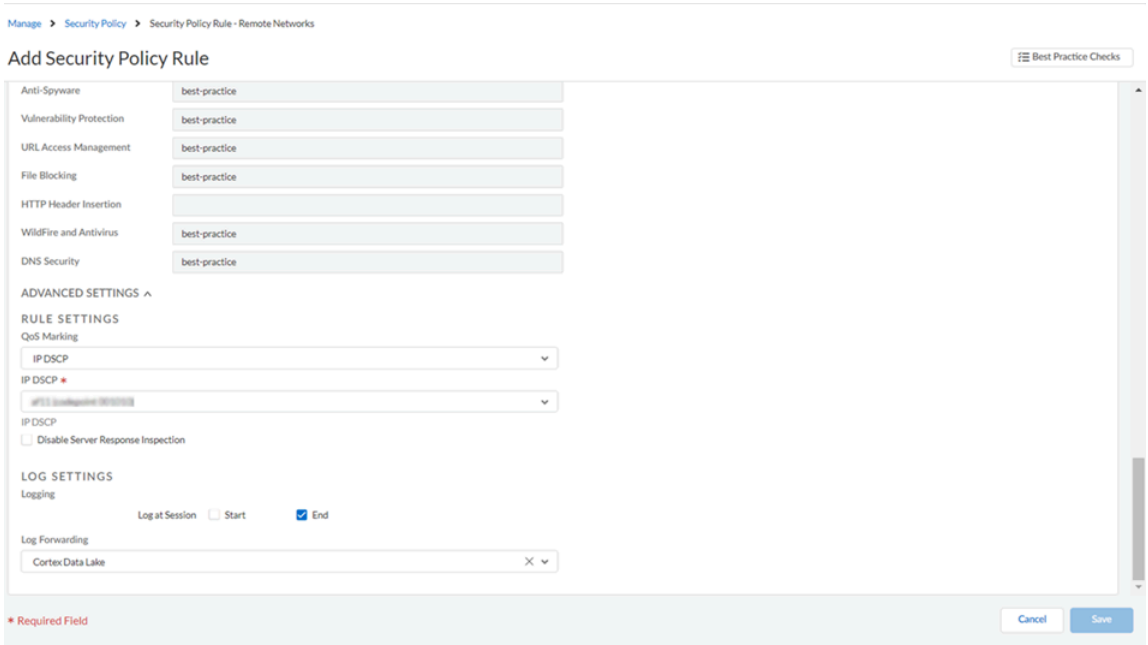
1. Wählen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Sicherheitsdienste** > **Sicherheitsrichtlinie** aus.

   Stellen Sie sicher, dass Sie die Richtlinie für Remote-Netzwerke erstellen.

2. **Regel hinzufügen**.




3. Markieren Sie den eingehenden Datenverkehr, indem Sie in **Erweiterte Einstellungen** einen DSCP-Wert zuweisen und die Richtlinie speichern.



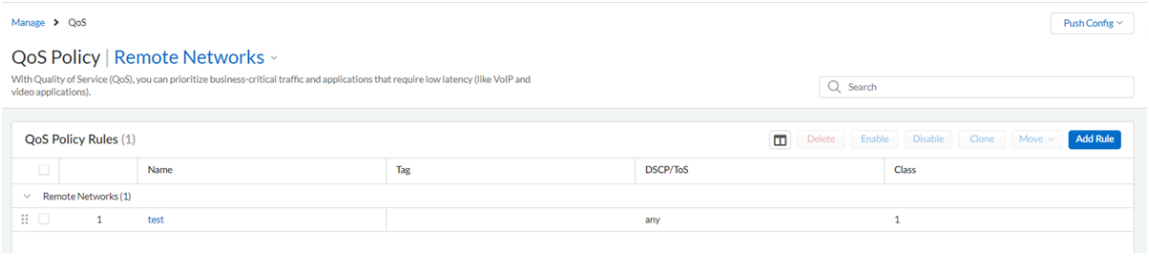

**STEP 2 |** Fügen Sie einzelne oder mehrere QoS-Richtlinienregeln hinzu.

Sie verwenden QoS-Richtlinien, um die DSCP-Markierung an eine von acht verfügbaren Klassen zu binden. In den nächsten Schritten definieren Sie die Behandlung, die eine QoS-

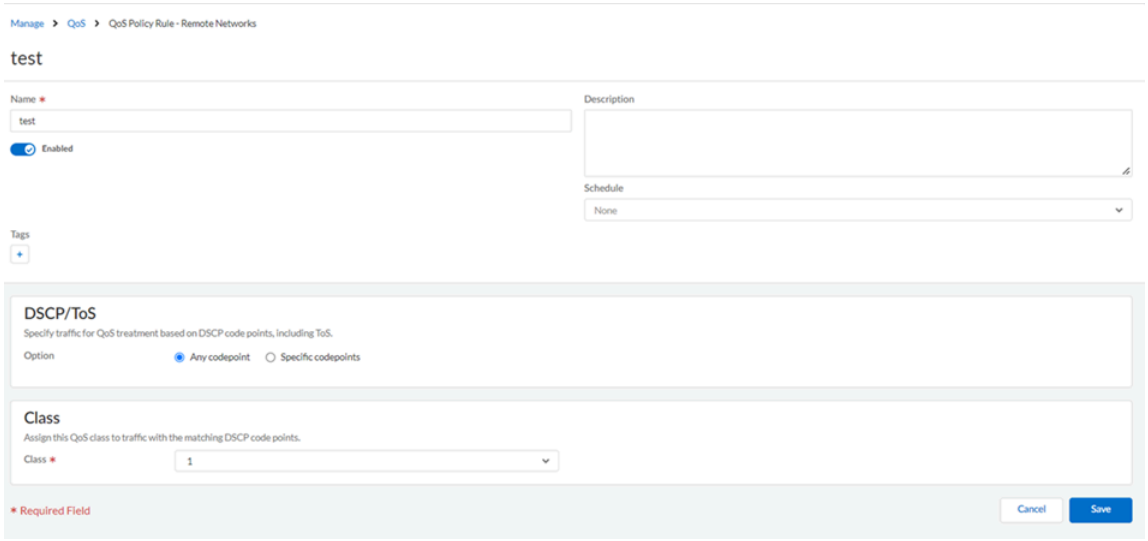
 ©2025 Palo Alto Networks, Inc.

Klasse erhält. Die QoS-Klasse bestimmt die Priorität und Bandbreite für den Datenverkehr, der der QoS-Richtlinienregel entspricht.

1. Wählen Sie **Überwachen** > **Netzwerkdienste** > **QoS** aus.
2. **Regel hinzufügen**.




3. Geben Sie Werte ein und speichern Sie die Richtlinie.



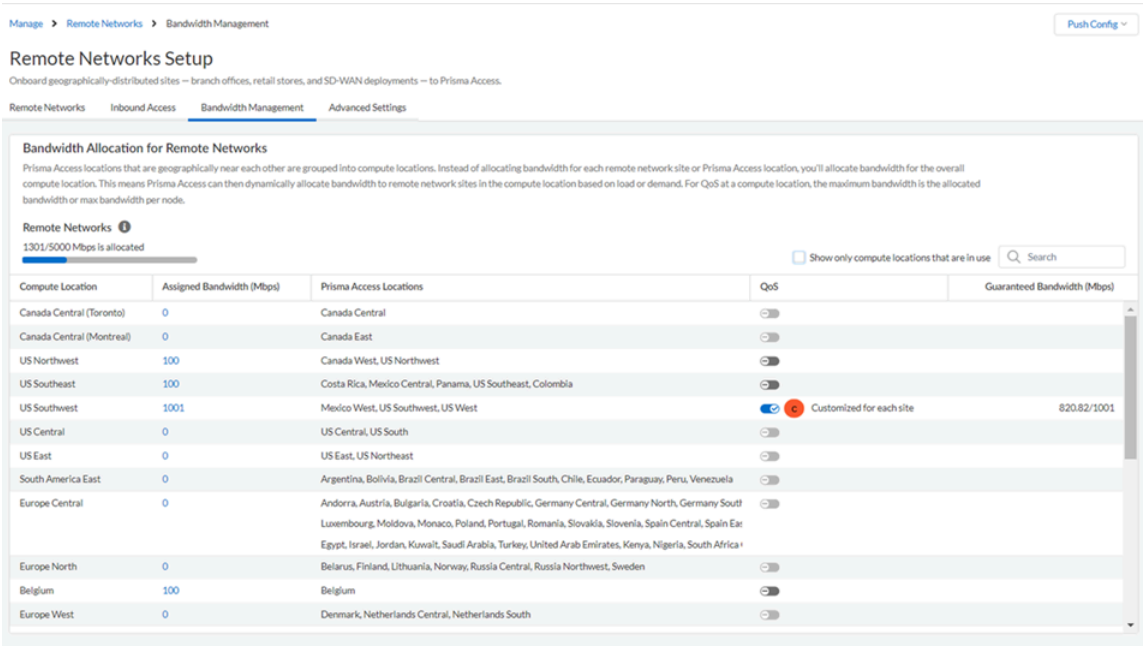

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Aktivieren Sie QoS für Ihre Remote-Netzwerkstandorte.

1. Wählen Sie **Verwalten** > **Diensteinrichtung** > **Remote-Netzwerke** > **Bandbreitenverwaltung** aus.
2. Bestimmen Sie die Prisma Access-Standorte, an denen Sie QoS bereitstellen möchten, und suchen Sie dann den Compute-Standort, der den einzelnen Prisma Access-Standorten entspricht.

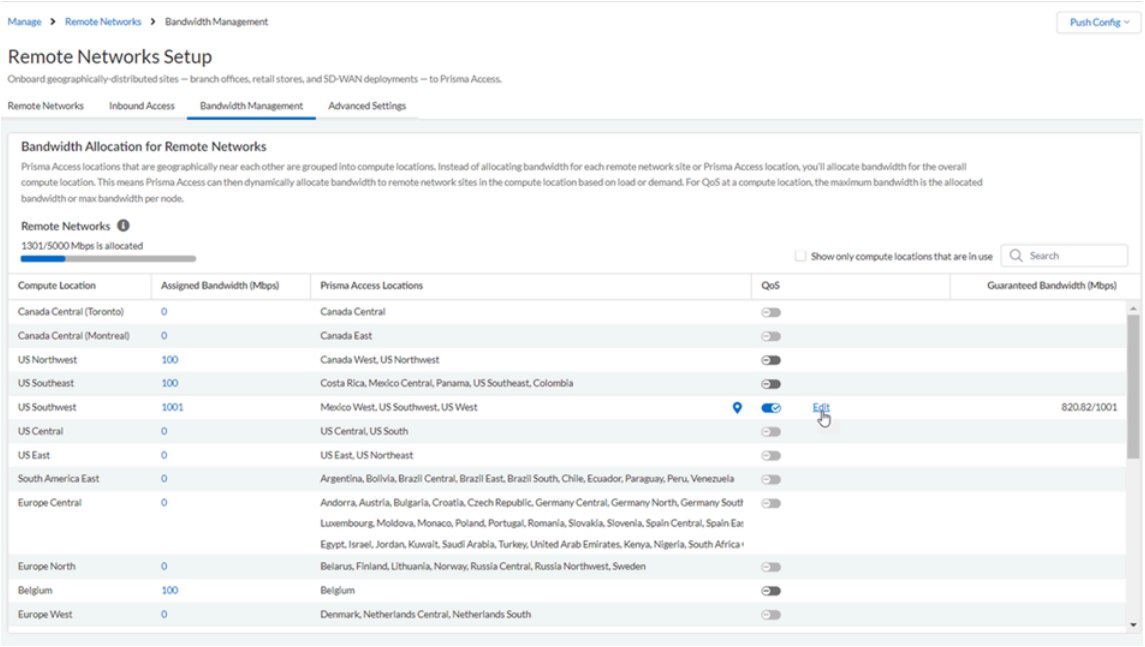
   Jedem Prisma Access-Standort wird Bandbreite von seinem Compute-Standort zugewiesen. Sie müssen den Namen des Compute-Standorts für die Standorte kennen, an denen Sie QoS zuweisen möchten.
3. Aktivieren Sie QoS auf Ebene eines Compute-Standorts in der Spalte **QoS**.

   Die von Ihnen eingegebenen Einstellungen gelten für alle Standorte, die diesem Compute-Standort entsprechen.




 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** **Bearbeiten** Sie die QoS-Einstellungen für den Compute-Standort.




1. Wählen Sie das garantierte Bandbreitenverhältnis aus, das auf der gesamten zugewiesenen Bandbreite für den Compute-Standort basiert.

   Wenn Sie beispielsweise für den Compute-Standort USA (Südwest) eine Bandbreite von 1.001 Mbit/s zugewiesen haben und ein **garantiertes Bandbreitenverhältnis** von 82 % eingeben, beträgt die garantierte Bandbreite für diesen Compute-Standort 820,82 Mbit/s.

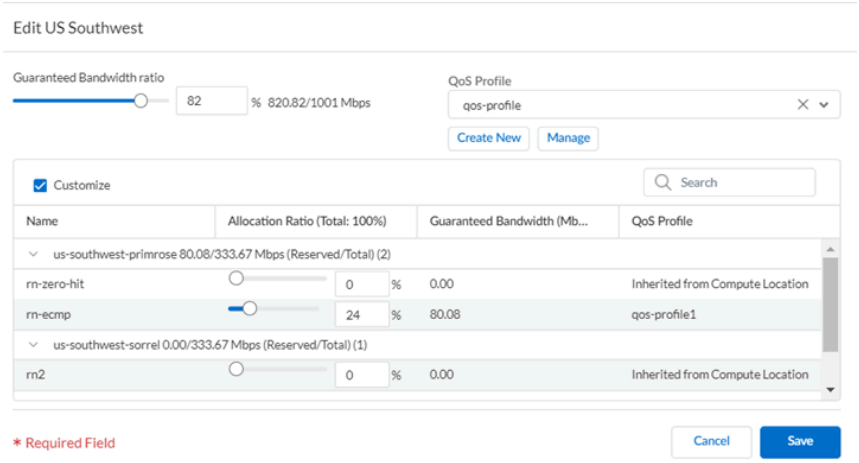
   Standardmäßig wird jedem Remote-Netzwerk ein Prozentsatz zugewiesen, der der Anzahl der Verbindungen entspricht. Bei 4 Verbindungen an einem Compute-Standort und einer garantierten Gesamtbandbreite von 820,82 Mbit/s erhält beispielsweise jeder Standort 25 % dieser Bandbreite, was 205,2 Mbit/s entspricht.

   Wenn die AIOps-Powered ADEM-Lizenz aktiviert ist, wird die Lizenz automatisch für alle Compute-Standorte aktiviert.
2. Verwenden Sie **Neu erstellen**, um ein neues QoS-Profil zu erstellen. Durch Auswahl von **Verwalten** können Sie ein bereits vorhandenes QoS-Profil benutzen.

   Sie verwenden QoS-Profile, um den Datenverkehr am Ausgangspunkt zu gestalten.
3. (Optional) Passen Sie die QoS-Einstellungen für Remote-Netzwerkstandorte an einem Compute-Standort an. Wenn Sie über mehrere Remote-Netzwerke pro Compute-Standort verfügen und entweder das Bandbreitenverhältnis oder das QoS-Profil für

 ©2025 Palo Alto Networks, Inc.

jedes Remote-Netzwerk ändern möchten, wählen Sie **Anpassen** aus und ändern Sie das Bandbreitenzuweisungsverhältnis und/oder das QoS-Profil.




*Wenn Sie **Anpassen** auswählen und dann zusätzliche Remote-Netzwerke im selben IPSec-Terminierungsknoten einbinden, erhalten die neu eingebundenen Standorte ein Zuordnungsverhältnis von 0. Sie müssen dann das Zuordnungsverhältnis zwischen vorhandenen Standorten und den neu eingebundenen Standorten manuell neu verteilen.*

**STEP 5 |** **Speichern** Sie die Änderungen.

**STEP 6 |** **Übertragen** Sie die Konfigurationen.

## QoS für Remote-Netzwerke (Panorama)

Konfigurieren Sie QoS (Quality of Service) in Prisma Access, indem Sie die folgende Aufgabe ausführen.

 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** Fügen Sie einzelne oder mehrere Sicherheitsrichtlinienregeln für Remote-Netzwerke und mobile Benutzer hinzu, um den eingehenden Datenverkehr für QoS zu markieren.

Sie verwenden diese Richtlinien, um einen Datenverkehrsfluss abzugleichen und ihm einen ausgewählten DSCP-Wert zuzuweisen.

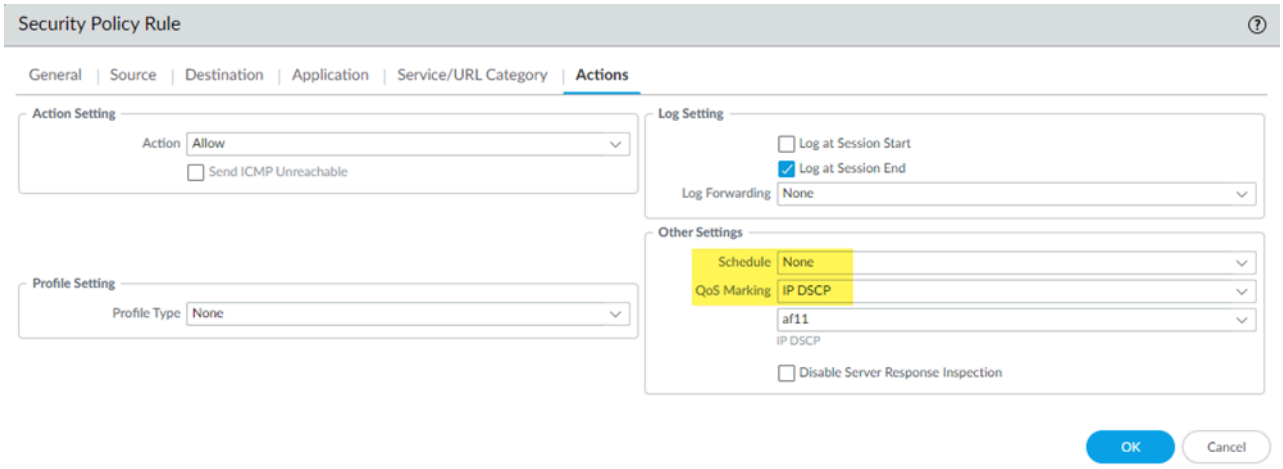
1. Wählen Sie **Richtlinien** > **Sicherheit** > **Vor-Regeln** aus.

   Alternativ hierzu können Sie auch **Richtlinien** > **Sicherheit** > **Nach-Regeln** auswählen, um am Ende der Regelreihenfolge eine Regel hinzuzufügen, die nach einer Vor-Regel ausgewertet wird.

   *Vergewissern Sie sich, dass Sie die richtige **Gerätegruppe** auswählen. Um eine Sicherheitsregel für ein Remote-Netzwerk zu erstellen, wählen Sie die Gerätegruppe für das Remote-Netzwerk aus (z. B. **Remote_Network_Device_Group**). Wählen Sie für mobile Benutzer die Gerätegruppe für die mobilen Benutzer aus (z. B. **Mobile_User_Device_Group**).*
2. Anschließend müssen Sie eine Sicherheitsrichtlinienregel **hinzufügen**.
3. Geben Sie einen **Namen** für die Regel ein.
4. Definieren Sie die Übereinstimmungskriterien für die Quell- oder Zielfelder im Paket.

   Weitere Informationen finden Sie unter Erstellen einer Sicherheitsrichtlinienregel.
5. Klicken Sie auf **Aktionen** und wählen Sie dann die **QoS-Markierung IP-DSCP** oder **IP-Präzedenz** aus.
6. Geben Sie den QoS-Wert im binären Format ein oder wählen Sie den Wert in der Dropdown-Liste aus.

   Der folgende Screenshot zeigt eine Sicherheitsrichtlinienregel, die Datenverkehr abgleicht, der mit dem **IP-DSCP**-Wert **af11** übereinstimmt.




 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Fügen Sie einzelne oder mehrere QoS-Richtlinienregeln hinzu.

Sie verwenden QoS-Richtlinien, um die DSCP-Markierung an eine von acht verfügbaren Klassen zu binden. Sie verwenden diese Klassen später, wenn Sie ein oder mehrere QoS-Profile erstellen.

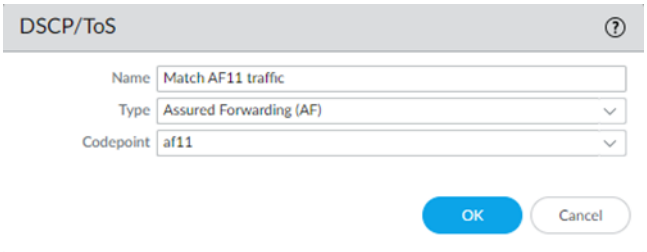
1. Wählen Sie **Richtlinien** > **QoS** > **Vor-Regeln** aus.

   Alternativ hierzu können Sie Nach-Regeln (**Richtlinien** > **QoS** > **Nach-Regeln**) verwenden, um am Ende der Regelreihenfolge eine Regel hinzuzufügen, die nach einer Vor-Regel ausgewertet wird.

   *Dienstverbindungen unterstützen keine QoS-Nach-Regeln. Verwenden Sie Vor-Regeln nur mit Dienstverbindungen.*

   Vergewissern Sie sich, dass Sie die richtige **Gerätegruppe** für die Dienstverbindung (z. B. **Service_Conn_Device_Group**) oder eine Remote-Netzwerkverbindung (z. B. **Remote_Network_Device_Group**) ausgewählt haben. Wenn für eine Regel in einer Gruppe gemeinsam genutzter Geräte Werte definiert sind, die von den Werten unter **Allgemein**, **DSCP/ToS** und **Andere** in den Einstellungsbereichen abweichen, wendet Prisma Access die Regel nicht auf das Remote-Netzwerk und die Dienstverbindung an.
2. Verwenden Sie **Hinzufügen**, um eine QoS-Richtlinienregel hinzuzufügen.
3. Klicken Sie auf **Allgemein** und geben Sie einen Namen für die Richtlinienregel ein.
4. Klicken Sie auf die Registerkarte **DSCP/ToS** und dann auf **Codepunkte** und **Hinzufügen**, um einzelne oder mehrere neue Codepunkte hinzuzufügen.

   Für Clean Pipe-Bereitstellungen können Sie zusätzliche QoS-Einstellungen in der Richtlinie angeben, z. B. Quelle, Ziel oder Anwendung.
5. Geben Sie einen **Namen** für die DSCP/ToS-Regel an und wählen Sie dann eine **Art** und einen **Codepunkt** aus.




   Alternativ hierzu können Sie den Standardwert (**Beliebig**) beibehalten, damit die Richtlinie unabhängig vom DSCP-Wert (Differentiated Services Code Point) oder der für

 ©2025 Palo Alto Networks, Inc.

den Datenverkehr definierten IP-Präzedenz/Dienstart (ToS) den Datenverkehrsabgleich durchführen kann.

6. Klicken Sie auf die Registerkarte **Weitere Einstellungen** und wählen Sie dann die **Klasse** für QoS aus, die der Regel zugewiesen werden soll.

   Definieren Sie Klasseneigenschaften im QoS-Profil.

7. Klicken Sie auf **OK**.




**STEP 3 |** Erstellen Sie einzelne oder mehrere QoS-Profile, um den ausgehenden QoS-Datenverkehr für Dienstverbindungen und Remote-Netzwerkverbindungen zu gestalten.

Sie verwenden Profile, um den Datenverkehr am Ausgangspunkt zu gestalten, indem Sie QoS-Klassen definieren und ihnen eine Bandbreite zuweisen. Sie müssen entweder ein vorhandenes QoS-Profil auswählen oder ein neues QoS-Profil erstellen, wenn Sie QoS für Prisma Access aktivieren.

1. Wählen Sie die richtige Vorlage für das Profil aus, das Sie erstellen möchten (**Remote_Network_Template** oder **Service_Conn_Template**). Wählen Sie dann **Netzwerk** > **Netzwerkprofile** > **QoS-Profil** aus und
2. wählen Sie **Hinzufügen**, um ein Profil hinzuzufügen.
3. Geben Sie einen **Namen** für das Profil ein.
4. Legen Sie die Grenzwerte für die Gesamtbandbreite für die QoS-Profilregel fest.
   - Geben Sie einen Wert für **Ausgang maximal** ein, der für den maximalen Durchsatz (in Mbit/s) für den Datenverkehr steht, der die Dienstverbindung oder Remote-Netzwerkverbindung verlässt.
     - Geben Sie für Dienstverbindungen eine Anzahl von bis zu 1 Gbit/s (1.000 Mbit/s) an.

       *Geben Sie keine Zahl größer als 1 Gbit/s ein. Prisma Access berechnet die Bandbreite der Dienstverbindung pro IPSec-Tunnel der Dienstverbindung und nicht kumulativ über mehrere Tunnel.*
   - Geben Sie für Remote-Netzwerkverbindungen den Wert **0** ein.
   - Geben Sie einen Wert für **Ausgang garantiert** ein. Hierbei handelt es sich um die garantierte Bandbreite für dieses Profil (in Mbit/s).
     - Geben Sie für Dienstverbindungen unter **Ausgang garantiert** einen Wert ein. Hierbei handelt es sich um die garantierte Bandbreite für dieses Profil (in Mbit/s).

       Für den Datenverkehr, der den Wert für „Ausgang garantiert“ überschreitet, wird zwar das beste Ergebnis angestrebt, das jedoch nicht garantiert werden kann.

 ©2025 Palo Alto Networks, Inc.

Garantierte Bandbreite, die jedoch ungenutzt bleibt, steht weiterhin für den gesamten Datenverkehr zur Verfügung.

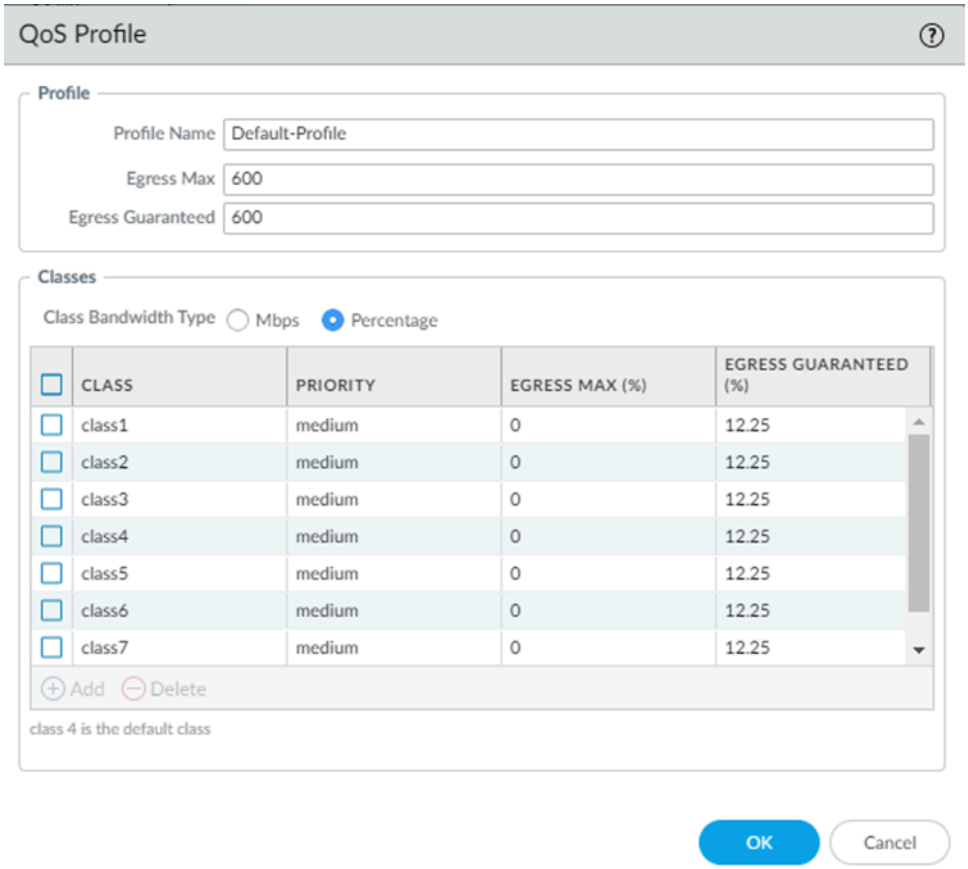
- Geben Sie für Remote-Netzwerkverbindungen den Wert **0** ein.

5. Verwenden Sie im Abschnitt „Klassen“ die Option **Hinzufügen**, um einzelne oder mehrere Klassen hinzuzufügen. Geben Sie an, wie bis zu acht einzelne QoS-Klassen markiert werden sollen.
   - Ändern Sie für QoS-Profile, die von Remote-Netzwerken verwendet werden, um die Bandbreite nach Compute-Standort zuzuweisen, den Wert für **Typ der Klassenbandbreite** in **Prozentsatz**. Geben Sie dann Prozentsätze für die Werte unter **Ausgang maximal** und **Ausgang garantiert** an, die Sie in diesem Bereich eingeben.
   - Geben Sie für QoS-Profile, die von Dienstverbindungen oder Remote-Netzwerken verwendet werden, die Bandbreite nach Standort zuweisen, den Typ **Mbit/s** an.
   - Wählen Sie die Option **Priorität** für die Klasse (entweder **Echtzeit**, **Hoch**, **Mittel**oder **Niedrig**) aus.
   - Geben Sie den Wert für **Ausgang maximal** für Datenverkehr ein, der jeder von Ihnen erstellten QoS-Klasse zugewiesen ist.
     - Geben Sie für Remote-Netzwerke, die die Bandbreite nach Compute-Standort zuweisen, **0** ein.
     - Geben Sie für bandbreitenbasierte QoS-Profile (die von Dienstverbindungen oder Remote-Netzwerken verwendet werden, die Bandbreite nach Standort zuweisen) einen Wert in Mbit/s ein. Der Wert für „Ausgang maximal“ einer QoS-Klasse muss kleiner oder gleich dem Wert für „Ausgang maximal“ für das QoS-Profil sein.
   - Geben Sie unter **Ausgang garantiert** den Prozentsatz oder die Bandbreite in Mbit/s für jede QoS-Klasse ein. Geben Sie für QoS-Profile für Remote-Netzwerke einen Prozentsatz ein.

     Die garantierte Bandbreite, die einer Klasse zugewiesen wird, ist nicht für diese Klasse reserviert – Bandbreite, die nicht verbraucht wird, bleibt weiterhin für den gesamten Datenverkehr verfügbar. Wenn eine Datenverkehrsklasse die garantierte Ausgangsbandbreite überschreitet, leitet Prisma Access diesen Datenverkehr nach dem Best-Effort-Prinzip weiter.

 ©2025 Palo Alto Networks, Inc.

- Geben Sie den **Typ der Klassenbandbreite** für das Profil ein.




6. Klicken Sie auf **OK**.

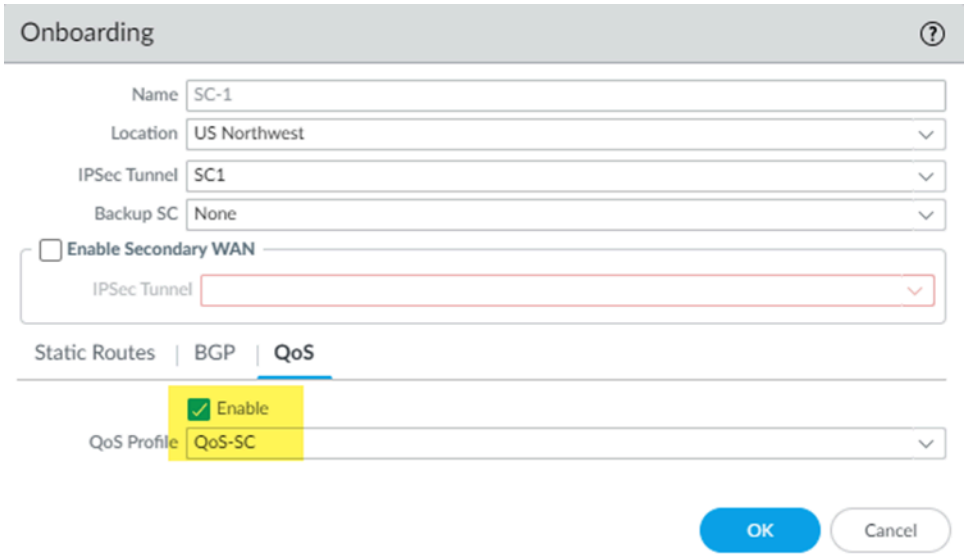
**STEP 4 |** (Nur Dienstverbindungen) Aktivieren Sie QoS für die Dienstverbindung, und wenden Sie das QoS-Profil auf die Verbindung an.

1. Aktivieren Sie QoS, indem Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Diensteinrichtung** auswählen. Wählen Sie dann einen Wert für **Verbindungsname** aus und klicken Sie auf die Registerkarte **QoS** und führen Sie die **Aktivierung** von QoS durch.

   Wenn Sie die Bandbreite des Remote-Netzwerks auf Basis von Prisma Access-Remote-Netzwerke anstatt des Compute-Standorts zuweisen, müssen Sie QoS auf die gleiche Weise wie Dienstverbindungen konfigurieren. Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Remote-Netzwerke** und dann unter **Name** den Hypertext für eine Remote-Netzwerkverbindung aus. Klicken Sie nun auf die Registerkarte **QoS** und führen Sie dort die **Aktivierung** von QoS durch. Wenn Sie Bandbreite nach Compute-Standort (Standardmethode) zuweisen, fahren Sie mit Schritt 5 fort, um QoS für Remote-Netzwerke zu konfigurieren.

 ©2025 Palo Alto Networks, Inc.

2. Wählen Sie ein QoS-Profil aus und klicken Sie auf **OK**.




**STEP 5 |** (Remote-Netzwerkbereitstellungen, die Bandbreite nur nach Compute-Standort zuweisen) Aktivieren Sie QoS für Ihre Remote-Netzwerkstandorte.

1. Bestimmen Sie die Prisma Access-Standorte, an denen Sie QoS bereitstellen möchten. Suchen Sie dann den Compute-Standort, der den einzelnen Standorten entspricht.

   Jedem Standort wird Bandbreite von seinem Compute-Standort zugewiesen, und Sie müssen den Namen des Compute-Standorts für die Standorte kennen, an denen Sie QoS zuweisen möchten. Eine Liste der Zuordnungen zwischen Compute-Standorten und Standorten finden Sie unter Prisma Access Standorte. Alternativ hierzu können Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Remote-Netzwerke** > **Aggregierte Bandbreite** auswählen und dann auf das Zahnradsymbol klicken. Die Zuordnungen werden in den Spalten **Compute-Standort** und **Prisma Access-Standort** angezeigt.
2. Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Remote-Netzwerke** > **Einstellungen** aus und klicken Sie dann auf das Zahnradsymbol, um die Einstellungen zu bearbeiten, und wählen Sie **QoS** aus.
3. **Aktivieren von QoS** auf der Ebene des Compute-Standorts.

   Die von Ihnen eingegebenen Einstellungen gelten für alle Standorte, die diesem Compute-Standort entsprechen.


©2025 Palo Alto Networks, Inc.

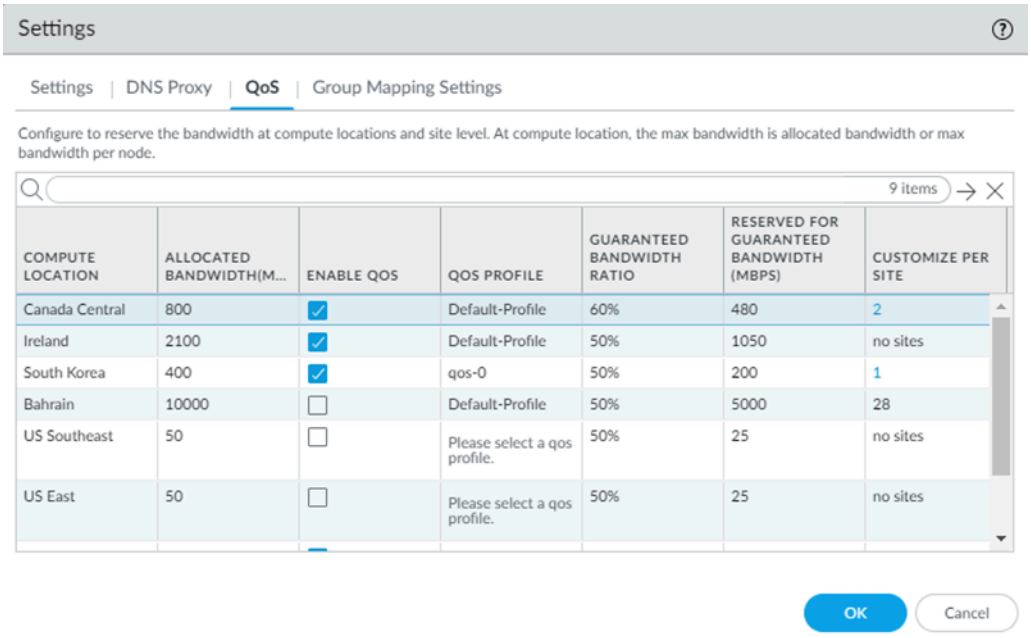
4. Geben Sie Werte für **QoS-Profil**, **Garantiertes Bandbreitenverhältnis** und **Reserviert für garantierte Bandbreite (Mbit/s)** ein.

   - Geben Sie das **QoS-Profil** ein, das für diesen Compute-Standort verwendet werden soll.

     Wenn Sie unterschiedliche QoS-Profile für die einzelnen Remote-Netzwerke verwenden möchten, dann benutzen Sie **Pro Standort anpassen**. Befolgen Sie dabei die in einem späteren Schritt beschriebene Vorgehensweise.
   - Geben Sie einen Wert für Garantiertes Bandbreitenverhältnis ein, bei dem es sich um ein Verhältnis handelt, das auf der gesamten zugewiesenen Bandbreite für den Compute-Standort basiert.

     Wenn Sie z. B. eine Bandbreite von 800 Mbit/s für den Compute-Standort „Kanada (zentral)“ zugewiesen haben und ein **Garantiertes Bandbreitenverhältnis** von **60 %** eingeben, dann beträgt der Wert für Garantierte Bandbreite für diesen Compute-Standort 480 Mbit/s.
   - Geben Sie die Bandbreite ein, die unter **Reserviert für garantierte Bandbreite (Mbit/s)** für das QoS-Profil und den Compute-Standort angegeben ist, das bzw. den Sie ausgewählt haben.

   Der folgende Screenshot zeigt QoS, das für die Compute-Standorte „Kanada (zentral)“, „Irland“ und „Südkorea“ aktiviert wurde.




5. (Optional) Wenn Sie über mehrere Remote-Netzwerkverbindungen pro Compute-Standort verfügen und entweder das Bandbreitenverhältnis oder das QoS-Profil für jeden Standort ändern möchten, führen Sie ein Onboarding Ihrer Remote-

 ©2025 Palo Alto Networks, Inc.

Netzwerkstandorte durch. Wählen Sie anschließend **Pro Standort anpassen** aus und ändern Sie das Bandbreitenzuweisungsverhältnis und/oder das QoS-Profil.

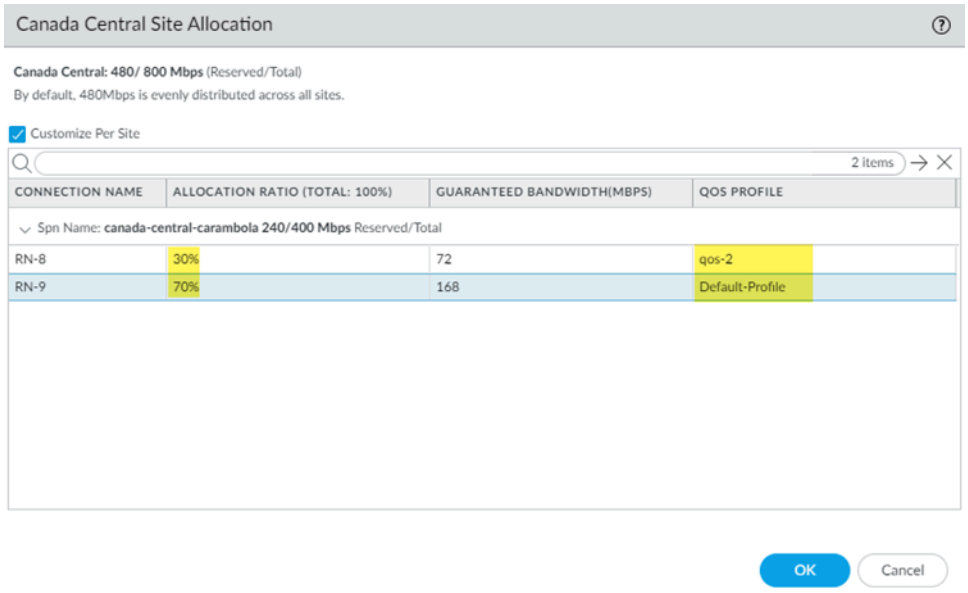
- Um die garantierte Bandbreite anzupassen, klicken Sie auf die Zahl im Bereich **Pro Standort anpassen**. Wählen Sie **Pro Standort anpassen** aus und ändern Sie das **Zuweisungsverhältnis**.

  Standardmäßig erhält jede Remote-Verbindung einen festgelegten Prozentsatz, der der Anzahl der Verbindungen entspricht. Bei vier Verbindungen an einem Compute-Standort und einer garantierten Gesamtbandbreite von 100 Mbit/s erhält beispielsweise jeder Standort 25 % dieser Bandbreite, was 25 Mbit/s entspricht.

  *Wenn Sie **Pro Standort anpassen** auswählen und dann zusätzliche Remote-Netzwerke in denselben IPSec-Terminierungsknoten einbinden, erhalten die neu eingebundenen Standorte ein Zuweisungsverhältnis von **0**. Sie müssen dann das Zuordnungsverhältnis zwischen vorhandenen Standorten und dem neu eingebundenen Standort manuell neu verteilen.*

  *Wenn Sie nicht die Option **Pro Standort anpassen** verwenden, wird der Bandbreitenprozentsatz automatisch neu verteilt, wenn Sie Remote-Netzwerke hinzufügen. Wenn Sie z. B. **Pro Standort anpassen** nicht ausgewählt und vier Remote-Netzwerke eingebunden haben, verfügt jedes dieser Remote-Netzwerke über ein Zuweisungsverhältnis von 25 %. Wenn Sie ein fünftes Remote-Netzwerk hinzufügen, wird das zur Verfügung stehende Volumen neu verteilt und alle fünf Standorte erhalten eine garantierte Bandbreite von 20 %.*

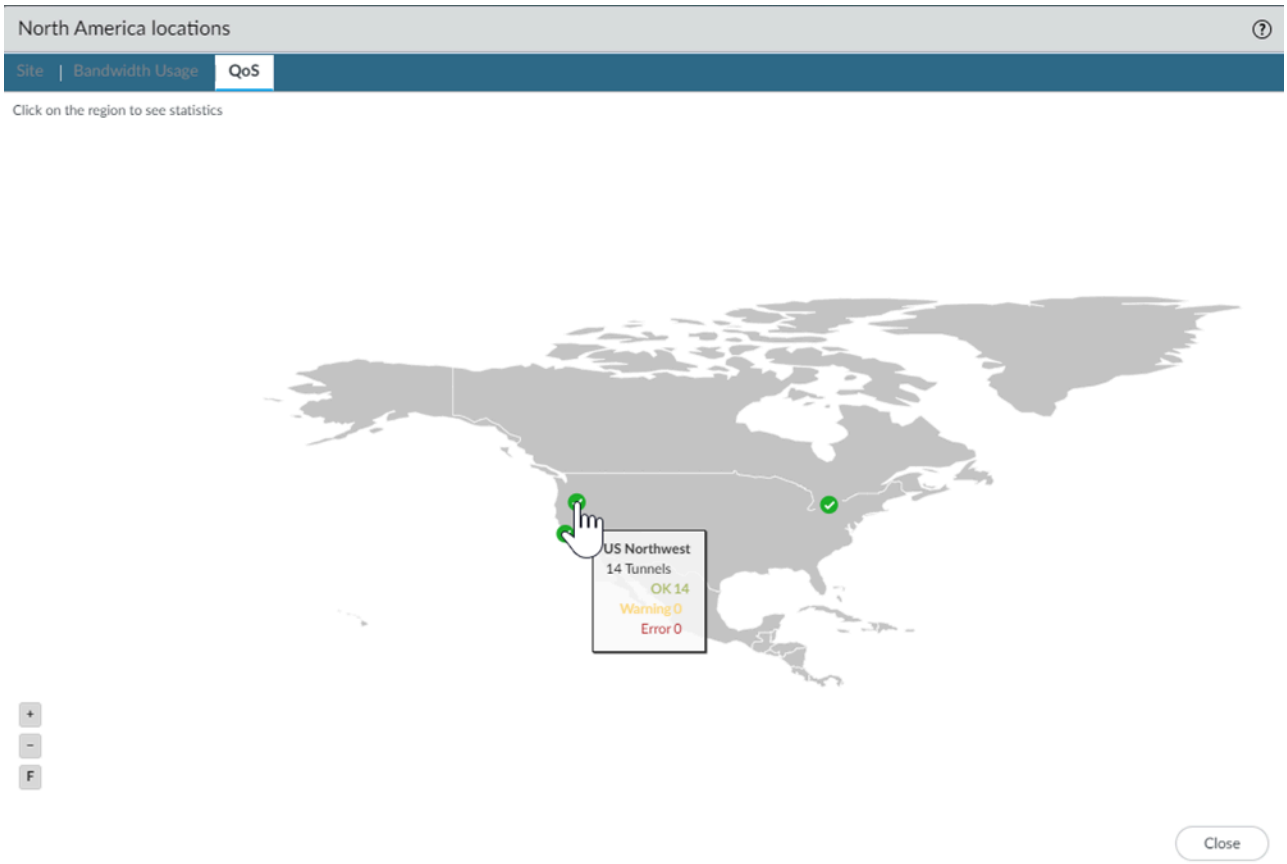
- Wenn Sie ein QoS-Profil auf Remote-Netzwerkebene angeben möchten, wählen Sie ein anderes **QoS-Profil** für das Remote-Netzwerk aus.




 ©2025 Palo Alto Networks, Inc.

**STEP 6 |** Überprüfen Sie den QoS-Status.

- Wählen Sie für Remote-Netzwerke **Panorama** > **Cloud Services** > **Status** > **Überwachen** > **Remote-Netzwerke** und dann eine Region in der Karte aus. Wählen Sie anschließend **QoS**und dann einen Standort aus.

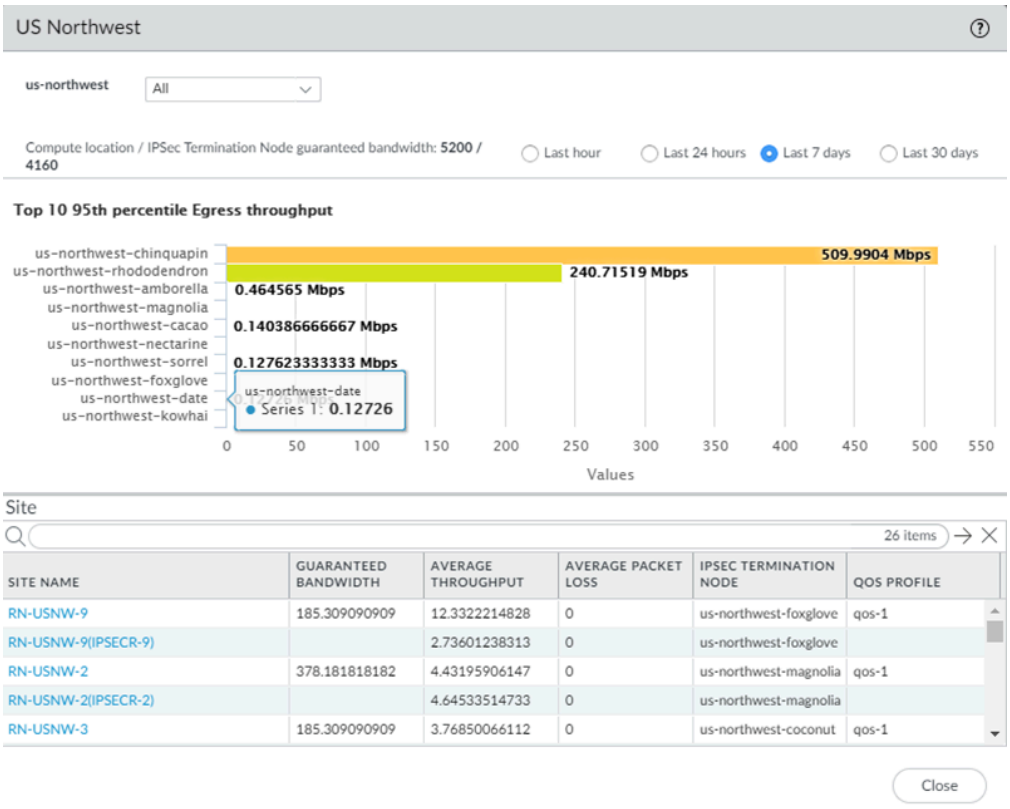



Remote-Netzwerkstatistiken werden für die 10 IPSec-Terminierungsknoten mit dem höchsten Durchsatz angezeigt. Prisma Access verwendet den 95. Perzentilstandard zum

 ©2025 Palo Alto Networks, Inc.

Sammeln von Statistiken, der die Bandbreite bei Spitzenauslastung nachverfolgt und die oberen 5 Prozent der Auslastungsspitzen und großer Bursts ignoriert.

Wählen Sie den Zeitraum (**Letzte Stunde**, **Letzte 24 Stunden**, **Letzte 7 Tage** oder **Letzte 30 Tage**) aus, um Statistiken für den entsprechenden Zeitraum anzuzeigen.

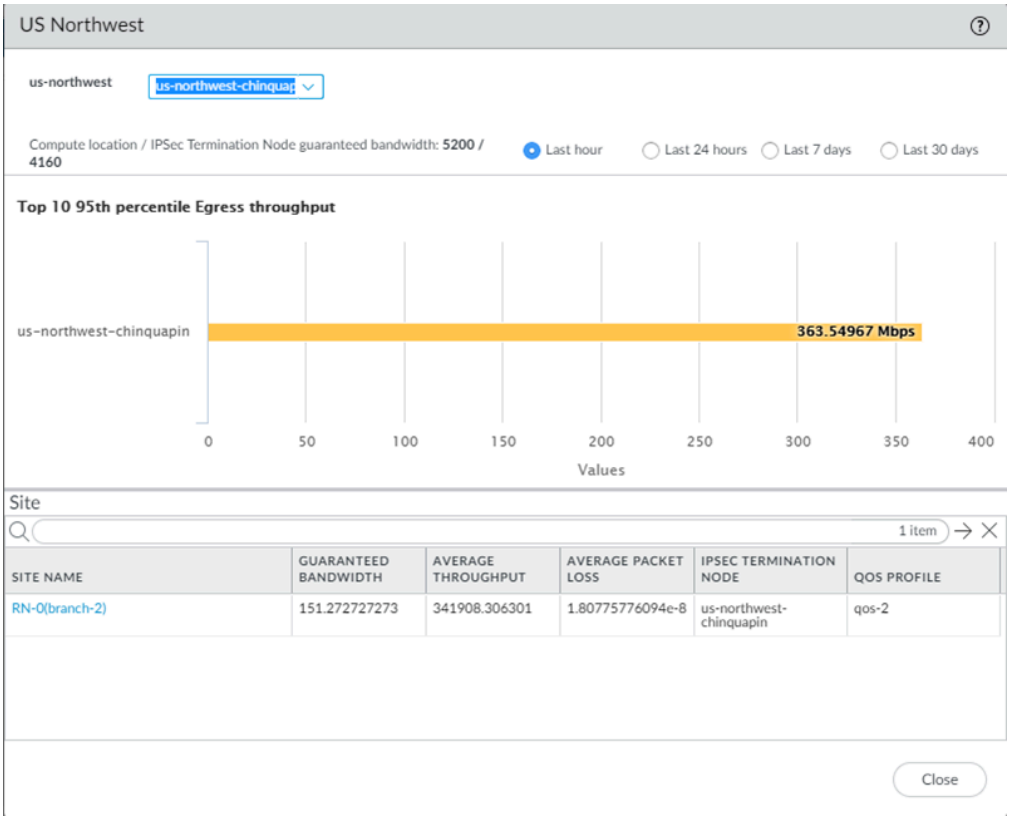



Die Remote-Netzwerke mit der höchsten Auslastung der Ausgangsbandbreite werden im Bereich **Standort** zusammen mit den Statistiken der Standorte der Remote-Netzwerke für **Garantierte Bandbreite**, **Durchschnittlicher Durchsatz**, **Durchschnittlicher Paketverlust** angezeigt. Ebenfalls angezeigt wird der **IPSec-Terminierungsknoten** und das **QoS-Profil**, die vom Remote-Netzwerk verwendet werden. Sie können auch nach einem Standort **suchen**.

Um die Remote-Netzwerke anzuzeigen, die einem bestimmten IPSec-Terminierungsknoten zugeordnet sind, ändern Sie in der Dropdown-Liste oben auf der Seite den Wert **Alle** in einen bestimmten IPSec-Terminierungsknoten, um Statistiken

 ©2025 Palo Alto Networks, Inc.

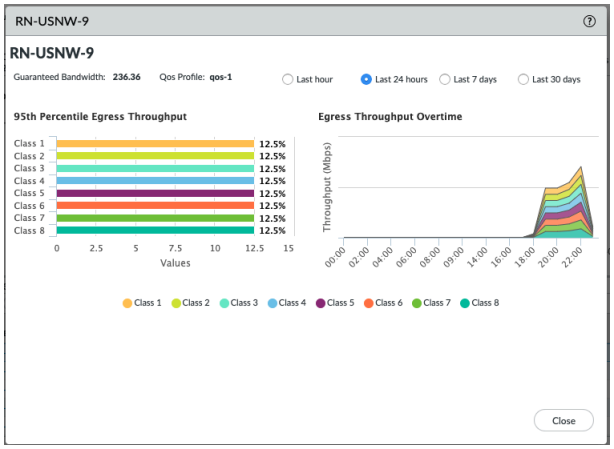
für diesen IPSec-Terminierungsknoten und die Remote-Netzwerke für diesen Standort anzuzeigen.



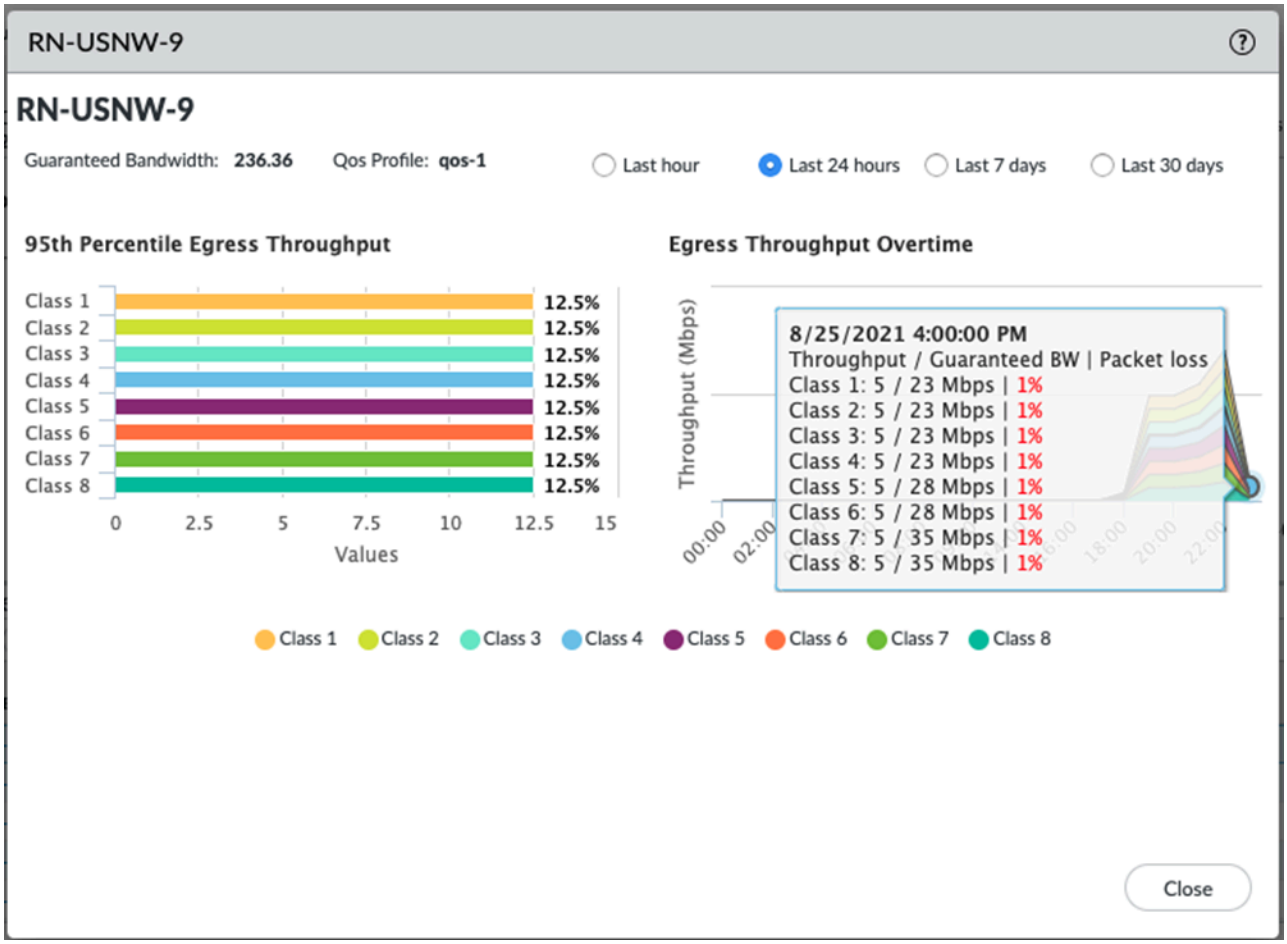

Um den spezifischen Datenverkehr für einen Standort anzuzeigen, der nach QoS-Klasse sortiert ist, klicken Sie auf **Standortname**. Die garantierte Bandbreite, der Ausgangsdurchsatz und der Durchsatz im Zeitverlauf werden für den Remote-

 ©2025 Palo Alto Networks, Inc.

Netzwerkstandort angezeigt. Sie können diese Informationen auch nach der letzten Stunde, den letzten 24 Stunden, den letzten 7 Tagen oder den letzten 30 Tagen sortieren.



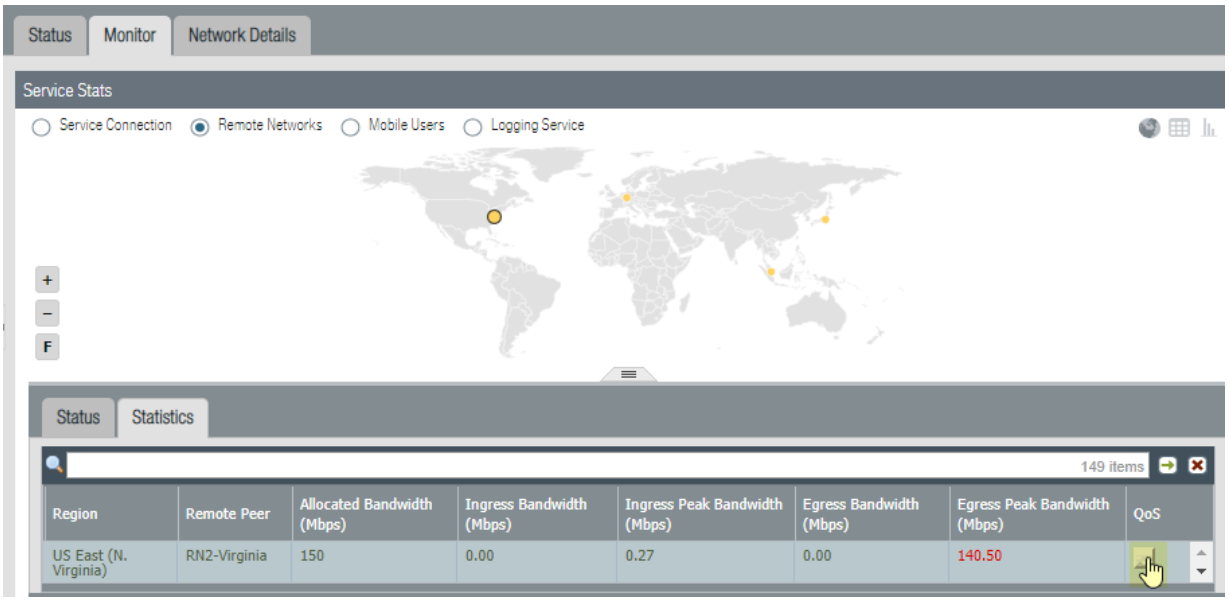

Bewegen Sie den Mauszeiger über das Diagramm auf der rechten Seite, um detaillierte Informationen für einen bestimmten Zeitraum zu erhalten.




- Wählen Sie für Dienstverbindungen **Panorama** > **Cloud Services** > **Status** > **Überwachen** > **Dienstverbindung** und dann eine Region und **Überwachen** für die **Statistik** aus.

Klicken Sie auf **QoS**, um eine Seite mit QoS-Statistiken anzuzeigen.

 ©2025 Palo Alto Networks, Inc.

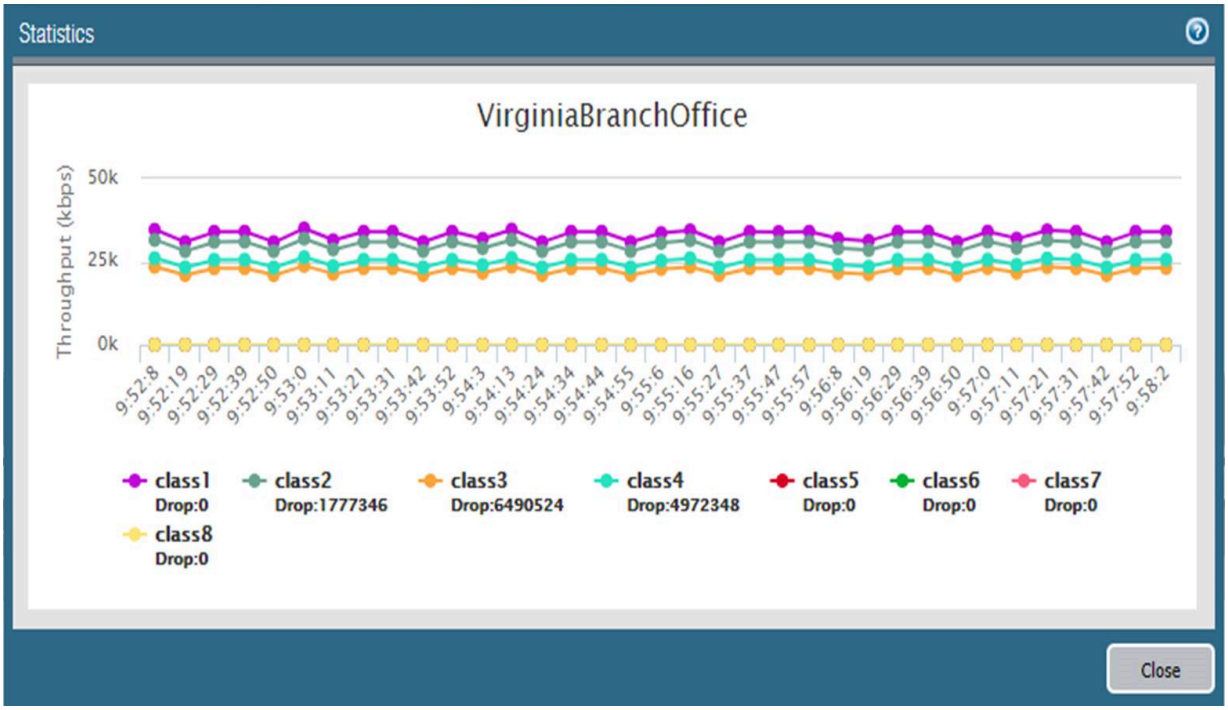



Auf dieser Seite wird ein Diagramm mit QoS-Echtzeit- und QoS-Langzeitstatistiken einschließlich der Anzahl der gelöschten Pakete pro Klasse angezeigt. Dieses Diagramm wird nur für Dienstverbindungen oder Remote-Netzwerkverbindungen angezeigt, für die QoS

 ©2025 Palo Alto Networks, Inc.

aktiviert ist. Es zeigt die letzten fünf Minuten der Netzwerkaktivität über die Verbindung an und wird alle 10 Sekunden aktualisiert.

Die folgende Abbildung zeigt den Datenverkehr, der für die Klassen 1, 2, 3 und 4 übergeben wird. Die Daten unter der Abbildung zeigen die Anzahl der gelöschten Pakete basierend auf der QoS-Konfiguration für die Klassen 2, 3 und 4 an.




Garantierte Bandbreite ändern

# Garantierte Bandbreite ändern

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Wenn Sie mehrere Remote-Netzwerkstandorte haben, die einem IPSec-Terminierungsknoten zugeordnet sind, können Sie die garantierte Bandbreite für jeden Standort ändern. Im folgenden Beispiel möchten Sie, dass der Standort Kanada (Ost) mehr Bandbreite als der Standort Kanada (Mitte) erhält. Führen Sie hierzu die folgenden Schritte aus.

**STEP 1 |** Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Remote-Netzwerke** > **Einstellungen** aus.

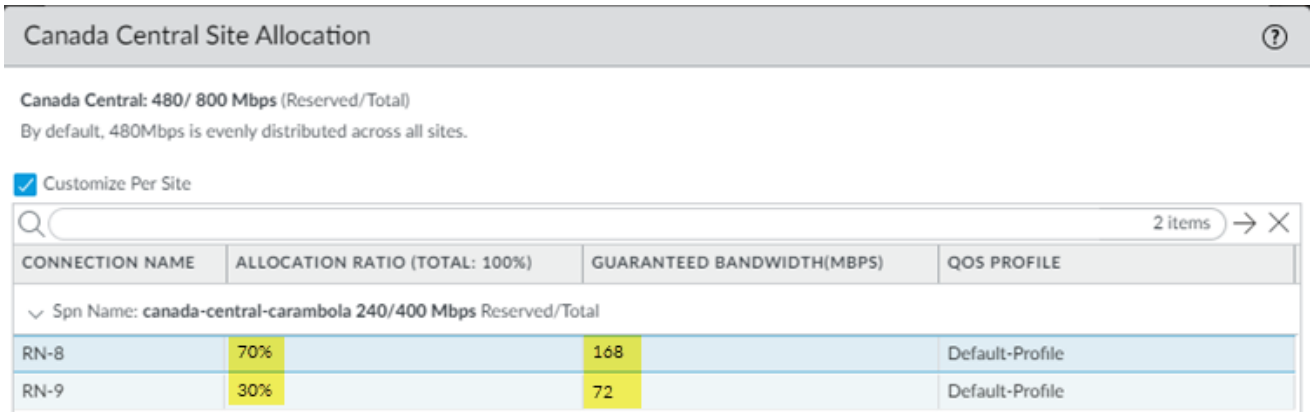
**STEP 2 |** Klicken Sie auf das Zahnradsymbol, um die Einstellungen zu bearbeiten, und wählen Sie dann **QoS** aus.

**STEP 3 |** **Aktivieren Sie QoS**, weisen Sie dem Compute-Standort Kanada (Mitte) ein **QoS-Profil** (in diesem Beispiel **Standardprofil**) und ein **Garantiertes Bandbreitenverhältnis** zu.

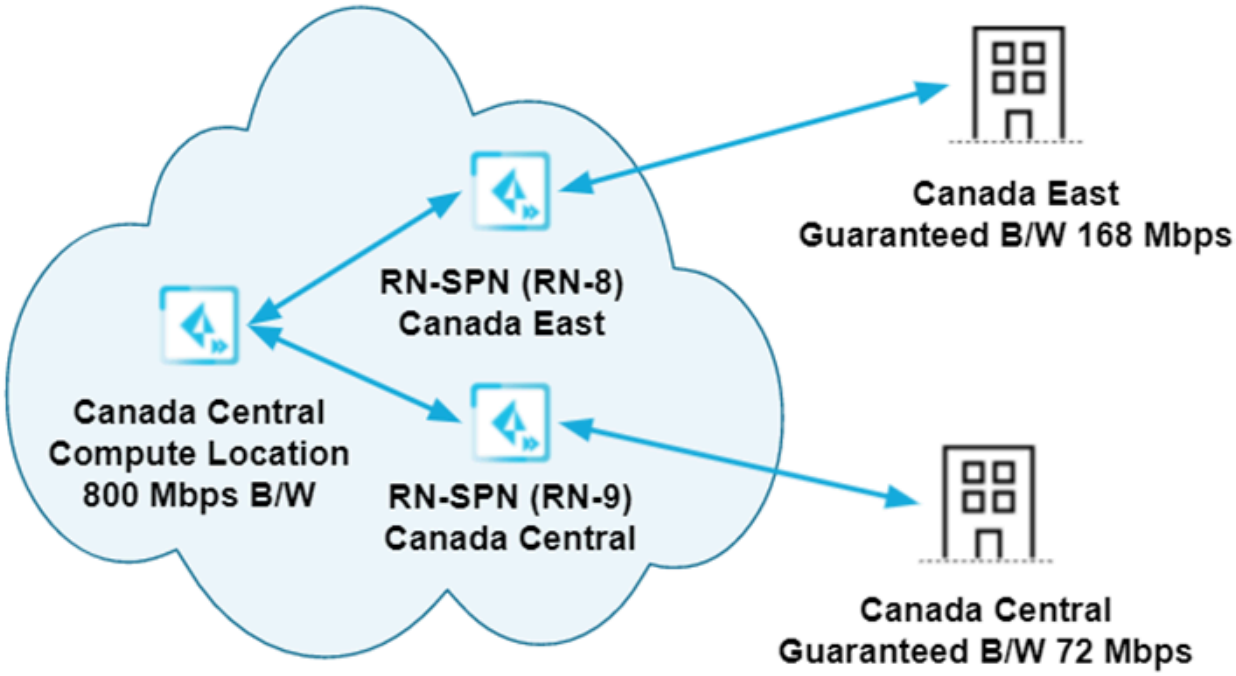
 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** Wählen Sie **Pro Standort anpassen** aus, aktivieren Sie **Pro Standort anpassen** und wenden Sie dann für das Remote-Netzwerk RN-8 (für den Standort Kanada (Ost)) ein höheres **Zuweisungsverhältnis** an als für das Remote-Netzwerk RN-9 (für den Standort Kanada (Mitte)).

Das folgende Beispiel zeigt ein **Zuweisungsverhältnis** von 70 % für RN-8 und 30 % für RN-9 an. Der Wert für **Garantierte Bandbreite (Mbit/s)** ändert sich entsprechend und zeigt die neuen garantierten Bandbreitenbeträge an.




Wenn Ihre Konfiguration abgeschlossen ist, verfügt sie über die folgende garantierte Bandbreitenzuweisung für die beiden Standorte.

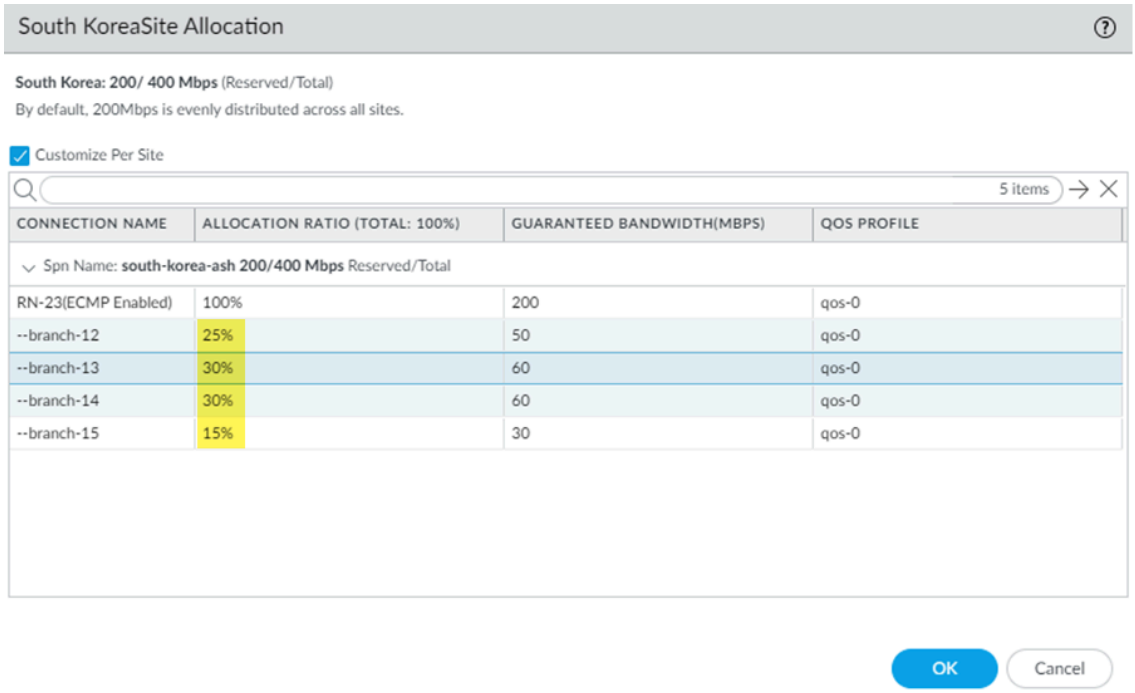



Sie können auch verschiedene QoS-Profile pro Remote-Netzwerkstandort zuweisen. Um verschiedene Profile zuzuweisen, aktivieren Sie die Funktion **Für jeden Standort anpassen** und wählen Sie für jeden Remote-Netzwerkstandort unterschiedliche QoS-Profile aus.

Wenn Sie über ein Remote-Netzwerk verfügen, in dem ECMP aktiviert ist, um mehrere IPSec-Tunnel für ein einzelnes Remote-Netzwerk zu verwenden, können Sie

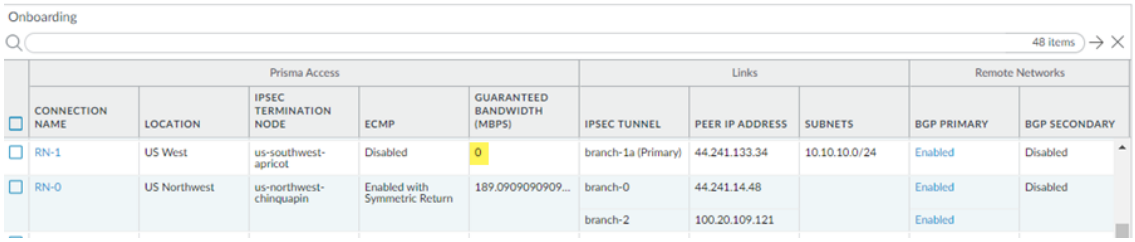
 ©2025 Palo Alto Networks, Inc.

das **Zuweisungsverhältnis** für die IPSec-Tunnel ändern, die Sie für diesen Remote-Netzwerkstandort verwenden.




**STEP 5 |** Speichern Sie Ihre Änderungen und schreiben Sie sie fest.

Die garantierten Bandbreitenwerte werden im Bereich **Panorama** > **Cloud Services** > **Status** > **Überwachen** > **Remote-Netzwerke** im Bereich **Garantierte Mbit/s** angezeigt. Wenn Sie keine Bandbreite angegeben haben, wird diese mit dem Wert 0 angezeigt.




 ©2025 Palo Alto Networks, Inc.

# Remote-Netzwerke – Hohe Leistung

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz<br><br>*Dies ist eine Version mit begrenzter Verfügbarkeit. Wenden Sie sich an Ihren Palo Alto Networks-Kontobetreuer, um diese Funktionalität zu aktivieren.* |

Da sich Ihre Unternehmensskalen und Ihre Bürostandorte geografisch verteilen, ermöglichen Ihnen Prisma Access-Remote-Netzwerke eine schnelle Integration in Ihre Zweigstellen und erstklassige Sicherheit für Ihre Benutzer. Prisma Access bietet Ihnen ein *leistungsstarkes Remote-Netzwerk* für das Onboarding einer Zweigstelle mit hoher Bandbreite.

Geben Sie den Standort der Zweigstelle an, um das Onboarding für ein leistungsstarkes Remote-Netzwerk durchzuführen. Prisma Access wählt dann den Standort aus, der am nächsten an der Zweigstelle liegt. Zur Gewährleistung von Redundanz und Ausfallsicherheit können Sie optional einen sekundären (Backup-)Standort zum Standort einrichten. Das leistungsstarke Remote-Netzwerk verwendet eine einzige Dienst-IP-Adresse für eine Bandbreite von 3 Gbit/s. Dadurch entfällt die Komplexität bei der Konfiguration und Verwaltung mehrerer IPSec-Geräte an jedem Remote-Standort.

*Ein sekundärer Standort wird für Prisma Access (Managed by Panorama)-Bereitstellungen nicht unterstützt.*

Nachdem Sie für Ihr leistungsstarkes Remote-Netzwerk geplant haben, können Sie mit dem Konfigurationsprozess beginnen. Dieser umfasst das Onboarding des leistungsstarken Remote-Netzwerks in Prisma Access und die Aktivierung von QoS und Routing.

## Leistungsstarke Remote-Netzwerke – Funktionen und Richtlinien

Ein leistungsstarkes Remote-Netzwerk bietet Ihnen folgende Kernfunktionen:

- Bis zu 3 Gbit/s aggregierte Bandbreite pro Knoten in einer Compute-Region
- Bis zu 2 Gbit/s Bandbreite pro Remote-Netzwerktunnel von einem Remote-Standort
- Bis zu 500 Remote-Zweigstellen pro Dienst IP-Adresse mit Prisma SD-WAN und erweiterten (Drittanbieter-)CPE-Bereitstellungen

Beachten Sie bei der Konfiguration eines leistungsstarken Remote-Netzwerks für eine Zweigstelle folgende Richtlinien und Unterschiede zwischen Standorten und Remote-Netzwerken:

- **Prisma Access-Standorte** – Leistungsstarke Remote-Netzwerke unterstützen eine Teilmenge von Prisma Access-Standorten.
- **Quality of Service (QoS)** – Bei Zweigstellen unterstützt Prisma Access QoS auf Standortebene. Das von Ihnen ausgewählte QoS-Profil bezieht sich auf den gesamten Standort.

 ©2025 Palo Alto Networks, Inc.

- **Committed Information Rate (CIR)** – Geben Sie eine CIR an, um die pro Standort verwendete Bandbreite zu sichern und festzuschreiben. Wenn es mehrere Remote-Netzwerke gibt, die sich Bandbreite an einem Compute-Standort teilen, empfängt das leistungsstarke Remote-Netzwerk mindestens die in der CIR angegebene Bandbreite, wenn es Konflikte mit anderen Standorten an diesem Compute-Standort gibt.
- **IPSec-Terminierungsknoten** – Im Gegensatz zu Remote-Netzwerken müssen Sie beim Onboarding für die Prisma Access (Managed by Strata Cloud Manager)-Bereitstellung keinen IPSec-Terminierungsknoten auswählen. Prisma Access gleicht die Last bei Remote-Netzwerkverbindungen automatisch aus, um die Bandbreitenzuweisung zu den Standorten zu maximieren.

  Sie müssen noch einen IPSec-Terminierungsknoten für Remote-Netzwerke auswählen, die von Panorama aus eingebunden werden.
- **Tunnel- und Compute-Standortredundanz und maximale Tunnel pro Standort** – Mit einem leistungsstarken Remote-Netzwerk können Sie sowohl die Standort- als auch die IPSec-Redundanz konfigurieren.
  - Standortredundanz (Angabe eines **primären Standorts** an einem Compute-Standort und Angabe eines **sekundären Standorts** an einem separaten Compute-Standort).

    Die Konfiguration eines sekundären Standorts ist optional, und der sekundäre Standort muss sich an einem anderen Compute-Standort als der primäre Standort befinden.
  - IPSec-Tunnelredundanz (Angabe von Tunneln als **Aktiv/Aktiv** oder **Aktiv/Passiv**).

  In dieser Tabelle finden Sie die minimale und maximale Anzahl von Standorten pro Tunnel.

| Bereitstellungstyp Standort | Bereitstellungstyp Tunnel | Minimale Anzahl von Tunneln | Maximale Anzahl von Tunneln |
|---|---|---|---|
| Nur primäre | Aktiv/Passiv | 1 | 2 |
| Nur primäre | Aktiv/Aktiv | 2 | 4 |
| Primäre und sekundäre | Aktiv/Passiv | 2 | 4 |
| Primäre und sekundäre | Aktiv/Aktiv | 4 | 8 |

- **Dienst-IP-Adresszuweisung basierend auf Bereitstellungstyp** – Wie viele Dienst-IP-Adressen empfangen werden, hängt davon ab, ob Sie Ihre leistungsstarken Remote-Netzwerke an einem einzigen Standort eingerichtet haben oder ob Sie sie an zwei verschiedenen Standorten in einer primären und sekundären Bereitstellung eingerichtet haben.
  - Wenn Sie Ihr leistungsstarkes Remote-Netzwerk an einem einzigen Standort ohne sekundären Standort eingerichtet haben, bietet Prisma Access Ihnen eine einzige Dienst-IP-Adresse.

 ©2025 Palo Alto Networks, Inc.

- Wenn Sie eine Compute-Standortredundanz in einer primären und sekundären Konfiguration einrichten, stellt Prisma Access Ihnen zwei Dienst-IP-Adressen zur Verfügung (eine für die primäre und eine für die sekundäre Konfiguration).

Wenn Sie IPSec-Tunnel in einer Aktiv/Passiv-Konfiguration einrichten, stellt Ihnen Prisma Access eine einzige Dienst-IP-Adresse für beide Tunnel zur Verfügung (entspricht einer Standardkonfiguration des Remote-Netzwerks von Prisma Access).

- **Dienst-IP-Adresszuweisung basierend auf Bandbreite** –Prisma Access bietet Ihnen eine einzige IP-Adresse oder FQDN für eine Bandbreite von 3 Gbit/s an einem Compute-Standort.
- **Bandbreite pro Compute-Standort** – Sie weisen Bandbreite pro Compute-Standort zu, genau wie beim Zuweisen von Bandbreite für ein standardmäßiges Remote-Netzwerk. Sie können die Bandbreite planen und zuweisen, bevor Sie mit der Konfiguration beginnen oder während der Erstellung eines leistungsstarken Remote-Netzwerks.
- **IPv6-Unterstützung** – IPv6 wird für leistungsstarke Remote-Netzwerke nicht unterstützt.

Verwenden Sie eines der folgenden Verfahren, um Ihre Remote-Netzwerke je nach Bandbreitenzuweisungstyp zu integrieren:

- Prisma Access (Managed by Strata Cloud Manager)
- Prisma Access (Managed by Panorama)

## Strata Cloud Manager

So fügen Sie mit Strata Cloud Manager ein leistungsstarkes Remote-Netzwerk hinzu.

**STEP 1 |** Gehen Sie über Strata Cloud Manager zu **Workflows** > **Einrichtung Prisma Access** > **Zweigstellen**.

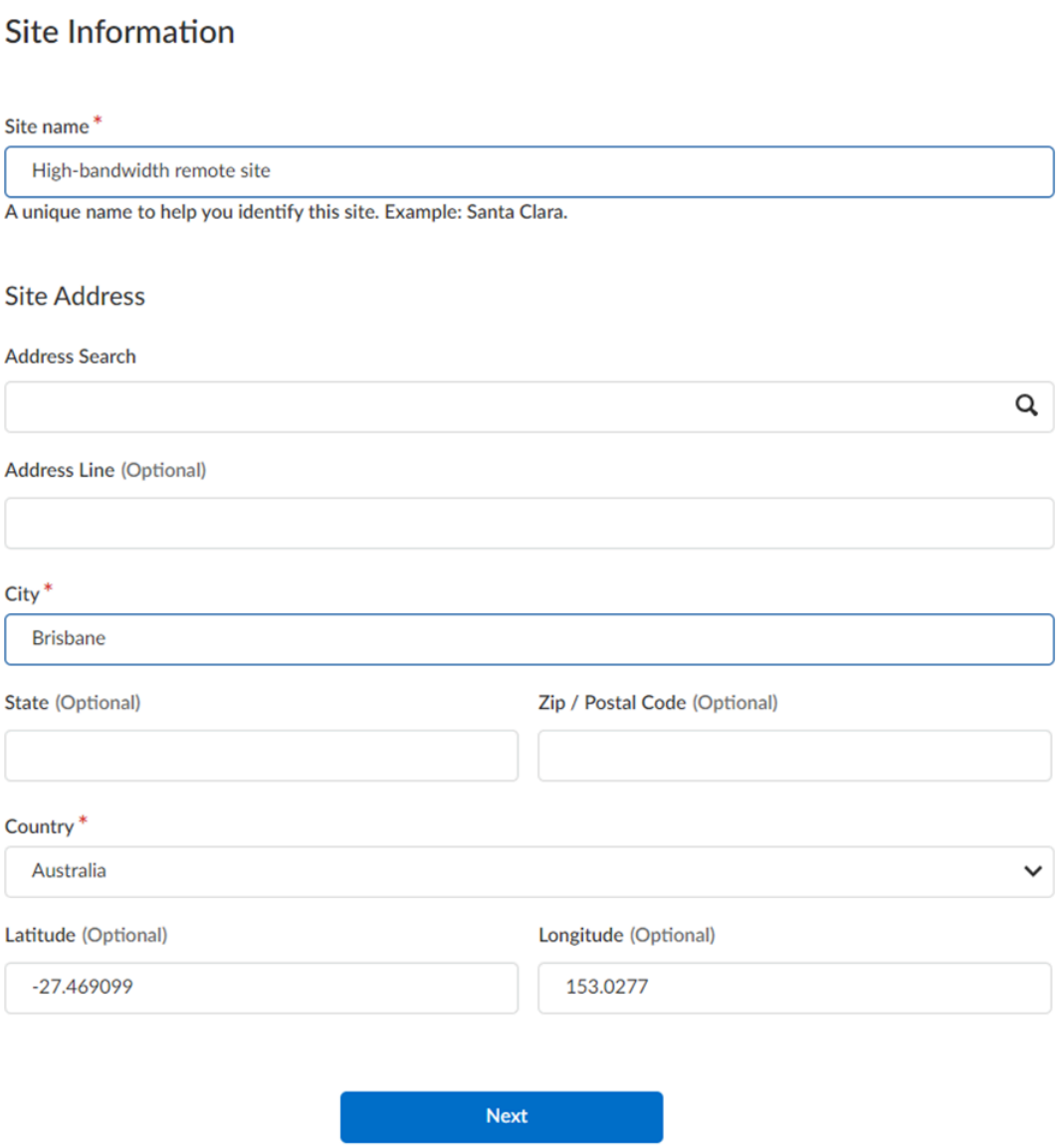
Diese Option zeigt an, dass der Tunnel, den Sie für die Zweigstellen erstellen, von Ihrem CPE (einer Palo Alto Networks-Firewall der nächsten Generation oder einem CPE von Drittanbietern) beendet wird.

**STEP 2 |** **Fügen Sie einen Standort hinzu** und geben Sie dem Remote-Netzwerk einen beschreibenden **Standortnamen**.

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Wählen Sie den **Ort** und das **Land** des Standorts aus.

Fügen Sie für genauere Suchvorgänge eine Adresse hinzu.




**STEP 4 |** Klicken Sie auf **Next (Weiter)**.

**STEP 5 |** Geben Sie die **QoS-CIR (Committed Information Rate)** in Mbit/s ein.

Wenn Sie über mehrere Remote-Netzwerke verfügen, die Bandbreite an einem Compute-Standort teilen, und Bandbreitenkonflikte mit anderen Standorten an diesem Compute-Standort bestehen, empfängt das leistungsstarke Remote-Netzwerk mindestens die in der CIR angegebene Bandbreite.

Wenn Sie primäre und sekundäre Standorte konfigurieren und Sie verschiedene Compute-Regionen angeben, erhält die sekundäre Region 20 % der CIR. Wenn Sie beispielsweise eine CIR von 100 Mbit/s für einen Standort konfigurieren, stellt Prisma Access dem primären

 ©2025 Palo Alto Networks, Inc.

Standort eine CIR von 100 Mbit/s und dem sekundären Standort eine CIR von 20 Mbit/s zur Verfügung.

Wenn die CIR 500 Mbit/s beträgt und die gesamte verbleibende Bandbreite am Compute-Standort von anderen Standorten genutzt wird, senkt Prisma Access die Bandbreite von mehr als 500 Mbit/s. Wenn andere Standorte jedoch keine Bandbreite nutzen, kann die Bandbreite für das leistungsstarke Remote-Netzwerk über 500 Mbit/s bis zur zugewiesenen Bandbreite am Compute-Standort gehen.

Geben Sie eine CIR von mindestens 1 Mbit/s und maximal 2.000 Mbit/s ein. Überschreiten Sie nicht die Bandbreite, die Sie für die Compute-Region angeben.

**STEP 6 |** Wählen Sie einen **primären Prisma Access-Standort** aus.

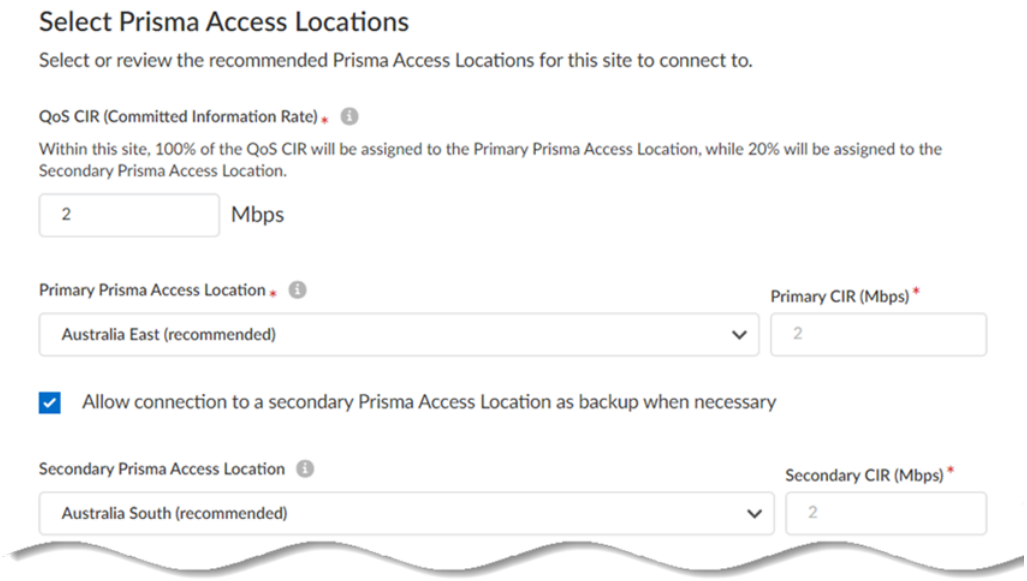
Wenn in der Liste mehrere Standorte **empfohlen** werden, wählen Sie den Standort aus, der für Ihre Bereitstellung am besten geeignet ist.

**STEP 7 |** (Optional) Wenn Sie als Backup einen sekundären Standort erstellen möchten, wählen Sie **bei Bedarf Verbindung zu einem sekundären Prisma Access-Standort als Backup zulassen** und dann einen **sekundären Prisma Access-Standort** aus.

Wenn Sie diese Option auswählen, füllt Prisma Access vorab die besten sekundären Standorte aus, die sich an einem anderen Compute-Standort als dem primären befinden. Wenn mehrere

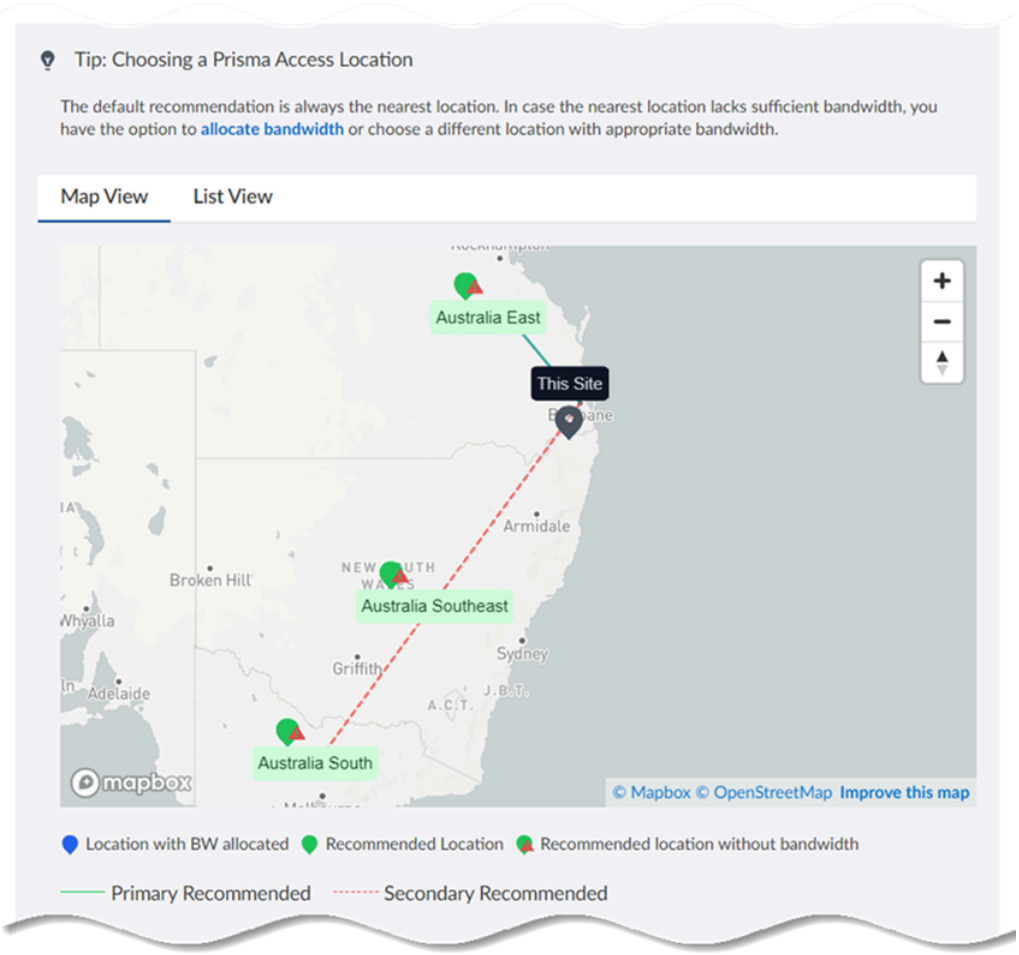
 ©2025 Palo Alto Networks, Inc.

Standorte **empfohlen** werden, wählen Sie den Standort aus, der für Ihre Bereitstellung am besten geeignet ist.




Prisma Access stellt Ihnen eine Karte mit empfohlenen Standorten zur Verfügung, die Ihnen bei der Auswahl eines Standorts helfen soll.

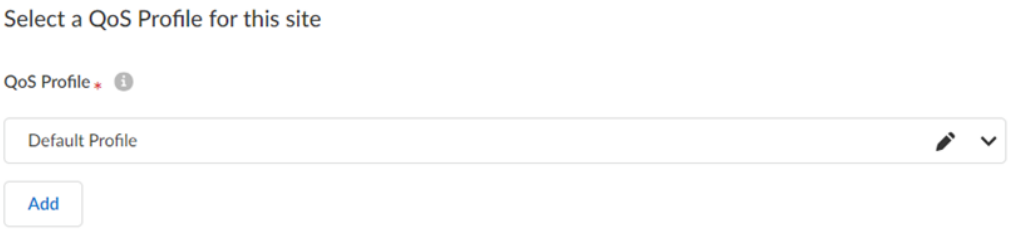
 ©2025 Palo Alto Networks, Inc.




 ©2025 Palo Alto Networks, Inc.

**STEP 8 |** Wählen Sie ein **QoS-Profil** aus, das für diesen Standort verwendet werden soll.

Leistungsstarke Remote-Netzwerke nutzen ein einziges QoS-Profil.

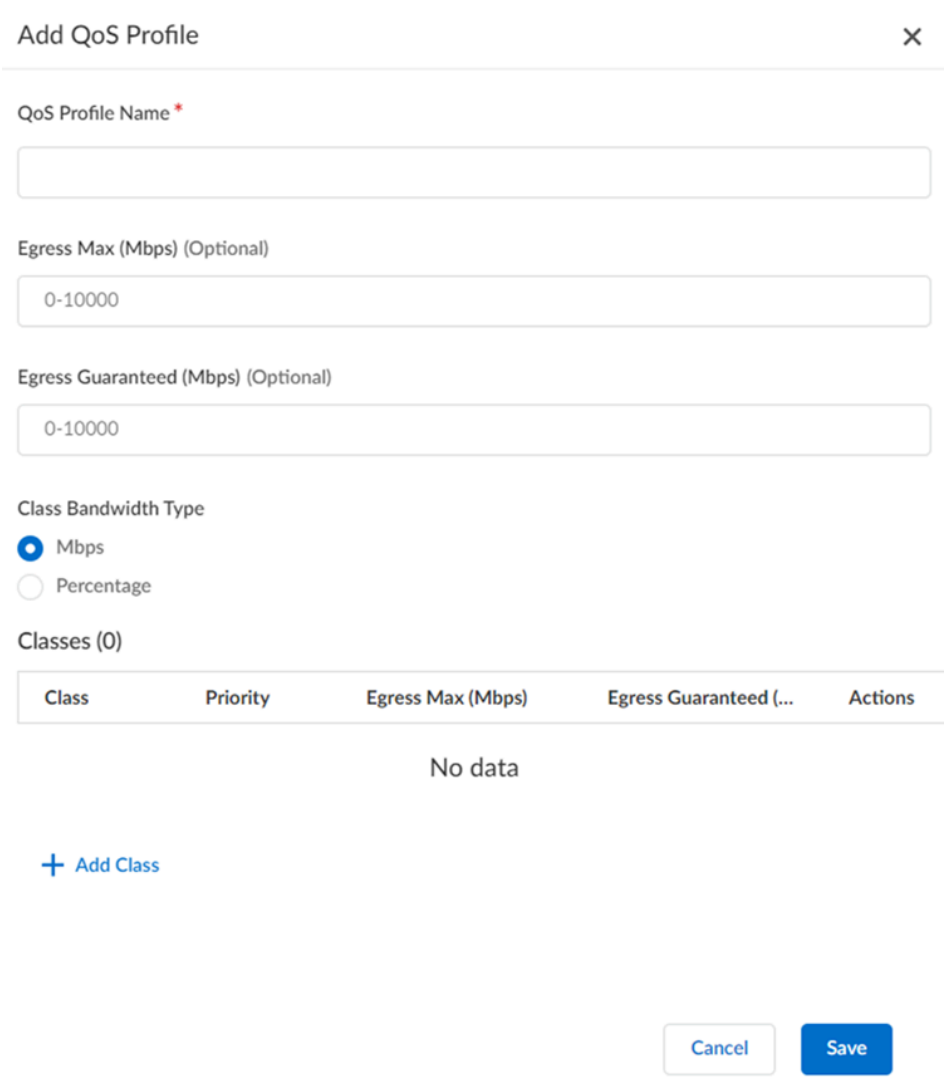



Wenn Sie noch kein QoS-Profil erstellt haben, sollten Sie ein QoS-Profil **hinzufügen**. Dabei werden folgende Werte angegeben:

- Geben Sie einen eindeutigen **QoS-Profilnamen** ein.
- (Optional) Geben Sie einen Wert für **Ausgang maximal (Mbit/s)** ein, der den maximalen Durchsatz in Mbit/s für Datenverkehr darstellt, der die Dienstverbindung oder Remote-Netzwerkverbindung verlässt.
- (Optional) Geben Sie einen Wert für **Ausgang garantiert (Mbit/s)** ein, der die garantierte Bandbreite für dieses Profil in Mbit/s darstellt.
- Geben Sie einen **Klassenbandbreitentyp** ein, entweder in **Prozent** oder **Mbit/s**.

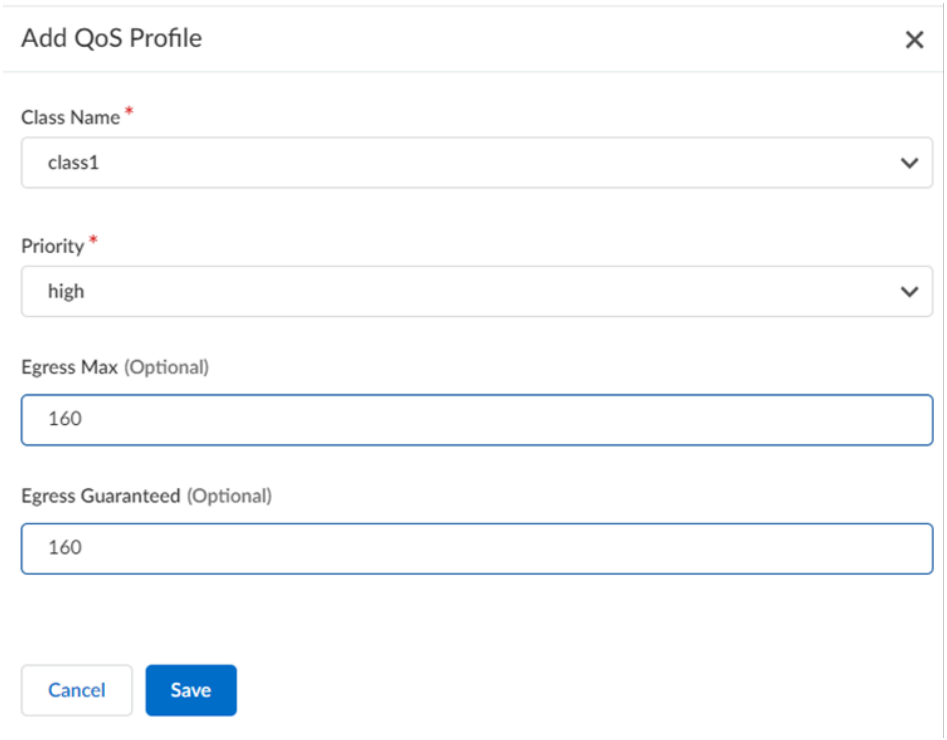
  QoS für leistungsstarke Remote-Netzwerke verwendet kein garantiertes Bandbreitenverhältnis.

 ©2025 Palo Alto Networks, Inc.




- Fügen Sie im Abschnitt „Klassen“ eine **Klasse** hinzu und geben Sie an, wie bis zu acht einzelne QoS-Klassen gekennzeichnet werden sollen.
  - Geben Sie einen **Klassennamen** ein.
  - Wählen Sie die **Priorität** für die Klasse aus (**Echtzeit**, **Hoch**, **Mittel** oder **Niedrig**).
  - Geben Sie einen Wert für **Ausgang maximal** ein, der den maximalen Durchsatz (in Mbit/s) für Datenverkehr darstellt, der die Dienstverbindung oder Remote-Netzwerkverbindung verlässt.
  - Geben Sie einen Wert für **Ausgang garantiert** ein, der die garantierte Bandbreite für dieses Profil darstellt (in Mbit/s).
- **Save (Speichern)** Sie Ihre Änderungen.

 ©2025 Palo Alto Networks, Inc.

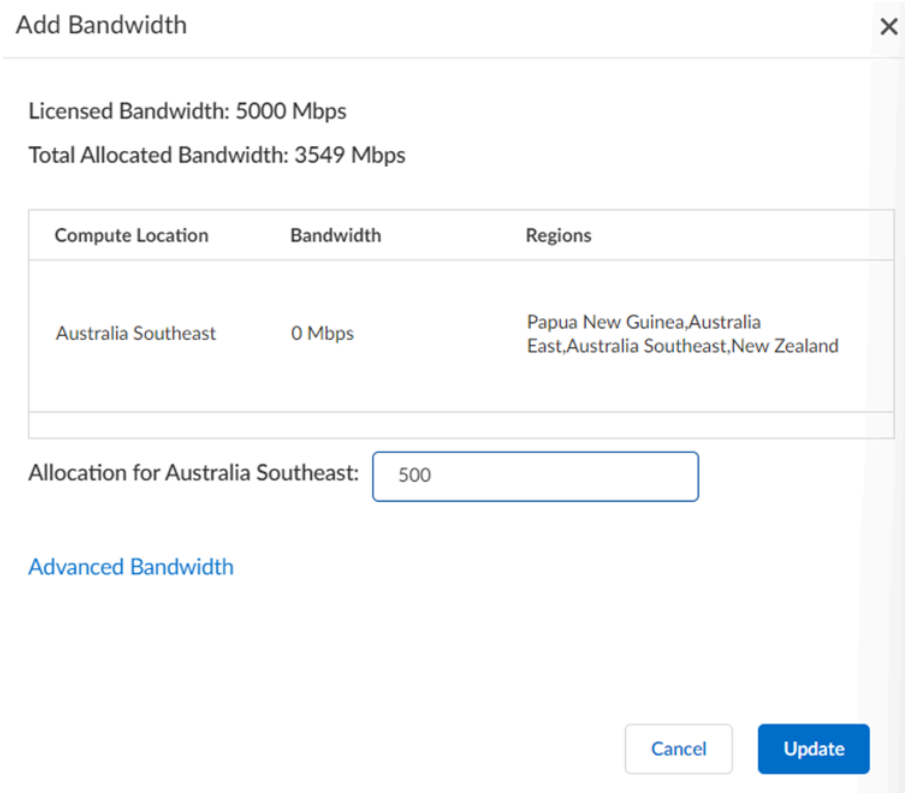



**STEP 9 |** Wenn Sie noch keine Bandbreite zugewiesen haben, werden Sie von Prisma Access aufgefordert, die Bandbreite für den Compute-Standort **zuzuweisen**, der dem ausgewählten Standort zugeordnet ist. Geben Sie eine Mindestbandbreite von 50 Mbit/s pro Compute-Standort an.




 ©2025 Palo Alto Networks, Inc.

**STEP 10 |** Sofern noch nicht geschehen, weisen Sie den ausgewählten Standorten Bandbreite zu. **Aktualisieren** Sie anschließend Ihre Änderungen.




**STEP 11 |** Klicken Sie auf **Next (Weiter)**.

**STEP 12 |** Definieren Sie **Einstellungen für Tunnel & Schaltkreise**.

1. Wählen Sie einen **Tunnelmodus** aus: **Aktiv/Aktiv** oder **Aktiv/Passiv**.

   Der Tunnelmodus gibt an, wie viele Ihrer ISP-Schaltkreise Sie für das leistungsstarke Remote-Netzwerk verwenden möchten.

   - Wenn Sie **Aktiv/Aktiv** auswählen, verwendet Prisma Access vier ISP-Schaltkreise, um entweder zwei oder vier aktive Tunnel zu erstellen.
   - Wenn Sie **Aktiv/Passiv** auswählen, verwendet Prisma Access zwei ISP-Schaltkreise, um zwei aktive Tunnel zu erstellen. Fällt der aktive Tunnel aus, wird der passive Tunnel aktiviert.
2. Wählen Sie die Anzahl der zu verwendenden **Internetschaltkreise** aus.

   Prisma Access weist Tunnel basierend auf der Anzahl der hier angegebenen Schaltkreise und der Frage zu, ob Ihre Bereitstellung Aktiv/Aktiv oder Aktiv/Passiv ist (siehe folgende Tabelle).

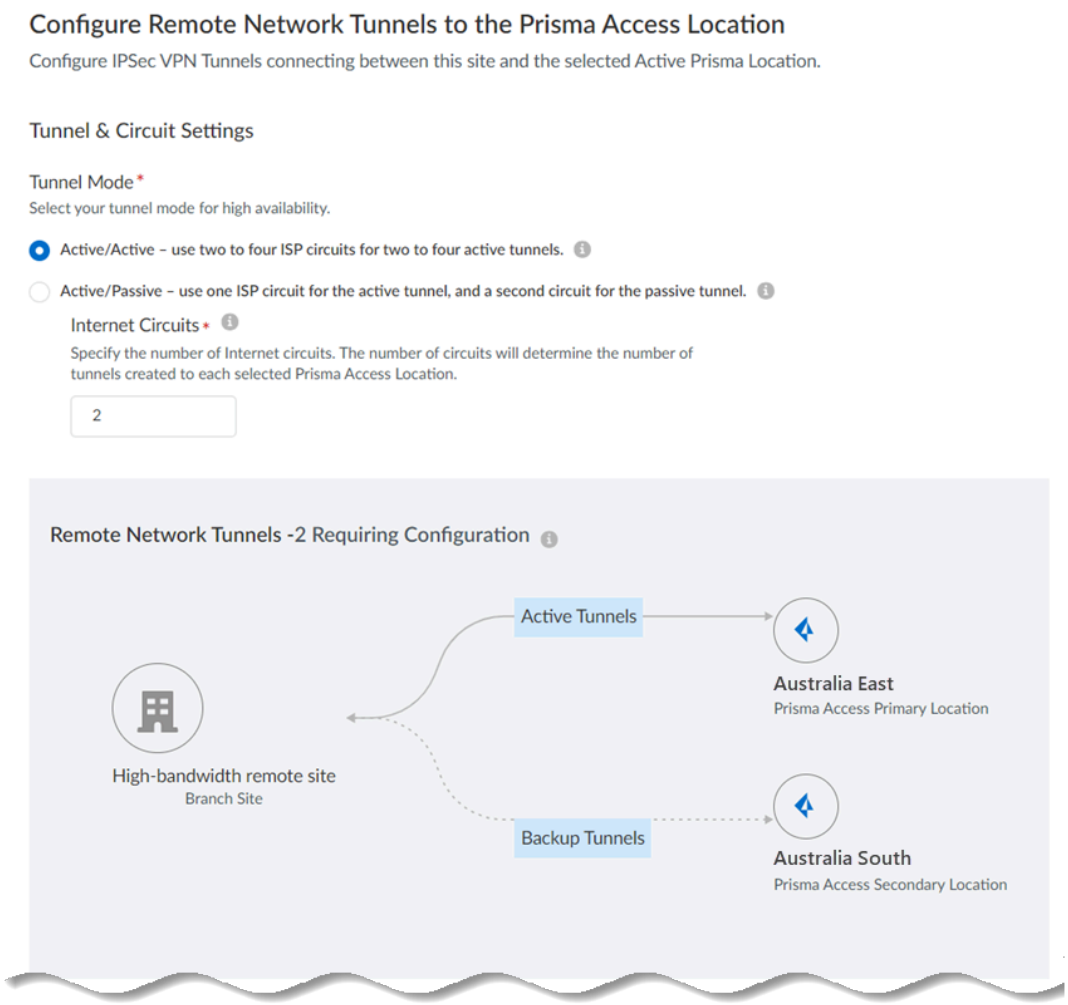
| Anzahl der Schaltkreise | Bereitstellungstyp | Anzahl der Tunnel |
|---|---|---|
| 1 | Aktiv/Passiv | 1 (einen für den aktiven Tunnel). |

 ©2025 Palo Alto Networks, Inc.

| Anzahl der Schaltkreise | Bereitstellungstyp | Anzahl der Tunnel |
|---|---|---|
| 2 | Aktiv/Aktiv | 2 (für jeden aktiven Tunnel einen).<br>Wenn Sie primäre und sekundäre Standorte auswählen, erstellt Prisma Access einen aktiven Tunnel für den primären Standort und einen aktiven Tunnel für den sekundären Standort. |
| 2 | Aktiv/Passiv | 2 (für jeden aktiven Tunnel einen).<br>Wenn Sie primäre und sekundäre Standorte auswählen, erstellt Prisma Access einen aktiven und passiven Tunnel für den primären Standort und einen aktiven und passiven Tunnel für den sekundären Standort. Fällt der aktive Tunnel aus, verwendet Prisma Access die gleiche Dienst-IP-Adresse bzw. den gleichen FQDN für den passiven Tunnel, der aktiviert wird. |
| 4 | Aktiv/Aktiv | 4 (einen für jeden aktiven Tunnel).<br>Wenn Sie primäre und sekundäre Standorte auswählen, erstellt Prisma Access zwei aktive Tunnel |


©2025 Palo Alto Networks, Inc.

| Anzahl der Schaltkreise | Bereitstellungstyp | Anzahl der Tunnel |
|---|---|---|
| | | für den primären Standort und zwei aktive Tunnel für den sekundären Standort. |



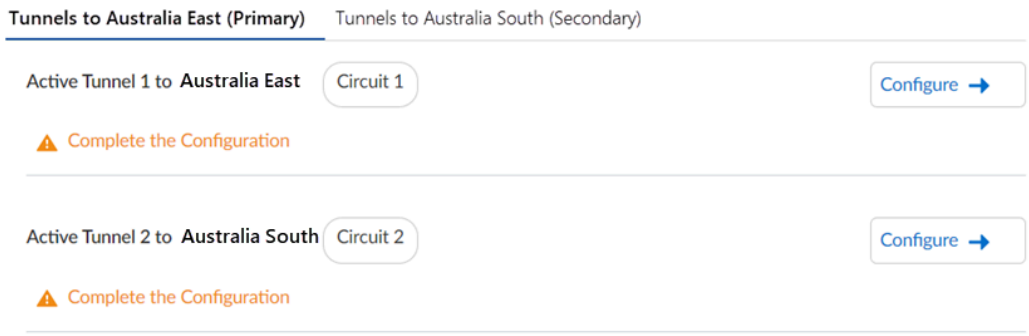

3. (Optional) **Konfigurieren** Sie Ihre IPSec-Tunneleinstellungen.

   Prisma Access bietet Ihnen die Standardeinstellungen für IPSec-Tunnel. Diese Einstellungen bestimmen die IPSec- und IKE-Verschlüsselungseinstellungen für den Remote-Netzwerktunnel. Wenn Sie sie ändern möchten, wählen Sie den **primären Tunnel** aus und **bearbeiten** Sie Ihre Einstellungen.

   Wenn Sie einen sekundären Standort angeben, füllt Prisma Access automatisch die Werte vom primären Tunnel beim sekundären Tunnel aus. Wenn Sie den sekundären

 ©2025 Palo Alto Networks, Inc.

Tunnel bearbeiten möchten, wählen Sie diesen Tunnel aus und **bearbeiten** Sie die Einstellungen.



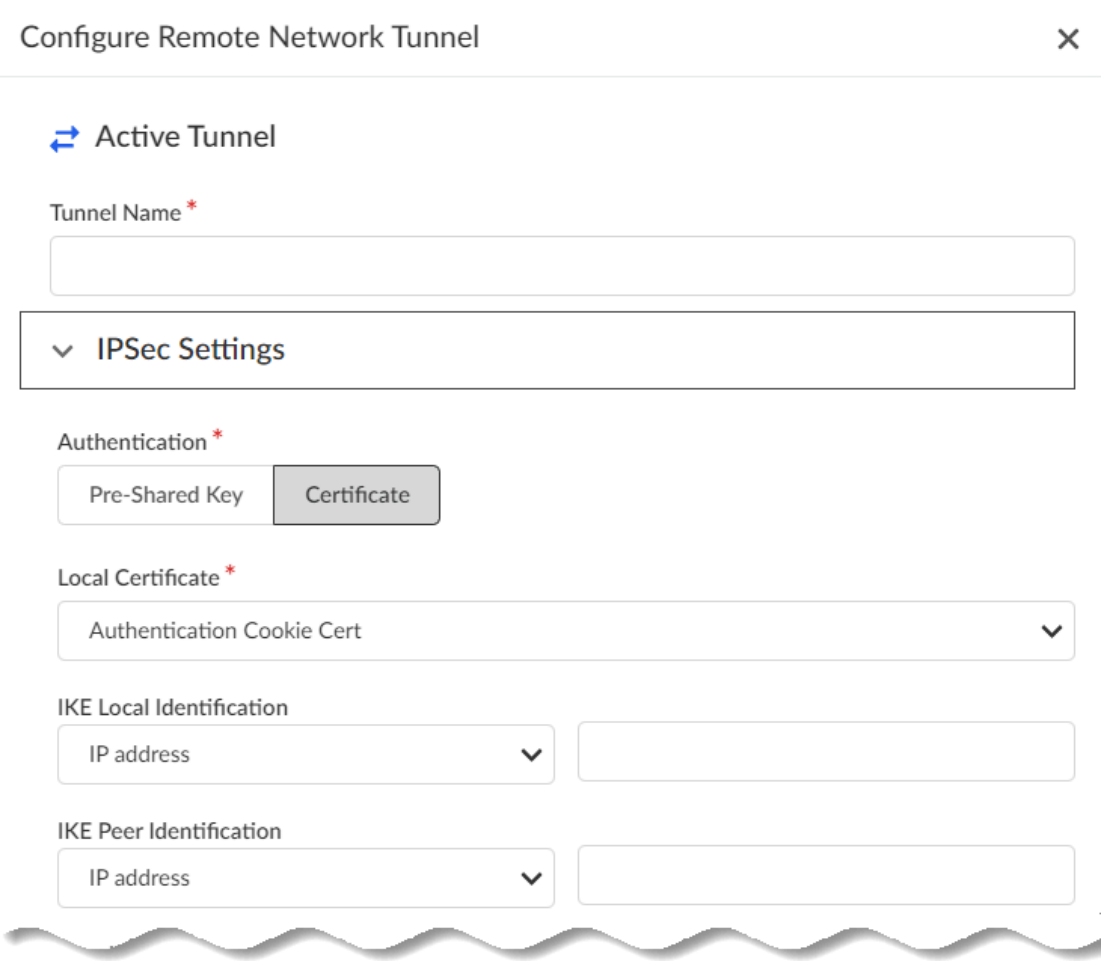

Notieren Sie sich diese Einstellungen; Sie müssen mit den Einstellungen auf dem CPE übereinstimmen, das den IPSec-Tunnel an Ihrem Standort beendet.

- Geben Sie dem aktiven Tunnel einen eindeutigen **Tunnelnamen**.
- Geben Sie **IPSec-Einstellungen** an.
  - Geben Sie einen **Authentifizierungstyp** an (entweder **Pre-Shared Key** oder **Zertifikat**).

    Wenn Sie **Pre-Shared Key** angeben, geben Sie den **Pre-Shared Key** ein und bestätigen Sie ihn.

    Wenn Sie ein **Zertifikat** angeben, geben Sie das zu verwendende **lokale Zertifikat** ein. Dieses Zertifikat muss bereits in Strata Cloud Manager vorhanden sein.
  - Geben Sie die **IKE Lokale Identifikation** an (**IP-Adresse**, **Ausgewählter Name (Subjekt)**, **Benutzer-FQDN (E-Mail-Adresse)** oder **FQDN (Hostname)** ).
  - Geben Sie die **IKE Peer-Identifikation** an (**IP-Adresse**, **Ausgewählter Name (Subjekt)**, **Benutzer-FQDN (E-Mail-Adresse)** oder **FQDN (Hostname)).**

 ©2025 Palo Alto Networks, Inc.

- 


- Geben Sie den Typ der Überprüfung der Peer-ID an:
  - **Exakt** – Stellt sicher, dass die lokale Einstellung und die Peer-IKE-ID-Nutzlast exakt übereinstimmen.
  - **Platzhalter** – Ermöglicht es, dass die Peer-Identifikation so lange übereinstimmt, wie jedes Zeichen vor dem Platzhalter (*) übereinstimmt. Die Zeichen nach dem Platzhalter müssen nicht übereinstimmen.
- (Optional) **Peer-Identifikation und Nichtübereinstimmung der Zertifikat-Nutzlast zulassen** – Ermöglicht eine erfolgreiche IKE-Sicherheitszuordnung (SA), auch wenn die Peer-Identifikation nicht mit der Peer-Identifikation im Zertifikat übereinstimmt.
- Wählen Sie ein **Zertifikatprofil** aus. Ein Zertifikatprofil enthält Informationen zur Authentifizierung des Peer-Gateways.
- (Optional)**Strikte Validierung der erweiterten Schlüsselverwendung von Peers ermöglichen** – Zur strikten Steuerung, wie der Schlüssel verwendet werden kann.
- Wählen Sie die **IP-Adresse des Zweiggeräts** aus (**Statisch** oder **Dynamisch**).
  - Wenn Sie **Statisch** auswählen, geben Sie die zu verwendende **Statische IP-Adresse** für den IPSec-Tunnel ein.
  - Geben Sie **Dynamisch** an, um die IP-Adresse automatisch abzurufen.

 ©2025 Palo Alto Networks, Inc.

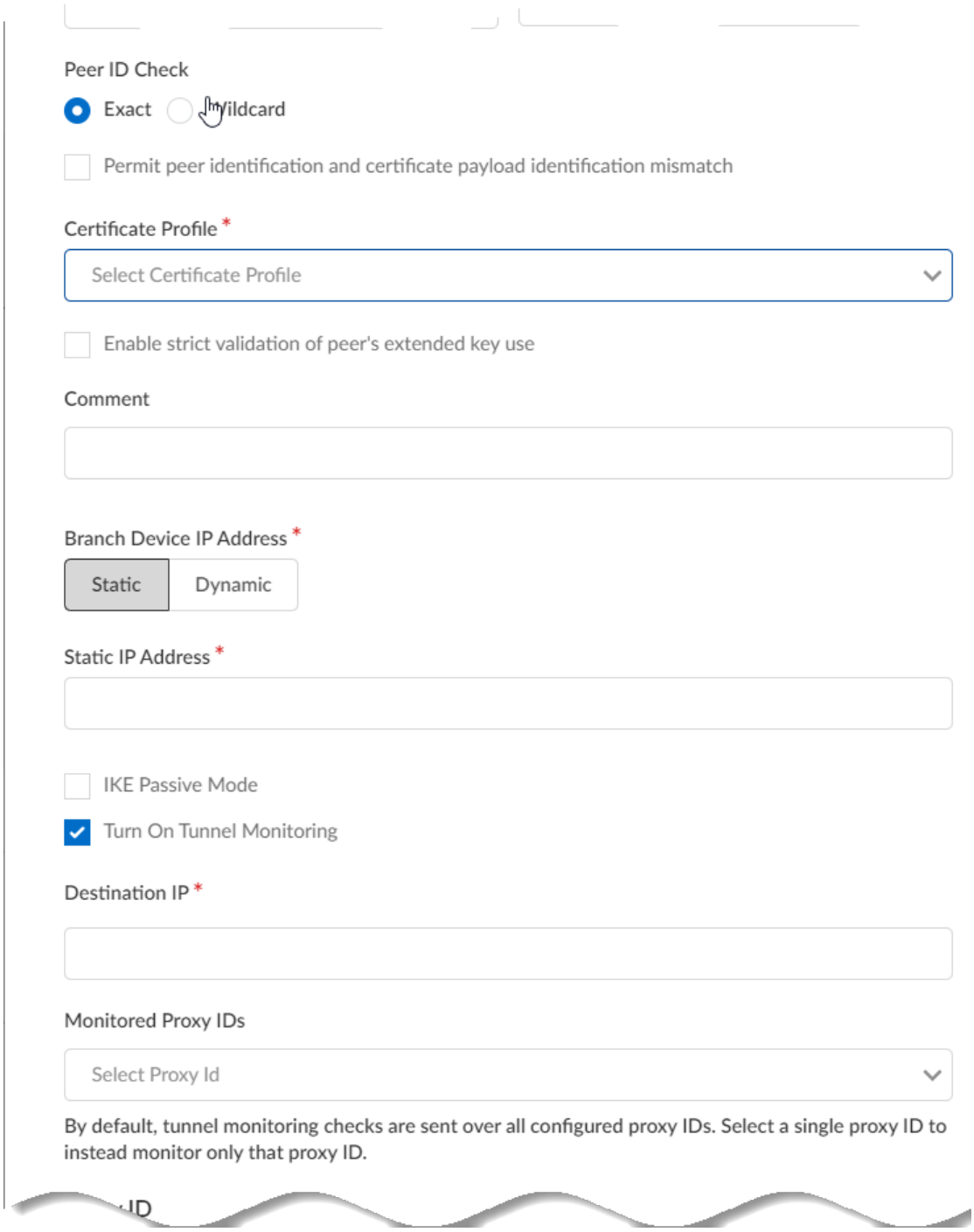
- (Optional, empfohlen) Aktivieren Sie den **den IKE Passivmodus**, damit Prisma Access auf IKE-Verbindungen reagieren kann, sie aber nicht initiieren muss.

  Die Einstellung **IKE Passivmodus** ist zwar nicht erforderlich, wird jedoch empfohlen.
- (Optional) **Tunnelüberwachung einschalten**.

  Geben Sie eine **Ziel-IP**-Adresse für die Tunnelüberwachung im Remote-Netzwerk für Prisma Access ein, um zu ermitteln, ob der Tunnel aktiv ist. Wenn Ihr IPSec-

 ©2025 Palo Alto Networks, Inc.

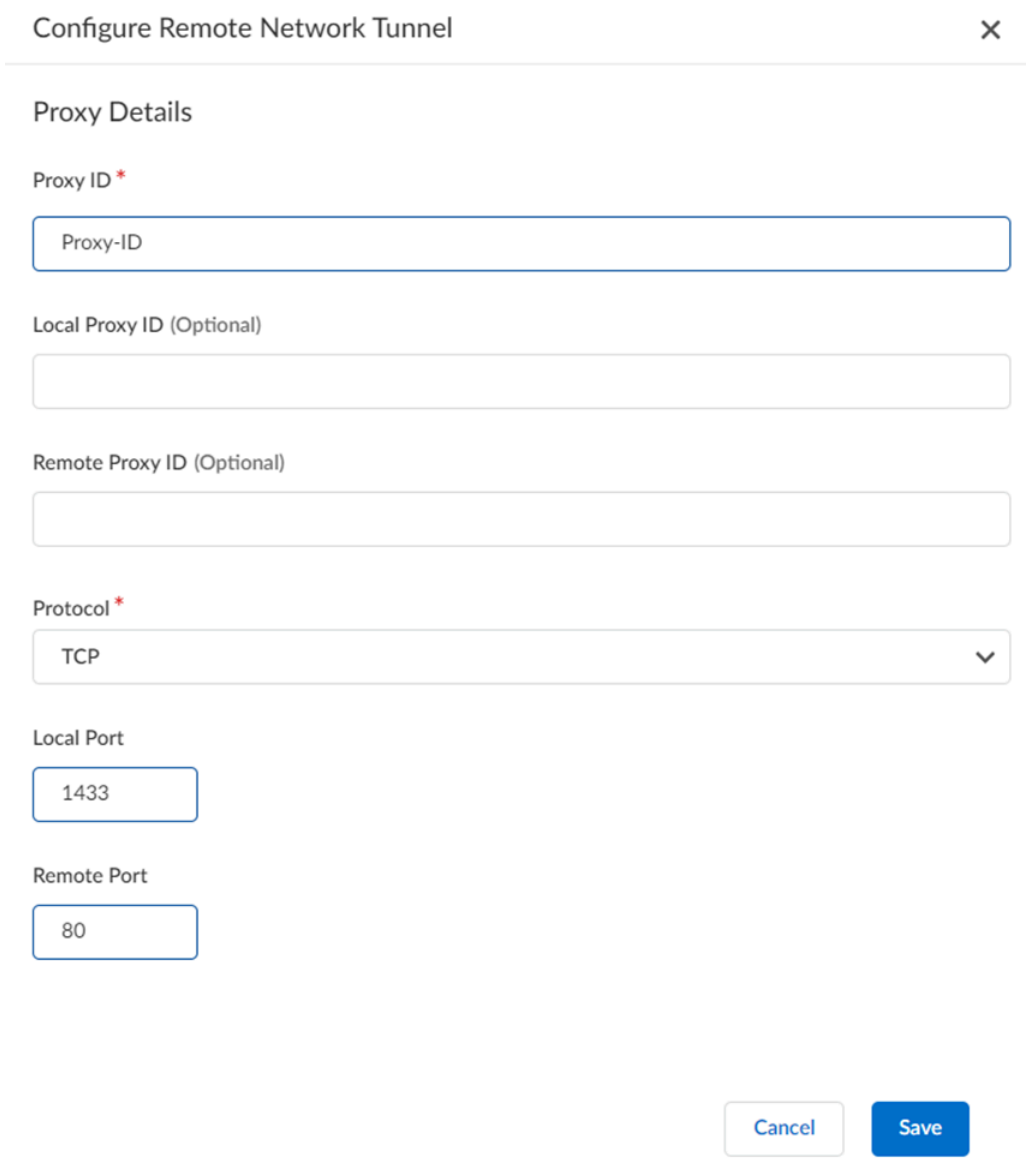
Zweiggerät richtlinienbasiertes VPN verwendet, geben Sie die zugehörige **Proxy-ID** als **überwachte Proxy-ID** ein.

- 


- (Optional) Wenn Sie eine Proxy-ID benötigen:
  - Wählen Sie **Proxy ID hinzufügen** aus und geben Sie die **Proxy-ID** ein.
  - Geben Sie optional die **lokale Proxy-ID** und die **Remote-Proxy-ID** ein.
  - Geben Sie das **Protokoll** ein, das für die Proxy-ID verwendet werden soll. Geben Sie eine **Nummer**, **TCP** oder **UDP** ein.

 ©2025 Palo Alto Networks, Inc.

- Geben Sie einen **lokalen Port** und **Remote-Port** für TCP oder UDP an.
- **Speichern** Sie Ihre Änderungen.



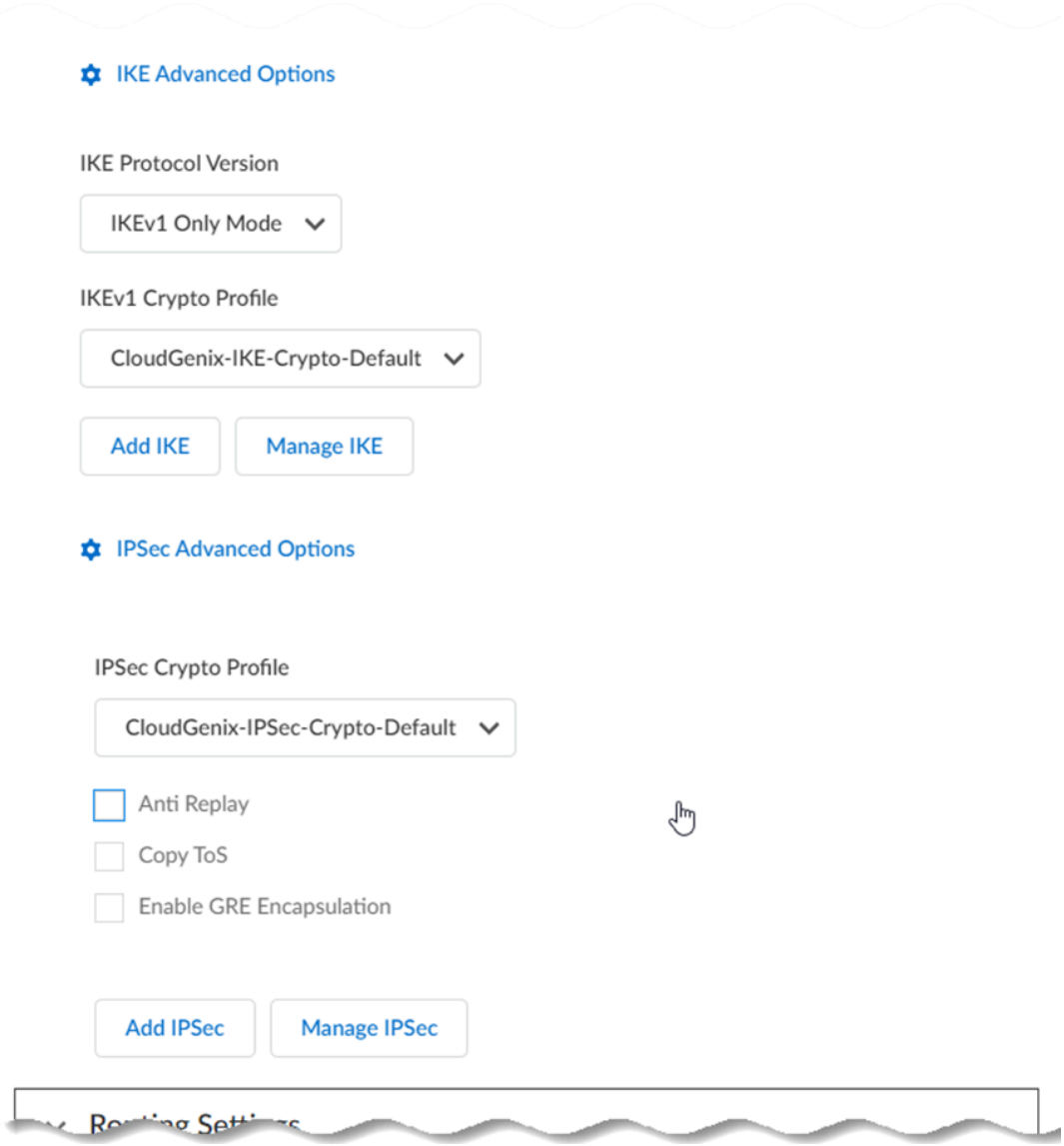

- Geben Sie **Erweiterte IKE-Optionen** an.
  - Wählen Sie eine **IKE Protokollversion** aus.
  - Wählen Sie ein **IKEv1-Verschlüsselungsprofil** aus.

    Wählen Sie **IKE hinzufügen** aus, um ein Verschlüsselungsprofil hinzuzufügen. Wählen Sie **IKE verwalten** aus und anschließend das Profil, das bearbeitet werden soll, um ein vorhandenes IKE-Profil zu verwalten.
  - Wählen Sie ein **IKEv2-Verschlüsselungsprofil** aus.

    Wählen Sie **IKE hinzufügen** aus, um ein Verschlüsselungsprofil hinzuzufügen. Wählen Sie **IKE verwalten** aus und anschließend das Profil, das bearbeitet werden soll, um ein vorhandenes IKE-Profil zu verwalten.

 ©2025 Palo Alto Networks, Inc.

- Geben Sie **Erweiterte IPSec-Optionen** an.
  - Wählen Sie ein **IPSec-Verschlüsselungsprofil** aus.

    Wählen Sie **IPSec hinzufügen** aus, um ein Verschlüsselungsprofil hinzuzufügen. Wählen Sie **IPSec verwalten** aus und anschließend das zu bearbeitende Profil, um ein vorhandenes IPSec-Profil zu verwalten.
- 

- Wählen Sie Ihre **Routing-Einstellungen** aus.
  - Wählen Sie den **Routingtyp** aus (**Statisch** oder **Dynamisch**).

    Wenn Sie **Statisch** auswählen, **fügen** Sie die IP-Subnetze oder IP-Adressen hinzu, die Sie am Standort sichern möchten.

    Gehen Sie wie folgt vor, wenn Sie **Dynamisch** auswählen:
    - Geben Sie das **Peer-AS** (das autonome System (AS) für Ihr Netzwerk) ein.

      Verwenden Sie eine RFC 6996-konforme private BGP-AS-Nummer.

 ©2025 Palo Alto Networks, Inc.

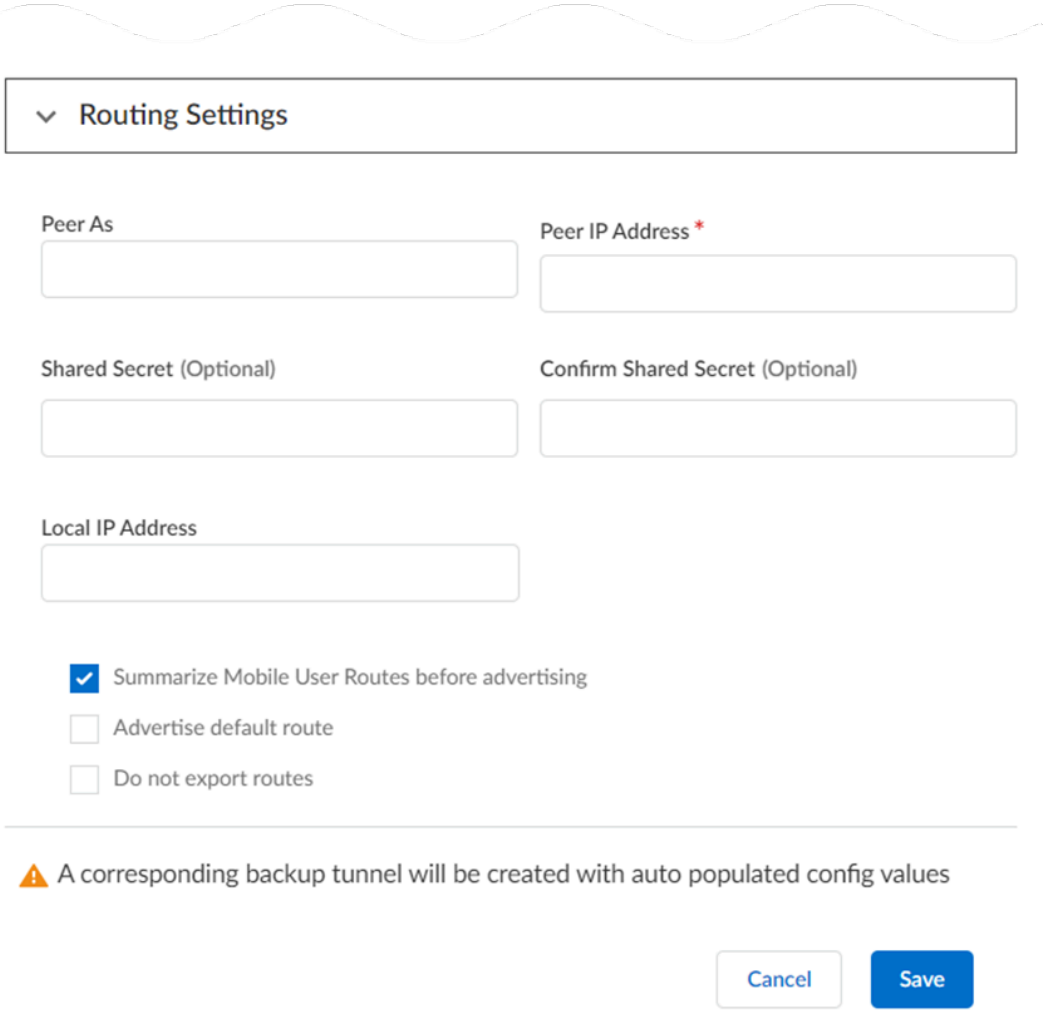
- Geben Sie die **Peer-IP-Adresse** ein, die als Router-ID des eBGP-Routers im Netzwerk der Zentrale oder des Rechenzentrums zugewiesen wurde.
- (Optional) Geben Sie ein **Geteiltes Geheimnis** ein, um die BGP-Peer-Kommunikation zu authentifizieren.
- Geben Sie die **lokale IP-Adresse** ein, die Prisma Access als lokale IP-Adresse für BGP verwendet.
- (Optional) Wählen Sie **Mobile Benutzerrouten vor dem Mitteilen zusammenfassen** aus, um die Anzahl der über BGP an Ihr Customer Premises Equipment (CPE) gesendeten IP-Subnetz-Mitteilungen für mobile Benutzer zu verringern, indem Prisma Access die Subnetze vor der Mitteilung zusammenfasst.
- (Optional) Wählen Sie **Standardroute mitteilen** aus, damit Prisma Access eine Standardroutenankündigung für das Remote-Netzwerk mithilfe von eBGP erstellt. Vergewissern Sie sich, dass für Ihr Netzwerk keine andere

 ©2025 Palo Alto Networks, Inc.

Standardroute vorhanden ist, die von BGP mitgeteilt wird, da es sonst zu Routing-Problemen in Ihrem Netzwerk kommen kann.

- (Optional) Wählen Sie **Routen nicht exportieren** aus, um zu verhindern, dass Prisma Access Routen an die Zentrale oder das Rechenzentrum weiterleitet.

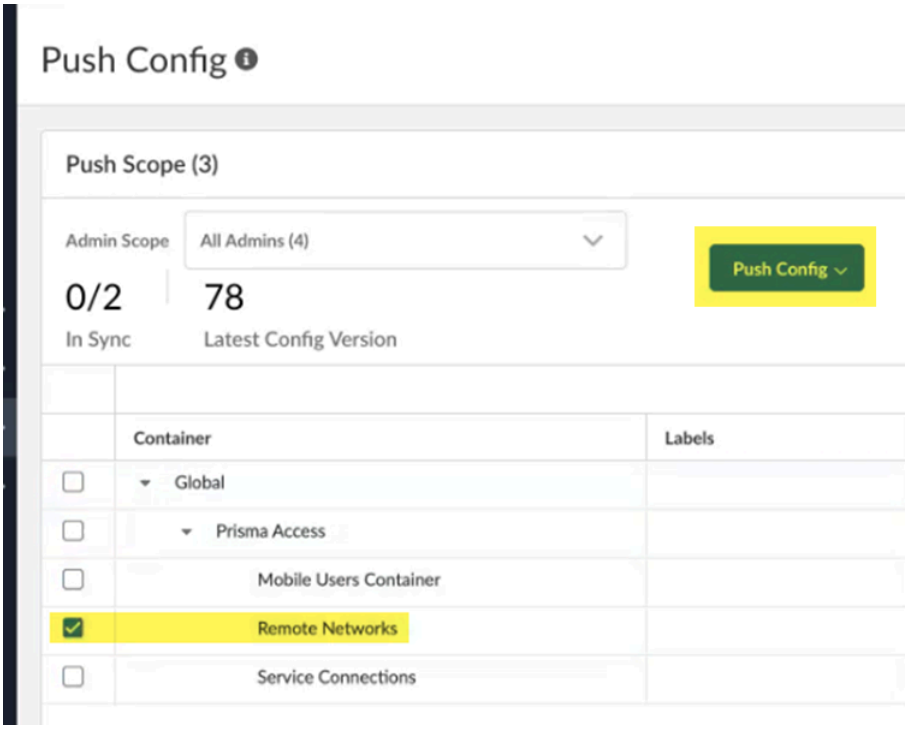
4. **Speichern** Sie die an Ihrem IPSec-Tunnel vorgenommenen Änderungen.




**STEP 13 | Speichern und beenden.**

 ©2025 Palo Alto Networks, Inc.

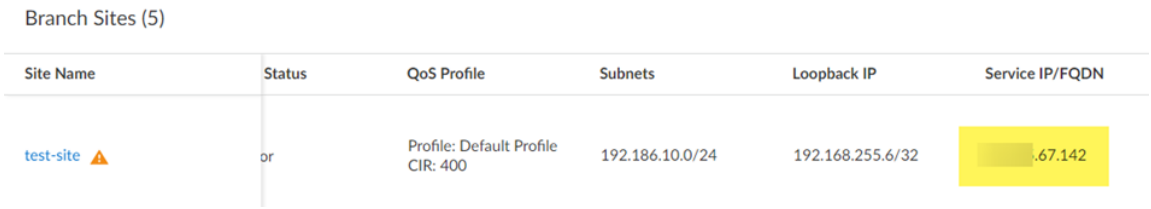
**STEP 14 |** **Push-Konfiguration** zum Speichern Ihrer Konfigurationsänderungen. Achten Sie dabei darauf, im **Übertragungsumfang** die Option **Remote-Netzwerke** auszuwählen.




**STEP 15 |** Suchen Sie nach der **Dienst-IP**-Adresse, die Sie auf Ihrem CPE angeben.

Verwenden Sie bei der Einrichtung des Remote-Netzwerks die Dienst-IP-Adresse als Peer-IP-Adresse auf Ihrem CPE, um den IPSec-Tunnel zu beenden.

1. Gehen Sie zu **Workflows** > **Prisma SASE einrichten** > **Zweigstellenverwaltung** > **Erweiterter CPE-Standort**.
2. Suchen Sie nach der **Dienst-IP-/FQDN-Adresse**.




## Panorama

Die Schritte zum Konfigurieren eines leistungsstarken Remote-Netzwerks entsprechen denen für das Onboarding eines standardmäßigen Remote-Netzwerks in Prisma Access (Managed by Panorama). Dies umfasst die Auswahl eines **IPSec-Terminierungsknotens** während des Onboardings.

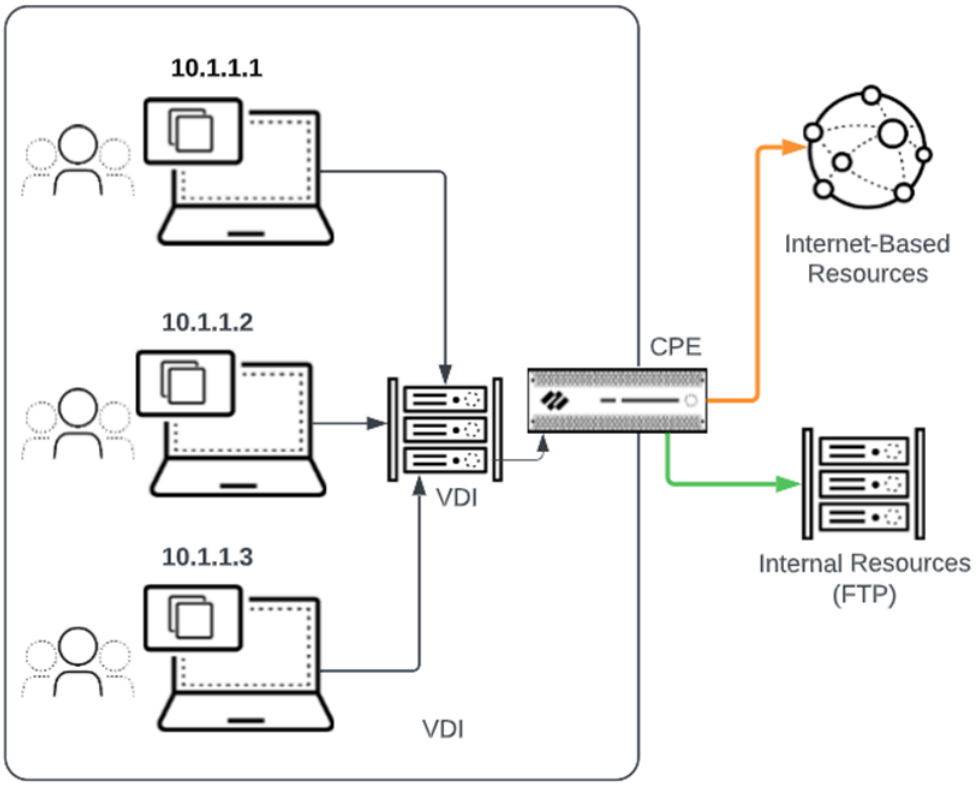
 ©2025 Palo Alto Networks, Inc.

# Freigegebene Desktop-VDI mithilfe eines Terminalservers in Prisma Access integrieren

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access-Lizenz |

Virtual Desktop Infrastructure (VDI) ist eine Technologie, die virtuelle Maschinen zur Bereitstellung und Verwaltung virtueller Desktops verwendet. VDI stellt Desktop-Umgebungen über einen verwalteten Server auf Anfrage für Endbenutzer bereit. Endbenutzer greifen von ihren bereitgestellten VDI-Desktops auf die für sie erforderlichen Ressourcen zu, z. B. auf öffentliche Apps und Ressourcen, bei denen es sich um internetbasierte oder private Apps handelt, sowie auf Ressourcen, die über eine FTP-Verbindung verfügbar sind.

Eine VDI-Topologie kann entweder mit freigegebenen oder dedizierten Desktops implementiert werden. Wenn die Desktops gemeinsam genutzt werden, stehen hinter einer einzigen IP-Adresse mehrere Benutzer, die anhand von Ports unterschieden werden.




Wenn Ihre VDI-Bereitstellung eine freigegebene Desktop-Implementierung verwendet, bietet Prisma Access eine Lösung, mit der Endbenutzer über eine einzige Anmeldung sicher auf Internet- und FTP-Ressourcen zugreifen können, während gleichzeitig die VDI-Benutzer Ihrer Organisation

 ©2025 Palo Alto Networks, Inc.

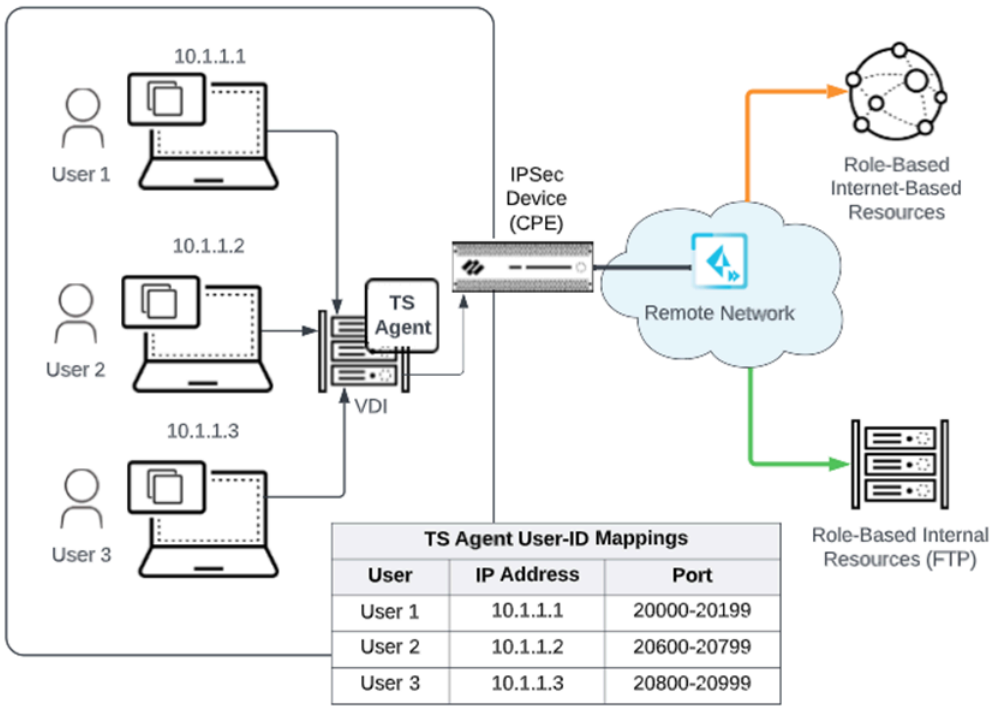
sowie interne und externe Ressourcen geschützt werden. Diese Lösung verwendet den Palo Alto Networks TS-Agent, den Sie auf den VDI-Servern installieren.

Der TS-Agent ist eine Benutzer-ID-Software, die installiert wird, um die Herausforderung zu lösen, die mit der Identifizierung von Zuordnungen zwischen Benutzernamen und IP-Adressen verbunden ist, wenn Benutzer IP-Adressen gemeinsam verwenden. Nach der Installation des TS-Agenten werden alle angemeldeten Benutzer überwacht und einzelnen Benutzern wird ein bestimmter Satz von Ports zugewiesen. Wenn Prisma Access diesen VDI-Netzwerkverkehr von der VDI empfängt, identifiziert dieser den Benutzer anhand des Quellports des Benutzers. Diese Bereitstellung bietet Ihnen eine cloudbasierte Lösung, mit der Administratoren Sicherheitsrichtlinienregeln für VDI-Endbenutzer erstellen können, um ihren Zugriff auf das Internet und interne Websites zu steuern.

Wenn Ihr Netzwerk über eine Standardroute verfügt, können Sie ein oder mehrere Remote-Netzwerke integrieren und den TS-Agent implementieren, um die Benutzer und Ressourcen in Ihrer Organisation komfortabel und einfach zu schützen.

Merkmale dieser Bereitstellung:

- Sie geben einen Portbereich im TS-Agent an, um bestimmte Benutzer auf Windows-basierten Terminalservern zu identifizieren. Der TS-Agent benachrichtigt Prisma Access über die zugewiesenen Portbereiche, sodass Prisma Access Richtlinien auf der Grundlage von Benutzern und Benutzergruppen durchsetzen kann.
- Das Remote-Netzwerk setzt die Sicherheit und Zugriffssteuerung für FTP- und internetbasierte Ressourcen durch.




| TS Agent User-ID Mappings | | |
|---|---|---|
| **User** | **IP Address** | **Port** |
| User 1 | 10.1.1.1 | 20000-20199 |
| User 2 | 10.1.1.2 | 20600-20799 |
| User 3 | 10.1.1.3 | 20800-20999 |

*Sie können Benutzerzuordnungsinformationen, die von einem TS-Agent gesammelt wurden, nicht umverteilen.*

 ©2025 Palo Alto Networks, Inc.

Gehen Sie wie folgt vor, um einen VDI mit dem TS-Agent und einem Prisma Access Remote-Netzwerk in von der Cloud verwaltetem Prisma Access zu integrieren.

**STEP 1 |** Installieren und konfigurieren Sie den TS-Agent von Palo Alto Networks auf den VDI-Servern.

Um alle Benutzer zuzuordnen, müssen Sie den TS-Agent auf allen Terminalservern installieren, bei denen sich Ihre Benutzer anmelden.

1. Installieren und konfigurieren Sie den TS-Agent von Palo Alto Networks auf den VDI Windows Servern.
2. Definieren Sie den Portbereich, den der TS-Agent den Endbenutzern zuweist.

   *Überprüfen Sie die unterstützte Skalenanzahl für den TS-Agent anhand der Kompatibilitätsmatrix.*
3. (Optional) Wenn mehrere VDI-Server vorhanden sind, konfigurieren Sie einen TS-Agent auf jedem Server.

**STEP 2 |** Binden Sie ein Remote-Netzwerk ein und verbinden Sie es mit der VDI-Zweigstelle in von der Cloud verwaltetem Prisma Access (sofern noch nicht geschehen).

**STEP 3 |** Konfigurieren Sie Optionen auf dem IPSec-Gerät (CPE) in der Zweigstelle, damit das Remote-Netzwerk mit dem VDI kommunizieren kann.

- Konfigurieren Sie IPSec- und IKE-Verschlüsselungsparameter für den IPSec-Tunnel, die den Parametern entsprechen, die Sie in Prisma Access konfiguriert haben.
- Verwenden Sie die **Service-IP**-Adresse (**Verwalten** > **Remote-Netzwerke** > **Dienst-IP**) als Prisma Access-Seite des IPSec-Tunnels für das Remote-Netzwerk.
- Konfigurieren Sie eine Route auf dem IPSec-Gerät, um VDI-Datenverkehr zum Remote-Netzwerktunnel zuzulassen.
- Konfigurieren Sie eine Route auf dem IPSec-Gerät, um den Remote-Netzwerkverkehr zum TS-Agent über den Tunnel zuzulassen.
- Konfigurieren Sie bei Bedarf eine Sicherheitsrichtlinie auf dem IPSec-Gerät, damit der Datenverkehr über den Tunnel geleitet werden kann.

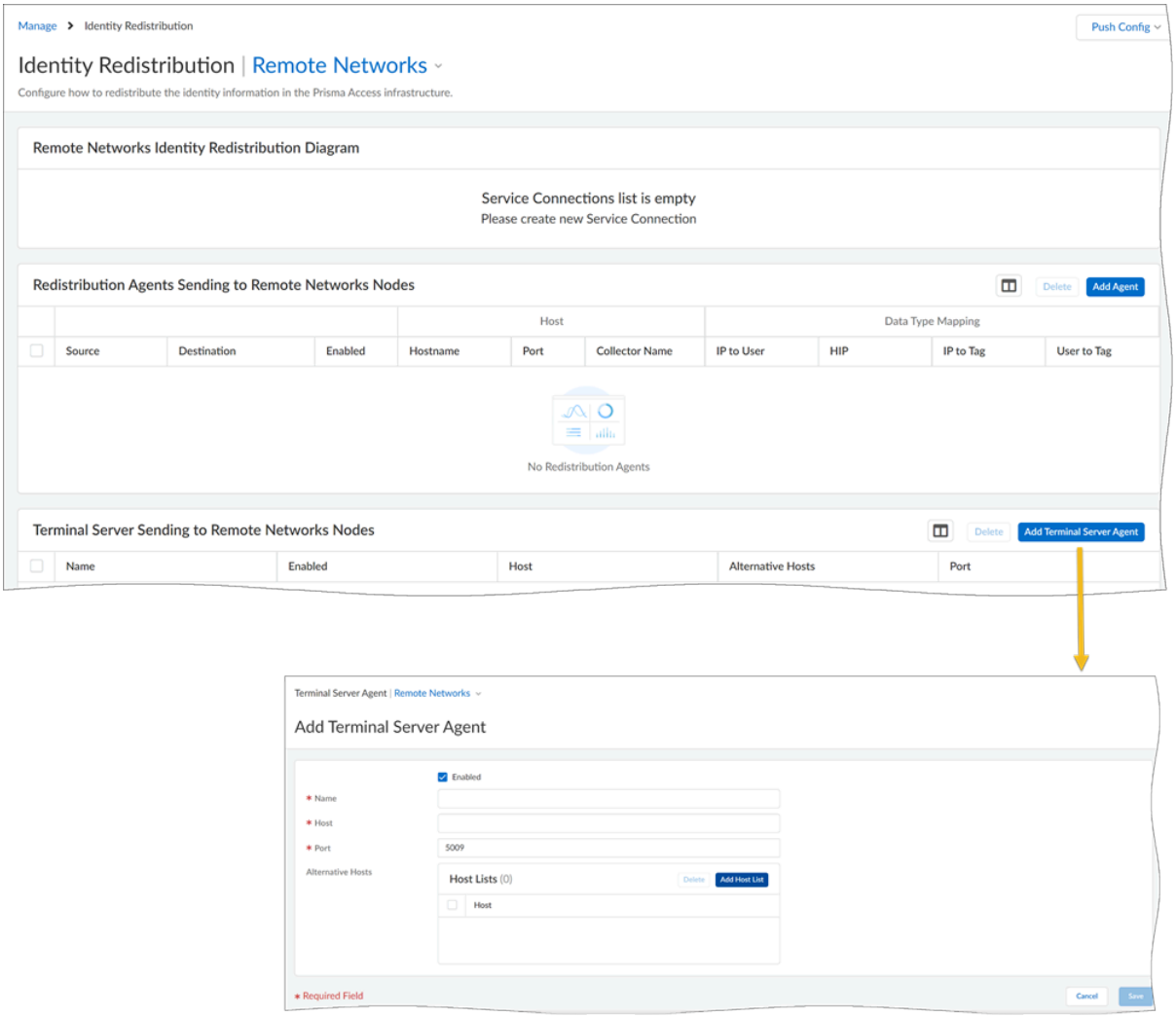
 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** Konfigurieren Sie den TS-Agent, um Benutzerzuordnungen im Remote-Netzwerk zu ermöglichen.

Gehen Sie zu **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Identitätsdienste** > **Identitätsweitergabe**, legen Sie den **Konfigurationsumfang** auf **Remote-Netzwerke** fest und wählen Sie **TS-Agent hinzufügen** aus.

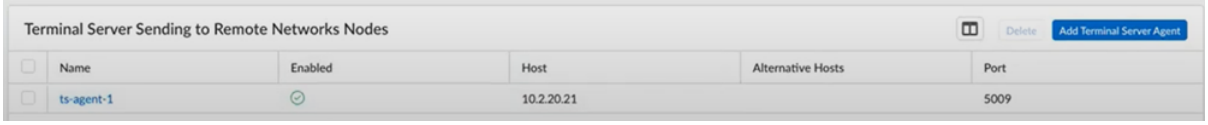
- Stellen Sie sicher, dass der Agent **aktiviert** ist.
- Geben Sie einen **Namen** für den TS-Agent ein.
- Geben Sie die IP des **Windows-Hosts** ein, auf dem der TS-Agent installiert ist.
- Geben Sie die Nummer des **Ports** ein, an dem der Agent auf Benutzerzuordnungsanfragen wartet.

  Der Port ist standardmäßig auf 5009 festgelegt.
- **Save (Speichern)** Sie Ihre Änderungen.




Im folgenden Beispiel ist ein Agent mit der Hostadresse 10.2.20.21 und dem Port 5009 konfiguriert.

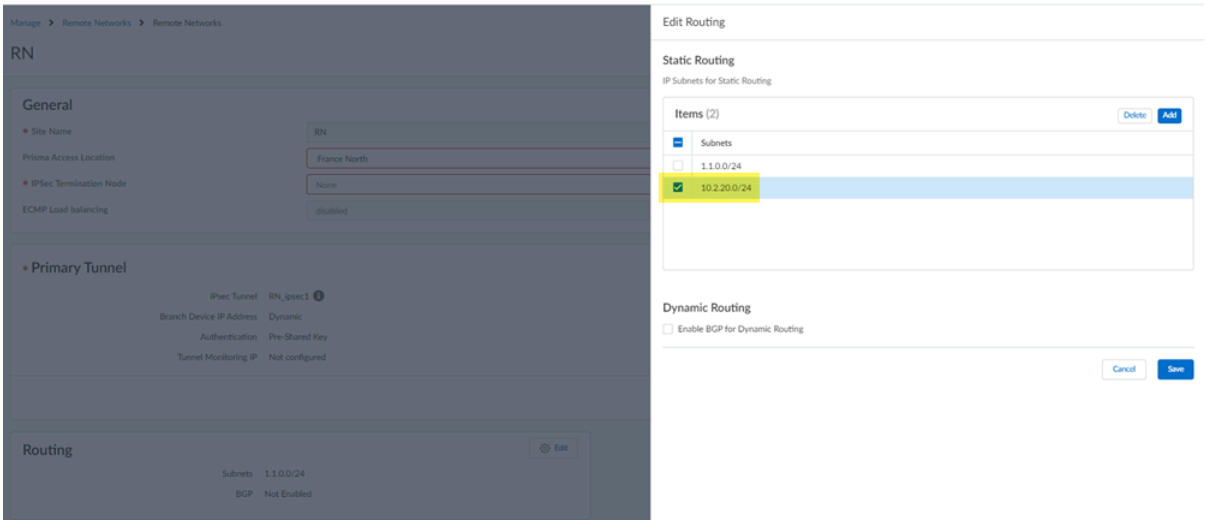
 ©2025 Palo Alto Networks, Inc.




**STEP 5 |** Lassen Sie das Routing zwischen dem VDI und dem Prisma Access-Remote-Netzwerk zu.

1. Wählen Sie **Verwalten** > **Diensteinrichtung** > **Remote-Netzwerke** > ***Name_des_Remote-Netzwerks*** > **Routing** und **Hinzufügen** aus, um eine Route zum VDI-Subnetz hinzuzufügen.

   Durch Hinzufügen dieses Subnetzes kann der TS-Agent mit dem Remote-Netzwerk kommunizieren. Im folgenden Beispiel-Screenshot lautet das VDI-Subnetz 10.2.20.0/24.




2. Gehen Sie zu **Verwalten** > **Konfiguration** > **Sicherheitsdienste** > **Sicherheitsrichtlinie**, legen Sie den Umfang auf **Remote-Netzwerke** fest und fügen Sie eine Sicherheitsrichtlinienregel hinzu (**Regel hinzufügen**), um Datenverkehr zwischen dem VDI-Subnetz und dem Remote-Netzwerk zuzulassen.

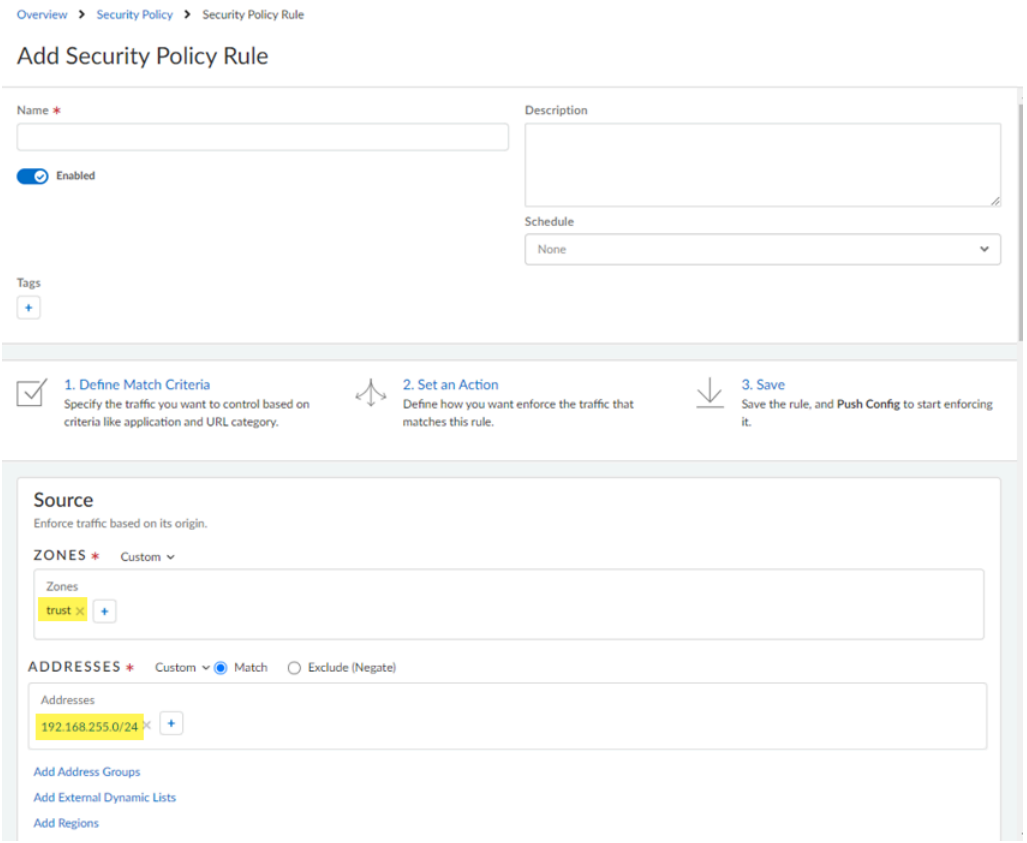
   Benutzern in Remote-Netzwerken, die über die VDI eine Verbindung mit Prisma Access herstellen, wird eine IP-Adresse aus dem Prisma Access-Infrastruktursubnetz zugewiesen, und Sie müssen das Routing zwischen dem Infrastruktursubnetz und dem VDI-Subnetz zulassen.

   - Stellen Sie sicher, dass die Regel **aktiviert** ist.

 ©2025 Palo Alto Networks, Inc.

- **Quelle** – Legen Sie die folgenden Parameter fest:
  - **Zonen** – Legen Sie den Wert **Vertrauenswürdig** fest.
  - **Adressen** – Erstellen Sie ein Adressobjekt für das Infrastruktursubnetz (**Verwalten** > **Freigegeben** > **Infrastruktureinstellungen** > **Infrastruktursubnetz**) und fügen Sie das Adressobjekt hier hinzu.

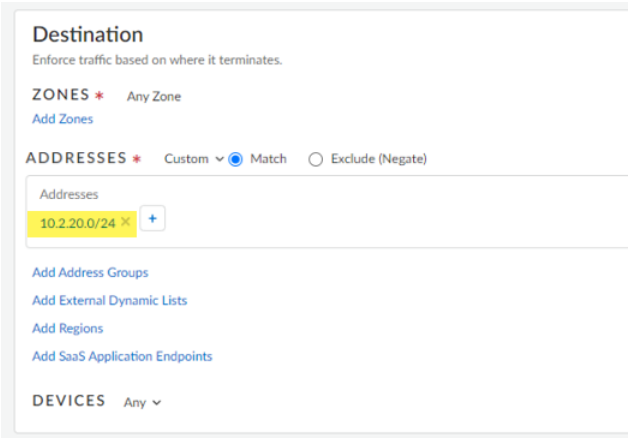
    *Ein Adressobjekt wird der Eingabe in das eigentliche Infrastruktursubnetz vorgezogen, da Sie bei einer Änderung des Subnetzes das Adressobjekt ändern können und die Änderung auf alle Konfigurationen angewendet wird, in denen das Adressobjekt verwendet wird.*



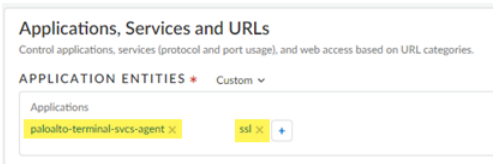

- **Ziel** – Fügen Sie den VDI-Host, auf dem der TS-Agent ausgeführt wird, zu den **Adressen** hinzu.

  Wenn Sie den TS-Agent auf mehreren VDI-Hosts konfiguriert haben, fügen Sie hier alle Hosts hinzu.

 ©2025 Palo Alto Networks, Inc.



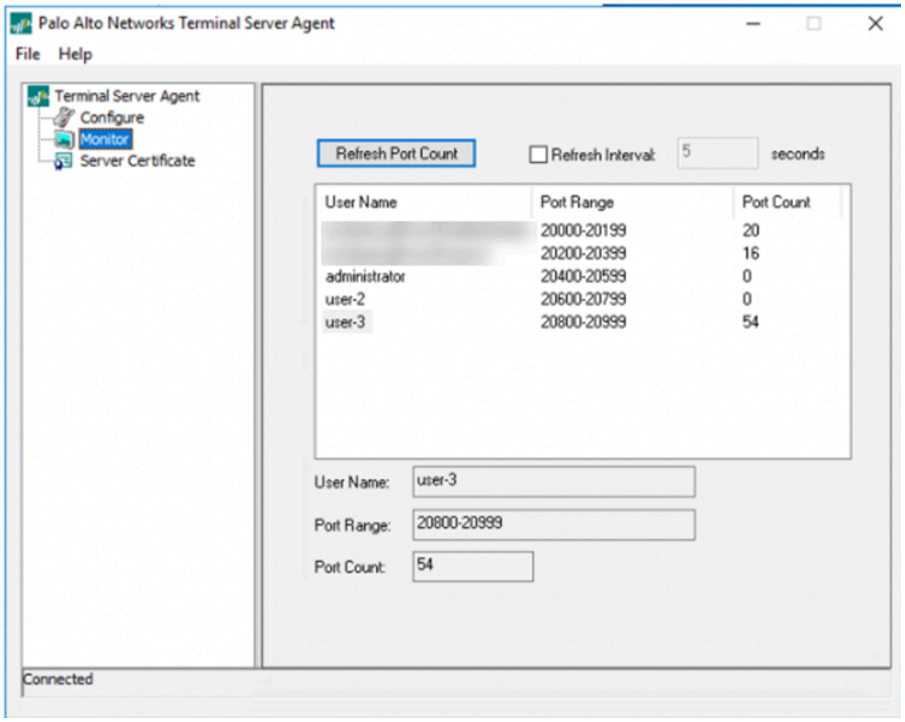

- **Anwendungen, Dienste und URLs** – Fügen Sie den Agent **paloalto-terminal-svcs-agent** und die **Anwendungsentitäten** hinzu.



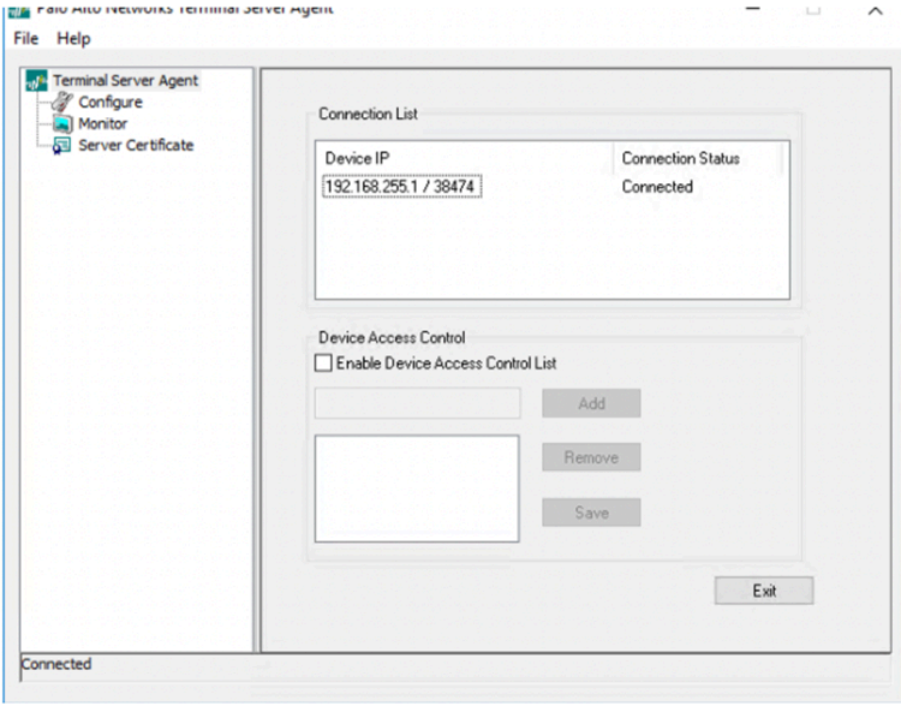

 ©2025 Palo Alto Networks, Inc.

**STEP 6 |** Überprüfen Sie, ob die Implementierung ordnungsgemäß funktioniert.

1. **Überwachen** Sie im TS-Agent den Status des Agenten und überprüfen Sie, ob der TS-Agent die korrekte Zuordnung des Benutzernamens zum Port widerspiegelt.

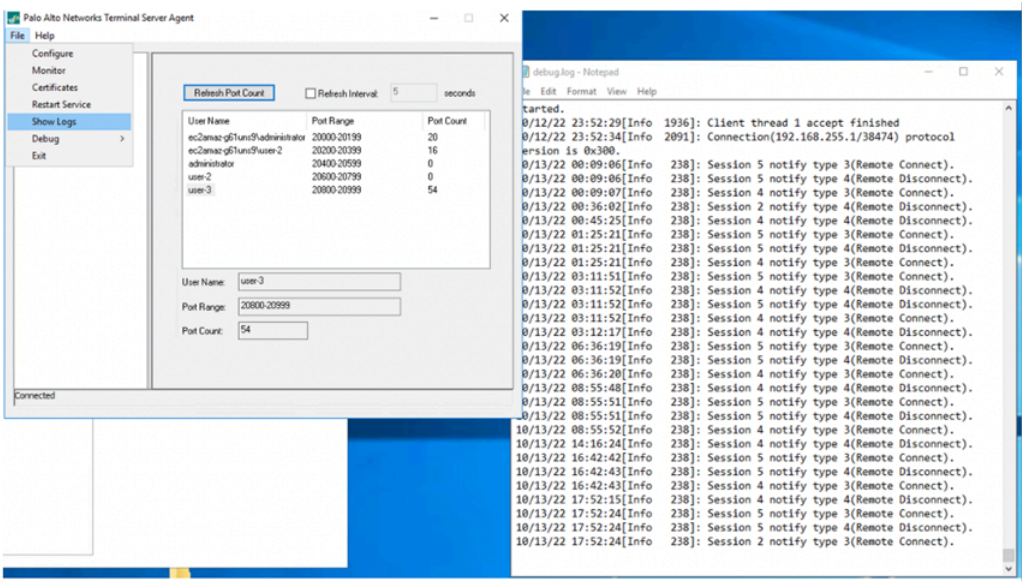



2. Stellen Sie sicher, dass die IP-Adresse des Remote-Netzwerks mit dem TS-Agent verbunden ist.

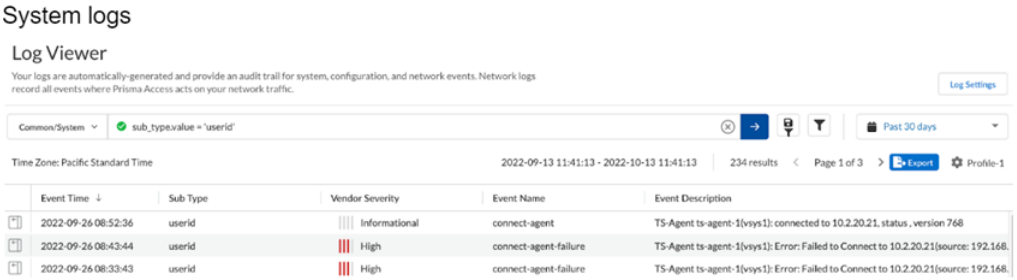



3. Gehen Sie zu **Datei** > **Protokolle anzeigen** und sehen Sie sich die Protokollnachrichten für den TS-Agent an.

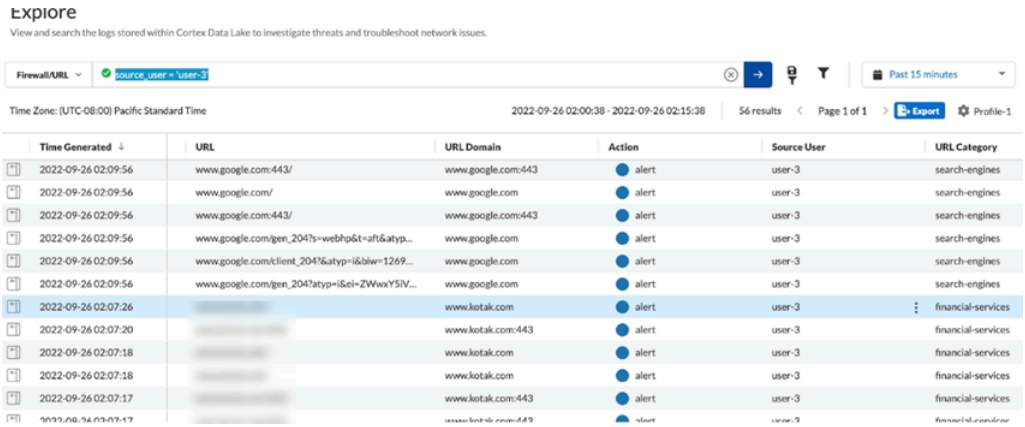
 ©2025 Palo Alto Networks, Inc.




4. Gehen Sie in Prisma Access (Managed by Strata Cloud Manager) zu **Aktivität** > **Protokoll-Viewer** > **Allgemein/System** und überprüfen Sie, ob die Remote-Netzwerke eine Verbindung zum TS-Agent herstellen können.




5. Gehen Sie zu **Aktivität** > **Protokoll-Viewer** > **Firewall/URL** und überprüfen Sie, ob die Remote-Netzwerke identitätsbasierte Richtlinien durchsetzen können.




 ©2025 Palo Alto Networks, Inc.

# Prisma Access – Überwachung und Transparenz

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz<br>❑ ADEM Observability-Lizenz ist erforderlich, um auf Autonomous DEM zuzugreifen. |

Prisma Access bietet die folgenden Funktionen, um Einblick in Ihre Sicherheitsaktivität zu erhalten und Ihre Bereitstellung zu überwachen. Diese Funktionen bieten Einblick in den Netzwerk- und Benutzerdatenverkehr durch Protokolle, Warnmeldungen über Remote-Netzwerke, Dienstverbindungen, mobile Benutzer, Ihre lizenzierten Entitäten sowie interaktive Dashboards, sodass Sie einen umfassenden Überblick über Daten zu Anwendungen, Bedrohungen, Benutzern und Sicherheitsabonnements bei der Arbeit in Ihrem Netzwerk erhalten. Sie können Prisma Access auch im Strata Cloud Manager überwachen.

- Protokolle von Prisma Access

  Ihre Protokolle werden automatisch generiert und stellen einen Audit-Trail für System-, Konfigurations- und Netzwerkereignisse bereit. Netzwerkprotokolle zeichnen alle Ereignisse auf, bei denen Prisma Access auf Ihren Netzwerkverkehr einwirkt. Beispielsweise werden Einträge aufgezeichnet, wenn Prisma Access den Datenverkehr auf der Grundlage einer Sicherheitsregel blockiert, einem Benutzer auf der Grundlage einer Authentifizierungsregel Zugriff gewährt oder den Datenverkehr auf der Grundlage einer QoS-Regel gestaltet. Sie können Prisma Access-Protokolle in den Verwaltungsschnittstellen von Strata Cloud Manager und Panorama anzeigen.
- Prisma Access Dashboards für Aktivitäten und Berichte

  „Aktivität“ bietet Ihnen einen umfassenden Überblick über die Vorgänge in Ihrem Netzwerk – von Ihren Protokolldaten bis hin zu wichtigen Ergebnissen, die Sie als Informationen für Richtlinienupdates und zum Schließen von Unternehmenssicherheitslücken und Benutzerproduktivitätslücken verwenden können.
- Prisma Access in Strata Cloud Manager überwachen
- Verschaffen Sie sich einen umfassenden Überblick über Ihren Netzwerkverkehr und die Produkte sowie Abonnements, die Sie mithilfe der Abschnitte Überwachen und Workflows in Strata Cloud Manager verwalten.
- Prisma Access und Autonomous DEM

  Autonomous DEM stellt native End-to-End-Transparenz und -Einblicke für den gesamten Benutzerdatenverkehr in Ihrer Secure Access Service Edge (Strata Cloud Manager) zur Verfügung. Autonomous DEM-Funktionalität ist nativ in die GlobalProtect-App und Prisma Access integriert und erfordert daher nicht die Bereitstellung zusätzlicher Appliances oder Agents. Sie können die Ursache von Problemen mit der digitalen Erfahrung schnell isolieren und die Problembehebung vereinfachen.

- Strata Cloud Manager Command Center

  Das Command Center ist eine interaktive, visuelle Zusammenfassung der IoT-Geräte, Benutzer, Hosts und des Datenverkehrs in Ihrem Netzwerk. Anhand der Daten Ihrer cloudbasierten Sicherheits- und ADEM-Abonnements zeigt das Command Center wichtige Informationen zu Bedrohungen, Benutzererfahrung und Sicherheit von Daten in Ihrem Netzwerk an.

  Das Command Center ermöglicht Ihnen die Interaktion mit den Daten und die Visualisierung der Beziehungen zwischen Ereignissen im Netzwerk, sodass Sie Anomalien aufdecken oder Möglichkeiten zur Verbesserung Ihrer Netzwerksicherheit finden können.

 ©2025 Palo Alto Networks, Inc.

# Protokolle von Prisma Access

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Ein Protokoll ist eine automatisch generierte Datei mit Zeitstempel, die einen Prüfpfad für Systemereignisse oder Netzwerkverkehrsereignisse bereitstellt, die von Prisma Access überwacht werden. Protokolleinträge enthalten Artefakte, bei denen es sich um Eigenschaften, Aktivitäten oder Verhaltensweisen im Zusammenhang mit dem protokollierten Ereignis handelt, z. B. Anwendungstyp oder IP-Adresse eines Angreifers. Jeder Protokolltyp zeichnet Informationen für einen separaten Ereignistyp auf. Beispielsweise kann Prisma Access ein Bedrohungsprotokoll erstellen, um Datenverkehr aufzuzeichnen, der einer Spyware, Sicherheitslücke oder Virensignatur entspricht. Prisma Access (Managed by Strata Cloud Manager) stellt Netzwerkprotokolle (wie Traffic, Threat, URL, Datei, HIP-Übereinstimmung), Endpunktprotokolle und allgemeine Protokolle (System und Konfiguration) bereit. Sie können Details für jeden Protokolleintrag anzeigen. Für Bedrohungsprotokolle können Sie Bedrohungsdetails überprüfen und sehen, ob Bedrohungsüberschreibungen vorhanden sind.

- Strata Cloud Manager
- Panorama

## Prisma Access-Protokolle (Strata Cloud Manager)

Wenn Sie **Strata Cloud Manager** verwenden, gehen Sie zu **Vorfälle und Benachrichtigungen** > **Protokoll-Viewer**.

Prisma Access (Managed by Strata Cloud Manager) bietet Netzwerkprotokolle (Verkehr, Bedrohung, URL, Datei, HIP-Übereinstimmung) und allgemeine Protokolle (System und Konfiguration).

Sie können Details für jeden Protokolleintrag anzeigen und Bedrohungsdetails für Bedrohungsprotokolle überprüfen, um festzustellen, ob Bedrohungsüberschreibungen vorhanden sind. Erfahren Sie mehr.

## Prisma Access-Protokolle (Panorama)

Sie können auch Prisma Access-Protokolle in der Oberfläche von Prisma Access (Managed by Panorama) anzeigen. Die Prisma Access-Infrastruktur leitet alle Protokolle an den Strata Logging Service weiter. Prisma Access ruft die Protokollergebnisse vom Strata Logging Service mithilfe des Cloud Services-Plug-ins ab und bietet eine aggregierte Ansicht der Protokolle Ihrer Remote-Netzwerke und des Datenverkehrs Ihrer mobilen Benutzer. Unabhängig von der Verwaltungsoberfläche, die Sie für Prisma Access–Panorama oder Strata Cloud Manager – verwenden, können Sie Ihre Protokolle in Prisma Access (Managed by Strata Cloud Manager) unter **Aktivität** > **Protokolle** > **Protokoll-Viewer** anzeigen.

 ©2025 Palo Alto Networks, Inc.

Neben den Protokollen aus der Prisma Access Cloud Service-Infrastruktur können Sie Protokolle auch direkt von der Panorama-Appliance aus anzeigen, von der Prisma Access verwaltet wird. Um Protokolle anzuzeigen, gehen Sie zu **Überwachen > Protokolle**. Erfahren Sie mehr.

 ©2025 Palo Alto Networks, Inc.

# Externe Protokolle und andere Daten

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Möglicherweise sind Sie bereits daran gewöhnt, die Protokolle von Prisma Access, die unterStrata Logging Service **Aktivität** > **Protokolle** gespeichert sind, anzuzeigen und mit ihnen zu interagieren. Aber wussten Sie, dass Prisma Access auch das Einlesen von Protokollen und anderen Daten aus einer Vielzahl externer Drittquellen unterstützt, wenn Sie einen Data Lake mit Cortex XDR Pro per TB-Lizenz haben? Sobald alles eingerichtet ist, können Sie mithilfe der Strata Logging Service-App auf dem Hub Protokolle anzeigen und die Protokollweiterleitung einrichten. Unterstützte Anbieter sind:

| | | |
|---|---|---|
| • Aktivieren der Windows-Ereignissammlung | • Corelight Zeek | • PAN IoT Security |
| • Amazon S3 | • Elasticsearch Filebeat | • PingFederate |
| • Apache Kafka | • Forcepoint DLP | • PingOne for Enterprise |
| • AWS | • Fortinet Fortigate | • Prisma Cloud |
| • AWS CloudTrail und Amazon CloudWatch | • Google Cloud Platform | • Prisma Cloud Compute |
| • Azure Event Hub | • Google Kubernetes Engine | • Proofpoint Targeted Attack Protection |
| • Azure Network Watcher | • Google Workspace | • ServiceNow CMDB |
| • BeyondTrust Privilege Management Cloud | • Microsoft Azure | • Windows DHCP mit Elasticsearch Filebeat |
| • Check Point FW1/VPN1 | • Microsoft Office 365 | • Workday |
| • Cisco ASA | • Okta | • Zscaler Cloud Firewall |

Sie können die Protokolle, die von Drittquellen eingelesen werden, als einzige Datenquelle nutzen oder diese Protokolle in Verbindung mit Prisma Access-Protokollen und zusätzlichen Datenquellen von Palo Alto Networks verwenden.

Reduzieren Sie mit Palo Alto Networks Ihre betriebliche Belastung und vereinfachen Sie Ihre SOC-Operationen radikal, indem Sie Daten aus allen Datenquellen – Netzwerk, Endpunkt und Cloud – sammeln, integrieren und normalisieren. Erhalten Sie eine einheitliche Ansicht und umsetzbare Einblicke in Anwendungsnutzung, Datenverkehrsmuster, Bedrohungen und Vorfälle in Ihrem gesamten Unternehmen.

 ©2025 Palo Alto Networks, Inc.

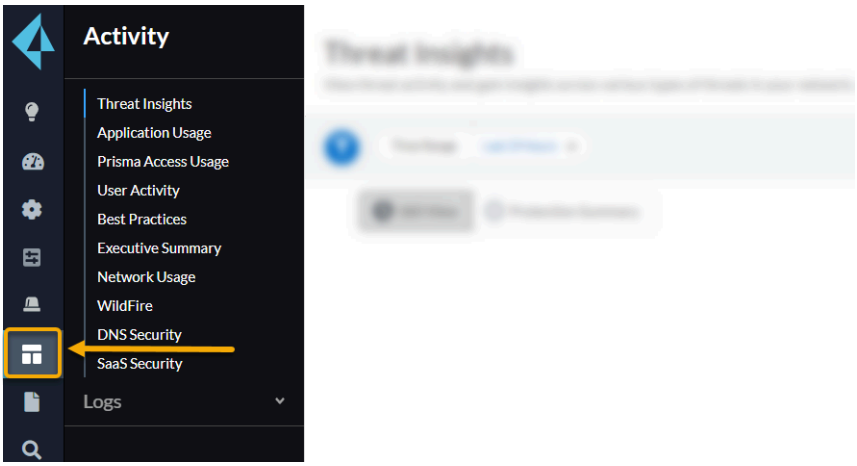
# Prisma Access Dashboards für Aktivitäten und Berichte

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Panorama Managed Prisma Access | ❑ Prisma Access-Lizenz<br>❑ Überprüfen Sie die Lizenzen und anderen Anforderungen der Dashboards für Aktivitäten und Berichte |

Aktivität identifiziert wichtige Ergebnisse, die Sie verwenden können, um über Ihre Richtlinienupdates zu informieren und Lücken in der Unternehmenssicherheit und Benutzerproduktivität zu schließen. Aktivität bietet Ihnen:

- Interaktive Dashboards, in denen Sie Daten zu Anwendungen, Bedrohungen, Benutzern und Sicherheitsabonnements bei der Arbeit in Ihrem Netzwerk erkunden können.
- Berichte, die Sie offline teilen und für die Sie regelmäßige Updates planen können.
- Der Protokoll-Viewer bietet einen Prüfpfad für System-, Konfigurations- und Netzwerkereignisse. Sie können von den Dashboards in den Protokoll-Viewer wechseln, um weiterführenden Kontext zu erhalten und einen Drilldown durchzuführen, um Ihre Daten eingehender zu analysieren.
- Die Suche nach Sicherheitsartefakten unterstützt Sie bei der Suche nach Artefakten wie einem Dateihash, einer URL, einer Domäne oder einer IP-Adresse (IPv4 oder IPv6), um die Daten speziell für dieses Artefakt zu nutzen. Die Suchergebnisse umfassen die Historie des Artefakts, Bedrohungsinformationen zum Artefakt und Analyseergebnisse von Drittanbietern für das Artefakt.

Benutzer von Prisma Access (Managed by Strata Cloud Manager) und Panorama Managed Prisma Access können **Aktivität** in der Prisma Access (Managed by Strata Cloud Manager)-App nutzen. Zunächst müssen Sie Prisma Access (Managed by Strata Cloud Manager) starten und dann im linken Navigationsfenster auf die Registerkarte **Aktivität** klicken.




Als Teil der Zertifizierung von Prisma SASE FedRAMP High „In Process“ wird Insights unterstützt. Aktivität wird als Teil der Zertifizierung von Prisma SASE FedRAMP High „In Process“ unterstützt.

 ©2025 Palo Alto Networks, Inc.

- Erste Schritte mit Activity

 ©2025 Palo Alto Networks, Inc.

# Prisma Access in Strata Cloud Manager anzeigen und überwachen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz<br>❑ Dies ist eine Funktion von Prisma Access Insights. |

Palo Alto Networks Strata Cloud Manager Command Center ist eine KI-basierte Netzwerksicherheitsplattform. Mit Strata Cloud Manager und Strata Cloud Manager Command Center können Sie Ihre gesamte Netzwerksicherheitsinfrastruktur von Palo Alto Networks problemlos über eine einzige, optimierte Benutzeroberfläche verwalten.

Über Activity Insights im Command Center sowie in den Bereichen Überwachen und Workflows im Command Center erhalten Sie umfassende Einblicke in Ihren Netzwerkverkehr und die von Ihnen verwalteten Produkte und Abonnements.

- **Anwendungen anzeigen und überwachen** – Informationen zu den von Ihnen verwendeten Anwendungen finden Sie unter **Activity Insights** > **Anwendungen**.
- **App-Beschleunigung anzeigen und überwachen** – Mit der App-Beschleunigung können die Ursachen für schlechte App-Leistung behoben werden – und das in Echtzeit. Auf diese Weise wird die Benutzererfahrung für Benutzer von Prisma Access GlobalProtect und Remote-Netzwerk verbessert. Gehen Sie zu **Activity Insights** > **Anwendungen**, um Details zu allen beschleunigten Anwendungen anzuzeigen.
- **Mobile Benutzer anzeigen** – Über **Alle Benutzer** erhalten Sie einen Überblick über alle Benutzer, die mit den Sicherheitslösungen von Palo Alto Networks verbunden sind, einschließlich Next-Generation Firewall (NGFW) und Prisma Access. Sie können den Verbindungsstatus eines Benutzers zu NGFW oder Prisma Access einfach ermitteln, unabhängig davon, ob es sich um eine Zweigstelle, eine Dienstverbindung oder einen Remote-Standort handelt. Gehen Sie zu **Activity Insights** > **Insights** > **Benutzer**, um Informationen über Ihre **Agent-Benutzer**, **Proxy-Benutzer ohne Agenten**, **Office-Benutzer** und **andere Benutzer** von Prisma Access anzuzeigen.
- **Zweigstellen anzeigen und überwachen** – Wählen Sie **Überwachen** > **Zweigstellen** > **Prisma Access** aus, um die Integrität und die Konnektivität Ihrer Remote-Netzwerke sowie die Nutzung all Ihrer Remote-Netzwerke anzuzeigen, die an verschiedenen Prisma Access-Standorten bereitgestellt werden. Sie werden über den Echtzeit-Konnektivitätsstatus und Details zum Bandbreitenverbrauch sowie andere Bereitstellungsdetails informiert. Mobile Benutzer, Zweigstellen und Einzelhandelsstandorte stellen eine Verbindung zu Remote-Netzwerken her. Sie können auch den Zustand der Tunnel anzeigen, die für Ihre Remote-Netzwerke und mobilen Benutzer konfiguriert sind.

 ©2025 Palo Alto Networks, Inc.

- **Rechenzentren anzeigen und überwachen** – Gehen Sie zu **Überwachen** > **Rechenzentren** > **Dienstverbindungen**, um aggregierte Daten zu Dienstverbindungen sowie Informationen zu einzelnen Dienstverbindungen anzuzeigen.

  Gehen Sie zu **Überwachen** > **Rechenzentren** > **ZTNA-Connectors**, um die Integrität und den Status einer ZTNA-Connector-Gruppe und einzelner ZTNA-Connectors anzuzeigen.
- Gehen Sie zu **Überwachen** > **Rechenzentren** > **ZTNA-Zugriffsobjekte**, um Einblick in Ihre ZTNA-Connector-Zugriffsobjekte zu erhalten.
- **Netzwerkdienste anzeigen und überwachen** – Gehen Sie zu **Überwachen** > **Netzwerkdienste** > **GlobalProtect-Authentifizierung**, um die Leistung gängiger Netzwerkdienste anzuzeigen, die sich auf Ihre Benutzererfahrung für den Zugriff auf Anwendungen auswirken. Netzwerkdienste umfassen Funktionen zur Meldung der Anzahl erfolgreicher und fehlgeschlagener GlobalProtect-Authentifizierungen als Maß dafür, ob mobile Benutzer eine Verbindung zu Prisma Access herstellen können. Gehen Sie zu **Überwachen** > **Netzwerkdienste** > **DNS**, um DNS-Proxyanfragen und -antworten anzuzeigen, die während des von Ihnen angegebenen Zeitraums an Server weitergeleitet werden.
- **Anzeigen und Überwachen der Abonnementnutzung** – Wählen Sie **Überwachen** > **Nutzung des Abonnements** aus, um Details zu Ihren **Prisma Access-Basisabonnements** anzuzeigen, einschließlich der Anzahl der Lizenzen, die Sie bisher verbraucht haben.
- **Prisma Access-Standorte anzeigen und überwachen** – Gehen Sie zu **Überwachen** > **Prisma Access-Standorte**, um eine Übersicht über den Zustand Ihrer Prisma Access-Standorte für Ihre Remote-Netzwerke und mobilen Benutzer anzuzeigen. Sie können einen Zeitbereich auswählen, um den Status des Prisma Access-Standorts und die Strata Logging Service-Konnektivität während dieser Zeit sowie eine Tabelle anzuzeigen, in der alle Prisma Access-Standorte aufgelistet sind. Außerdem können Sie einen einzelnen Prisma Access-Standort nach Namen auswählen, um dessen Details anzuzeigen.
- **Prisma Access-Upgrades anzeigen** – Wählen Sie **Workflows** > **Software-Upgrades** > **Prisma Access** aus, um Informationen zum Upgrade-Prozess von Prisma Access anzuzeigen.
- **Geräte-IDs von Drittanbietern anzeigen und überwachen** – Gehen Sie zu **Überwachen** > **Geräte** > **IOT**, um Einblicke in Ihre IoT-Geräte zu erhalten, z. B. die Anzahl der IoT-Geräte, die in den letzten 30 Minuten verbunden waren, aller im ausgewählten Zeitraum verbundenen IoT-Geräte und Details zu allen verbundenen IoT-Geräten.
- **Remote-Browser-Isolation anzeigen und überwachen** – Wählen Sie **Überwachen** > **Benutzer** aus, um Einblick in Ihre RBI-Bereitstellung zu erhalten, indem Sie Metriken wie die Anzahl der aktiven RBI-Benutzer, Trends, Verbindungsstatus, RBI-Standortstatus, Datenverkehrsmessungen und Lizenzverbrauch anzeigen.

## Erste Schritte bei der Prisma Access-Überwachung in Strata Cloud Manager

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz<br>❑ Dies ist eine Funktion von Prisma Access Insights. |

 ©2025 Palo Alto Networks, Inc.

Prisma Access bietet Ihnen die Möglichkeit, Ihre Prisma Access-Umgebung im Strata Cloud Manager Command Center kontinuierlich zu überwachen. Mehrere Dashboards bieten Ihnen einen fokussierten Überblick über Ihre verschiedenen Bereitstellungen, Ihre Warnungen und die Prisma Access-Infrastruktur. Wenn ein Ereignis oder ein Status Ihre Aufmerksamkeit erfordert, sendet Prisma Access Ihnen Warnmeldungen, sodass Sie Probleme schnell lokalisieren und beheben können. Sie erhalten auch einen Überblick über die Korrekturen, an denen das Prisma Access-Team arbeitet. Sie können die Daten filtern, die Sie sehen möchten, indem Sie einen Zeitraum auswählen bzw. festlegen und Basisinformationen auf Überwachungsseiten mit einer Autonomous DEM-Lizenz anzeigen.

## Auswahlfilter für den Zeitbereich

Der Auswahlfilter **Zeitbereich** wird oben in den Dashboards angezeigt, in denen Sie Informationen nach Zeitbereich filtern möchten.

Die Uhrzeit ist lokalisiert, sodass Sie anhand der Ortszeit für Ihre Region filtern können. Daten werden jede Minute abgerufen, aber die in den meisten Histogrammen angezeigten Datenpunkte variieren je nach ausgewähltem **Zeitbereich**.

Prisma Access lässt Sie den **Zeitbereich** aus einigen vordefinierten Bereichen auswählen oder Ihren eigenen Datums- und Zeitbereich konfigurieren:

- **Letzte 15 Min.**

  1 Datenpunkt alle 3 Minuten für insgesamt 5 Datenpunkte.
- **Letzte 1 Stunde**

  1 Datenpunkt alle 3 Minuten für insgesamt 20 Datenpunkte.
- **Letzte 3 Stunden**

  1 Datenpunkt alle 3 Minuten für insgesamt 60 Datenpunkte.
- **Letzte 24 Stunden**

  1 Datenpunkt alle 5 Minuten für insgesamt 288 Datenpunkte.
- **Letzte 7 Tage**

  1 Datenpunkt alle 30 Minuten für insgesamt 336 Datenpunkte.
- **Letzte 30 Tage**

  1 Datenpunkt alle 3 Stunden für insgesamt 180 Datenpunkte.

 ©2025 Palo Alto Networks, Inc.

- **Benutzerdefiniert**

  Sie können ein benutzerdefiniertes Zeitintervall festlegen (beispielsweise Startdatum und #zeit am 1. Juni um 17:00 Uhr und Enddatum und #zeit am 2. Juni um 16:00 Uhr), zusätzlich zu den im Filter verfügbaren Auswahlmöglichkeiten für den vorab ausgefüllten **Zeitbereich**.

  Um eine Startzeit festzulegen, wählen Sie zuerst im Kalender das Datum und dann unter **Start** die Uhrzeit aus. **Übernehmen** Sie die Startzeit und legen Sie dann die Endzeit fest, indem Sie im Kalender ein Enddatum und unter **Ende** eine Uhrzeit auswählen.

  Sobald Sie einen benutzerdefinierten Zeitbereich festgelegt haben, wird er gespeichert und auf alle Widgets in Insights angewendet, die den Zeitbereichsfilter verwenden, um Daten anstelle von Echtzeitdaten anzuzeigen.

  Sie können aus einer vorab ausgefüllten Auswahl für den **Zeitbereich** benutzerdefinierte Zeitintervalle wählen:

  - **Letzte 15 Min.**

    1 Datenpunkt alle 3 Minuten für insgesamt 5 Datenpunkte.
  - **Letzte 1 Stunde**

    1 Datenpunkt alle 3 Minuten für insgesamt 20 Datenpunkte.
  - **Letzte 3 Stunden**

    1 Datenpunkt alle 3 Minuten für insgesamt 60 Datenpunkte.
  - **Letzte 24 Stunden**

    1 Datenpunkt alle 5 Minuten für insgesamt 288 Datenpunkte.
  - **Letzte 48 Stunden**

    1 Datenpunkt alle 30 Minuten für insgesamt 96 Datenpunkte.
  - **Letzte 7 Tage**

    1 Datenpunkt alle 30 Minuten für insgesamt 336 Datenpunkte.
  - **Letzte 30 Tage**

    1 Datenpunkt alle 3 Stunden für insgesamt 240 Datenpunkte.

## Basislinien in Widgets

Wenn Sie die AI-Powered ADEM-Lizenz gekauft haben, wird in den Trend-Widgets auf den folgenden Überwachungsseiten ein Datenband mit Basislinien angezeigt: Benutzer, Zweigstellen, Rechenzentren und Netzwerkdienste. Die Widgets zeigen die Basislinie im Hintergrund entlang der Trendlinien. So können Sie auf einen Blick erkennen, ob Ihre Daten die obere oder untere Grenze der Basislinie überschritten haben.

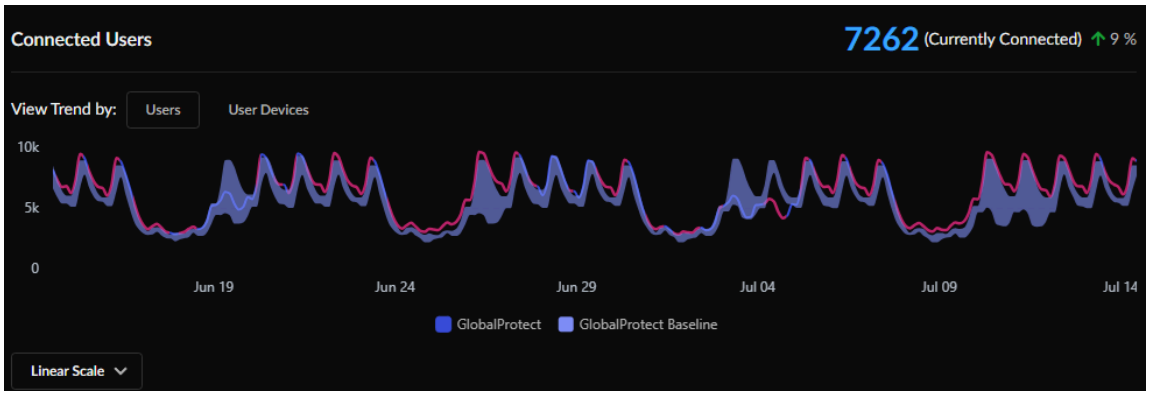
Die Basisliniendaten werden in Bin-Größen von einer Stunde berechnet und berücksichtigen die Daten der letzten 28 Tage aus diesen einstündigen Bins für einen bestimmten Tunnel, eine bestimme Zweigstelle, einen bestimmten Prisma Access-Standort oder eine bestimmte Anzahl von GlobalProtect-Benutzern. Beispielsweise wird die Basislinie von 13:00 Uhr bis 14:00 Uhr am Dienstag anhand des Zeitrahmens von 13:00 Uhr bis 14:00 Uhr der letzten vier Dienstage berechnet. Die Untergrenze ist das 10. Perzentil der gesammelten historischen Daten und die Obergrenze ist das 90. Perzentil. Auf diese Weise können Sie Trends für Bandbreite, Benutzerzahlen, Authentifizierungszahlen sowie DNS-Proxy-Anfragen und #Antworten sehen.

 ©2025 Palo Alto Networks, Inc.

Da die Basisliniendaten aus den historischen Daten der letzten 28 Tage stammen, müssen die neu hinzugekommenen Mandanten 28 Tage lang aktiv und datenreich sein, damit die Basislinie korrekt berechnet werden kann. Wenn Ihre Daten weniger als 28 Tage alt sind, sind Diskrepanzen möglich.

Wenn die Werte in der Trendlinie im Widget von den Ober- oder Untergrenzen der Basislinie abweichen, wird die Trendlinie für diesen Zeitraum in der Weboberfläche rot dargestellt.

Das folgende Beispiel zeigt die GlobalProtect-Basislinie aus dem Widget **Verbundener Benutzer** auf der Seite „Benutzer“.




# Anzeigen und Überwachen von Anwendungen

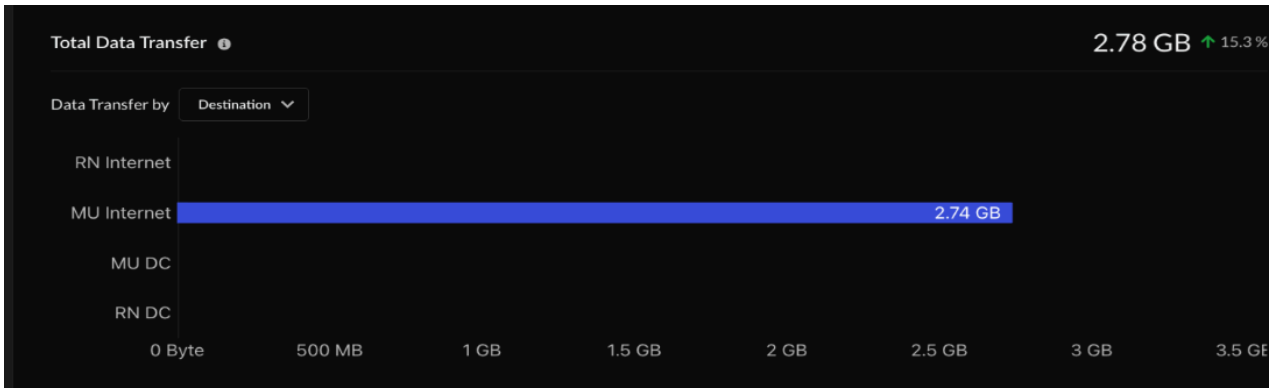
| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz<br>❑ Dies ist eine Funktion von Prisma Access Insights. |

Verwenden Sie das Strata Cloud Manager Command Center, um Prisma Access-Anwendungen in Ihrem Netzwerk sowie Benutzer, die die Anwendung verwenden, und deren potenzielle Sicherheitsauswirkungen zu überwachen. Gehen Sie zu **Insights** > **Anwendungen** um Einblick in die Prisma Access-Anwendungen sowie Informationen zu Bedrohungen, Benutzern, Datenübertragungen, Risiko-Scores (Bewertungen) und Benutzererfahrungen der Anwendungen zu erhalten.

## Gesamte Datenübertragung

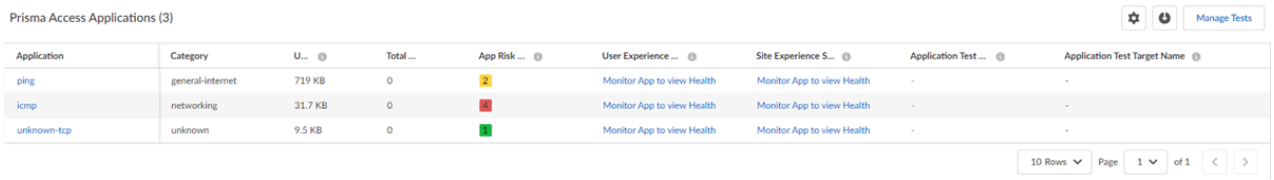
**Gesamte Datenübertragung** zeigt Ihnen die gesamte Datenübertragung über die Prisma Access Firewalls im ausgewählten Zeitbereich an. Verwenden Sie das Dropdown-Menü **Filter hinzufügen** für weitere Filteroptionen. Im Beispiel sehen Sie den Datentransfer nach **Anwendungskategorie**. Hier werden die wichtigsten Anwendungen und der gesamte Datentransfer für diese Anwendungen angezeigt. Sie können auch die gesamten Übertragungsdaten nach **Ziel** anzeigen.

 ©2025 Palo Alto Networks, Inc.




## Prisma Access-Anwendungen

Verwenden Sie dieses Widget, um zu sehen, welche Anwendungen mit synthetischen Tests überwacht werden. In der Tabelle sind auch die Erfahrungsbewertungen aufgeführt, die Aufschluss über den Zustand der einzelnen Anwendungen geben. Klicken Sie auf die Schaltfläche **Tests verwalten**, um in der Tabelle „Anwendungstests“ alle synthetischen Tests anzuzeigen, die für sämtliche Anwendungen eingerichtet sind.




| Spalte | Beschreibung |
|---|---|
| Anwendung | Die App-ID der überwachten Anwendung |
| Kategorie | Der Anwendungstyp |
| Verwendung | Der gesamte Datenverkehr in der Prisma Access-Infrastruktur, der für die jeweilige Anwendung festgestellt wurde |
| Bedrohungen insgesamt | Gesamtzahl der für die Anwendung aufgetretenen Bedrohungen |
| App-Risiko-Score | Bedrohungsdaten für diese konkrete Anwendung 1 steht für das niedrigste Risiko, 5 für das höchste Risiko. |
| Benutzererfahrung | Von Autonomous DEM erfasste Anwendungserfahrungswerte. Sie werden über alle Benutzer aggregiert, die für diese Anwendung überwacht werden. |
| Erfahrungswerte für den Standort | Anwendungserfahrungswerte für den jeweiligen Zweigstellenstandort |

 ©2025 Palo Alto Networks, Inc.

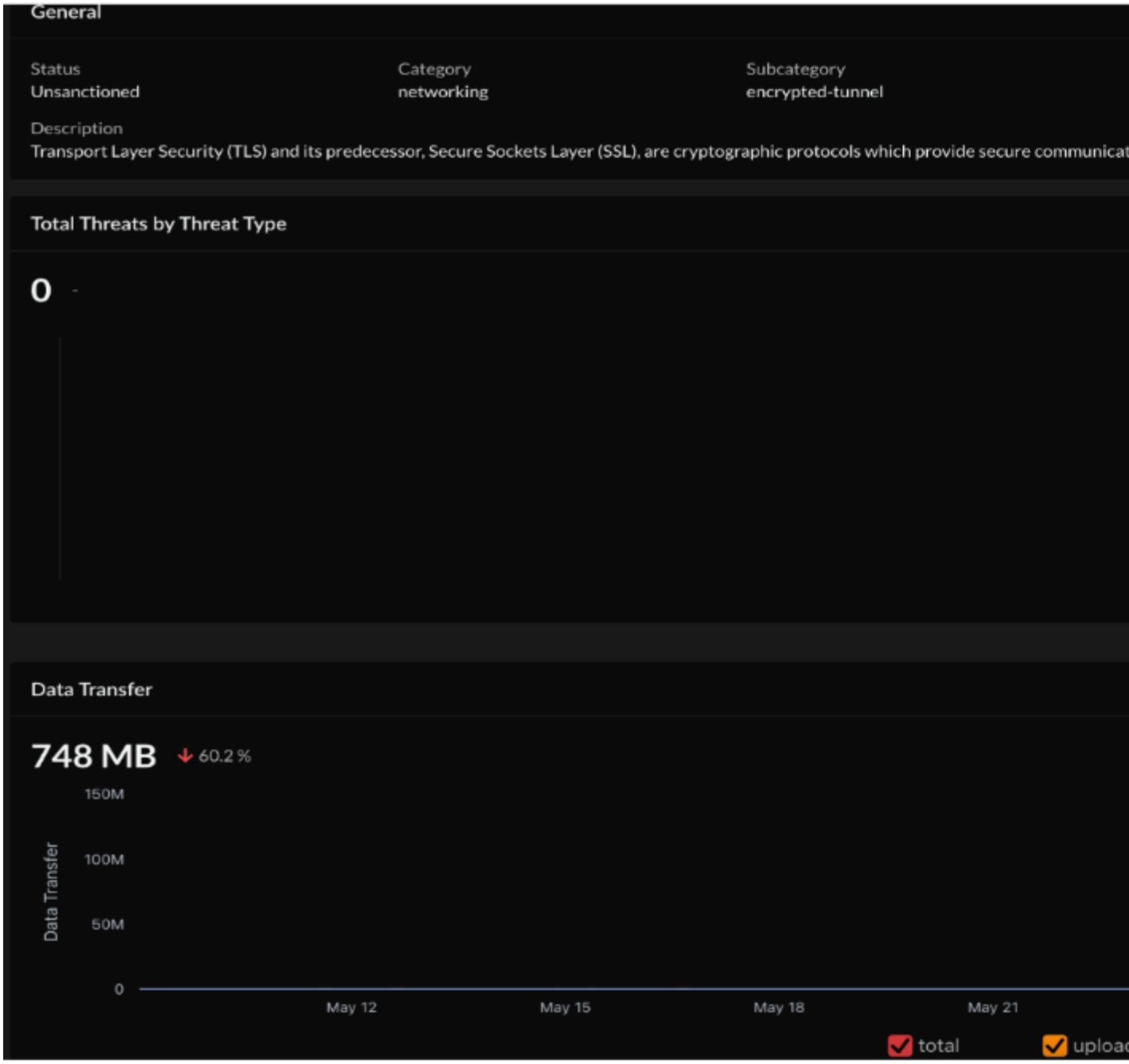
| Spalte | Beschreibung |
|---|---|
| Name Anwendungstest | Der Name des Testsets, das der Benutzer für diese Anwendung eingerichtet hat |
| Zielname Anwendungstest | IP-Adresse des FQDN, auf den die synthetischen Tests von verschiedenen Endpunkten abzielen. |

### Anwendungsdetails

Wählen Sie eine Anwendung aus, um deren **allgemeine** Details wie Status, Kategorie, Unterkategorie, Ports, Technologie und Risiko-Score anzuzeigen.

- **Bedrohungen insgesamt nach Bedrohungstyp** – Aktuelle Bedrohungen für die Anwendung
- **Benutzer insgesamt** – Die Gesamtzahl der Benutzer, die während des angegebenen Zeitraums auf diese Anwendung zugreifen
- **Datenübertragung** – Zeigt die Daten an, die für diese Anwendung hoch- bzw. heruntergeladen wurden

 ©2025 Palo Alto Networks, Inc.




# Anzeigen und Überwachen der App-Beschleunigung

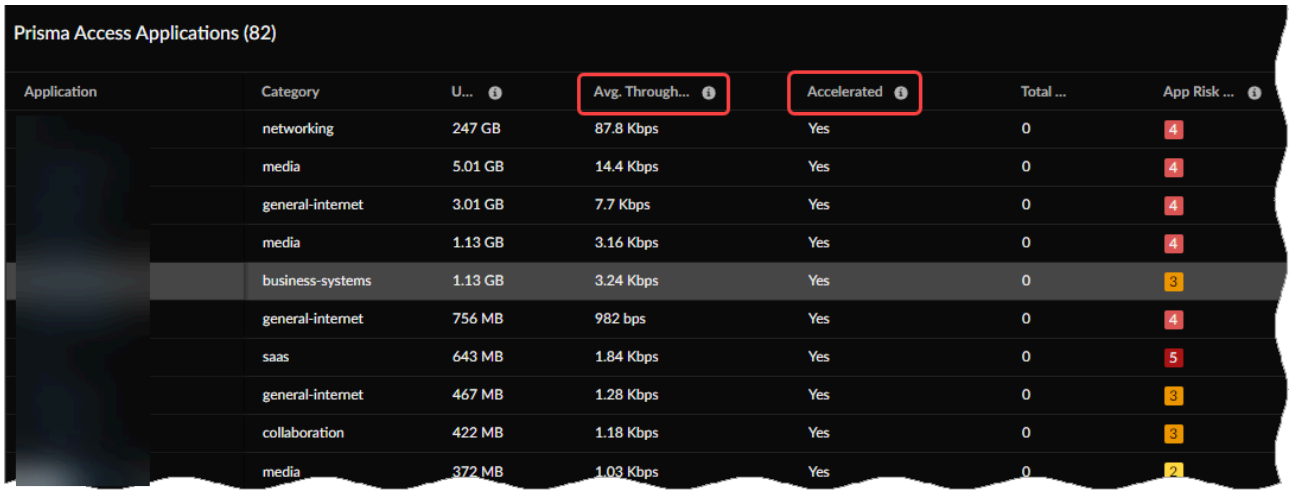
| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

 ©2025 Palo Alto Networks, Inc.

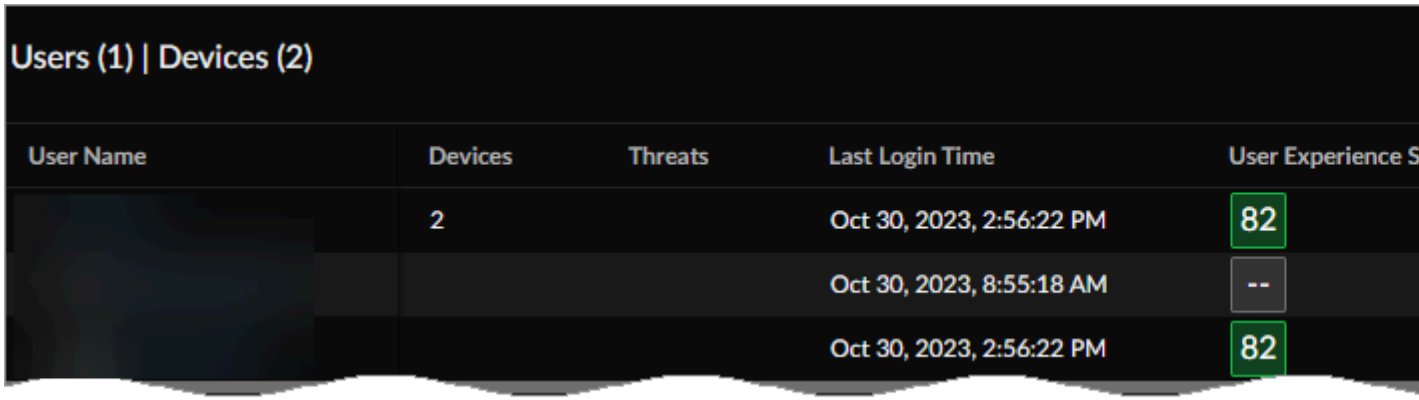
Durch die App-Beschleunigung können Sie die Ursachen einer schlechten App-Leistung beseitigen. Sie arbeitet im Echtzeitmodus, um die Auswirkungen der Ursachen zu mildern. Dadurch wird die Benutzererfahrung für Benutzer von Prisma Access GlobalProtect und Remote-Netzwerken verbessert.

Wenn Ihre Benutzer auf Apps zugreifen, könnte es zu einer schlechten App-Performance kommen, die durch verringerten Durchsatz verursacht wird, was wiederum durch verschlechterte drahtlose Konnektivität, Netzwerküberlastung und andere Faktoren verursacht werden kann. Diese Netzwerkprobleme können ihrerseits die Erfahrung der Mitarbeiter beeinträchtigen und ihre Produktivität verringern. Die App-Beschleunigung passt sich in Echtzeit an sich verändernde Netzwerkbedingungen an und liefert Daten, die zu einem soliden Verständnis der Fähigkeiten des Geräts, des Netzwerks und des Anwendungskontexts zur Durchsatzmaximierung verhelfen.

Gehen Sie im Strata Cloud Manager Command Center zu **Insights** > **Anwendungen** um detaillierte Angaben zu den Anwendungen anzuzeigen, die in Ihrer Umgebung beschleunigt wurden. Die Spalte „Durchschnittlicher Durchsatz“ in der Tabelle „Prisma Access-Anwendungen“ wird nur bei einem beschleunigten Datenverkehr Ihrer Benutzer angezeigt. In der Tabellenspalte „Beschleunigt“ wird angezeigt, dass ein Teil oder der gesamte Datenverkehr Ihrer Anwendung beschleunigt wurde.




Gehen Sie zu **Insights** > **Benutzer**, um Informationen zu den Benutzern der App-Beschleunigung in Ihrer Umgebung anzuzeigen. Benutzern mit aktivierter App-Beschleunigung in ihren Umgebungen wird die Tabelle „Benutzer | Geräte“ mit der Spalte „Beschleunigter Datenverkehr“ angezeigt. Aus dieser Spalte ist ersichtlich, dass der Anwendungsverkehr einiger oder aller Benutzer beschleunigt wurde.




 ©2025 Palo Alto Networks, Inc.

KI-gestütztes autonomes DEM (AI-powered Autonomous DEM, ADEM) ermöglicht die Integration mit der App-Beschleunigung und liefert Ihnen Metriken wie die Anzahl der Anwendungen, die beschleunigt wurden, und die insgesamt erzielte Leistungssteigerung. Gehen Sie zu **SASE-Zustand** > **Erfahrung** um ADEM-Leistungskennzahlen auf den Registerkarten **Beschleunigte Anwendungen** und **Überwachte Anwendungen** anzuzeigen.

## Anzeigen mobiler Benutzer

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma® Access (verwaltet von Strata Cloud Manager) | • Prisma Access-Lizenz<br>• KI-gestützte ADEM-Lizenz |

Sehen Sie sich Activity Insights: Benutzer an, um eine Übersicht aller Benutzer und Hosts zu erhalten, die mit den Prisma Access-Sicherheitslösungen von Palo Alto Networks verbunden sind. Mithilfe von Prisma Access können Sie den Verbindungsstatus eines Benutzers oder Hosts ganz einfach ermitteln, unabhängig davon, ob es sich um eine Zweigstelle, eine Dienstverbindung oder einen Remote-Standort handelt. Zeigen Sie Folgendes an:

- Die Gesamtzahl der eindeutigen Benutzer, die derzeit mit Sicherheitslösungen von Palo Alto Networks verbunden sind, und der Benutzer, die mit Prisma Access verbunden sind
- Die Anzahl der in einem bestimmten Zeitraum verbundenen Benutzer, aufgeschlüsselt nach Benutzern, die über Prisma Access verbunden sind
- Agentenbasierte Benutzer, die über Prisma Access verbunden sind
- Agentenbasierte oder browserbasierte Benutzer des expliziten Proxys, die mit Prisma Access verbunden sind
- Benutzer, die über Prisma Access Browser verbunden sind
- Eine Liste der nicht verwalteten Gerätebenutzer, die auf Prisma Access zugreifen
- Eine Liste der Benutzer, die sich von Zweigstellen aus mit Prisma Access verbinden
- Eine Liste der Benutzer, die ihre Rechenzentren über bestimmte Dienstverbindungen verbinden

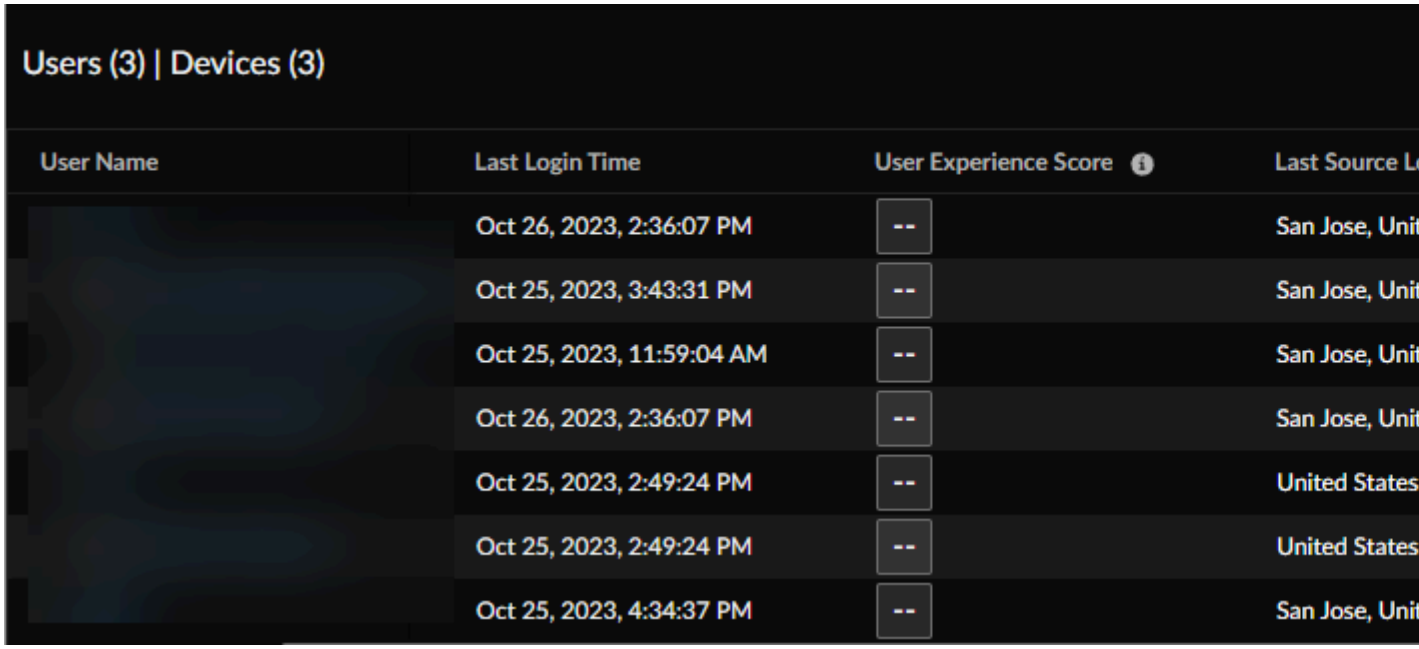
## Anzeigen und Überwachen von IPv6 für mobile Benutzer

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 5.0 Innovation<br>❑ Prisma Access-Lizenz |

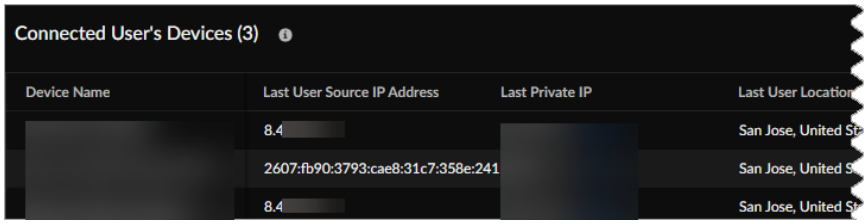
Wenn Sie IPv6-Netzwerke in Ihrer Bereitstellung Mobile Benutzer – GlobalProtect verwenden, können Sie Prisma Access so konfigurieren, dass IPv6-Adressen in Ihrem mobilen Benutzer-Networking verwendet werden. Außerdem müssen Sie IPv6-Netzwerke global in Ihrer Prisma Access-Infrastruktur aktivieren, bevor Sie IPv6-Adressierung verwenden können.

 ©2025 Palo Alto Networks, Inc.

Mit IPv6 in Ihrer GlobalProtect-Bereitstellung zeigt die Tabelle „Benutzer | Geräte“ in der Spalte „Quell-IP-Adresse“ entweder eine IPv4- oder eine IPv6-Adresse an.

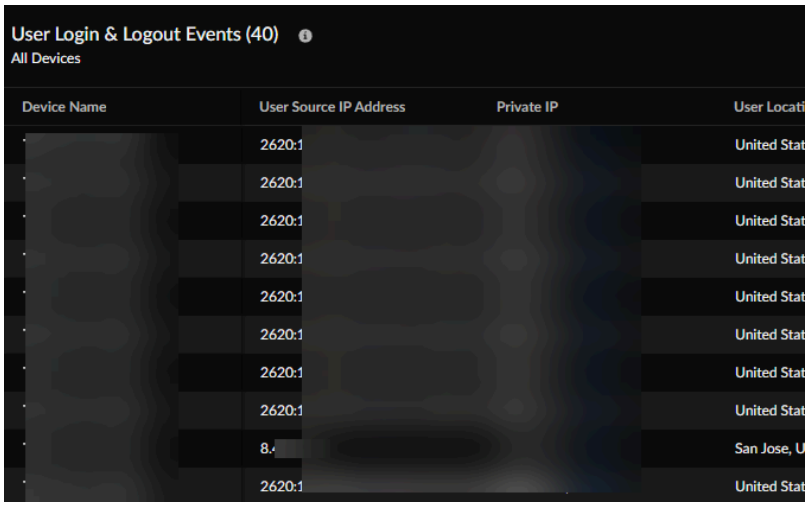



Wählen Sie einen verbundenen Benutzer aus, um Informationen zum Trend seiner Geräte anzuzeigen. In der Tabelle „Geräte eines verbundenen Benutzers“ werden Daten zu den Geräten eines Benutzers angezeigt, einschließlich der Quell-IP-Adresse und der privaten IP-Adresse des letzten Benutzers, die beide IPv4- und IPv6-Adressen für einen einzelnen Geräteeintrag enthalten können.




Sie können IPv6-Adressinformationen in der Tabelle „Benutzeranmeldung und -abmeldung“ anzeigen. In den Spalten „Quell-IP-Adresse des Benutzers“ und „Private IP-Adresse“ wird entweder eine IPv4- oder eine IPv6-Adresse angezeigt.

 ©2025 Palo Alto Networks, Inc.




# Anzeigen und Überwachen von Zweigstellen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz<br>❑ adem-aiops-Wert |

Wählen Sie **Überwachen** > **Zweigstellen** > **Prisma Access**aus, um den Zustand und die Konnektivität Ihrer Remote-Netzwerke sowie die Nutzung Ihrer gesamten Remote-Netzwerke anzuzeigen, die an verschiedenen Prisma Access-Standorten bereitgestellt werden. Hier sehen Sie den Echtzeit-Konnektivitätsstatus, Details zum Bandbreitenverbrauch sowie andere Bereitstellungsdetails. Sie können auch den Zustand der in Ihren Remote-Netzwerken konfigurierten Tunnel anzeigen.

Weitere Informationen zur Planung Ihrer Remote-Netzwerke, zur Zuweisung der Remote-Netzwerkbandbreite und zum Onboarding von Remote-Netzwerken finden Sie unter Prisma Access-Remote-Netzwerke. Wählen Sie zum Anzeigen Ihrer Zweigstellen die Optionen **Überwachen** > **Zweigstellen** > **Prisma Access**aus.

## Standorte nach Status

Zeigen Sie bei Ihrem Remote-Netzwerk die **Standorte nach Status** an. Sie können sehen, wie viele Standorte **aktiv**, **ausgefallen**, **inaktiv** oder **nicht verfügbar** sind und für wie viele Standorte im ausgewählten **Zeitbereich** eine **Warnung** angezeigt wird.




 ©2025 Palo Alto Networks, Inc.

## Bandbreitenverbrauch

Der **Bandbreitenverbrauch** zeigt die höchste Spitzenbandbreite an, die in einer Rechenregion über alle Rechenregionen des Mandanten im aggregierten Bandbreitenzuweisungsmodell verbraucht wird. Für das Modell der Bandbreitenzuweisung pro Standort wird die höchste Spitzenbandbreite angezeigt, die ein Standort über alle Standorte hinweg verbraucht. Die Spitzenwerte werden für die gewählte Zeitfilterdauer berechnet.

Wählen Sie **Verbrauch nach Rechenregion anzeigen** aus, um Verbrauchswerte und Trenddiagramme für alle Rechenregionen und deren konfigurierte IPSec-Abschlussknoten anzuzeigen.

### Verbrauch nach Rechenregionen anzeigen

Navigieren Sie zu **Überwachen** > **Zweigstellen** > **Prisma Access**. Wenn Sie das Modell für die Aggregate-Bandbreitenzuweisung verwenden, wählen Sie im Widget **„Bandbreitenverbrauch**“ die Option „**Verbrauch nach Rechenregionen anzeigen**“, um den Bandbreitenverbrauch und Trends für Ihre Regionen anzuzeigen.

Auf der Seite **Rechenregionen** werden Bandbreitenverbrauchsdaten während des von Ihnen ausgewählten **Zeitbereichs** angezeigt. Sie können eine Tabelle mit der **durchschnittlichen Bandbreite**, der **mittleren Bandbreite** und der **höchsten Bandbreite** Ihrer Rechenregionen anzeigen.

Das Diagramm **Trend für Bandbreitenverbrauch nach Rechenregion** zeigt Daten zu Ihrer Rechenregion an. Filtern Sie die Daten, um die Informationen zu präzisieren, die Sie anzeigen möchten.

- Wählen Sie **Kumulativ (Ein- und Ausgang)**, **Eingang**, **Ausgang** oder **Eingang vs. Ausgang** aus der Dropdown-Liste aus.
- Sie können den Trend für den **höchsten**, **mittleren** oder **durchschnittlichen** Bandbreitenverbrauch während des ausgewählten Zeitraums anzeigen. Standardmäßig wird der **höchste** Bandbreitenverbrauch angezeigt.
- **Logarithmische Skala** oder **Lineare Skala**.
- **Rechenregion** – Wählen Sie eine oder mehrere Regionen aus, die Sie anzeigen möchten.

Im Diagramm **Nutzung des IPSec-Terminierungsknotens** können Sie den Bandbreitenverbrauch für die IPSec-Terminierungsknoten anzeigen, die in einer bestimmten Rechenregion konfiguriert sind. Filtern Sie die Daten, um die Informationen zu präzisieren, die Sie anzeigen möchten:

- Wählen Sie die Rechenregion aus, für die Sie Daten anzeigen möchten.
- Wählen Sie den Standort der Rechenregion aus, die Sie anzeigen möchten.
- Wählen Sie **Knotenaggregat** oder **Aufschlüsselung nach Standorten** aus, um den Trend für Bandbreitenverbrauch für die Standorte anzuzeigen, die am ausgewählten IPSec-Terminierungsknoten enden.
- Zeigen Sie den **höchsten**, **durchschnittlichen** oder **mittleren** Bandbreitenverbrauch an.

 ©2025 Palo Alto Networks, Inc.

- Zeigen Sie die **logarithmische Skala** oder die **lineare Skala** an.




## Trend für Bandbreitenverbrauch

Auf der Hauptseite der **Zweigstellen** können Sie Ihre **„Trend für Bandbreitenverbrauch“-Standorte pro Rechenregion** für alle Rechenregionen anzeigen, wenn Sie das Modell für die Gesamtbandbreitenzuweisung verwenden. Mit dem **Modell für Zuweisung von Bandbreite pro Standort** zeigen Sie den **Trend für Bandbreitenverbrauch pro Zweigstellen** an. Für das Modell für Zuweisung von aggregierter Bandbreite können Sie eine Rechenregion und dann die Standorte in dieser Rechenregion auswählen, deren Bandbreiten-Verbrauchstrend für Sie von Interesse ist. Filtern Sie die Daten, um die Informationen zu präzisieren, die Sie anzeigen möchten. Wenn Sie mit dem Mauszeiger über das Diagramm fahren, können Sie den Bandbreitenverbrauch der Standorte zum aktuellen Zeitpunkt anzeigen:

- Standardmäßig wird der Bandbreitenverbrauch **Kumulativ (Ein- und Ausgang)** angezeigt. Weitere Optionen sind **Eingang**, **Ausgang** oder **Eingang vs. Ausgang**.
- Zeigen Sie den Trend für den **höchsten**, **mittleren** oder **durchschnittlichen** Bandbreitenverbrauch während des ausgewählten Zeitraums an. Standardmäßig wird der **höchste** Bandbreitenverbrauch angezeigt.

 ©2025 Palo Alto Networks, Inc.

- **Logarithmische Skala** oder **Lineare Skala**.
- **Rechenregion**: Zeigen Sie die Rechenregionen mit einer Aufschlüsselung der Standorte an, die in der Region enden, wenn der Mandant das Modell für Zuweisung von aggregierter Bandbreite verwendet. Wählen Sie für jede Rechenregion die Standorte aus, die in der Rechenregion enden, um deren Bandbreiten-Verbrauchstrend anzuzeigen.
- **Zweigstellen**: Wählen Sie mindestens einen Standort und maximal zehn Standorte aus, um deren Trendlinien im ausgewählten Zeitraum grafisch anzuzeigen.



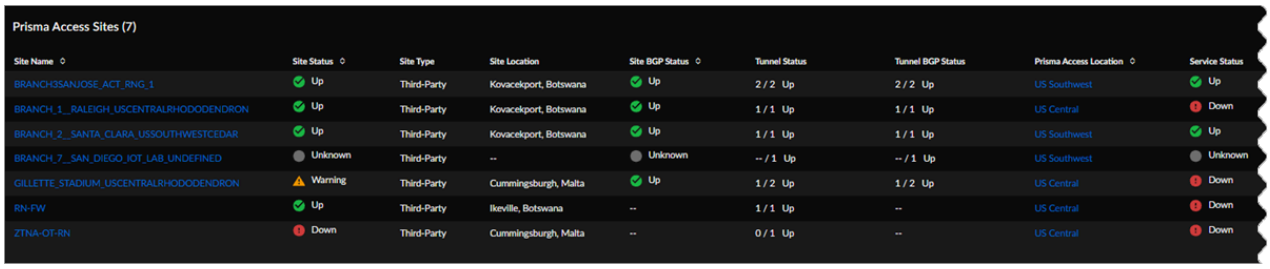

## Prisma Access-Standorte

In der Tabelle **Prisma Access-Standorte** werden Ihre Remote-Standorte von Prisma Access mit den zugehörigen Informationen aufgelistet.

- **Standortname**: Der eindeutige Name des Prisma Access-Standorts.
- **Standortstatus**: **Aktiv**, **Inaktiv**, **Warnung** oder **Unbekannt**.
- **Standorttyp**: Drittpartei.
- **Standort**: Der Prisma Access-Standort.

 ©2025 Palo Alto Networks, Inc.

- **BGP-Status des Standorts**: Zeigt an, ob der BGP-Status des Standorts **aktiv**, **inaktiv** oder **unbekannt** ist.
- **Tunnelstatus**: Die Anzahl der Tunnel des Standorts und wie viele dieser Tunnel aktiv sind.
- **BGP-Status des Tunnels**: Der BGP-Status für jeden Tunnel.
- **Prisma Access-Standort**: Aktueller Prisma Access-Standort. Wählen Sie einen Standort aus, um die Details der Prisma Access-Standorte anzuzeigen.
- **Dienststatus**: Dieses Feld gibt den Status der Instanz oder Firewall an, mit der der Standort verbunden ist. Der Status kann **Aktiv**, **Inaktiv** oder **Unbekannt** sein.
- **Compute-Standort**: Alle Prisma Access-Standorte werden basierend auf optimierter Leistung und Latenz einem Compute-Standort oder einer Region für die Sicherheitsverarbeitung zugeordnet. Mindestens zwei (und häufig weitere) geografisch nahe beieinander liegende Prisma Access-Standorte werden in Compute-Standorte gruppiert.
- **Zugeordnete aggregierte Bandbreite**: Die zugewiesene aggregierte Bandbreite für den Standort während des ausgewählten Zeitraums. Diese Spalte wird nur angezeigt, wenn Sie das aggregierte Bandbreitenmodell verwendet haben.
- **Höchste verbrauchte Burst-Bandbreite**: Der kumulative Spitzenwert, der durch die Kombination der Ein- und Ausgangswerte für diesen Standort während des ausgewählten Zeitraums ermittelt wurde.
- **Durchschn. verbrauchte Bandbreite**: Der kumulative Durchschnittswert, der durch die Kombination der Ein- und Ausgangswerte für diesen Standort während des ausgewählten Zeitraums ermittelt wurde.
- **Trennungen**: Zeigt an, wie viele Verbindungsabbrüche an diesem Standort im ausgewählten Zeitraum aufgetreten sind.
- **Trennungsdauer**: Zeigt an, wie lange die Verbindungsabbrüche des Standorts während des ausgewählten Zeitraums insgesamt dauerten (in Sekunden).




### Transparente Einblicke in leistungsstarke Zweigstellen

Leistungsstarke Zweige (RN-HP) haben andere Attribute als ältere Zweige, und beide werden in Ihrem Mandant koexistieren. Leistungsstarke Zweigstellen in Prisma Access haben folgende Vorteile:

- Die Architektur zielt auf eine effiziente Nutzung der Kapazitäten ab, indem sie die Netzwerkverarbeitungsfunktionen von den Sicherheitsverarbeitungsfunktionen trennt. Ein ION-Gerät mit großer Paketverarbeitungsfähigkeit terminiert mehrere Zweigverbindungen mit bis zu 5 Gbit/s Kapazität und verteilt die Sicherheitsverarbeitung auf SPNs.
- Sie können eine einzelne IP oder FQDN verwenden, um mehrere Zweige in der Region an einem einzigen Netzwerkverarbeitungsknoten (NPN) zu beenden.

 ©2025 Palo Alto Networks, Inc.

- Sie müssen die Terminierung von Zweigstellen zu IPSec-Terminierungsknoten nicht mehr überwachen und verwalten. Geeignete SPNs führen Zweigverkehrsinspektionen durch, und das NPN übernimmt den Lastausgleich.
- Eine echte Hochverfügbarkeit erreichen Sie, indem Sie verschiedene Regionen für die Redundanz angeben können.

Sie können sowohl leistungsstarke als auch ältere Zweige in Ihrer Umgebung anzeigen. Gehen Sie in Strata Cloud Manager zu **Überwachen** > **Zweigstellen** > **Prisma Access**, und wählen Sie in der Tabelle **Prisma Access-Standorte** eine Zweigstelle aus.

*Prisma Access-Standortdetails*

Wählen Sie einen beliebigen Prisma Access-**Standortnamen** aus, um den **Standortstatus** anzuzeigen, aus dem der **Konnektivitäts-** und **BGP-Status** (**Aktiv**, **Ausgefallen**, **Inaktiv** oder **Nicht verfügbar**) hervorgeht. Zeigen Sie den **Spitzenverbrauch** für den ausgewählten Zeitraum an.

Im Diagramm **Trend für Bandbreitenverbrauch** können Sie Informationen zu **Kumulativ (Ein- und Ausgang)** anzeigen.

- Verwenden Sie das Dropdown-Menü, um das Diagramm zum Bandbreitenverbrauch nach **Eingang**, **Ausgang**, **Eingang vs. Ausgang** oder **Kumulativ (Ein- und Ausgang)** anzuzeigen.
- Sehen Sie sich die Diagrammkennzahlen zum Trend des Bandbreitenverbrauchs nach **höchstem** (Standardeinstellung), **durchschnittlichem** oder **mittlerem** Bandbreitenverbrauch für die Zweigstelle an.

### Transparente Einblicke in die Routentabelle

Um Ihnen bei der Lösung von Erreichbarkeitsproblemen zu helfen, bieten wir transparente Einblicke in die Routentabelle an jedem Remote-Netzwerkstandort. Sie können eine Routentabellensuche nach einer Ziel-IP-Adresse durchführen, um festzustellen, ob eine Route verfügbar ist, um das gewünschte Ziel zu erreichen. Mit diesen Informationen können Sie andere mögliche Ursachen für Fehler untersuchen. Mit diesem Wissen können Sie sich auf die Lösung von Problemen konzentrieren, die die Erreichbarkeit beeinträchtigen könnten.

Wählen Sie **Routingtabelle anzeigen** aus, um die **Routingtabelle** dieses Zweigs anzuzeigen, die IP-Routen für Ziele enthält, die in dem Zweig von Prisma Access aus verfügbar sind.

- Über die Suchleiste können Sie das Ziel auswählen oder nach der Route suchen.
- Verwenden Sie das Dropdown-Menü, um nach **Markierung** zu filtern.

Die Routingtabelle zeigt Folgendes an:

- **Nr. (#)** – Routennummer.
- **Ziel**: IP-Adresse und Subnetz des erreichbaren Netzwerks.
- **Nächster Hop**: IP-Adresse des Gateways beim nächsten Hop in Richtung Zielnetzwerk. Ein nächster Hop von 0.0.0.0 gibt die Standardroute an.
- **Metrik**: Zeigt die Metrik für die Route an, die das Routingprotokoll festlegt.
- **Markierung**: Zeigt folgende Informationen für diese Route an:

 ©2025 Palo Alto Networks, Inc.

- - **A B**: Aktiv und erhalten von BGP.
  - **A C**: Aktiv und verbunden. Ziel: Netzwerk.
  - **A H**: Aktiv und verbunden. Ziel: Nur Host.
  - **A R**: Aktiv und von RIP erhalten.
  - **O1**: Externe OSPF-Route vom Typ 1.
  - **O2**: Externe OSPF-Route vom Typ 2.
  - **Oi**: OSPF-Intra-Area-Route.
  - **Oo**: OSPF-Inter-Area-Route.
  - **S**: Inaktiv und statisch.
  - **A S**: Aktiv und statisch

.

### Tunnel

Zeigen Sie Tunnel und Tunneldaten für diesen Standort an.

- **Tunnelname** – Der eindeutige Name des Tunnels
- **Prisma Access-Standort** – Der Prisma Access-Standort für dieses Remote-Netzwerk
- **Tunnelstatus** – **Aktiv**, **Inaktiv**, **Init** oder **Nicht verfügbar**
- **BGP-Status des Tunnels** – **Aktiv**, **Inaktiv** oder **Unbekannt**
- **Tunnelüberwachung** – Wenn Sie die **Tunnelüberwachung** aktiviert haben, wird in dieser Spalte angezeigt, ob sie **aktiv** oder **inaktiv** ist. Wenn Sie sie nicht aktiviert haben, zeigt diese Spalte **Nicht konfiguriert** an.
- **Durchschnittlicher Durchsatz**: Die durchschnittliche Bandbreite für den Tunnel im ausgewählten Zeitraum unter Berücksichtigung des von Ihnen ausgewählten Werts für **Eingang**, **Ausgang**, **Eingang vs. Ausgang** oder **Kumulativ (Ein- und Ausgang)**.
- **Höchster Durchsatz**: Die höchste Bandbreite für den Tunnel für den ausgewählten Zeitbereich unter Berücksichtigung von **Eingang**, **Ausgang**, **Eingangs vs. Ausgang** oder **Kumulativ (Ein- und Ausgang)**.
- **Quell-IP-Adresse**: Die Quell-IP-Adresse.
- **Zielendpunktadresse**: IP- oder FQDN-Adresse, mit der Prisma Access feststellt, ob der Tunnel aktiv ist.
- **Trennungen**: Anzahl der Trennungen während des ausgewählten Zeitraums.
- **Trennungsdauer**: Zeigt an, wie lange (in Sekunden) die Verbindungsabbrüche des Tunnels während des ausgewählten Zeitraums dauerten.

Wählen Sie einen **Tunnelnamen** aus, um dessen **Tunnelstatus**, **Trend für Bandbreitenverbrauch** und andere Tunneldetails anzuzeigen.

#### *Tunneltrends*

Wenn die **Tunnelüberwachung** aktiviert ist, können Sie mehrere Tunnel auswählen und deren mittlere **Paketumlaufzeit** anzeigen. Wenn Sie keine bestimmten Tunnel angeben, wird

 ©2025 Palo Alto Networks, Inc.

standardmäßig die mittlere Paketumlaufzeit für die zehn Tunnel mit der höchsten beobachteten Paketumlaufzeit berechnet.

**Aggregierte Tunnelkonnektivität** zeigt die Gesamtzahl der angeschlossenen Tunnel für den ausgewählten Zeitraum an. Bewegen Sie den Mauszeiger über eines der Diagramme, um die Anzahl der Verbindungen zu einem bestimmten Zeitpunkt anzuzeigen.

**Commits gepusht** zeigt an, wie viele Commits im ausgewählten **Zeitbereich** gepusht wurden und wann das **letzte Push Commit** erfolgte.

#### Standortstatus

Der **Standortstatus** zeigt die Verfügbarkeit des Standorts im ausgewählten Zeitraum an. **Grün** bedeutet, dass der Standort während dieser Zeit aktiv war, **rot** bedeutet, dass der Standort inaktiv war, und **grau** bedeutet, dass während der angezeigten Zeit keine Daten verfügbar waren.

# Anzeigen und Überwachen von Rechenzentren

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

## Dienstverbindungen

Eine Dienstverbindung, auch als Corporate Access Node (CAN) bezeichnet, ermöglicht mobilen Benutzern und Benutzern in Remote-Netzwerken den Zugriff auf private Apps und Ressourcen sowie die Kommunikation zwischen mobilen Benutzern und Remote-Netzwerken. Palo Alto Networks empfiehlt, in Ihrer Prisma Access-Bereitstellung immer eine Dienstverbindung zu erstellen. Alle Dienstverbindungen ermöglichen den Zugriff auf die Ressourcen in Ihrem Hauptsitz (Zentrale) oder Ihrem Rechenzentrum sowie die Kommunikation zwischen Remote-Netzwerken und mobilen Benutzern.

Die Anzahl der Dienstverbindungen, die Sie erhalten, hängt von Ihrer Prisma Access-Lizenz ab. Weitere Informationen zu Dienstverbindungen und ihrer Konfiguration finden Sie unter Prisma Access-Dienstverbindungen.

Wählen Sie in Strata Cloud Manager die Optionen **Überwachen** > **Rechenzentren** > **Dienstverbindungen**aus, um Einblick in Ihre Dienstverbindungen zu erhalten.

## ZTNA-Connectors

Mit dem Zero Trust Network Access (ZTNA)-Connector können Sie Prisma Access mit den privaten Apps Ihres Unternehmens verbinden. ZTNA-Connector bietet mobilen Benutzern und Benutzern in Zweigstellen über einen automatisierten sicheren Tunnel Zugriff auf Ihre privaten Apps. ZTNA-Connector richtet die Tunnel automatisch ein, sodass Sie IPSec-Tunnel und Routing zu den Rechenzentrums- oder Hauptsitzstandorten, öffentlichen Cloud-Standorten und Partnernetzwerken, in denen sich Ihre privaten Apps befinden, nicht manuell einrichten müssen.

 ©2025 Palo Alto Networks, Inc.

Wählen Sie in Strata Cloud Manager die Optionen **Überwachen** > **Rechenzentren** > **ZTNA-Connectors** aus, um Einblick in Ihre ZTNA-Connectors zu erhalten.

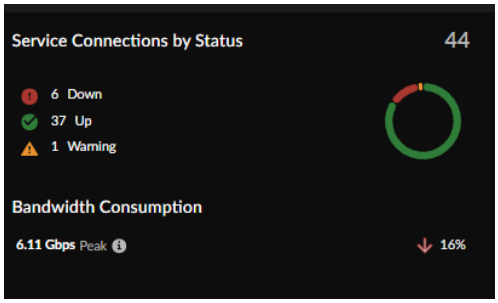
## Anzeigen und Überwachen von Dienstverbindungen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Zeigen Sie aggregierte Dienstverbindungsdaten sowie Informationen zu einzelnen Dienstverbindungen an. Dienstverbindungen stehen sowohl mobilen Benutzern als auch Remote-Netzwerken zur Verfügung. Neben dem Zugriff auf Unternehmensressourcen ermöglichen Dienstverbindungen Ihren mobilen Benutzern auch die Verbindung zu Zweigstellen. Sie können Ihre Dienstverbindungen in Strata Cloud Manager anzeigen, um den Status der Dienstverbindung, Trends bei der Bandbreitennutzung, Tunneldaten und -trends sowie Informationen zum allgemeinen Zustand der Dienstverbindung anzuzeigen. Wählen Sie **Überwachen** > **Rechenzentren** > **Dienstverbindungen** aus, um zu beginnen.

### Dienstverbindungen nach Status

Sie können den Status Ihrer Dienstverbindungen anzeigen. Das farbcodierte Diagramm zeigt eine Verteilung der Anzahl der Dienstverbindungen, die aktiv oder inaktiv sind oder Ihre Aufmerksamkeit erfordern. Sie können eine Zusammenfassung der Bandbreite anzeigen, die Ihre Dienstverbindungen in den letzten 30 Tagen verbraucht haben.




**Bandbreitenverbrauch** zeigt für das Modell der Bandbreitenzuweisung pro Standort die höchste Spitzenbandbreite an, die ein Standort über alle Standorte hinweg verbraucht. Die Spitzenwerte werden für die ausgewählte Zeitfilterdauer berechnet.

### Trend für Bandbreitenverbrauch

Sehen Sie sich den **Trend des Bandbreitenverbrauchs pro Dienstverbindung** an. Der Trend zeigt den Bandbreitenverbrauch der einzelnen Dienstverbindungen sowie die durchschnittliche und die Spitzenauslastung an.

- Die Standardansicht zeigt den **kumulativen (Ein- und Ausgang)** Bandbreitenverbrauch an. Weitere Anzeigeoptionen sind **Eingang**, **Ausgang**oder **Eingang vs. Ausgang**.
- Sie können den Trend für den **höchsten**, **mittleren** oder **durchschnittlichen** Bandbreitenverbrauch während des ausgewählten Zeitraums anzeigen. Standardmäßig wird der **höchste** Bandbreitenverbrauch angezeigt.

 ©2025 Palo Alto Networks, Inc.

- **Logarithmische Skala** oder **Lineare Skala**.
- Wählen Sie eine bis zehn **Dienstverbindungen** aus, um ihre Trendlinien im Diagramm während des ausgewählten Zeitraums anzuzeigen. Bewegen Sie den Mauszeiger über das Diagramm, um Informationen zu den einzelnen ausgewählten Dienstverbindungen anzuzeigen.

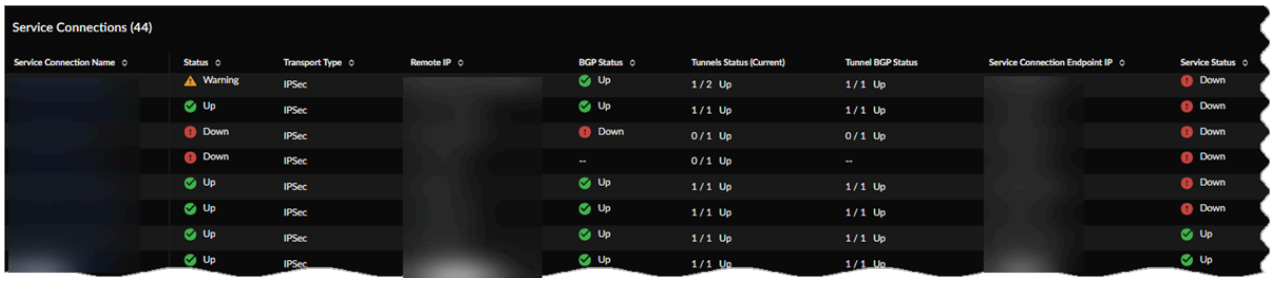



### Tabelle „Dienstverbindungen“

Die Tabelle **Dienstverbindungen** zeigt Daten zu Ihren Dienstverbindungen an, beispielsweise den Status, die Remote-IP-Adresse, den BGP-Status, den aktuellen Tunnelstatus und andere Daten. Wählen Sie einen **Dienstverbindungsnamen** aus, um weitere Informationen zu dieser Dienstverbindung zu erhalten.

- **Dienstverbindungsname**: Der eindeutige Name der Dienstverbindung.
- **Status**: **Aktiv**, **Inaktiv**, **Warnung** oder **Unbekannt**.
- **Transporttyp**: IPSec.
- **Remote IP**: Die Remote-IP-Adresse.
- **BGP-Status**: Zeigt an, ob der BGP-Status des Standorts **Aktiv**, **Inaktiv** oder **Unbekannt** ist.
- **Tunnelstatus (aktuell)**: Zeigt an, wie viele Tunnel der Standort hat und wie viele dieser Tunnel aktiv sind.
- **BGP-Status des Tunnels**: Zeigt den BGP-Status für jeden Tunnel an.
- **IP-Adresse des Dienstverbindungsendpunkts**: Zeigt die IP-Adresse des Endpunkts der Dienstverbindung an.
- **Dienststatus**: Dieses Feld zeigt den Status der Instanz oder Firewall an, mit der der Standort verbunden ist. Der Status kann **Aktiv**, **Inaktiv** oder **Unbekannt** sein.
- **Prisma Access-Standort**: Der Prisma Access-Standort der Dienstverbindung.
- **Durchschnittlicher Bandbreitenverbrauch**: Zeigt den durchschnittlichen Bandbreitenverbrauch in Kbit/s an.
- **Höchster Bandbreitenverbrauch**: Zeigt den höchsten Bandbreitenverbrauch in Kbit/s an.

 ©2025 Palo Alto Networks, Inc.




**Details zu Dienstverbindungen**

Wählen Sie einen beliebigen **Dienstverbindungsnamen** aus, um die Details zur jeweiligen Dienstverbindung anzuzeigen. Sehen Sie sich den jeweiligen **Dienstverbindungsstatus** und die in den letzten 30 Tagen **verbrauchte Bandbreite** an. Das Diagramm **Trend für Bandbreitenverbrauch** zeigt den Bandbreitenverbrauch der einzelnen Dienstverbindungen während des ausgewählten Zeitraums an.

*Standortstatus*

Wählen Sie einen beliebigen **Dienstverbindungsnamen** aus, um den jeweiligen **Standortstatus** anzuzeigen. Dort sehen Sie die **Konnektivität** und den **BGP-Status** (**Aktiv**, **Ausgefallen**, **Inaktiv** oder **Nicht verfügbar**). Zeigen Sie den **höchsten Bandbreitenverbrauch** für den ausgewählten Zeitraum an.

## Transparente Einblicke in die Routentabelle

Um Ihnen bei der Lösung von Erreichbarkeitsproblemen zu helfen, bieten wir transparente Einblicke in die Routentabelle an jeder Dienstverbindung. Sie können eine Routentabellensuche nach einer Ziel-IP-Adresse durchführen, um festzustellen, ob eine Route verfügbar ist, um das gewünschte Ziel zu erreichen. Mit diesen Informationen können Sie sich von der Prisma Access-Infrastruktur anleiten lassen, um andere mögliche Fehlerursachen zu untersuchen. Mit diesem Wissen können Sie sich auf die Lösung von Problemen konzentrieren, die die Erreichbarkeit beeinträchtigen könnten.

Wählen Sie **Routingtabelle anzeigen** aus, um die **Routingtabelle** dieses Zweigs anzuzeigen, die IP-Routen für Ziele enthält, die in dem Zweig von Prisma Access aus verfügbar sind.

- Über die Suchleiste können Sie das Ziel auswählen oder nach der Route suchen.
- Verwenden Sie das Dropdown-Menü, um nach **Markierung** zu filtern.

Die Routing-Tabelle zeigt Folgendes an:

- **#**: Nummer der Route
- **Ziel**: IP-Adresse und Subnetz des erreichbaren Netzwerks.
- **Nächster Hop**: IP-Adresse des Gateways beim nächsten Hop in Richtung Zielnetzwerk. Ein nächster Hop von 0.0.0.0 gibt die Standardroute an.
- **Metrik**: Zeigt die Metrik für die Route an, die das Routingprotokoll festlegt.
- **Markierung**: Zeigt folgende Informationen für diese Route an:
- - **A B**: Aktiv und gelernt von BGP.
  - **A C**: Aktiv und verbunden. Ziel: Netzwerk.
  - **A H**: Aktiv und verbunden. Ziel: Nur Host.

 ©2025 Palo Alto Networks, Inc.

- **A R**: Aktiv und von RIP gelernt.
- **O1**: Externe OSPF-Route vom Typ 1.
- **O2**: Externe OSPF-Route vom Typ 2.
- **Oi**: OSPF-Intra-Area-Route.
- **Oo**: OSPF-Inter-Area-Route.
- **S**: Inaktiv und statisch.
- **A S**: Aktiv und statisch.

*Trend für Bandbreitenverbrauch*

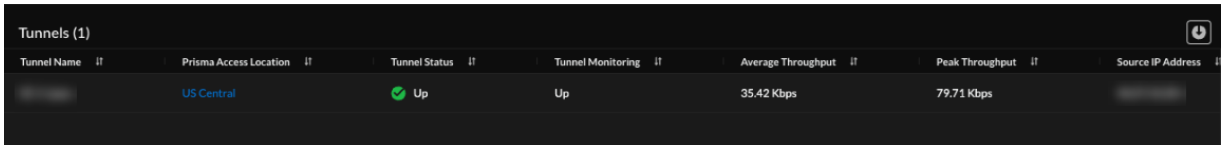
Das Diagramm **Trend für Bandbreitenverbrauch** zeigt standardmäßig Informationen zu **Kumulativ (Ein- und Ausgang)** an.

- Verwenden Sie das Dropdown-Menü, um das Diagramm zum Bandbreitenverbrauch nach **Eingang**, **Ausgang**, **Eingang vs. Ausgang** oder **Kumulativ (Ein- und Ausgang)** anzuzeigen.

- Sehen Sie sich die Diagrammkennzahlen zum Trend des Bandbreitenverbrauchs nach **höchstem** (Standardeinstellung), **durchschnittlichem** oder **mittlerem** Bandbreitenverbrauch für die Zweigstelle an.

### Tunnel

Sehen Sie sich an, wie viele **Tunnel** es für diese Dienstverbindung gibt, und zeigen Sie die Details der einzelnen Tunnel an. Wählen Sie zum Herunterladen der **Tunneldaten** das Symbol „Herunterladen“ aus.



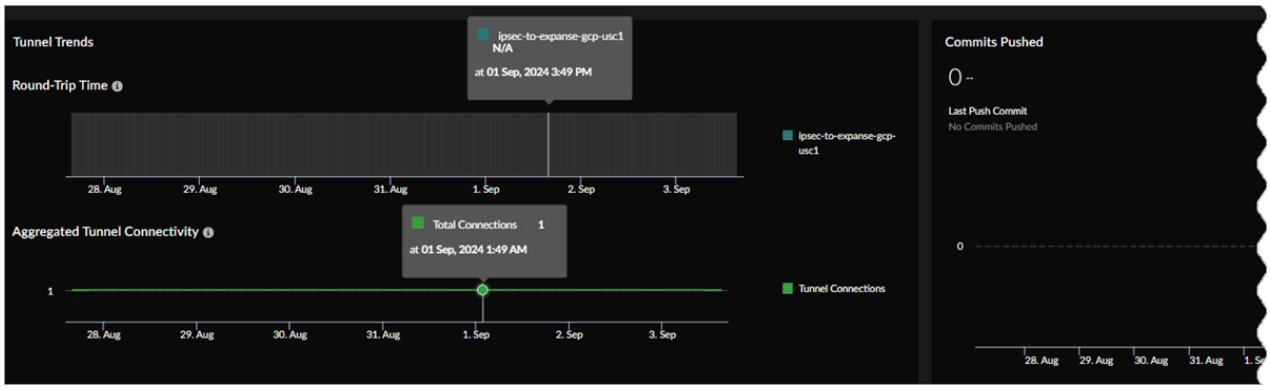

### Tunneltrends

Sie können eine Reihe von Tunneln auswählen und deren mittlere **Paketumlaufzeit** anzeigen. Wenn Sie keine bestimmten Tunnel angeben, wird die mittlere Paketumlaufzeit für die zehn Tunnel mit der höchsten beobachteten Paketumlaufzeit berechnet.

**Aggregierte Tunnelkonnektivität** zeigt die Gesamtzahl der angeschlossenen Tunnel für den ausgewählten Zeitraum an. Bewegen Sie den Mauszeiger über eines der Diagramme, um die Anzahl der Verbindungen zu einem bestimmten Zeitpunkt anzuzeigen.

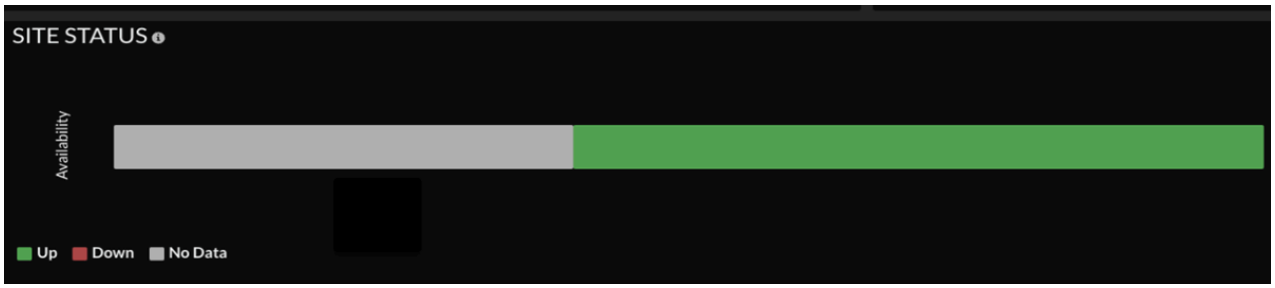
**Commits gepusht** zeigt an, wie viele Commits im ausgewählten **Zeitbereich** gepusht wurden und wann der **letzte Push Commit** erfolgte.

 ©2025 Palo Alto Networks, Inc.



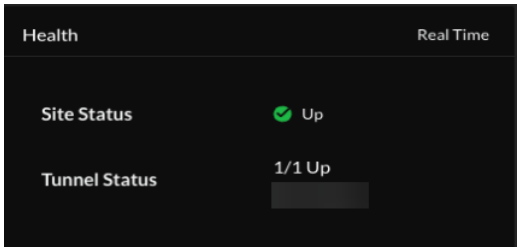

### Standortstatus

Der **Standortstatus** zeigt die Verfügbarkeit des Standorts im ausgewählten Zeitraum an. Grün bedeutet, dass der Standort während dieser Zeit aktiv war, rot bedeutet, dass der Standort inaktiv war, und grau bedeutet, dass während der angezeigten Zeit keine Daten verfügbar waren.



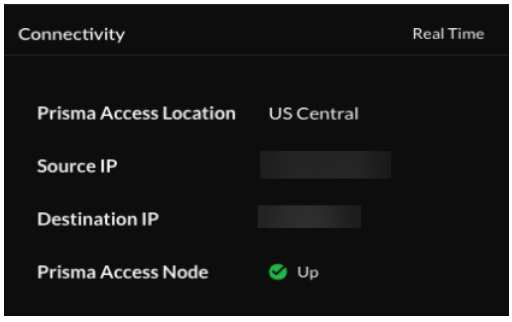

### Zustand

**Zustand** zeigt den **Standortstatus** sowie den Namen und den Status jedes Tunnels am Standort an.




### Konnektivität

**Konnektivität** zeigt den Prisma Access-Standort an, mit dem die Site verbunden ist, ihre Quell- und Ziel-IPs sowie den Prisma Access-Knotenstatus.




 ©2025 Palo Alto Networks, Inc.

### Verbrauch

**Verbrauch** zeigt Details zum Bandbreitenverbrauch an.

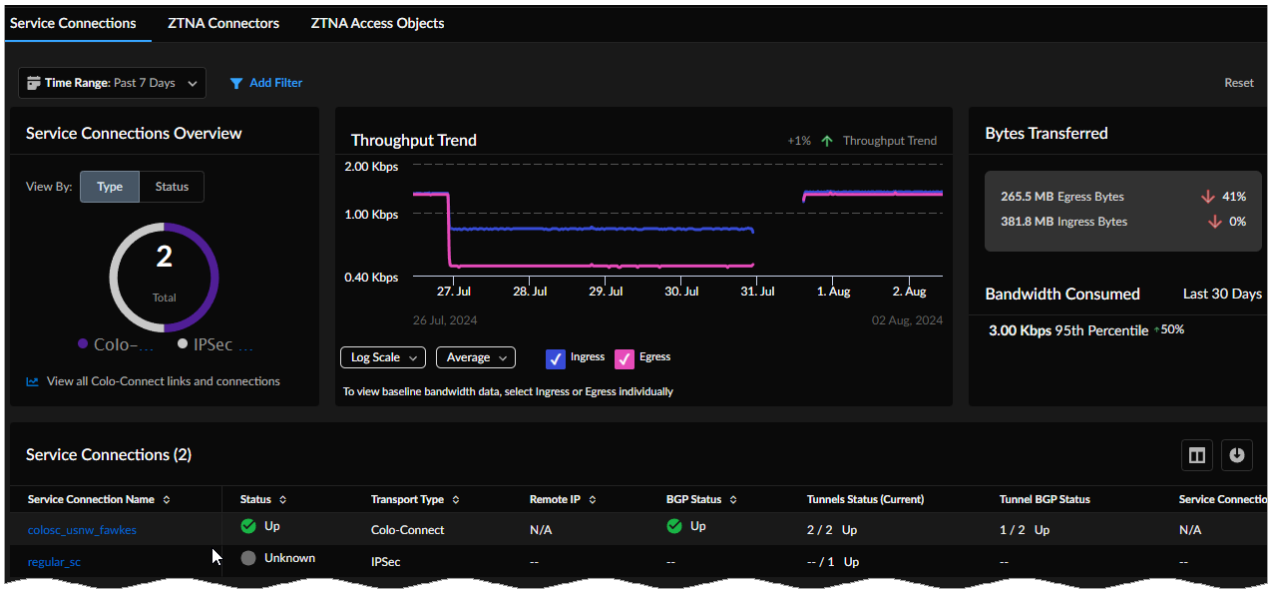


## Anzeige und Überwachung – Colo-Connect

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | Prisma Access-Lizenz |

Prisma AccessColo-Connect nutzt die Cloud-native GCP-Verbindungstechnologie, um Dienstverbindungen mit hoher Bandbreite zu Ihren privaten Anwendungen bereitzustellen. Colo-Connect koexistiert mit den vorhandenen tunnelbasierten IPSec-Dienstverbindungen. Wenn Sie also Zugriff auf private Apps für kleinere Rechenzentren bereitstellen müssen, die keinen Durchsatz mit hoher Bandbreite benötigen, können Sie auch Dienstverbindungen zu diesen Rechenzentren verwenden. Erhalten Sie Einblick in Ihre Colo-Connect-Bereitstellung, indem Sie Metriken wie die Anzahl der Colo-Connect-Links und den Status, Durchsatztrends sowie einzelne Tunnel-, Verbindungs- und Linkdetails anzeigen. Mithilfe der Daten zu Ihren Colo-Connect-Dienstverbindungen können Sie sich ein Gesamtbild über den Zustand und die Konnektivität Ihrer Bereitstellung verschaffen.

Gehen Sie zu **Überwachen** > **Rechenzentren** > **Dienstverbindungen**, um Ihre private Konnektivität zu Hybrid Cloud und zu lokalen Rechenzentren über Cloud-Verbindungen anzuzeigen und zu überwachen.




### Dienstverbindungen im Überblick

**Dienstverbindungen im Überblick** zeigt die Anzahl der Dienstverbindungen nach Transport-**Typ** an.

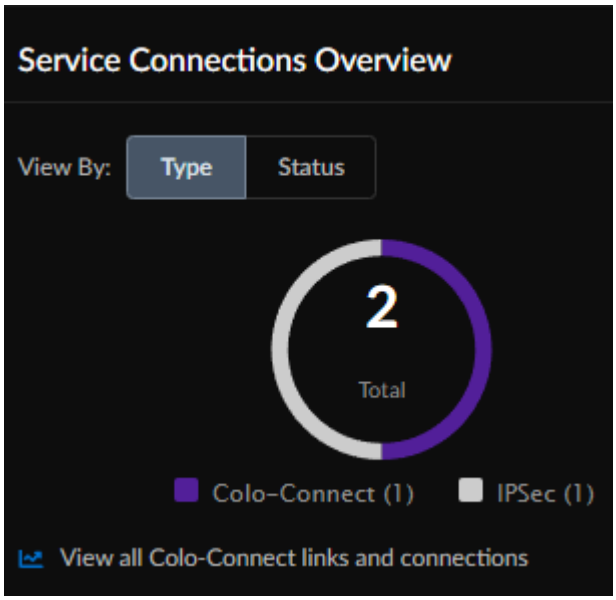
Sie können eine Aggregation der verbundenen Transporte nach **Typ** oder deren Verfügbarkeits-**Status** sehen.

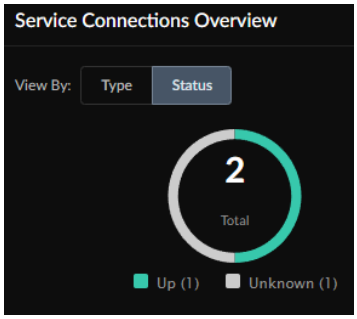
 ©2025 Palo Alto Networks, Inc.

- **IPSec**
- **Colo-Connect**

Sie können den Tunneltransporttyp nach Status anzeigen: **Aktiv**, **Inaktiv**, **Herabgestuft** oder **Unbekannt**.

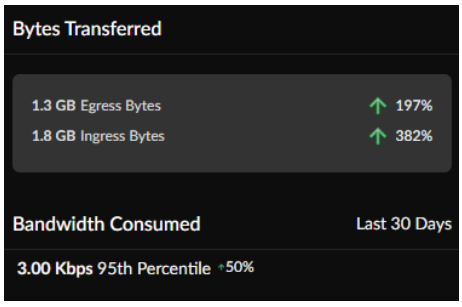
Wählen Sie **Alle Colo-Connect-Links und -Verbindungen anzeigen** aus, um die Seite mit den Colo-Connect-Details anzuzeigen.




### Dienstverbindungen im Überblick: Übertragene Bytes und verbrauchte Bandbreite

**Übertragene Bytes** zeigt eine Aggregation der verbrauchten Eingangs- und Ausgangs-Bytes sowie der Verbrauchsdifferenz zum zuvor ausgewählten Zeitraum an. **Verbrauchte Bandbreite** zeigt das 95. Perzentil der in den letzten 30 Tagen verbrauchten Bandbreite.

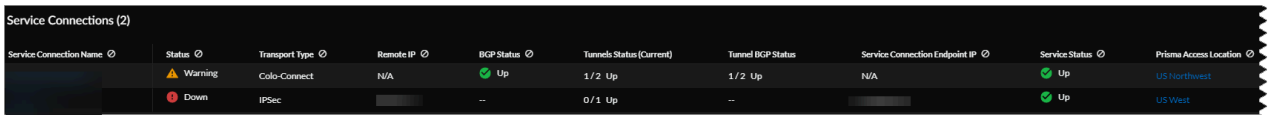



 ©2025 Palo Alto Networks, Inc.

### Dienstverbindungen

In der Tabelle **Dienstverbindungen** sind für jede angegebene Dienstverbindung folgende Details aufgeführt:

- **Dienstverbindungsname**: Name der Colo-Connect- oder IPSec-Dienstverbindung. Wählen Sie einen **Dienstverbindungsnamen** aus, um die Detailseite der entsprechenden Dienstverbindung aufzurufen.
- **Status**: Aktiv, Inaktiv, Herabgestuft oder Unbekannt.
- **Transporttyp**: Colo-Connect oder IPSec.
- **Remote IP**: Ziel-IP.
- **BGP-Status**: Aktiv, Inaktiv oder Warnung, wenn einige BGP-Tunnel aktiv und einige inaktiv sind.
- **Tunnelstatus (aktuell)**: Aktueller Tunnelstatus.
- **BGP-Status des Tunnels**: Anzahl der Tunnel nach BGP-Status (aktiv, inaktiv oder Warnung).
- **IP-Adresse des Dienstverbindungsendpunkts**: Die IP-Adresse des Prisma Access-Knotens.
- **Dienststatus**: Der Dienststatus wird durch den Status der aktiven Dienstverbindung oder des bzw. der Rechenzentrumscluster(s) (aktiv, inaktiv oder Warnung) bestimmt.
- **Prisma Access-Standort**: Wählen Sie einen **Prisma Access-Standort** aus.
- **Durchschnittlicher Bandbreitenverbrauch**: Der durchschnittliche Bandbreitenverbrauch für die Website während des ausgewählten Zeitraums.
- **Höchster Bandbreitenverbrauch**: Der höchste Bandbreitenverbrauch für den Standort während des ausgewählten Zeitraums.




### Details zu Dienstverbindungen

Wählen Sie auf der Hauptseite in der Tabelle **Dienstverbindungen** eine **Dienstverbindung** mit dem Transport-**Typ** als Colo-Connect aus, um zu deren Detailseite zu gelangen.




 ©2025 Palo Alto Networks, Inc.

*Dienstverbindungsstatus, Colo-Connect und gleichzeitige Sitzungen*

- Sehen Sie sich den **Zugriffsort** und die **GRE-Tunnel** der Dienstverbindung (aktiv, inaktiv oder Warnung) an.
- Sehen Sie sich die Gesamtzahl der **Colo-Connect**-Links und -Verbindungen an.
- **Gleichzeitige Sitzungen** zeigt die Anzahl der aktuellen Sitzungen und der gesamten Sitzungen während der letzten 30 Tage an.

*Durchsatztrend*

**Durchsatztrend** zeigt den von dieser Dienstverbindung im ausgewählten Zeitraum verbrauchten ein- und ausgehenden Durchsatzverkehr an.

*Übertragene Bytes und verbrauchte Bandbreite*

**Übertragene Bytes** zeigt eine Aggregation der verbrauchten Eingangs- und Ausgangs-Bytes sowie die Verbrauchsdifferenz im Vergleich zum zuvor ausgewählten Zeitraum an. **Verbrauchte Bandbreite** zeigt das 95. Perzentil der in den letzten 30 Tagen verbrauchten Bandbreite an.

*GRE-Tunnel*

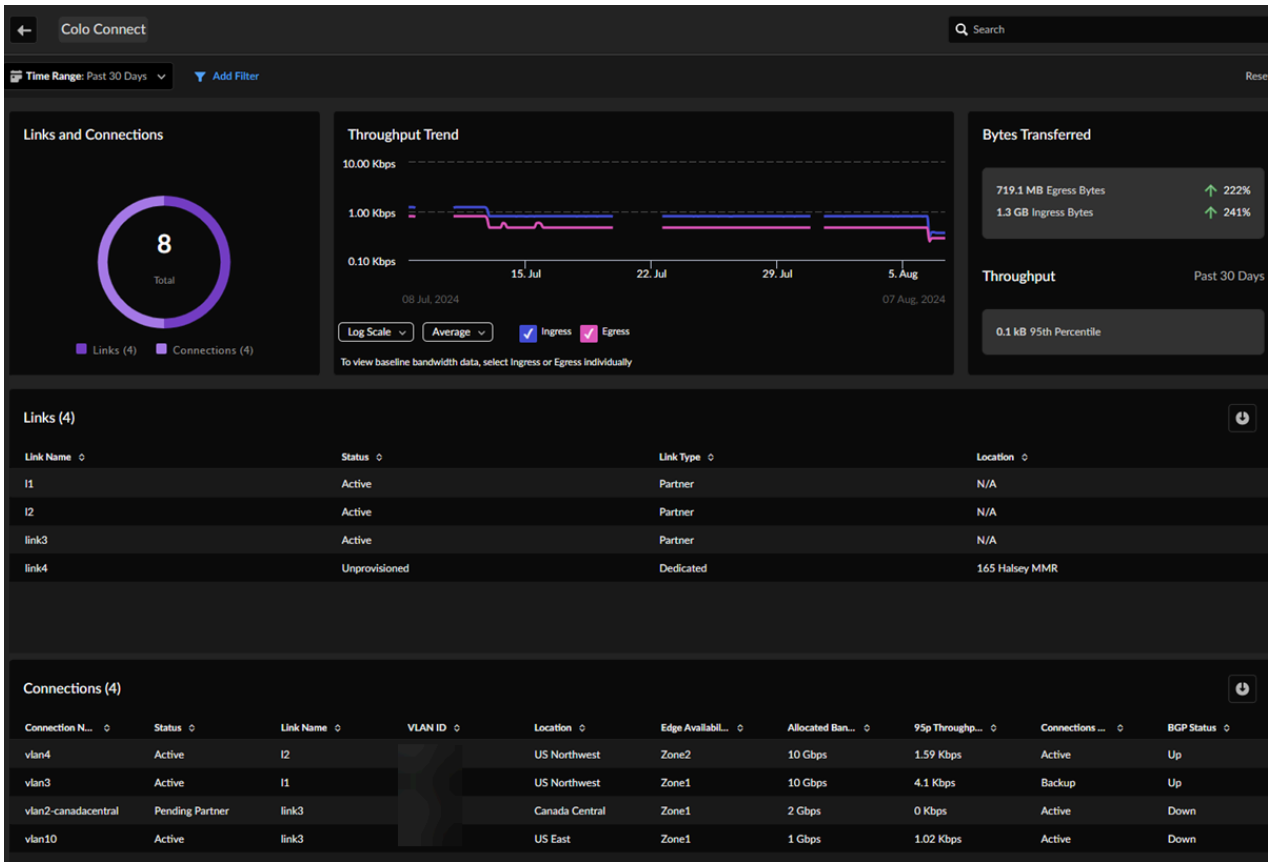
Anzeigen der Details zu den Tunneln in dieser Dienstverbindung:

- **Tunnelname**: Der eindeutige Tunnelname.
- **Tunnelstatus**: Aktiv, Inaktiv oder Unbekannt.
- **Verbindungsname**: Der eindeutige Name der Verbindung.
- **Tunnelstatus**: Der Verbindungsstatus (Aktiv oder Backup).
- **Remote IP**: Ziel-IP-Adresse.
- **Quell-IP**: IP-Adresse des lokalen Geräts.
- **95 % Durchsatz**: Das 95. Perzentil der Bandbreite, die in den letzten 30 Tagen verbraucht wurde.
- **Höchster Durchsatz**: Spitzendurchsatz im ausgewählten Zeitraum.
- **BGP-Status**: Aktiv, Inaktiv, Herabgestuft oder Unbekannt.
- **Lokale BGP-IP**: Die lokale BGP-IP.
- **Trennungen**: Anzahl der Verbindungsabbrüche dieses Tunnels.
- **Trennungsdauer**: Zeigt an, wie lange die Verbindungsabbrüche dauerten.
- **Eingangs-Bytes**: Anzahl der verbrauchten Eingangs-Bytes im ausgewählten Zeitraum.
- **Ausgangs-Bytes**: Anzahl der verbrauchten Ausgangs-Bytes im ausgewählten Zeitraum.
- **Anzahl der Eingangspakete**: Die Anzahl der Eingangspakete.
- **Anzahl der Ausgangspakete**: Die Anzahl der Ausgangspakete.

*Colo-Connect-Details*

Wählen Sie auf der Hauptseite **Dienstverbindungen** im Widget **Dienstverbindungen im Überblick** die Option **Alle Colo-Connect-Links und -Verbindungen anzeigen** aus, um die **Colo-Connect**-Detailseite zu öffnen. Widgets auf dieser Seite zeigen Ihre aktuellen Details (aktuell definiert als die letzten 20 Minuten).

 ©2025 Palo Alto Networks, Inc.




*Links und Verbindungen*

Das Kreisdiagramm zeigt die Gesamtzahl der aktuellen Colo-Connect-Links und -Verbindungen an.

*Links*

Die Tabelle zeigt Details zu Ihren aktuellen Colo-Connect-Links an.

- **Linkname**: Eindeutiger Name des Colo-Connect-Links.
- **Status**: Aktiv oder Wartung.
- **Linktyp**: Partner oder Dediziert.
- **Standort**: Prisma Access-Standort.

*Verbindungen*

Zeigen Sie die Details zu jedem Ihrer aktuellen Colo-Connect-Links an. Bewegen Sie den Mauszeiger über Verbindungen, um Informationen zum angezeigten Status anzuzeigen.

- **Verbindungsname**: Eindeutiger Name der Colo-Connect-Verbindung.
- **Status**: Aktiv, Ausstehender Partner, Ungültig.
- **Linkname**: Linkname der Verbindung.
- **VLAN-ID**: VLAN-ID der Verbindung.
- **Standort**: Prisma Access-Standort.
- **Edge-Verfügbarkeitszone**: Zone 1 oder Zone 2.

 ©2025 Palo Alto Networks, Inc.

- **Zugeordnete Bandbreite**: 1 Gbit/s, 2 Gbit/s, 5 Gbit/s, 10 Gbit/s oder 20 Gbit/s.
- **95 % Durchsatz**: Das 95. Perzentil der verbrauchten Bandbreite.
- **Verbindungsstatus**: Aktiv oder Backup.
- **BGP-Status**: Aktiv oder Inaktiv.

## Anzeigen und Überwachen von ZTNA-Connectors

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz<br>❑ Dies ist eine Funktion von Prisma Access Insights. |

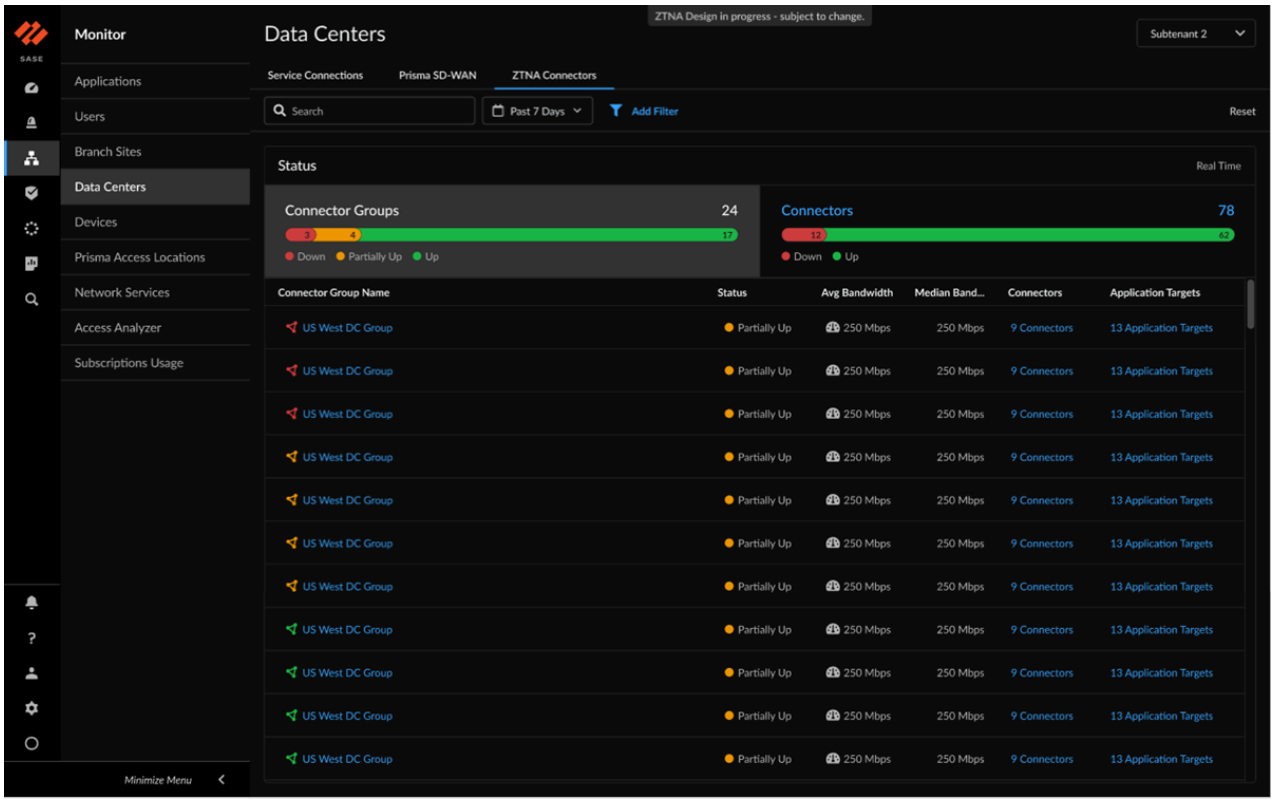
Der ZTNA-Connector (Zero Trust Network Access) vereinfacht den Zugriff auf private Anwendungen für all Ihre Anwendungen. Die ZTNA-Connector-VM in Ihrer Umgebung bildet automatisch Tunnel zwischen Ihren privaten Anwendungen und Prisma Access. Zeigen Sie eine Übersicht aller konfigurierten ZTNA-Connectors an, einschließlich der mit dem Connector verknüpften **Anwendungsziele** , seiner durchschnittlichen und mittleren Bandbreite und des **Status** (aktiv, teilweise aktiv oder inaktiv). Navigieren Sie in Strata Cloud Manager zu **Überwachen** > **Rechenzentren** > **ZTNA-Connectors**, um sich die Performance Ihrer ZTNA-Connectors und Konnektorgruppen anzusehen.

### Status der ZTNA-Connector-Gruppen

Die Konnektoren in jeder Gruppe bestimmen den **Status** einer Konnektorgruppe.

- Wenn alle **Konnektoren** einer **Konnektorgruppe** aktiv sind, lautet der **Status Aktiv** (grün).
- Wenn alle **Konnektoren** ausgefallen sind, ist der Status **Inaktiv** (rot).
- Wenn einige Konnektoren aktiv und einige inaktiv sind, ist der **Status Teilweise aktiv** (orange).
- Deaktivierte Konnektoren werden in Grau angezeigt.

 ©2025 Palo Alto Networks, Inc.




**Status der ZTNA-Connectors**

Zeigen Sie eine Übersicht aller konfigurierten ZTNA-Connectors an, einschließlich der mit dem Konnektor verknüpften Anwendungsziele und des **Status** an.

Wählen Sie einen beliebigen **Konnektornamen** aus, um Details zu den zugeordneten Konnektorgruppen und Anwendungszielen anzuzeigen, die jedem Konnektor zugeordnet sind.

## Anzeigen und Überwachen von ZTNA-Connector-Zugriffsobjekten

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Verschaffen Sie sich einen Überblick über Ihre privaten Apps, die über ZTNA-Connector-Zugriffsobjekte hinzugefügt wurden, indem Sie Daten wie die Anzahl der von FQDNs, IP-Subnetzen und Platzhaltern hinzugefügten Apps, den Konnektivitätsstatus jedes Zugriffsobjekts sowie die Konnektorgruppen und Konnektoren anzeigen, die jedem Zugriffsobjekt zugeordnet sind. Mithilfe dieser Informationen können Sie sich ein Gesamtbild über den Zustand und die Konnektivität Ihrer Bereitstellung verschaffen.

Die privaten Apps in den Rechenzentren verbinden sich über Ihre virtuellen Connector-Maschinen (VMs) mit Prisma Access. Sie können Apps basierend auf diesen Zugriffsobjekten hinzufügen: FQDNs, FQDN-Platzhalter oder IP-Subnetze.

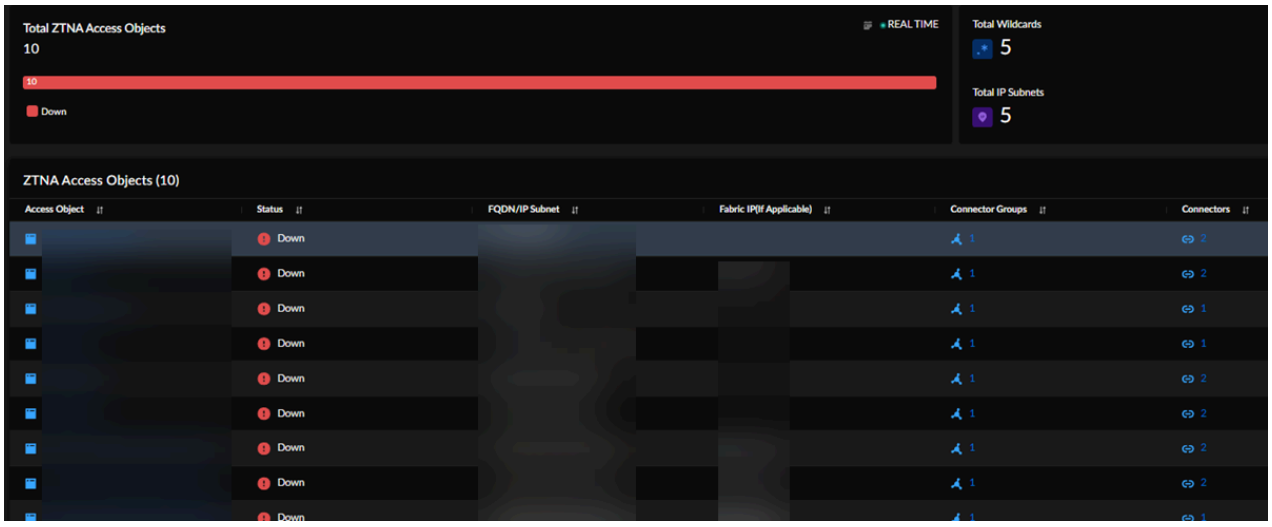
 ©2025 Palo Alto Networks, Inc.

- **FQDNs**: Prisma Access löst die FQDNs der Anwendungen, die Sie in den ZTNA-Connector integrieren, in die IP-Adressen im IP-Adressblock der Anwendung auf.
- **Platzhalter**: Erstellen Sie für platzhalterbasierte Apps eine FQDN-basierte Konnektorgruppe und geben Sie dann den Platzhalter an, der für das App-Ziel verwendet werden soll (z. B. *.example.com). Wenn Benutzer auf Sites zugreifen, die mit dem Platzhalter übereinstimmen, werden diese Apps automatisch für den Zugriff über den ZTNA-Connector für Ihre mobilen Benutzer und Benutzer von Remote-Netzwerken integriert.
- **IP-Subnetze**: Erstellen Sie eine IP-subnetzbasierte Konnektorgruppe und geben Sie dann das IP-Subnetz ein, das für das App-Ziel verwendet werden soll.

Navigieren Sie in Strata Cloud Manager zu **Überwachen** > **Rechenzentren** > **ZTNA-Zugriffsobjekte**, um Einblick in Ihre ZTNA-Connector-Zugriffsobjekte zu erhalten.

### Alle Zugriffsobjekte

Sehen Sie sich die **ZTNA-Zugriffsobjekte insgesamt** an, um Informationen zu allen Ihren ZTNA-Connector-Zugriffsobjekten – FQDNs, Platzhaltern und IP-Subnetzen – in Echtzeit zu erhalten. Die Zahl in **ZTNA-Zugriffsobjekte insgesamt** und in der Tabelle **ZTNA-Zugriffsobjekte** sollte übereinstimmen und die Anzahl der FQDN-Apps, Subnetz-Apps und ermittelten Platzhalter-Apps wiedergeben.




- Zeigen Sie ein Diagramm der **ZTNA-Zugriffsobjekte insgesamt** in Ihrer Umgebung nach Status an – d. h., dass die automatisierten sicheren Tunnel für das Zugriffsobjekt „Aktiv“, „Teilweise aktiv“, „Inaktiv“ oder „Deaktiviert“ sind. Wenn der Status „Inaktiv“ ist, kann der Konnektor, der diesem Zugriffsobjekt zugeordnet ist, Ihre Anwendung nicht erreichen.
  - **Aktiv**: Alle Tunnel sind aktiv und in Betrieb.
  - **Teilweise aktiv**: Einige Tunnel sind aktiv, andere sind inaktiv oder deaktiviert.
  - **Inaktiv**: Alle Tunnel sind inaktiv (ausgefallen).

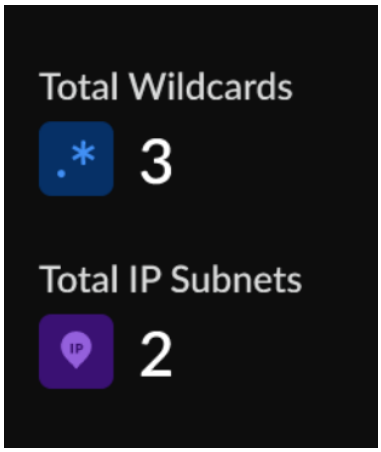
 ©2025 Palo Alto Networks, Inc.

- **Deaktiviert**: Alle Tunnel sind deaktiviert.

Wählen Sie ein Statusfarbquadrat im Widget **ZTNA-Zugriffsobjekte insgesamt** aus, um Zugriffsobjekte in der Tabelle **ZTNA-Zugriffsobjekte** nach Status zu sortieren.

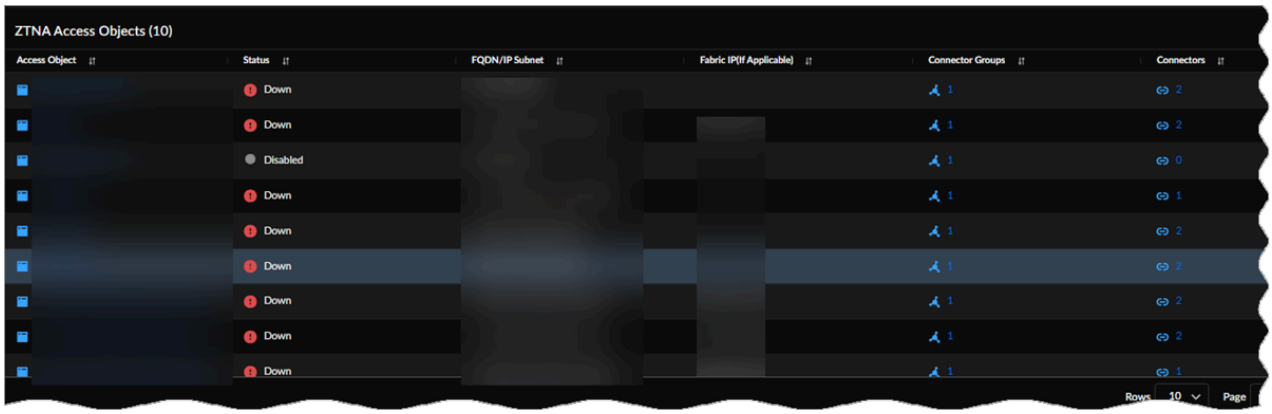



- **Platzhalter insgesamt und IP-Subnetze insgesamt** fasst zusammen, wie viele IP-Subnetze und Platzhalterregeln Sie integriert haben. Dies ist die Anzahl der Platzhalterregeln, die Sie erstellt haben. Sie ist nicht mit der Anzahl der Apps identisch, die als Ergebnis der Erstellung dieser Regeln erkannt wurden.




 ©2025 Palo Alto Networks, Inc.

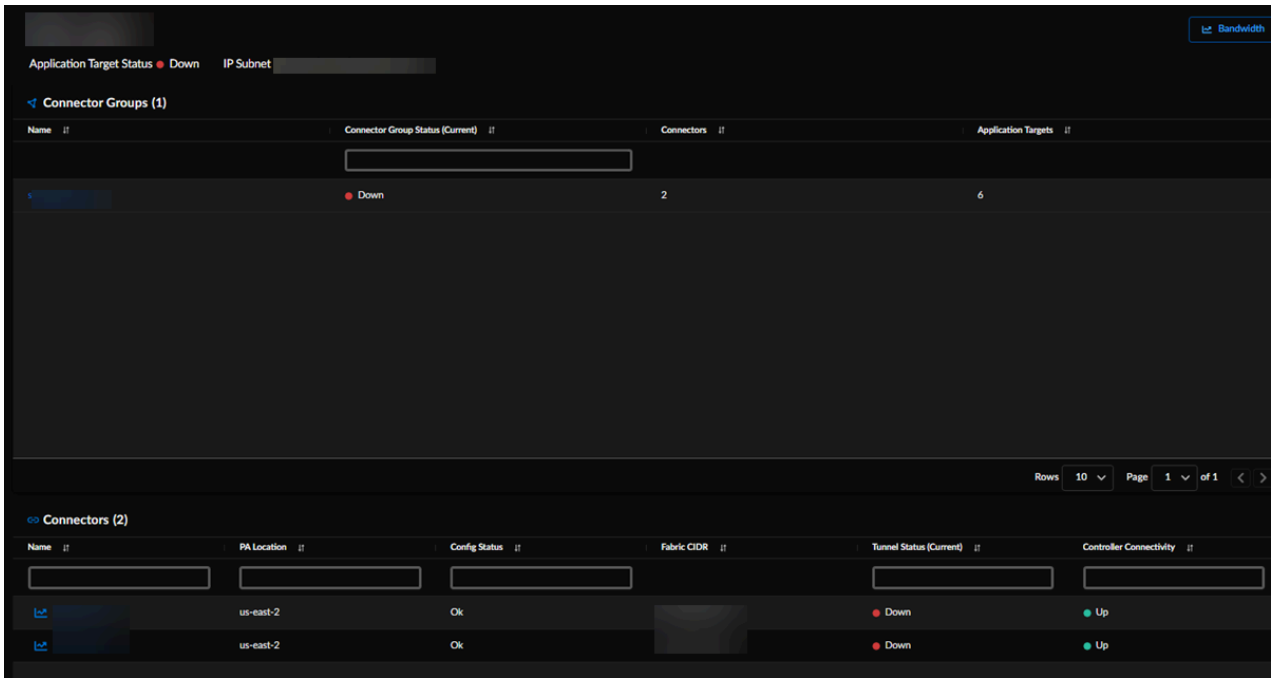
- **ZTNA-Zugriffsobjekte** zeigt Informationen zu allen Zugriffsobjekten an.
  - **Zugriffsobjekt**: Wählen Sie ein bestimmtes Zugriffsobjekt aus, um die Details dazu anzuzeigen.
  - **Status**: Der automatisierte sichere Tunnel für das Zugriffsobjekt ist „Aktiv“, „Teilweise aktiv“, „Inaktiv“ oder „Deaktiviert“.
  - **FQDN/IP-Subnetz**: Der FQDN oder das IP-Subnetz, der bzw. das zum Hinzufügen dieses Zugriffsobjekts verwendet wird.
  - **Fabric-IP (falls zutreffend)**: Die Fabric-IP, die diesem Zugriffsobjekt zugeordnet ist.
  - **Konnektorgruppen**: Konnektorgruppen sind logische Gruppierungen von Konnektoren und Anwendungen. Zeigen Sie die Konnektorgruppen an, die einem Zugriffsobjekt zugeordnet sind.
  - **Konnektoren**: Konnektoren stellen die in Ihren Rechenzentren ausgeführten VMs dar, die eine Verbindung zu Prisma Access herstellen. Zeigen Sie die Konnektoren an, die einem Zugriffsobjekt zugeordnet sind.




Wählen Sie ein beliebiges **Zugriffsobjekt** aus, um die Details dazu anzuzeigen.

- **Konnektorgruppen**: Zeigt an, wie viele Konnektorgruppen diesem Zugriffsobjekt zugeordnet sind. Wählen Sie eine Konnektorgruppe aus, um Informationen zu ihren Dienstverbindungen anzuzeigen.
- **Status der Konnektorgruppe (aktuell)**: Aktiv, Teilweise aktiv, Inaktiv oder Deaktiviert.
- **Konnektoren**: Zeigt die Anzahl der Konnektoren in dieser Konnektorgruppe an.
- **Anwendungsziele**: Zeigt die Anzahl der Anwendungsziele in dieser Konnektorgruppe an.
- **Bandbreite**: Wählen Sie die Option **Bandbreite** aus, um Bandbreiteninformationen zu diesem Zugriffsobjekt anzuzeigen.

 ©2025 Palo Alto Networks, Inc.



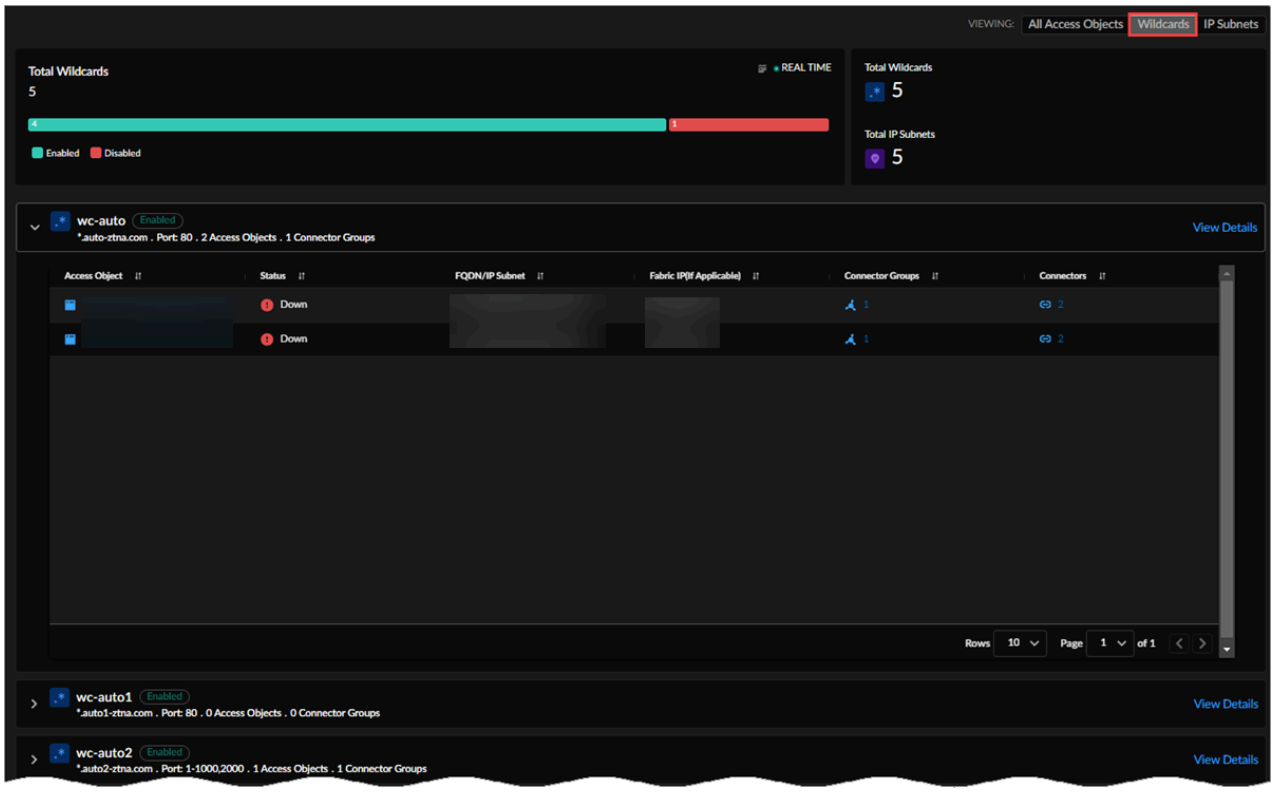

Wählen Sie beliebige **Konnektoren** eines Zugriffsobjekts aus, um die Details dazu anzuzeigen.

- **PA (Prisma Access)-Standort**: Zeigt den Prisma Access-Standort an, der jedem Konnektor zugeordnet ist.
- **Konfigurationsstatus**: Der Konfigurationsstatus des Konnektors lautet „OK“ oder „Fehler“. Wenn der Status „Fehler“ lautet, ist das Onboarding des ZTNA-Connectors noch nicht abgeschlossen.
- **Fabric-CIDR**: Das Fabric-CIDR, das diesem Konnektor zugeordnet ist.
- **Tunnelstatus (aktuell)**: Der Status des automatisierten sicheren Tunnels für diesen Konnektor.
- **Controller-Konnektivität**: Aktiv, Teilweise aktiv, Inaktiv oder Deaktiviert.

### Platzhalter

Wählen Sie **Platzhalter** aus, um die Zugriffsobjekte dieses Platzhalters anzuzeigen. Sehen Sie sich die **Platzhalter insgesamt** nach Status sowie der Anzahl der **Platzhalter insgesamt** und der **IP-Subnetze insgesamt** an.

 ©2025 Palo Alto Networks, Inc.




Wählen Sie den Pfeil neben einem Platzhalter oder die Option **Details anzeigen** aus, um Informationen zu den Zugriffsobjekten zu erhalten, aus denen sich dieser Platzhalter zusammensetzt.

- **Zugriffsobjekt**: Wählen Sie ein bestimmtes Zugriffsobjekt aus, um die Details dazu anzuzeigen.
- **Status**: Der automatisierte sichere Tunnel für das Zugriffsobjekt ist „Aktiv“, „Teilweise aktiv“, „Inaktiv“ oder „Deaktiviert“.
- **FQDN/IP-Subnetz**: Der FQDN oder das IP-Subnetz, der bzw. das zum Hinzufügen dieses Zugriffsobjekts verwendet wird.
- **Fabric-IP (falls zutreffend)**: Die Fabric-IP, die diesem Zugriffsobjekt zugeordnet ist.
- **Konnektorgruppen**: Konnektorgruppen sind logische Gruppierungen von Konnektoren und Anwendungen. Zeigen Sie die Konnektorgruppen an, die einem Zugriffsobjekt zugeordnet sind.
- **Konnektoren**: Konnektoren stellen die in Ihren Rechenzentren ausgeführten VMs dar, die eine Verbindung zu Prisma Access herstellen. Zeigen Sie die Konnektoren an, die einem Zugriffsobjekt zugeordnet sind.




Wählen Sie ein beliebiges **Zugriffsobjekt** aus, um die Details dazu anzuzeigen.

- **Konnektorgruppen**: Zeigt an, wie viele Konnektorgruppen diesem Zugriffsobjekt zugeordnet sind. Wählen Sie eine Konnektorgruppe aus, um Informationen zu ihren Dienstverbindungen anzuzeigen.

 ©2025 Palo Alto Networks, Inc.

- **Status der Konnektorgruppe (aktuell)**: Aktiv, Teilweise aktiv, Inaktiv oder Deaktiviert.
- **Konnektoren**: Zeigt die Anzahl der Konnektoren in dieser Konnektorgruppe an.
- **Anwendungsziele**: Zeigt die Anzahl der Anwendungsziele in dieser Konnektorgruppe an.
- **Bandbreite**: Wählen Sie die Option **Bandbreite** aus, um Bandbreiteninformationen zu diesem Zugriffsobjekt anzuzeigen.

Wählen Sie **Konnektorgruppen** oder **Konnektoren** aus, um die eindeutigen Konnektorgruppen oder Konnektoren anzuzeigen, die den Zugriffsobjekten im Platzhalter zugeordnet sind.

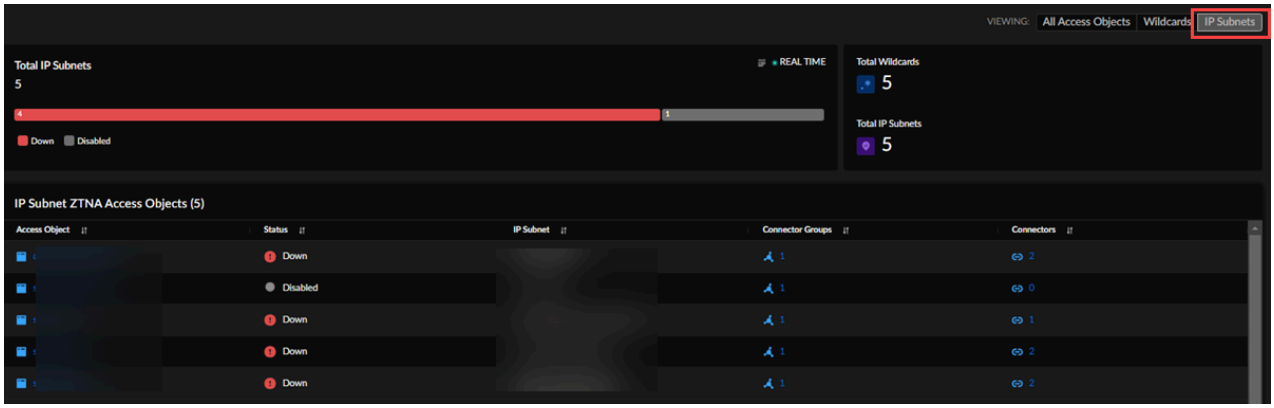
### IP-Subnetze

Wählen Sie **IP-Subnetze** aus, um die Gesamtzahl der IP-Subnetz-Zugriffsobjekte anzuzeigen. Ein IP-Subnetz-Zugriffsobjekt besteht aus einer Gruppierung mehrerer verschiedener Apps.

Sehen Sie sich die **IP-Subnetze insgesamt** in Ihrer Umgebung nach Status (Aktiv, Teilweise aktiv, Inaktiv oder Deaktiviert) an.

**ZTNA-Zugriffsobjekte für IP-Subnetze** zeigt Informationen zu allen Ihren Zugriffsobjekten an.

- - **Zugriffsobjekt**: Wählen Sie ein bestimmtes Zugriffsobjekt aus, um die Details dazu anzuzeigen.
  - **Status**: Aktiv, Teilweise aktiv, Inaktiv oder Deaktiviert.
  - **IP-Subnetz**: Das IP-Subnetz, das zum Hinzufügen dieses Zugriffsobjekts verwendet wird.
  - **Konnektorgruppen**: Konnektorgruppen sind logische Gruppierungen von Konnektoren und Anwendungen. Zeigen Sie die Konnektorgruppen an, die einem Zugriffsobjekt zugeordnet sind.
  - **Konnektoren**: Konnektoren stellen die in Ihren Rechenzentren ausgeführten VMs dar, die eine Verbindung zu Prisma Access herstellen. Zeigen Sie die Konnektoren an, die einem Zugriffsobjekt zugeordnet sind.




Wählen Sie ein beliebiges **Zugriffsobjekt** aus, um die Details dazu anzuzeigen.

- **Konnektorgruppen**: Zeigt an, wie viele Konnektorgruppen diesem Zugriffsobjekt zugeordnet sind. Wählen Sie eine Konnektorgruppe aus, um Informationen zu ihren Dienstverbindungen anzuzeigen.
- **Status der Konnektorgruppe (aktuell)**: Aktiv, Teilweise aktiv, Inaktiv oder Deaktiviert.
- **Konnektoren**: Zeigt die Anzahl der Konnektoren in dieser Konnektorgruppe an.
- **Anwendungsziele**: Zeigt die Anzahl der Anwendungsziele in dieser Konnektorgruppe an.

 ©2025 Palo Alto Networks, Inc.

- **Bandbreite**: Wählen Sie die Option **Bandbreite** aus, um Bandbreiteninformationen zu diesem Zugriffsobjekt anzuzeigen.

Wählen Sie **Konnektorgruppen** oder **Konnektoren** aus, um die eindeutigen Konnektorgruppen oder Konnektoren anzuzeigen, die den Zugriffsobjekten im IP-Subnetz zugeordnet sind.

# Anzeigen und Überwachen von Netzwerkdiensten

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz<br>❑ Dies ist eine Funktion von Prisma Access Insights. |

Sie können die Leistung allgemeiner Netzwerkdienste anzeigen, die sich auf die Benutzererfahrung beim Zugriff auf Anwendungen auswirken. Netzwerkdienste umfassen Funktionen zur Meldung der Anzahl erfolgreicher und fehlgeschlagener GlobalProtect-Authentifizierungen als Maß dafür, ob mobile Benutzer eine Verbindung zu Prisma Access herstellen können. Sie können sich zudem DNS-Proxy-Anfragen und -Antworten ansehen, die während eines von Ihnen festgelegten Zeitraums an Server weitergeleitet wurden.

## GlobalProtect-Authentifizierung

Navigieren Sie in Strata Cloud Manager zu **Überwachen** > **Netzwerkdienste** > **GlobalProtect-Authentifizierung**, um die erfolgreichen und fehlgeschlagenen GlobalProtect-Authentifizierungen anzuzeigen, die sich auf Ihre Umgebung auswirken.

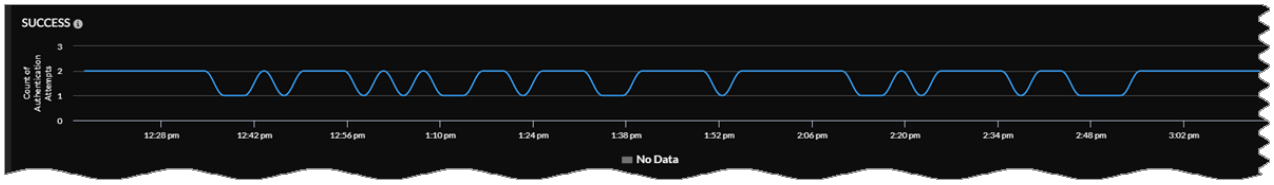
- Legen Sie den **Zeitbereich**-Filter fest, um die Netzwerkdienstdaten für diesen Zeitraum zu überprüfen.
- Legen Sie einen **Prisma Access-Standort** fest, um erfolgreiche Authentifizierungen, fehlgeschlagene Authentifizierungen insgesamt sowie die Timeoutfehler im ausgewählten Zeitraum anzuzeigen.

Die Daten geben an, wie viele mobile Benutzer zu einem bestimmten Zeitpunkt versuchen, sich bei einem GlobalProtect-Portal zu authentifizieren, das dann die Anmeldeinformationen der mobilen Benutzer zur Verifizierung an einen lokalen Active Directory (AD)-Server sendet, was zu einer erfolgreichen oder fehlgeschlagenen Authentifizierung führt. Wenn eine große Anzahl von fehlgeschlagenen Authentifizierungen angezeigt wird, können Sie diese mit einem Netzwerkereignis korrelieren, das auf ein Problem mit einem bestimmten Standort oder einem ausgefallenen lokalen Authentifizierungsserver hinweist. Die Daten in diesen Diagrammen bieten Netzwerkadministratoren Einblicke in die Behebung von Netzwerkproblemen. Sie können die Anzahl der Trends der Authentifizierungserfolge oder -fehler für mobile Benutzer auf GlobalProtect-Portalen und Gateways anzeigen, anhand dieser Daten die Muster von Authentifizierungserfolgen oder -fehlern im Zeitverlauf erfahren und Zählbereiche festlegen, die in Ihrer Prisma Access-Bereitstellung normal oder anomal sein können. Anomale Zählungen können beispielsweise darauf hinweisen, dass bestehende Benutzer keine Verbindung zu Prisma Access herstellen können, da es bei GlobalProtect-Portalen oder langsamen Authentifizierungsservern zu Verfügbarkeitsproblemen kommt. Anomale Zählungen können auch möglicherweise eine große Anzahl von Benutzern repräsentieren, die gleichzeitig in das Kundennetzwerk eingebunden sind.

 ©2025 Palo Alto Networks, Inc.

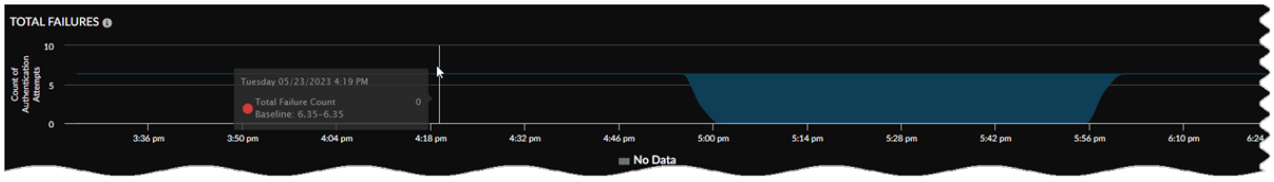
### Erfolgreiche GlobalProtect-Authentifizierungen

Sehen Sie sich spezielle Angaben zur Anzahl erfolgreicher GlobalProtect-Authentifizierungen für verschiedene Standorte an. Bewegen Sie den Mauszeiger über einen beliebigen Punkt im Diagramm, um Details zu den Benutzerzahlen für erfolgreiche Authentifizierungen an verschiedenen Prisma Access-Standorten zu erhalten, die zu einem bestimmten Zeitpunkt angezeigt werden.



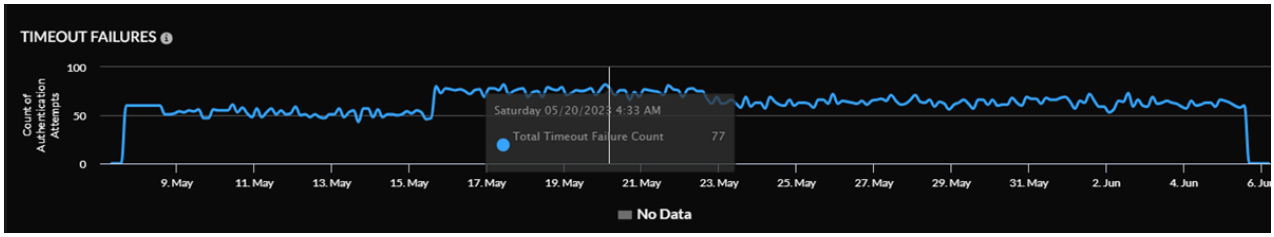

### Insgesamt fehlgeschlagene GlobalProtect-Authentifizierungen

Sehen Sie sich spezielle Angaben zur Anzahl fehlgeschlagener GlobalProtect-Authentifizierungen für verschiedene Standorte an. Fahren Sie mit dem Mauszeiger über eine beliebige Stelle im Diagramm, um Einzelheiten zur Anzahl der Benutzer für fehlgeschlagene Authentifizierungen an verschiedenen angezeigten Prisma Access-Standorten wie USA (Ost) und Kanada (Ost) zu einem bestimmten Zeitpunkt anzuzeigen.




### Timeoutfehler bei der GlobalProtect-Authentifizierung

Sehen Sie sich spezielle Angaben zur Anzahl fehlgeschlagener GlobalProtect-Authentifizierungen für verschiedene Standorte an. Fahren Sie mit dem Mauszeiger über eine beliebige Stelle im Diagramm, um Einzelheiten zur Anzahl der Benutzer für fehlgeschlagene Authentifizierungen an verschiedenen angezeigten Prisma Access-Standorten wie USA (Ost) und Kanada (Ost) zu einem bestimmten Zeitpunkt anzuzeigen.




## DNS

Navigieren Sie in Strata Cloud Manager zu **Überwachen** > **Netzwerkdienste** > **GlobalProtect-Authentifizierung**, um sich die DNS-Proxy-Anfragen und -Antworten anzusehen, die während eines von Ihnen festgelegten Zeitraums an Server weitergeleitet wurden.

Verfügbare Filter:

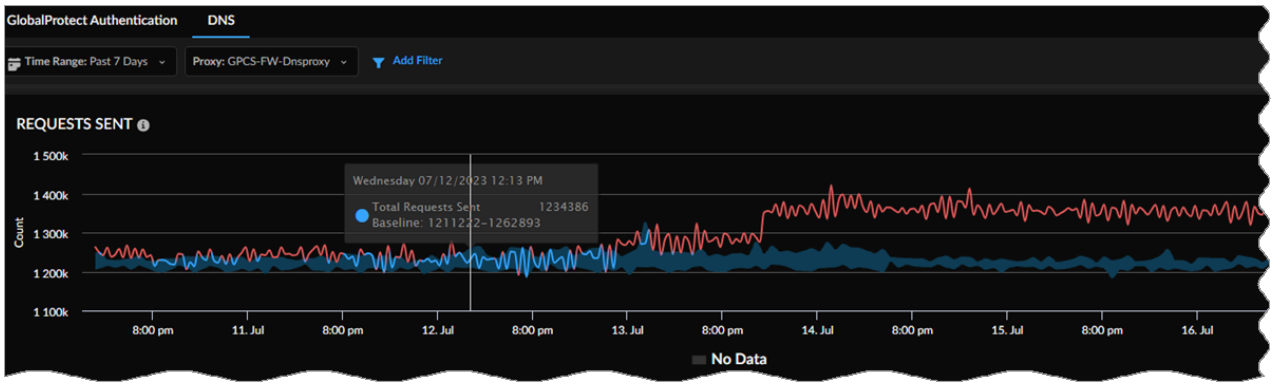
- **Zeitbereich**
- **DNS-Proxy-Namen**

 ©2025 Palo Alto Networks, Inc.

Die DNS-Proxy-Filterwerte beziehen sich auf die letzten 30 Tage und werden beim Laden automatisch ausgewählt (d. h., wenn keine Daten für explizite Proxys vorhanden sind, gibt es keinen Filter für explizite Proxys). Bewegen Sie den Mauszeiger über das Diagramm, um Einzelheiten zu allen an den DNS-Proxyserver **gesendeten Anfragen** und **empfangenen Anfragen** anzuzeigen.

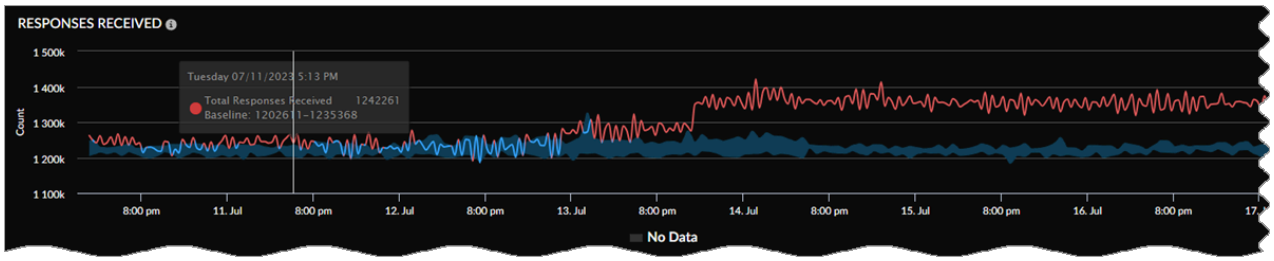
### Gesendete Anfragen

Zeigen Sie Netzwerkanfragen und -abfragen an, die in dem von Ihnen festgelegten Zeitraum an Server weitergeleitet wurden. Bewegen Sie den Mauszeiger über einen beliebigen Punkt im Diagramm, um Informationen über die zu diesem Zeitpunkt an die DNS-Proxyserver gesendeten Anforderungen anzuzeigen. Wenn Sie einen Proxynamen ausgewählt haben, nach dem gefiltert werden soll, werden die Daten für diesen Proxy angezeigt.




### Eingegangene Antworten

Zeigen Sie die Gesamtantworten an, die Sie während des von Ihnen angegebenen Zeitraums für alle Mandanten erhalten haben. Bewegen Sie den Mauszeiger über einen beliebigen Punkt im Diagramm, um Informationen über die zu diesem Zeitpunkt eingegangenen Antworten anzuzeigen. Wenn Sie einen Proxynamen ausgewählt haben, nach dem gefiltert werden soll, werden die Daten für diesen Proxy angezeigt.




## Anzeigen und Überwachen von Netzwerkdiensten: GlobalProtect-Authentifizierung

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz<br>❑ Dies ist eine Funktion von Prisma Access Insights. |

Netzwerkdienste umfassen Funktionen zur Meldung der Anzahl erfolgreicher und fehlgeschlagener GlobalProtect-Authentifizierungen als Maß dafür, ob mobile Benutzer eine

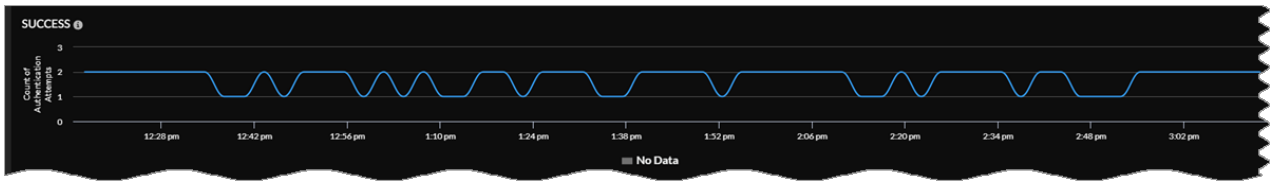
 ©2025 Palo Alto Networks, Inc.

Verbindung zu Prisma Access herstellen können. Wählen Sie als ersten Schritt in Strata Cloud Manager die Optionen **Überwachen** > **Netzwerkdienste** > **GlobalProtect-Authentifizierung** aus.

- Legen Sie den **Zeitbereich**-Filter fest, um die Netzwerkdienstdaten für diesen Zeitraum zu überprüfen.
- Legen Sie einen **Prisma Access-Standort** fest, um erfolgreiche Authentifizierungen, fehlgeschlagene Authentifizierungen insgesamt sowie die Timeoutfehler im ausgewählten Zeitraum anzuzeigen.

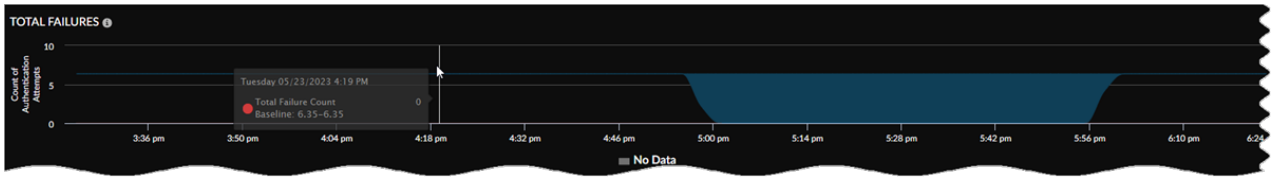
### Erfolgreiche GlobalProtect-Authentifizierungen

Sehen Sie sich spezielle Angaben zur Anzahl erfolgreicher GlobalProtect-Authentifizierungen für verschiedene Standorte an. Bewegen Sie den Mauszeiger über einen beliebigen Punkt im Diagramm, um Details zu den Benutzerzahlen für erfolgreiche Authentifizierungen an verschiedenen Prisma Access-Standorten zu erhalten, die zu einem bestimmten Zeitpunkt angezeigt werden.



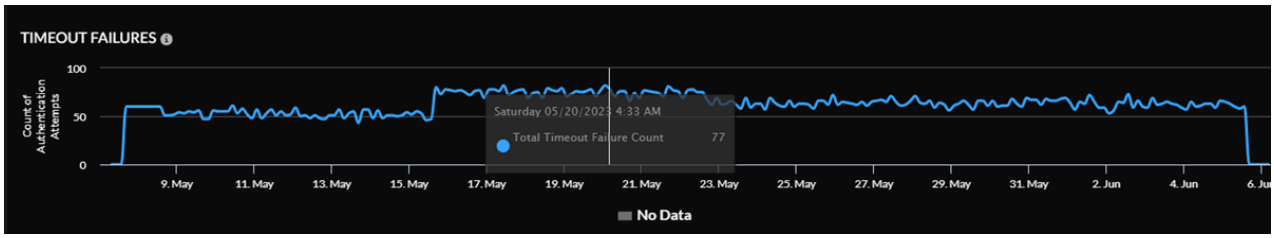

### Insgesamt fehlgeschlagene GlobalProtect-Authentifizierungen

Sehen Sie sich spezielle Angaben zur Anzahl fehlgeschlagener GlobalProtect-Authentifizierungen für verschiedene Standorte an. Fahren Sie mit dem Mauszeiger über eine beliebige Stelle im Diagramm, um Einzelheiten zur Anzahl der Benutzer für fehlgeschlagene Authentifizierungen an verschiedenen angezeigten Prisma Access-Standorten wie USA (Ost) und Kanada (Ost) zu einem bestimmten Zeitpunkt anzuzeigen.




### Timeoutfehler bei der GlobalProtect-Authentifizierung

Sehen Sie sich spezielle Angaben zur Anzahl fehlgeschlagener GlobalProtect-Authentifizierungen für verschiedene Standorte an. Fahren Sie mit dem Mauszeiger über eine beliebige Stelle im Diagramm, um Einzelheiten zur Anzahl der Benutzer für fehlgeschlagene Authentifizierungen an verschiedenen angezeigten Prisma Access-Standorten wie USA (Ost) und Kanada (Ost) zu einem bestimmten Zeitpunkt anzuzeigen.




 ©2025 Palo Alto Networks, Inc.

## Anzeigen und Überwachen von Netzwerkdiensten: DNS

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz<br>❑ Dies ist eine Prisma Access Insights-Funktion. |

**Netzwerkdienste: DNS** zeigt DNS-Proxy-Anfragen und -Antworten an, die während eines von Ihnen angegebenen Zeitraums an Server weitergeleitet werden.

Verfügbare Filter:

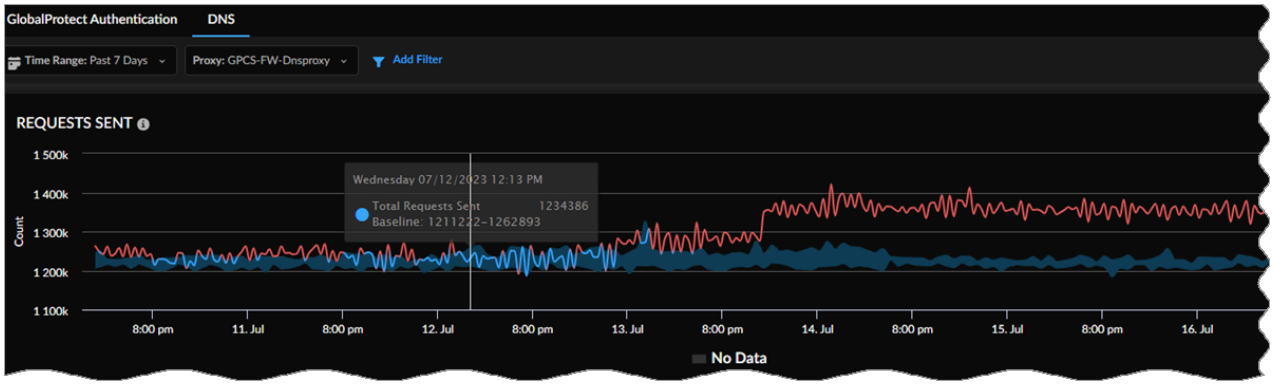
- **Zeitbereich**
- **DNS-Proxy-Namen**

Die DNS-Proxy-Filterwerte beziehen sich auf die letzten 30 Tage und werden beim Laden automatisch ausgewählt (d. h., wenn keine Daten für explizite Proxys vorhanden sind, gibt es keinen Filter für explizite Proxys).

Bewegen Sie den Mauszeiger über das Diagramm, um Einzelheiten zu allen an den DNS-Proxyserver **gesendeten Anfragen** und **empfangenen Anfragen** anzuzeigen.

### Gesendete Anfragen

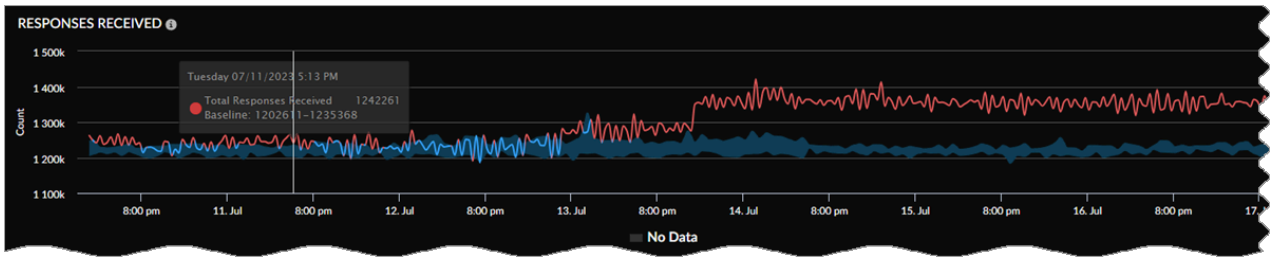
Zeigen Sie Netzwerkanfragen und -abfragen an, die in dem von Ihnen festgelegten Zeitraum an Server weitergeleitet wurden. Bewegen Sie den Mauszeiger über einen beliebigen Punkt im Diagramm, um Informationen über die zu diesem Zeitpunkt an die DNS-Proxyserver gesendeten Anforderungen anzuzeigen. Wenn Sie einen Proxynamen ausgewählt haben, nach dem gefiltert werden soll, werden die Daten für diesen Proxy angezeigt.




### Eingegangene Antworten

Zeigen Sie die Gesamtantworten an, die Sie während des von Ihnen angegebenen Zeitraums für alle Mandanten erhalten haben. Bewegen Sie den Mauszeiger über einen beliebigen Punkt im Diagramm, um Informationen über die zu diesem Zeitpunkt eingegangenen Antworten anzuzeigen. Wenn Sie einen Proxynamen ausgewählt haben, nach dem gefiltert werden soll, werden die Daten für diesen Proxy angezeigt.

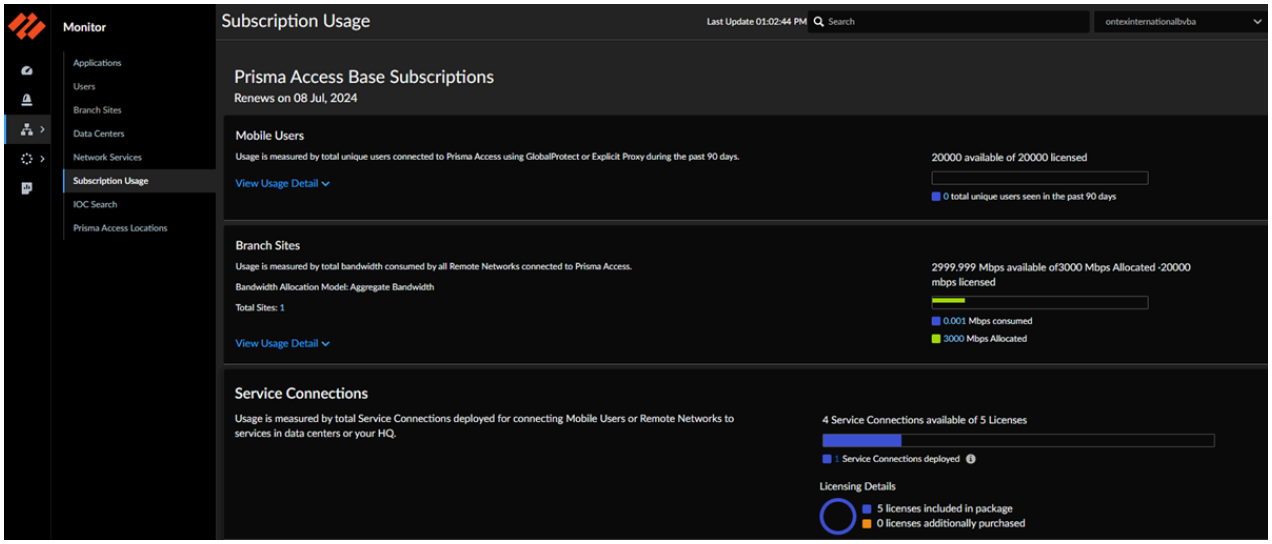

©2025 Palo Alto Networks, Inc.




# Anzeigen der Abonnementnutzung

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Wählen Sie **Überwachen** > **Nutzung des Abonnements** um Details zu Ihren **Prisma Access-Basisabonnements**, einschließlich der Anzahl der Lizenzen, die Sie bisher verbraucht haben, anzuzeigen.

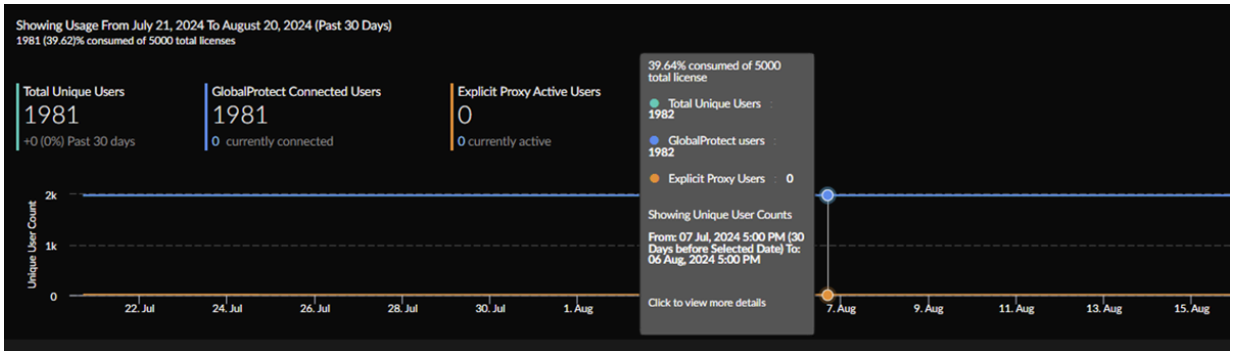



- **Mobile Benutzer**: Zeigen Sie an, wie viele Lizenzen für eindeutige **mobile Benutzer** Sie bisher verbraucht haben. Das Widget zeigt an, wie viele Lizenzen insgesamt von eindeutigen mobilen Benutzern verbraucht wurden, die in den letzten 30 Tagen eine Verbindung zu Prisma Access hergestellt haben, da Lizenzen immer auf den Prisma Access-Anmeldedaten der letzten 30 Tage basieren. Ein Benutzer, der sich in den letzten 30 Tagen mindestens einmal bei Prisma Access angemeldet hat, trägt zum Verbrauch einer Lizenz für mobile Benutzer bei.

  Wählen Sie **Nutzungsdetails anzeigen** aus, um Details zur Lizenznutzung während der letzten 30 Tage anzuzeigen. Sie können die Gesamtzahl der eindeutigen Benutzer in den letzten 30 Tagen, die Gesamtzahl der verbundenen GlobalProtect-Benutzer und die Gesamtzahl

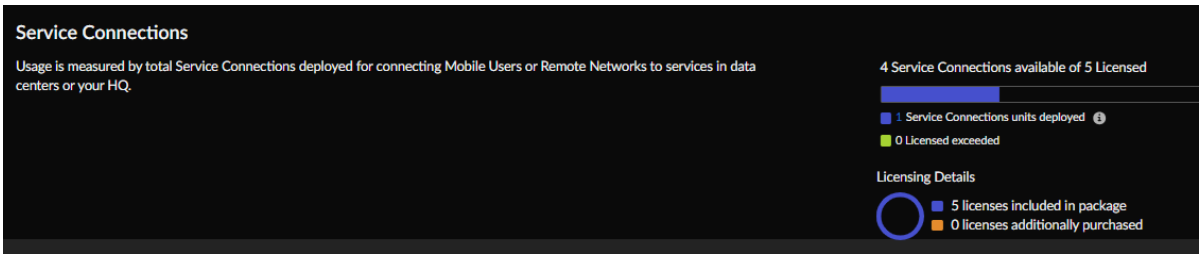
 ©2025 Palo Alto Networks, Inc.

der aktiven Benutzer des expliziten Proxys anzeigen. Bewegen Sie den Mauszeiger über das Diagramm, um die zum aktuellen Zeitpunkt verbrauchten Lizenzen anzuzeigen.




- **Zweigstellen**: Zeigen Sie die gesamte Bandbreitennutzung aller Remote-Netzwerke an, die mit Prisma Access verbunden sind. Sehen Sie sich an, wie viel Bandbreite Sie zugewiesen und wie viel Sie verbraucht haben (in Mbit/s). Zeigen Sie die Nutzung anhand der gesamten Bandbreite an, die von allen mit Prisma Access verbundenen Remote-Netzwerken verbraucht wird.

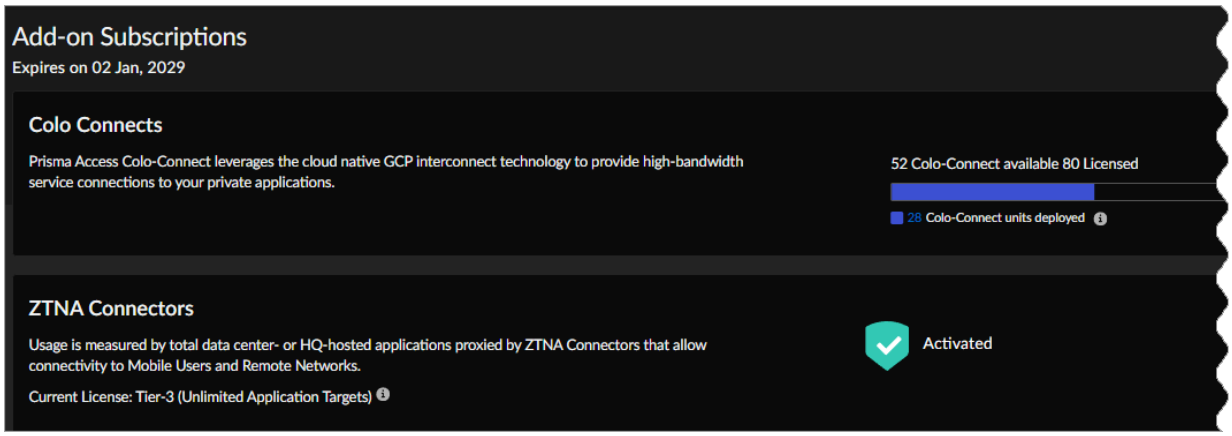
  Wählen Sie die Option **Nutzungsdetails anzeigen** aus, um basierend auf Ihrem Bandbreitenzuweisungsmodell den Verbrauch an lizenzierter Bandbreite nach Rechenregionen oder Zweigstellen anzuzeigen. In beiden Fällen wird für jeden der 30 Tage, die für die Lizenzberechnung berücksichtigt werden, ein täglicher Spitzenwert für den Bandbreitenverbrauch angegeben. Sie können die Diagrammansicht filtern, indem Sie Rechenregionen oder Zweigstellen auswählen. Das Diagramm enthält drei Linien, die pro Rechenregion oder pro Standort dargestellt sind und die täglichen Spitzenverbrauchswerte, die der Rechenregion oder dem Standort zugewiesene Bandbreite und den 95. Perzentilwert angeben, der aus den täglichen Spitzenwerten ermittelt wurde.
- **Dienstverbindungen**: Zeigt an, wie viele Lizenzen für **Dienstverbindungen** Sie bisher verbraucht haben.



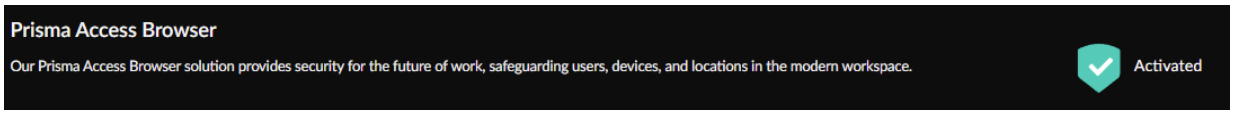

Im Abschnitt **Add-on-Abonnements** auf dieser Seite sehen Sie Ihre zusätzlich erworbenen Lizenzen. Sie können die Gesamtzahl der erworbenen Lizenzen sowie die Anzahl der bisher nicht genutzten Lizenzen sehen. In den folgenden Abbildungen werden einige der zusätzlichen Lizenzen beschrieben, die Sie erwerben können.

 ©2025 Palo Alto Networks, Inc.

- **Colo-Connects**: Prisma Access Colo-Connect nutzt die cloudnative GCP-Technologie, um Dienstverbindungen mit hoher Bandbreite für Ihre privaten Anwendungen bereitzustellen.




- **Prisma Access Browser**: Prisma Access Secure Enterprise Browser (Prisma Access Browser) ist die einzige Lösung, die sowohl verwaltete als auch nicht verwaltete Geräte über einen nativ integrierten Unternehmensbrowser schützt, der den Schutz auf nicht verwaltete Geräte ausweitet. Prisma Access Browser schützt Geschäftsanwendungen und -daten, indem er die Sicherheit in den Browser integriert. Ihr Prisma Access Browser-Abonnement wird in **Add-on-Abonnements** oder in **Prisma Access-Basisabonnements** angezeigt.
  - **Prisma Access-Basisabonnements**: Der Mandant verfügt über eine eigenständige Prisma Access Browser-Lizenz.
  - **Add-on-Abonnements**: Wenn Sie die Prisma Access Browser-Lizenz für alle mobilen Benutzer erworben haben, wird das Prisma Access Browser-Abonnement **aktiviert**.




# Anzeigen und Überwachen von Prisma Access-Standorten

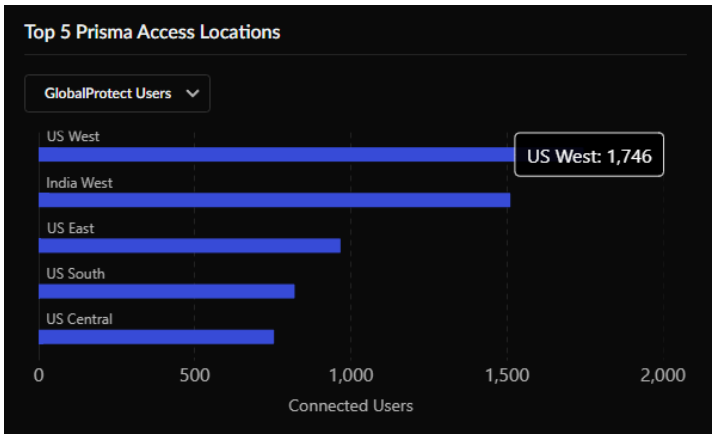
| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz<br>❑ Dies ist eine Funktion von Prisma Access Insights. |

Wählen Sie **Überwachen** > **Prisma Access-Standorte** um eine Übersicht über den Zustand aller Ihrer Prisma Access-Standorte für Ihre Remote-Netzwerke und mobilen Benutzer anzuzeigen.

## Top 5 Prisma Access-Standorte

Die Balken zeigen Daten zu den Top 5 Prisma Access-Standorten für Remote-Netzwerke, Dienstverbindungen, mobile GlobalProtect-Benutzer oder mobile Benutzer von explizitem Proxy an (ausgewählt im Dropdown-Menü), basierend auf der gesamten Bandbreite, die im ausgewählten Zeitraum verbraucht wurde. Bewegen Sie den Mauszeiger über eine beliebige Leiste, um zu sehen, wie viele Benutzer sich an diesem bestimmten Standort befinden.

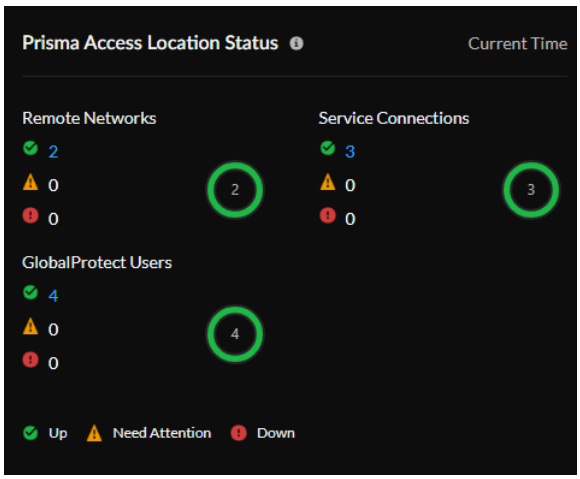
 ©2025 Palo Alto Networks, Inc.




## Prisma Access-Standortstatus

Abhängig von Ihrer Lizenz zeigt dieses Widget die Anzahl der verbundenen Remote-Netzwerkstandorte, Dienstverbindungsstandorte, eindeutigen GlobalProtect-Benutzer und eindeutigen Benutzer von explizitem Proxy an, die bei Prisma Access angemeldet sind. Der Farbcode des Widgets basiert darauf, wie viele Remotenetzwerke, Dienstverbindungen, GlobalProtect-Benutzer und Benutzer von explizitem Proxy sich im folgenden Status befinden:

- **Verbunden** (grün): Alle Prisma Access-Standorte sind verbunden.
- **Getrennt** (rot): Alle Prisma Access-Standorte sind getrennt.
- **Teilweise verbunden** (orange): Ein oder mehrere Prisma Access-Standort(e) sind getrennt.



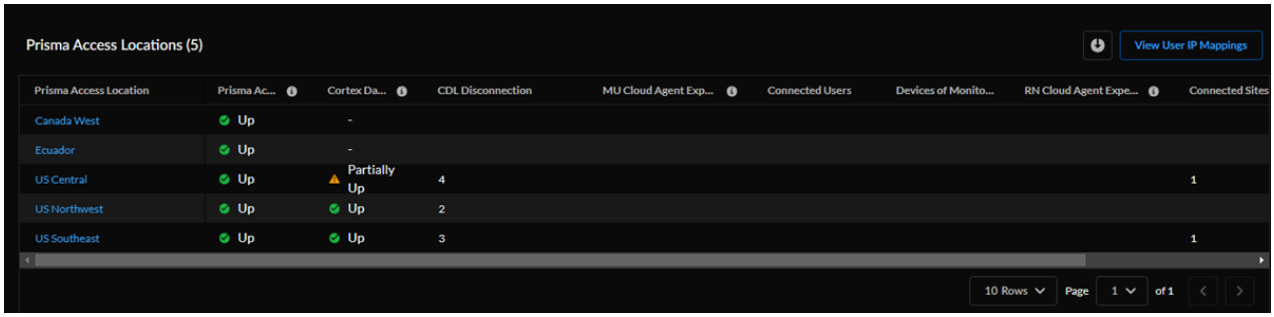

## Strata Logging Service-Konnektivität

Das Widget **Strata Logging Service-Konnektivität** vermittelt Ihnen Einblicke in den Strata Logging Service-Konnektivitätsstatus von allen Ihren Prisma Access-Instanzen für die Strata Logging Service-Region, die Sie während der Lizenzaktivierung von Prisma Access ausgewählt haben. Es hilft Ihnen festzustellen, ob die Verbindung von Firewalls zu Strata Logging Service getrennt wurde und Sie keine Firewall-Protokolle mehr erhalten. Jeder Mandant kann sich mit nur einem Strata Logging Service in einer Region seiner Wahl verbinden. Prisma Access fragt die Strata Logging Service-Datenbank alle 5 Minuten ab, um die Konnektivität zwischen den Knoten (Mobile Benutzer, Remote-Netzwerke und Dienstverbindungen) und der Strata Logging Service-Datenbank zu überprüfen.

 ©2025 Palo Alto Networks, Inc.

### Status der Prisma Access-Standorte

Zeigen Sie den Status der **Prisma Access-Standorte** in Echtzeit an. Meldet sich ein Benutzer innerhalb eines bestimmten Standorts von mehreren Hosts an, wird er als einzelner Benutzer gezählt. Meldet sich ein Benutzer jedoch von zwei verschiedenenPrisma Access-Standorten aus an, indem er die Verbindung zu einem Standort trennt und sich innerhalb des Zeitraums von einem anderen Standort aus anmeldet, wird der Benutzer als zwei Benutzer gezählt. Wählen Sie einen Standort aus, um Details wie verbrauchte Bandbreite, Status, Strata Logging Service-Konnektivität sowie Benutzer-ID und Gruppenzuordnungen anzuzeigen.




# Anzeigen und Überwachen der IDs von Drittanbietergeräten

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ☐ Prisma Access-Lizenz |

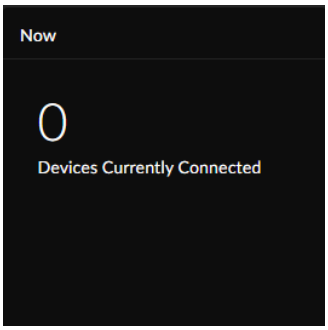
Sie können die Cloud Identity Engine zusammen mit Prisma Access verwenden, um Informationen aus IoT-Erkennungsquellen von Drittanbietern anzuwenden und die Erkennung und Schließung von Sicherheitslücken für Geräte in Ihrem Netzwerk zu vereinfachen. Weitere Informationen zur Einrichtung und Konfiguration finden Sie unter Konfigurieren der Drittanbietergeräte-ID in Prisma Access.

Gehen Sie zu **Überwachen** > **Geräte** > **IOT**, um Einblicke in Ihre IoT-Geräte zu erhalten, z. B. bezüglich der Anzahl der in den letzten 30 Minuten verbundenen IoT-Geräte, aller im ausgewählten Zeitraum verbundenen IoT-Geräte und zu den Details aller verbundenen IoT-Geräte.

### Derzeit verbundene Geräte

Zeigen Sie die Anzahl der in den letzten 30 Minuten angeschlossenen Geräte an. **Aktuell** zeigt immer nur die **derzeit verbundenen Geräte** der letzten 30 Minuten an.


©2025 Palo Alto Networks, Inc.

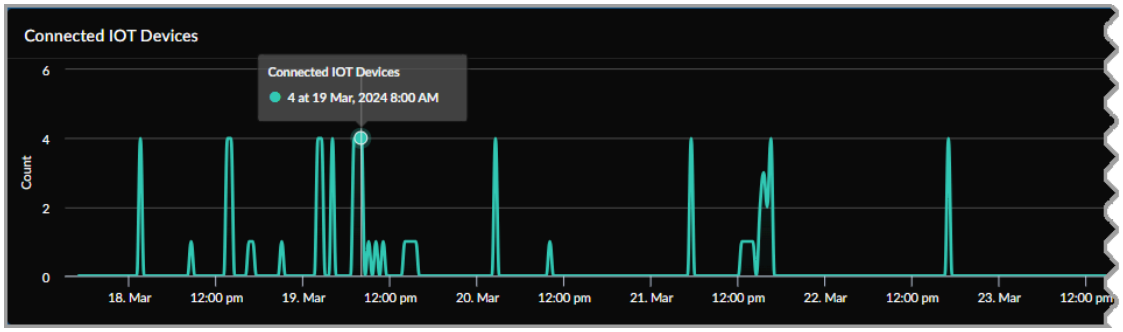



## Verbundene IoT-Geräte

**Verbundene IoT-Geräte** zeigt die Anzahl der verbundenen Geräte gefiltert nach **Zeitbereich** an. Passen Sie die angezeigten Daten an, indem Sie andere Filteroptionen aus dem Dropdown-Menü **Filter hinzufügen** auswählen.

- **Kategorie**: Die Kategorie, zu der dieses Gerät gehört.
- **MAC-Adresse**: Die MAC-Adresse des Geräts.
- **Profil**: Das Geräteprofil.
- **Anbieter**: Der Geräteanbieter.
- **Quell-IP**: Die IP-Adresse des Geräts.
- **Prisma Access-Standort**: Prisma Access-Standort des Geräts.
- **Zweigstelle**: Die Zweigstelle, an der sich das Gerät befindet.

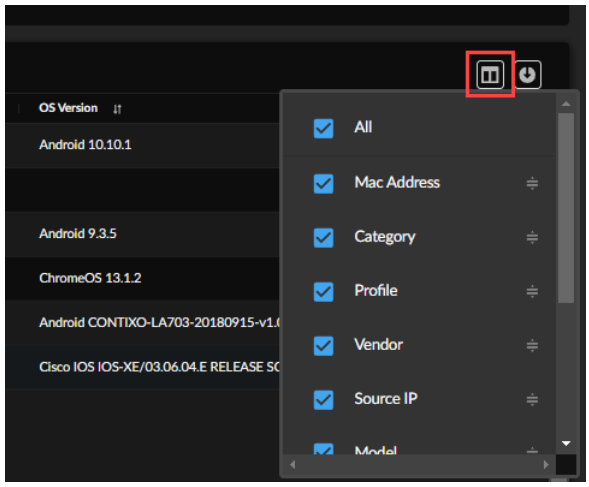
Bewegen Sie den Mauszeiger über einen Punkt im Diagramm, um die Anzahl der Benutzer zu einem bestimmten Zeitpunkt anzuzeigen. Wenn Sie die Benutzertrends über einen bestimmten Zeitraum kennen, können Sie die Nutzung überwachen und ungewöhnliche Muster untersuchen.




## IoT-Geräte

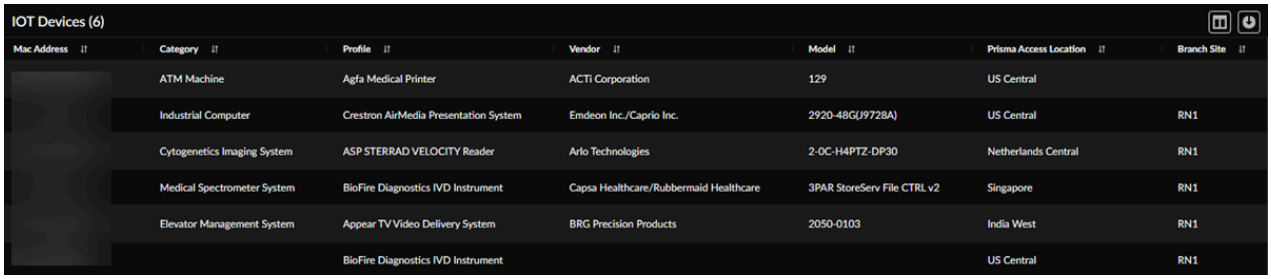
Zeigen Sie die Anzahl der IoT-Geräte an, die im ausgewählten **Zeitbereich** verbunden sind. Verwenden Sie das Spalten-Dropdown-Menü, um die in der Tabelle angezeigten Spalten auszuwählen oder abzuwählen.

 ©2025 Palo Alto Networks, Inc.




- **MAC-Adresse**: Die MAC-Adresse des Geräts.
- **Kategorie**: Die Kategorie, zu der dieses Gerät gehört.
- **Profil**: Das Geräteprofil.
- **Anbieter**: Der Geräteanbieter.
- **Quell-IP**: Die IP-Adresse des Geräts.
- **Modell**: Das Gerätemodell.
- **Betriebssystemversion**: Die Version des Betriebssystems (OS-Version).
- **OS-Familie**: Die Betriebssystemfamilie, zu der das Gerät gehört.
- **Prisma Access-Standort**: Der verwendete Prisma Access-Standort.
- **Zweigstelle**: Die Zweigstelle, an der sich das Gerät befindet.

Die folgende Tabelle „IoT-Geräte“ zeigt eine benutzerdefinierte Spaltenauswahl. Um alle Spalten in der Tabelle anzuzeigen, wählen Sie alle Optionen im Dropdown-Menü aus.




# Anzeigen und Überwachen der Remote-Browser-Isolation

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access 5.0 Innovation |

 ©2025 Palo Alto Networks, Inc.

Mit Strata Cloud Manager können Sie sich einen umfassenden Überblick über Ihren Netzwerkverkehr verschaffen und die Remote-Browser-Isolation (RBI) nutzen, indem Sie die Abschnitte Überwachen und Workflows in Strata Cloud Manager verwenden. Verschaffen Sie sich Einblick in Ihre RBI-Bereitstellung, indem Sie Metriken wie die Anzahl der aktiven RBI-Benutzer, Trends, den Verbindungsstatus, den RBI-Standortstatus, Datenverkehrsmessungen und den Lizenzverbrauch anzeigen. Mithilfe der Daten zu Ihren Benutzern können Sie sich ein Gesamtbild über den Zustand und die Konnektivität Ihrer Bereitstellung verschaffen.

RBI leitet die Internet-Browsing-Aktivitäten der Benutzer in eine isolierte Umgebung um, die von einem RBI-Anbieter gehostet wird. Die Website ist für die Benutzer gedacht, die die benötigten Ressourcen anzeigen können, ohne direkt von ihren Geräten und ihrem Netzwerk aus auf unbekannte oder riskante Sites zuzugreifen. Für diese Art der Browserumleitung lässt sich Prisma Access problemlos in Lösungen von RBI-Anbietern integrieren.

 ©2025 Palo Alto Networks, Inc.

# Prisma Access und Autonomous DEM

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Strata Cloud Manager Managed Prisma Access<br>• Panorama Managed Prisma Access | ❑ Prisma Access-Lizenz<br>❑ Autonomous DEM-Lizenz |

Machen Sie sich mit Autonomous DEM in Prisma Access vertraut, um die digitale Erfahrung für alle Benutzer, Anwendungen und Remote-Standorte in Ihrer SASE-Umgebung kontinuierlich zu überwachen. Solange Sie über die entsprechenden Lizenzen verfügen, können Sie Autonomous DEM für Ihre mobilen GlobalProtect-Benutzer aktivieren, die eine Verbindung zu Prisma Access herstellen.

- Cheat-Sheet: ADEM mit Prisma Access
- Erste Schritte mit Autonomous DEM
- Benutzerdatenverkehr und Anwendungen mit Autonomous DEM überwachen


©2025 Palo Alto Networks, Inc.

# Benutzerbasierte Richtlinie in Prisma Access

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>• Cloud Identity Engine | • Prisma Access-Lizenz |

Prisma Access erfordert, dass Sie die Zuordnung von IP-Adresse zu Benutzername konfigurieren, um benutzerbasierte Richtlinien für mobile Benutzer und Benutzer an Remote-Netzwerkstandorten konsequent durchzusetzen. Darüber hinaus müssen Sie die Zuordnung von Benutzername zu Benutzergruppe konfigurieren, wenn Sie Richtlinien basierend auf der Gruppenmitgliedschaft durchsetzen möchten.

Wenn Sie Richtlinien in Panorama erstellen und konfigurieren, können Sie für die Auswahl der Gruppen aus einer Dropdown-Liste Panorama auch so konfigurieren, dass die Liste der Benutzergruppen aus der Zuordnung von Benutzername zu Benutzergruppe abgerufen wird.

Die folgenden Abschnitte enthalten eine Übersicht und die Schritte, die Sie zum Konfigurieren und Implementieren der Benutzer-ID sowie zur Verwendung der Cloud Identity Engine durchführen, um die Zuordnung von IP-Adresse zu Benutzername und von Benutzername zu Benutzergruppe in Prisma Access abzurufen.

# Konfigurieren benutzerbasierter Richtlinien für Prisma Access

- Strata Cloud Manager
- Panorama

 ©2025 Palo Alto Networks, Inc.

# Benutzerbasierte Richtlinie in Prisma Access (Strata Cloud Manager)

Nach dem Integrieren der Cloud Identity Engine in Prisma Access müssen Sie bestätigen, dass Prisma Access mit der Cloud Identity Engine verbunden ist und die Cloud Identity Engine Verzeichnisinformationen mit Prisma Access gemeinsam verwendet.

- Überprüfen Sie, ob Sie Ihre Verzeichnisse in Prisma Access sehen können.

  Gehen Sie zu **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Identitätsdienste** > **Cloud Identity Engine**.

- Überprüfen Sie, ob Sie einer Richtlinienregel Benutzer und Gruppen hinzufügen können.

  Wählen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Sicherheitsdienste** > **Entschlüsselung** aus.

  Überprüfen Sie in einer Sicherheits- oder Entschlüsselungsrichtlinienregel, ob in der Dropdown-Liste **Benutzer** Ihre Active Directory-Benutzer- und -Gruppeneinträge angezeigt werden. Jetzt können Sie damit beginnen, diese Benutzer und Gruppen zu Ihren Sicherheits- und Entschlüsselungsrichtlinienregeln hinzuzufügen.

Wenn Sie bestätigt haben, dass die Verbindung zur Cloud Identity Engine erfolgreich hergestellt wurde, können Sie mit der Ausführung von Benutzeraktivitätsberichten beginnen, um einen besseren Einblick in das Verhalten Ihrer Benutzerbasis zu erhalten.

 ©2025 Palo Alto Networks, Inc.

# Benutzerbasierte Richtlinie in Prisma Access (Panorama)

In diesem Abschnitt finden Sie die Schritte, die Sie zum Konfigurieren der Benutzer-ID für Prisma Access ausführen.

**STEP 1 |** Konfigurieren Sie die Zuordnung von IP-Adressen zu Benutzernamen für Ihre mobilen Benutzer und für Benutzer an Remote-Netzwerkstandorten.

- Für Bereitstellungen des Typs „Mobile Benutzer – GlobalProtect“ führt der GlobalProtect-Agent in Prisma Access automatisch eine Benutzer-ID-Zuordnung durch.
- Für Benutzer in Remote-Netzwerken konfigurieren Sie die Benutzer-ID für Remote-Netzwerkbereitstellungen, um IP-Adressen Benutzer-IDs zuzuordnen.

**STEP 2 |** Konfigurieren Sie die Zuordnung von Benutzernamen zu Benutzergruppen für Ihre mobilen Benutzer und Benutzer an Remote-Netzwerkstandorten.

Für Bereitstellungen des Typs Mobile Benutzer – GlobalProtect, Expliziter Proxy und Remote-Netzwerk konfigurieren Sie die Komponente „Verzeichnissynchronisierung“ der Cloud Identity Engine, um Benutzer- und Gruppeninformationen aus Ihrem Active Directory (AD) abzurufen. Konfigurieren Sie anschließend **Einstellungen für die Gruppenzuordnung** in Ihren Bereitstellungen des Typs Mobile Benutzer – GlobalProtect oder Remote-Netzwerk.

Alternativ können Sie mithilfe eines LDAP-Serverprofils die Zuordnung von Benutzernamen zu Benutzergruppen für mobile Benutzer und für Benutzer in Remote-Netzwerken aktivieren.



*Wir empfehlen, im LDAP-Serverprofil eine Gruppeneinschlussliste zu verwenden, damit Sie angeben können, welche Gruppen Sie abrufen möchten, anstatt alle Gruppeninformationen abzurufen.*

**STEP 3 |** Erlauben Sie Panorama, die Zuordnung von Benutzernamen zu Benutzergruppen in Sicherheitsrichtlinien zu verwenden, indem Sie eine der folgenden Aktionen ausführen:

- Konfigurieren Sie die Komponente „Verzeichnissynchronisierung“ der Cloud Identity Engine, um Benutzer- und Gruppeninformationen aus Ihrem Active Directory (AD) abzurufen. Anschließend konfigurieren Sie **Einstellungen für die Gruppenzuordnung** in Ihrer Bereitstellung des Typs Mobile Benutzer – GlobalProtect, Mobile Benutzer – Expliziter Proxy oder Remote-Netzwerk.
- Konfigurieren Sie gruppenbasierte Richtlinien durch Angabe des vollständigen ausgewählten Namens (Full Distinguished Name (DN) der Gruppe.

**STEP 4 |** Verteilen Sie HIP-Informationen an Panorama um.

 ©2025 Palo Alto Networks, Inc.

# Cloud Identity Engine in Prisma Access integrieren

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

- Strata Cloud Manager
- Panorama

## Cloud Identity Engine in Prisma Access integrieren (Strata Cloud Manager)

Cloud Identity Engine (Directory Sync) gewährt Prisma Access schreibgeschützten Zugriff auf Ihre Active Directory-Informationen, sodass Sie Sicherheits- und Entschlüsselungsrichtlinien für Benutzer und Gruppen einfach einrichten und verwalten können.

Cloud Identity Engine funktioniert sowohl mit lokalem Active Directory als auch mit Azure Active Directory.

Um die Cloud Identity Engine mit Prisma Access einzurichten, gehen Sie zunächst zum Hub, um die Cloud Identity Engine zu aktivieren und zu Prisma Access hinzuzufügen. Prüfen Sie anschließend in Prisma Access, ob Prisma Access auf Verzeichnisdaten zugreifen kann.

 ©2025 Palo Alto Networks, Inc.



**STEP 1 |** Aktivierung von Cloud Identity Engine

Die Cloud Identity Engine kann Active Directory-Informationen mit jeder unterstützten Anwendung im Hub teilen. Sie ist kostenlos und erfordert zum Einstieg keinen Authentifizierungscode. Zur Einrichtung der Cloud Identity Engine gehört das Aktivieren der Cloud Identity Engine-Anwendung im Hub, das Konfigurieren des Cloud Identity Engine-Agents zum Erfassen von Active Directory-Zuordnungen sowie die Konfiguration der gegenseitigen Authentifizierung zwischen Cloud Identity Engine und dem Agent.

Stellen Sie sicher, dass die Cloud Identity Engine-Instanz in derselben Region bereitgestellt wird, in der Sie Prisma Access und Strata Logging Service bereitgestellt haben.

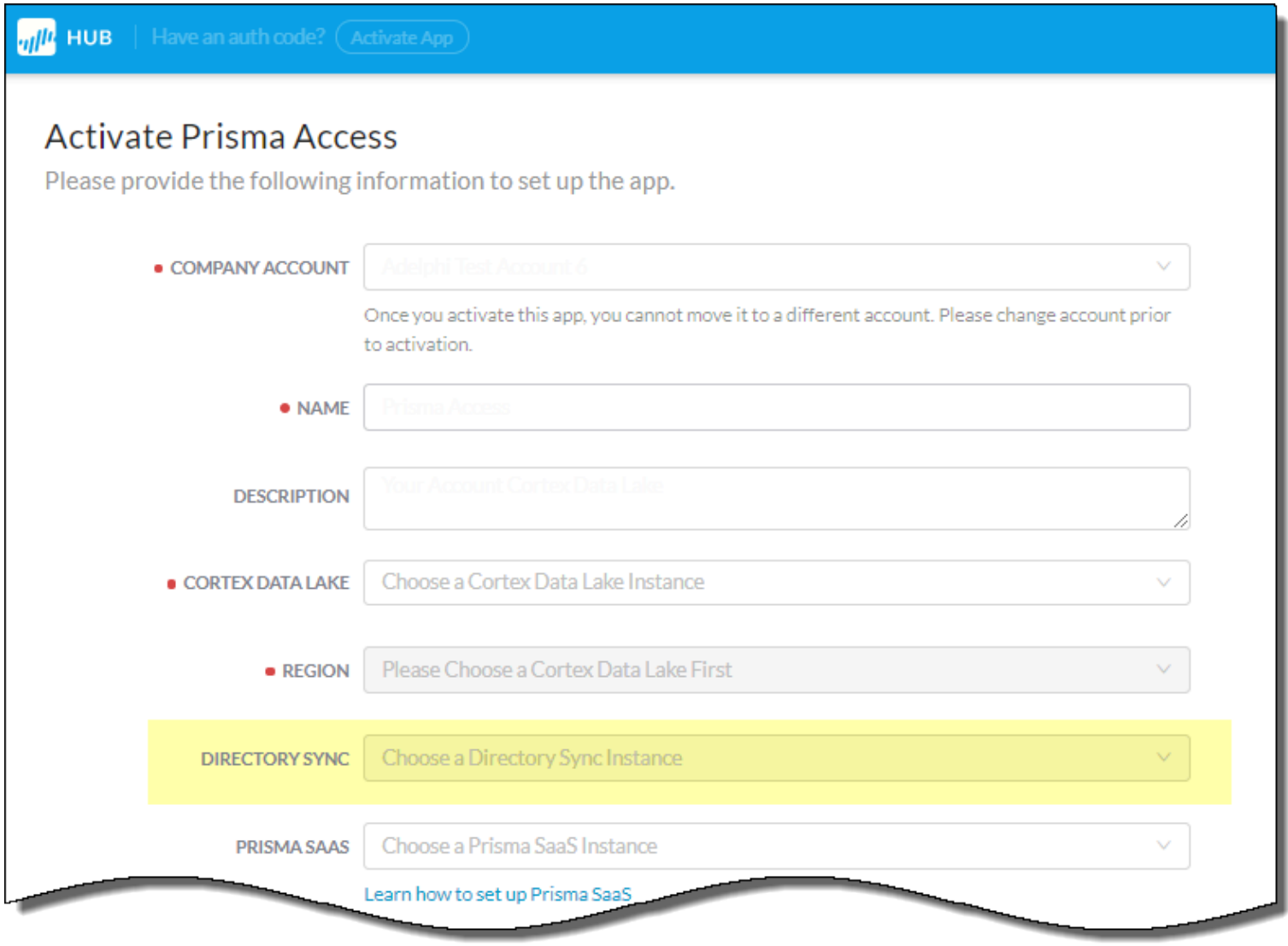
**STEP 2 |** Aktivieren Sie die Cloud Identity Engine für Prisma Access.

Sie können Prisma Access bei Ihrer ersten Prisma Access-Aktivierung oder zu einem beliebigen späteren Zeitpunkt mit der Cloud Identity Engine verknüpfen:

- **Während der Aktivierung von Prisma Access:** Wenn Sie von der Cloud verwaltetes Prisma Access zum ersten Mal aktivieren, können Sie eine Cloud Identity Engine-Instanz

 ©2025 Palo Alto Networks, Inc.

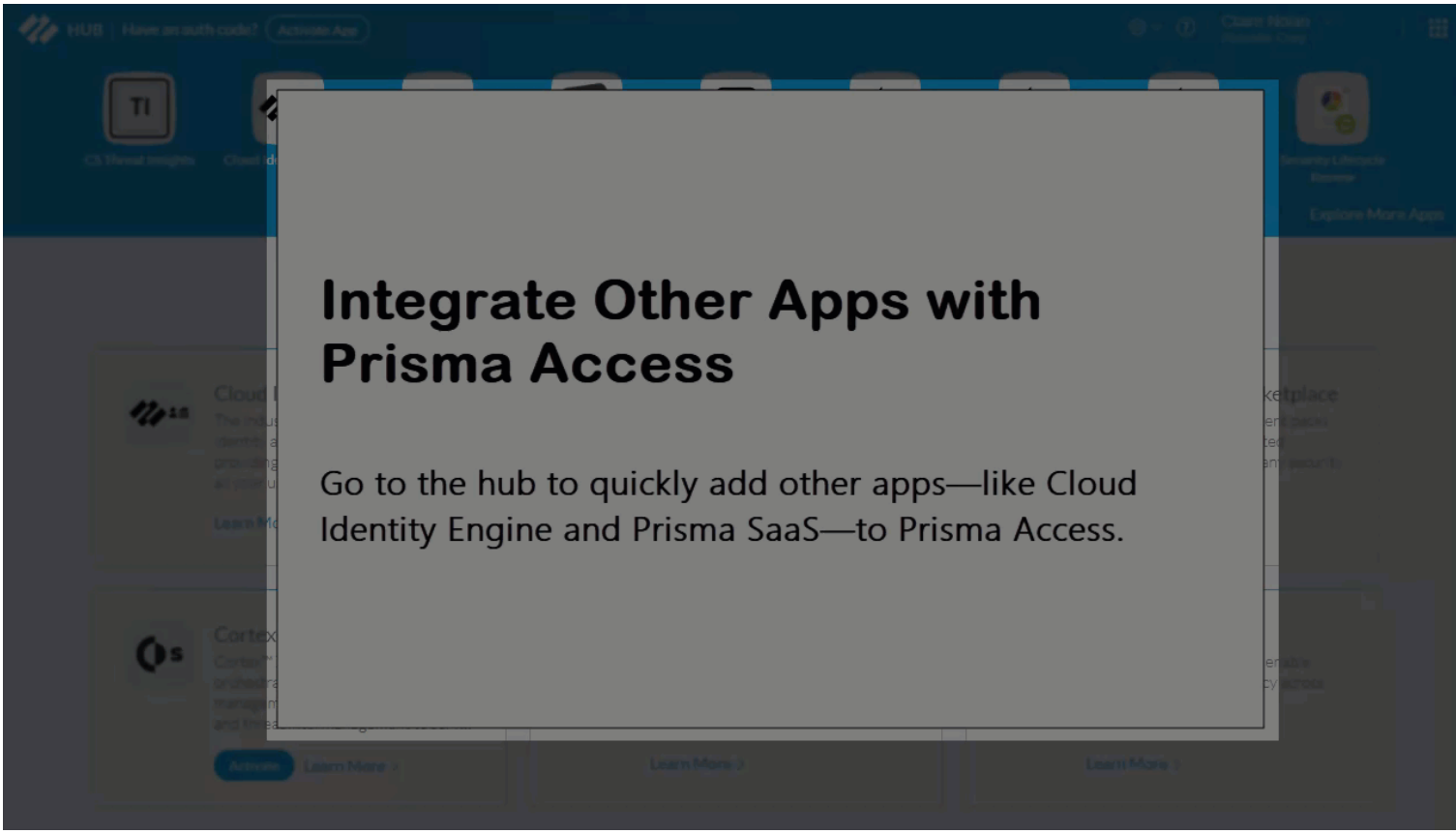
auswählen, die Prisma Access verwenden kann. Stellen Sie sicher, dass Sie eine Instanz auswählen, die in derselben Region wie Prisma Access bereitgestellt wird.




- **Nach der Aktivierung von Prisma Access:** Um die Cloud Identity Engine für eine vorhandene Prisma Access-Instanz zu aktivieren, melden Sie sich beim Hub an. Wählen Sie im Dropdown-Menü der Hub-Einstellungen (siehe Zahnrad in der oberen Menüleiste) die Option **Apps verwalten** aus. Suchen Sie die Prisma Access-Instanz, die Sie aktualisieren

 ©2025 Palo Alto Networks, Inc.

möchten, und wählen Sie die Cloud Identity Engine-Instanz aus, die Prisma Access verwenden soll.




**STEP 3 |** Stellen Sie sicher, dass Prisma Access mit der Cloud Identity Engine verbunden ist.

## Cloud Identity Engine in Prisma Access integrieren (Panorama)

Prisma Access ruft Benutzer- und Gruppeninformationen aus dem Cloud-Verzeichnis oder Active Directory (AD) Ihrer Organisation ab, um benutzer- und gruppenbasierte Richtlinien durchzusetzen. Optional ruft Prisma Access auf Benutzerverhalten basierende Risikosignale von einigen Cloud-Verzeichnisanbietern ab, z. B. Azure Active Directory, um automatisierte Sicherheitsaktionen durchzusetzen. Mit der Cloud Identity Engine können Sie das Abrufen von Benutzer- und Gruppeninformationen vereinfachen.

Die Integration der Cloud Identity Engine in Prisma Access vereinfacht nicht nur den Abruf von Benutzer- und Gruppeninformationen, sondern kann auch Bandbreite in Ihrem Cloud-Verzeichnis oder AD freisetzen und diese entlasten.

Sie können die Cloud Identity Engine verwenden, um Benutzer- und Gruppeninformationen für Prisma Access für mobile Benutzer und/oder Remote-Netzwerke abzurufen, indem Sie wie folgt vorgehen.

Die Integration der Cloud Identity Engine in Prisma Access hat folgende Implementierungseinschränkungen:

 ©2025 Palo Alto Networks, Inc.

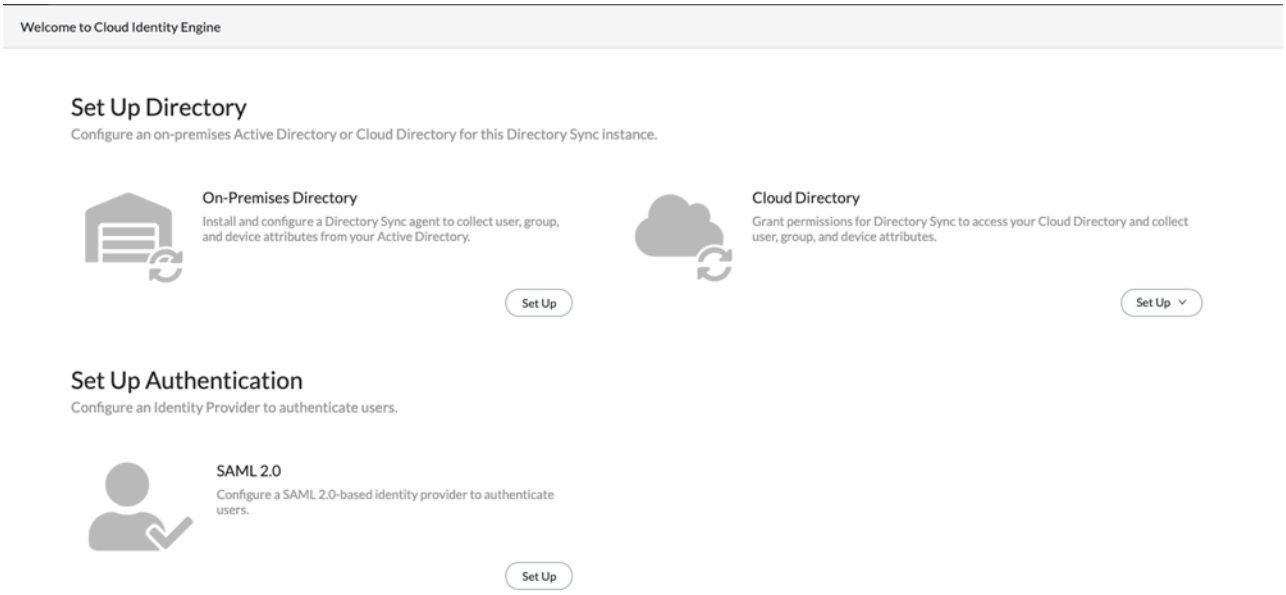
- Stellen Sie sicher, dass die Gruppen, die Sie mit der Cloud Identity Engine verwenden, keine der folgenden Sonderzeichen haben, da Prisma Access die Verwendung der folgenden Sonderzeichen in Gruppen nicht unterstützt und Commit-Vorgänge fehlschlagen:
  - " (doppelte Anführungszeichen)
  - ' (Apostroph)
  - < (Kleiner-als-Zeichen)
  - > (Größer-als-Zeichen)
  - & (Et-Zeichen)
- Wenn Sie die Cloud Identity Engine mit Prisma Access verknüpfen, müssen Ihre Benutzernamen das NetBIOS-Format verwenden, das die Domäne umfasst. Sie können Benutzernamen im E-Mail-Format (*Benutzername*@*Domäne*), im Format **NetBIOS \sAMAccountName** oder im User Principal Name(UPN)-Format (*Benutzername*@*Domäne*.com) angeben.
- Geben Sie Gruppennamen im **DistinguishedName(DN)**-Format ein (z. B. **CN=Users,CN=Builtin,DC=Example,DC=com**).
- Die Cloud Identity Engine wendet keine Einstellungen an, die Sie in der Gruppeneinschlussliste (**Gerät** > **Benutzeridentifikation** > **Einstellungen für die Gruppenzuordnung** > **Gruppeneinschlussliste**) angegeben haben; stattdessen werden Benutzer- und Gruppeninformationen aus Ihrer gesamten Konfiguration abgerufen, einschließlich Gruppen, die in allen Gerätegruppen und Vorlagen verwendet werden.

**STEP 1 |** Erstellen Sie eine Cloud Identity Engine-Instanz für Prisma Access und notieren Sie sich den Instanznamen.

Wenn Sie die Cloud Identity Engine aktivieren, erstellt sie eine Instanz. Sie verwenden den Instanznamen, wenn Sie die Cloud Identity Engine in einem späteren Schritt mit Prisma Access verknüpfen. Wenn Sie optional eine separate Instanz für Prisma Access erstellen müssen, erstellen Sie diese und notieren Sie sich den Instanznamen.

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Konfigurieren Sie die Cloud Identity Engine, um Ihre Verzeichnisdaten abzurufen.




**STEP 3 |** (Nur Bereitstellungen mit lokalem Active Directory) Wenn Sie ein lokales Active Directory verwenden, installieren und konfigurieren Sie den Cloud Identity Agent, um mit Ihrem lokalen AD zu kommunizieren und die gegenseitige Authentifizierung zwischen dem Cloud Identity Engine-Dienst und dem Agent zu konfigurieren.

**STEP 4 |** Aktivieren Sie die Cloud Identity Engine auf Prisma Access.

1. Wählen Sie in der Panorama-Instanz, die Prisma Access verwaltet, die Registerkarte mit den Einstellungen für die Zuordnung von Benutzernamen und Benutzergruppen aus.
   - Wählen Sie für eine Bereitstellung des Typs „Mobile Benutzer – GlobalProtect“ die Optionen **Panorama** > **Cloud Services** > **Konfiguration** > **Mobile Benutzer – GlobalProtect** aus, klicken Sie auf das Zahnradsymbol, um die Einstellungen zu bearbeiten, und wählen Sie dann **Einstellungen für die Gruppenzuordnung** aus.
   - Wählen Sie für eine Bereitstellung des Typs „Mobile Benutzer – Expliziter Proxy“ die Optionen **Panorama** > **Cloud Services** > **Konfiguration** > **Mobile Benutzer – Expliziter Proxy** aus, klicken Sie auf das Zahnradsymbol, um die Einstellungen zu bearbeiten, und wählen Sie dann **Einstellungen für die Gruppenzuordnung** aus.
   - Wählen Sie für eine Remote-Netzwerkbereitstellung die Optionen **Panorama** > **Cloud Services** > **Konfiguration** > **Remote-Netzwerke** aus, klicken Sie auf das Zahnradsymbol, um die Einstellungen zu bearbeiten, und wählen Sie dann **Einstellungen für die Gruppenzuordnung** aus.
2. Wählen Sie **Verzeichnissynchronisierung aktivieren** aus, um die Cloud Identity Engine mit Prisma Access zu aktivieren.
3. Geben Sie folgende Informationen ein:
   - Geben Sie den **Primären Benutzernamen** ein. Dieses Feld ist erforderlich

     Das Attribut **Primärer Benutzername** steuert die Formatierung, die in Protokollen und Berichten verwendet wird. Wenn das Attribut „Primärer Benutzername“ den Wert **userPrincipalName** (UPN) aufweist, wird in allen Protokoll- und Berichtseinträgen

 ©2025 Palo Alto Networks, Inc.

der Quellbenutzer in diesem Format angezeigt. Viele Bereitstellungen verwenden entweder das Format UPN, **sAMAccountName** oder **mail**. Wenn Ihre Organisation ein anderes Attribut verwendet, können Sie es hier angeben, um die Konsistenz für die Protokollierung und Berichterstattung in Ihrer gesamten Organisation sicherzustellen.

Wenn Sie Azure AD oder Okta Directory als Identitätsanbieter (IdP) in der Cloud Identity Engine konfigurieren, geben Sie den **Primären Benutzernamen** als **userPrincipalName** an. Prisma Access unterstützt das Attribut „userPrincipalName (UPN)“, das mit Azure AD und Okta Directory verwendet wird.

- (Optional) Geben Sie das **E-Mail**-Attribut ein (z. B. **mail**).
- (Optional) Wenn Sie alternative Namensattribute für den Benutzer verwenden, geben Sie diese ein. Sie können bis zu drei alternative Benutzernamen eingeben (**Alternativer Benutzername 1**, **Alternativer Benutzername 2** und **Alternativer Benutzername 3**).

4. Klicken Sie abschließend auf **OK**.

**STEP 5 |** Führen Sie einen Commit durch und übertragen Sie Ihre Änderungen per Push (**Commit** > **Commit und Push**).

 ©2025 Palo Alto Networks, Inc.

# Abrufen von Benutzer-ID-Gruppenzuordnungen für Prisma Access

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Panorama)<br>• Cloud Identity Engine | • Prisma Access-Lizenz |

Nachdem Sie die Benutzer-ID-Zuordnung in Prisma Access konfiguriert haben, müssen Sie die Informationen zur aktuellen Zuordnung von Benutzernamen zu Benutzergruppen für mobile Benutzer und Benutzer in Remote-Netzwerken abrufen können. Beim Konfigurieren der Gruppenzuordnung in der Cloud Identity Engine wird zwar eine Zuordnung von Benutzernamen zu Benutzergruppen durchgeführt, diese Benutzergruppen können in Sicherheitsrichtlinienregeln jedoch nicht ausgewählt werden. Sie können die Gruppen ausfüllen, damit diese in Dropdown-Listen für Sicherheitsrichtlinienregeln ausgewählt werden können. Hierzu können Sie entweder eine Firewall der nächsten Generation als Mastergerät konfigurieren oder die Cloud Identity Engine konfigurieren.

- Cloud Identity Engine
- Mastergerät
- Einträge mit der Langform ausgewählter Namen

## Cloud Identity Engine

Sie können die Cloud Identity Engine nicht nur zum Abrufen von Benutzer- und Gruppeninformationen verwenden, sondern auch, um Namen von Benutzergruppen in Sicherheitsrichtlinienregeln auszufüllen. Durch diese Integration muss zu diesem Zweck keine lokale Firewall oder Firewall der nächsten Generation der VM-Serie als Mastergerät mehr konfiguriert werden. Mastergeräte werden jedoch weiterhin unterstützt.

Sie können die Cloud Identity Engine auch zum Ausfüllen von Gruppennamen in von Panorama verwalteten Bereitstellungen mit mehreren Mandanten verwenden. Dies ist bei Verwendung eines Mastergeräts nicht möglich.

Führen Sie die folgenden Schritte aus, damit die Cloud Identity Engine Gruppennamen in Sicherheitsrichtlinienregeln ausfüllen kann.

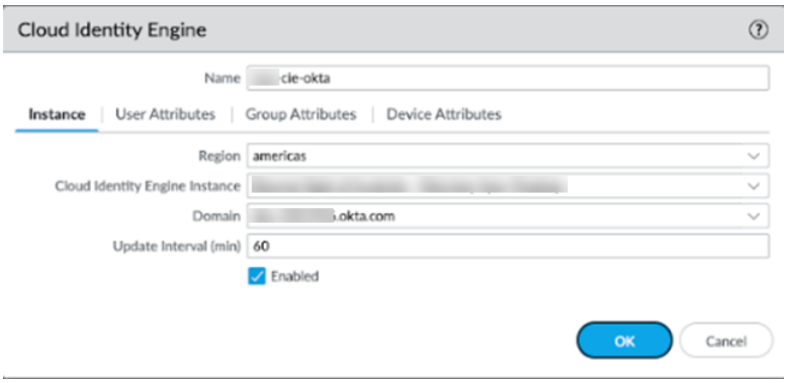
**STEP 1 |** Aktivieren Sie in der Cloud Identity Engine die Cloud Identity Engine und fügen Sie, sofern nicht bereits geschehen, ein lokales oder cloudbasiertes Verzeichnis hinzu.

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Konfigurieren Sie die Cloud Identity Engine als Zuordnungsquelle.

1. Wählen Sie im Panorama, das Prisma Access verwaltet, **Panorama** > **Benutzeridentifikation** > **Cloud Identity Engine** aus und **fügen Sie ein Profil hinzu**.
2. Geben Sie für die **Instanz** folgende Parameter an:
   - **Region** – Wählen Sie den regionalen Endpunkt für Ihren Mandanten aus.

     *Die Region, die Sie auswählen, muss mit der Region übereinstimmen, die Sie bei der Aktivierung Ihres Cloud Identity Engine-Mandanten ausgewählt haben.*
   - **Cloud Identity Engine-Instanz** – Wählen Sie die Cloud Identity Engine-Instanz aus, die dem Profil zugeordnet werden soll.
   - **Domäne** – Wählen Sie die Domäne aus, die die zu verwendenden Verzeichnisse enthält.
   - **Aktualisierungsintervall (Min.)** – Geben Sie die Anzahl der Minuten ein, die Panorama zwischen Aktualisierungen von der Cloud Identity Engine-App auf Panorama warten soll (auch als Aktualisierungsintervall bezeichnet). Die Standardeinstellung beträgt 60 Minuten und die Reichweite 5–1.440.
3. Überprüfen Sie, ob das Profil **aktiviert** ist.

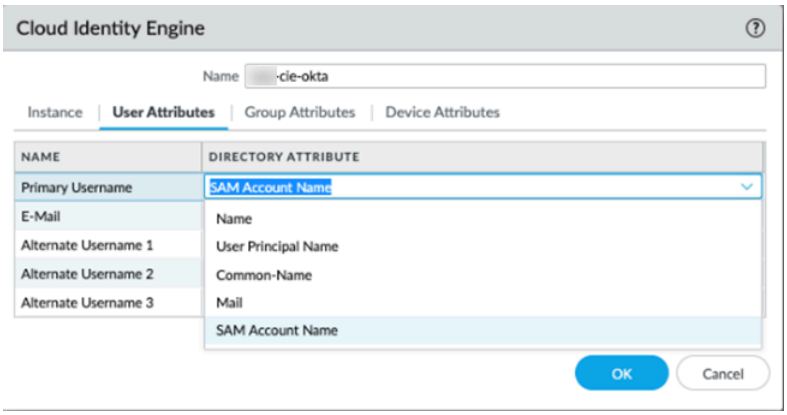



4. Wählen Sie bei den **Benutzerattributen** das Format für den **primären Benutzernamen** aus. Sie können optional die Formate für die E-Mail und einen alternativen Benutzernamen auswählen. Sie können bis zu drei alternative Benutzernamenformate

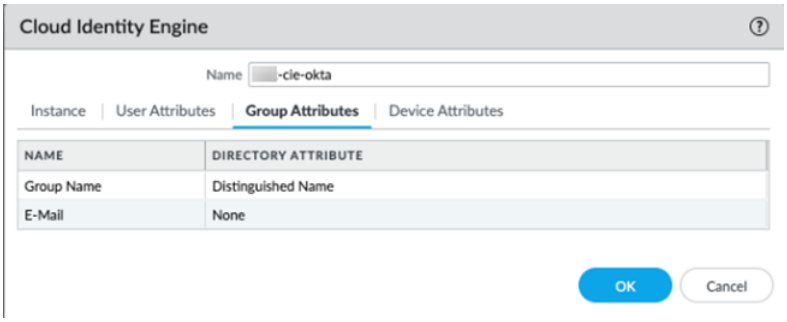
 ©2025 Palo Alto Networks, Inc.

konfigurieren, wenn sich Ihre Benutzer mit mehreren Benutzernamenformaten anmelden.

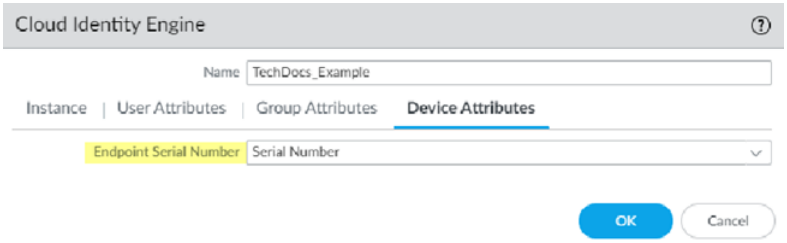
Wenn Sie Benutzer in Sicherheitsrichtlinienregeln anzeigen, wird der Benutzername in dem primären Benutzernamenformat angezeigt, das Sie hier auswählen.




5. Wählen Sie bei den **Gruppenattributen** das Format für den **Gruppennamen** aus.




6. Belassen Sie die **Geräteattribute** in der Einstellung **Keine**.

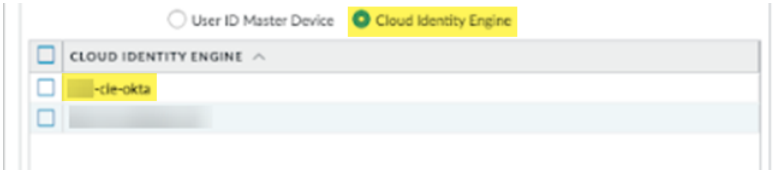



7. Klicken Sie auf **OK** und dann auf **Commit und Push**.

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Verbinden Sie Ihr Profil mit Ihrer Prisma Access-Konfiguration.

1. Gehen Sie zu den Einstellungen für die Bereitstellung, die Sie hinzufügen.
   - Wählen Sie bei einer GlobalProtect-Bereitstellung für mobile Benutzer **Panorama** > **Cloud Services** > **Konfiguration** > **Mobile Benutzer – GlobalProtect** aus und klicken Sie auf das Zahnrad, um die **Einstellungen** zu bearbeiten.
   - Wählen Sie bei einer Bereitstellung für mobile Benutzer mit explizitem Proxy **Panorama** > **Cloud Services** > **Konfiguration** > **Mobile Benutzer – Expliziter Proxy** aus und klicken Sie auf das Zahnrad, um die **Einstellungen** zu bearbeiten.
   - Wählen Sie bei einer Remote-Netzwerkbereitstellung für mobile Benutzer **Panorama** > **Cloud Services** > **Konfiguration** > **Mobile Benutzer – Remote-Netzwerke** aus und klicken Sie auf das Zahnrad, um die **Einstellungen** zu bearbeiten.
2. Wählen Sie **Cloud Identity Engine** aus.
3. Wählen Sie das von Ihnen erstellte Profil der Cloud Identity Engine aus.



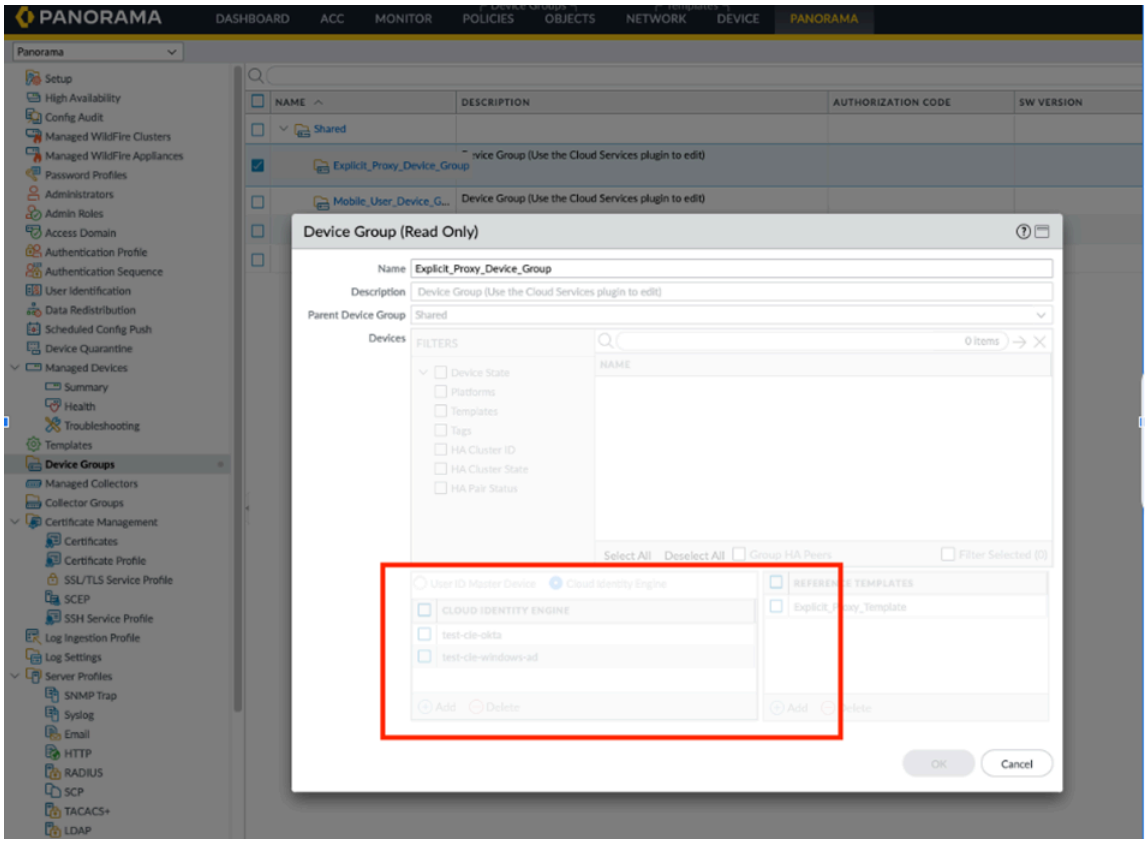

**STEP 4 |** Wählen Sie **Commit** > **Commit in Panorama** aus, um ein **Commit** für Ihre Änderungen durchzuführen.

 ©2025 Palo Alto Networks, Inc.

**STEP 5 |** Stellen Sie sicher, dass Prisma Access über die Zuordnungsinformationen der Cloud Identity Engine verfügt.

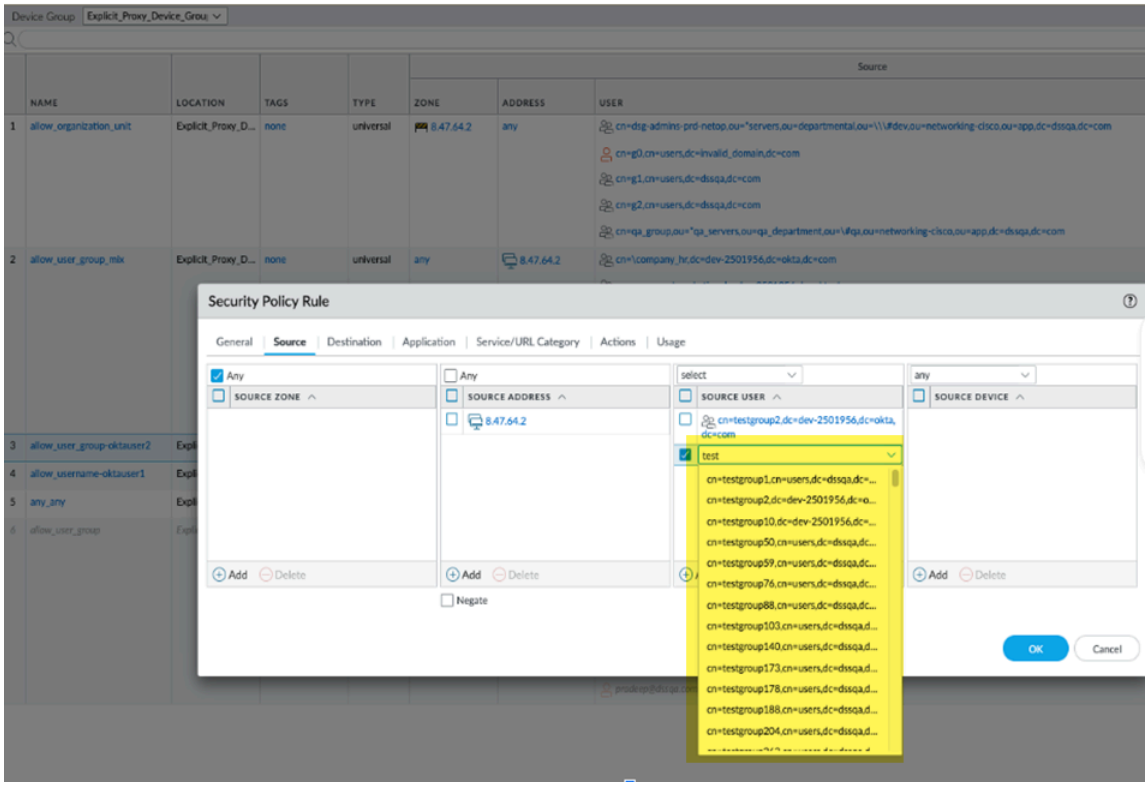
1. Wählen Sie **Panorama** > **Gerätegruppen** > ***<template-name>*** aus, wobei *<template-name>* die Vorlage für die von Ihnen konfigurierte Bereitstellung ist, und überprüfen Sie, ob das Profil der Cloud Identity Engine an die Gerätegruppe angehängt ist.

   Das folgende Beispiel zeigt, dass die Gerätegruppe erfolgreich an die Vorlage „Explicit_Proxy_Device_Group“ angehängt wurde.




2. Wählen Sie **Objekte** > **Sicherheit** > **Vor-Regeln** aus. Anschließend können Sie eine Sicherheitsrichtlinienregel **hinzufügen** und überprüfen, ob die Gruppen im Benutzerbereich ausgefüllt wurden.

 ©2025 Palo Alto Networks, Inc.




## Mastergerät

Beim Konfigurieren der Gruppenzuordnung in der Cloud Identity Engine wird eine Zuordnung von Benutzernamen zu Benutzergruppen durchgeführt. Diese Benutzernamen und Benutzergruppen werden jedoch nicht in die Sicherheitsrichtlinien übernommen. Für eine einfachere Erstellung oder Änderung von benutzer- und gruppenbasierten Richtlinien können Sie ein Mastergerät verwenden, um die Gruppennamen zu Dropdown-Listen in Sicherheitsrichtlinienregeln hinzuzufügen. Sie müssen für jede Gerätegruppe eine Firewall als Mastergerät festlegen. Nachdem Sie ein Mastergerät hinzugefügt haben, übernimmt die Gerätegruppe alle auf dem Mastergerät definierten Richtlinien. Aus diesem Grund sollte für diese Gerätegruppe ein eigenständiges, dediziertes Gerät verwendet werden.

Palo Alto Networks empfiehlt, für jede Gerätegruppe ein **Mastergerät** festzulegen, um die Auswahl von Gruppennamen aus Dropdown-Listen in Sicherheitsrichtlinien zu ermöglichen. Sie können entweder eine lokale Firewall oder eine Firewall der VM-Serie als Mastergerät konfigurieren.

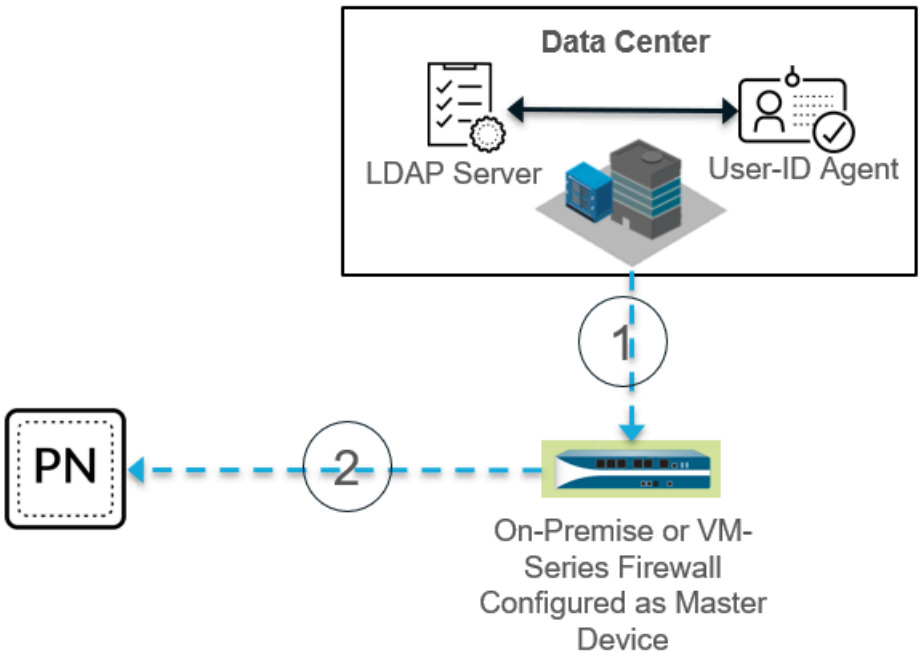
Die folgende Abbildung zeigt eine Benutzer-ID-Bereitstellung, bei der der Administrator ein lokales Gerät als **Mastergerät**konfiguriert hat. Die Beschriftungen in der Abbildung veranschaulichen den Vorgang.

1. Eine lokale Firewall der nächsten Generation oder eine Firewall der VM-Serie, die der Administrator als Mastergerät konfiguriert hat, ruft die neueste Zuordnung von Benutzernamen zu Benutzergruppen vom LDAP-Server und dem Benutzer-ID-Agenten im Rechenzentrum ab.

 ©2025 Palo Alto Networks, Inc.

2. Panorama erhält die Zuordnung von Benutzernamen zu Benutzergruppen vom Mastergerät.

   Panorama verwendet diese Zuordnung nur zum Auffüllen der Gruppennamen in Dropdown-Listen in Sicherheitsrichtlinien und vereinfacht so die Erstellung von Richtlinien auf Basis von Gruppen.




## Lokale Firewall oder Firewall der VM-Serie als Mastergerät konfigurieren

Gehen Sie wie folgt vor, um eine lokale Firewall oder eine Firewall der VM-Serie als Mastergerät zu konfigurieren.

*Sie können nur ein Mastergerät pro Gerätegruppe verwenden. Wenn Sie ein Mastergerät für verschiedene Gerätegruppen konfigurieren müssen, müssen Sie für jede Gerätegruppe ein separates Mastergerät erstellen.*

**STEP 1 |** Stellen Sie sicher, dass das Gerät, das Sie als Mastergerät verwenden möchten, von demselben Panorama verwaltet wird, das auch Prisma Access verwaltet.

Sie können Ihre verwalteten Geräte unter **Panorama** > **Verwaltete Geräte** überprüfen.

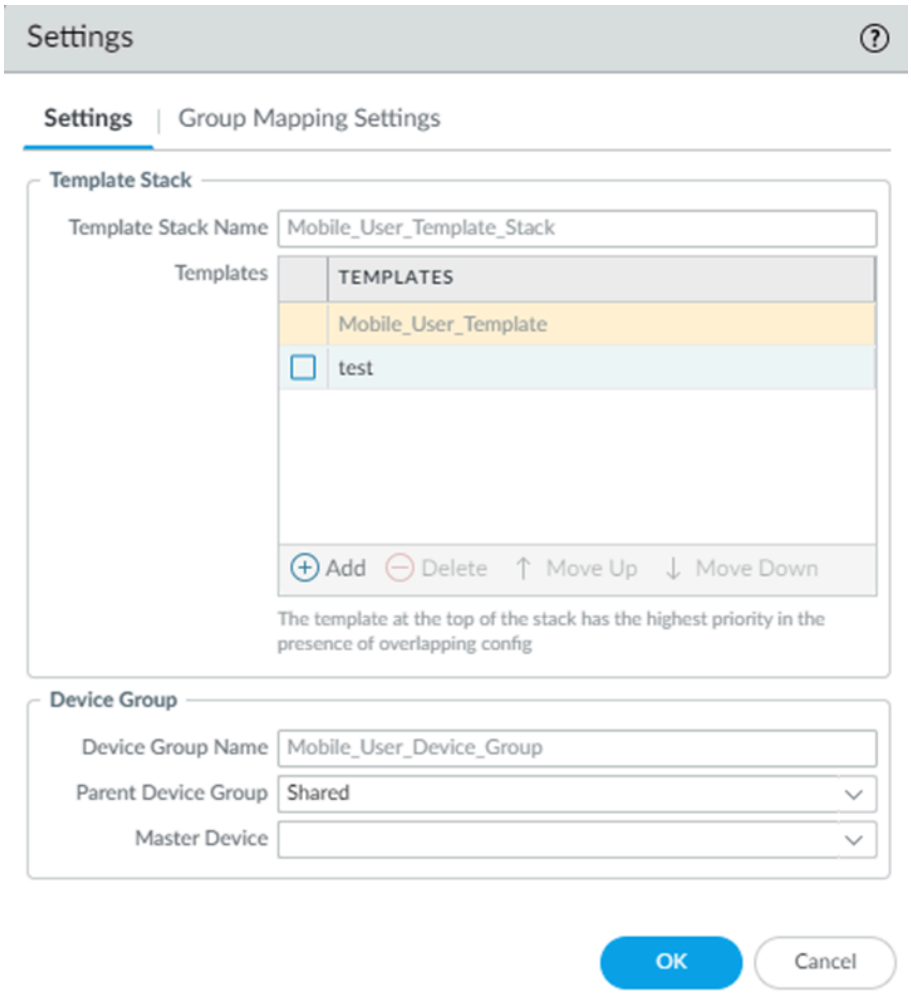
**STEP 2 |** Fügen Sie das Mastergerät zu Ihrer Bereitstellung für mobile Benutzer oder Ihrer Remote-Netzwerkbereitstellung von Prisma Access hinzu.

- Wählen Sie bei einer GlobalProtect-Bereitstellung für mobile Benutzer **Panorama** > **Cloud Services** > **Konfiguration** > **Mobile Benutzer – GlobalProtect** aus, klicken Sie bei den

 ©2025 Palo Alto Networks, Inc.

**Einstellungen** auf das Zahnradsymbol und wählen Sie anschließend die lokale Firewall aus, die als **Mastergerät** angegeben werden soll.

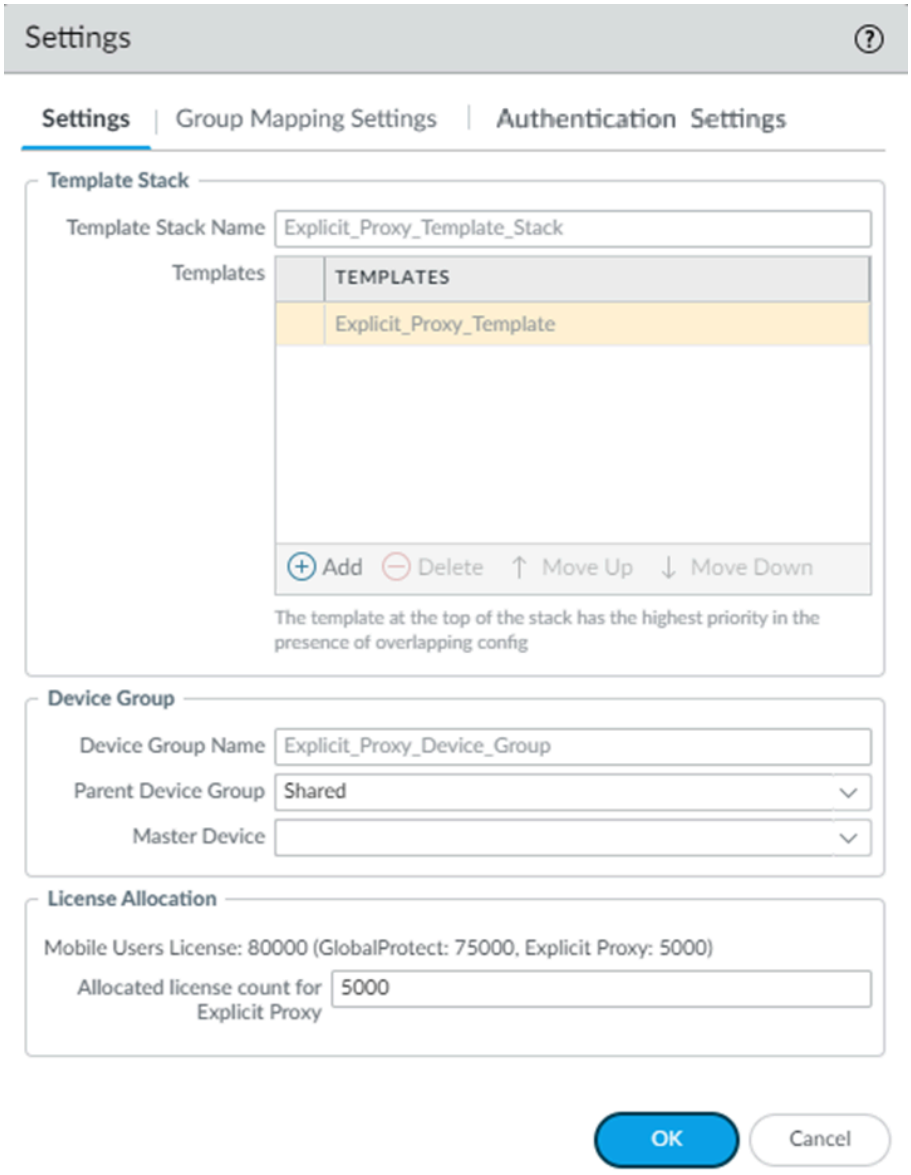
*Wenn Sie den standardmäßigen **Gerätegruppennamen** (in diesem Fall **Mobile_User_Device_Group**) und die **übergeordnete Gerätegruppe** (in diesem Fall **Freigegeben**) verwenden, werden in der Dropdown-Liste alle Geräte angezeigt, die keiner anderen Gerätegruppe zugeordnet sind. Wenn Sie das Mastergerät einer anderen Gerätegruppe zugeordnet haben, wählen Sie die mit dieser Gerätegruppe verknüpfte **übergeordnete Gerätegruppe** aus, damit sie in der Dropdown-Liste angezeigt wird.*




- Wählen Sie bei einer Bereitstellung mit explizitem Proxy für mobile Benutzer **Panorama** > **Cloud Services** > **Konfiguration** > **Mobile Benutzer – Expliziter Proxy**aus, klicken Sie

 ©2025 Palo Alto Networks, Inc.

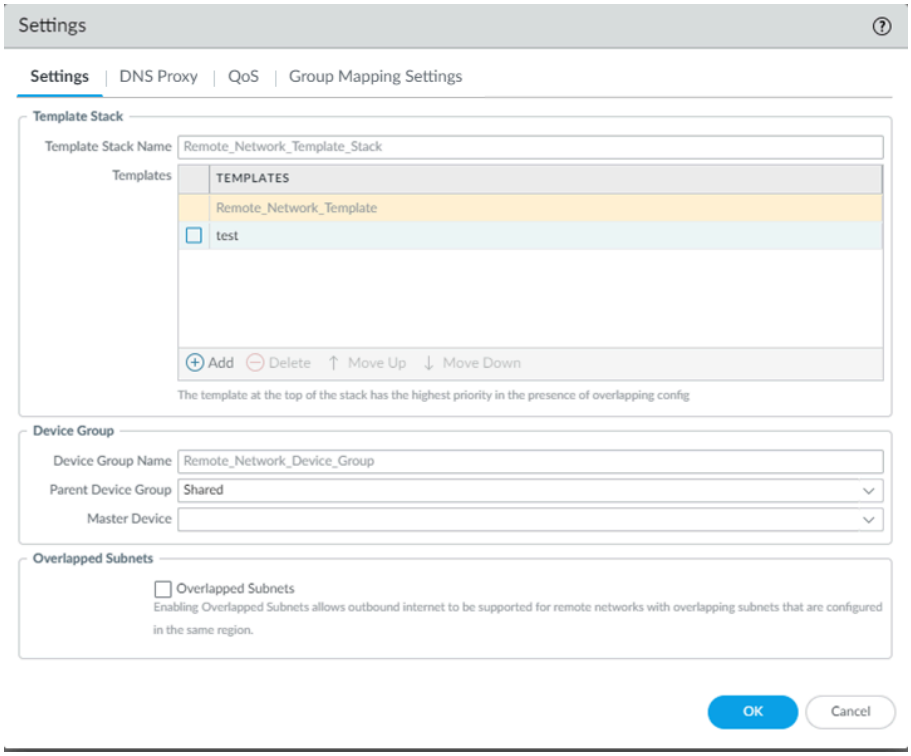
bei den **Einstellungen** auf das Zahnradsymbol und wählen Sie anschließend das von Ihnen erstellte **Mastergerät** aus.




- Wählen Sie bei Remote-Netzwerkbereitstellungen, der Gerätegruppe mit einer Remote-Netzwerkverbindung, **Panorama** > **Cloud Services** > **Konfiguration** > **Remote-**

 ©2025 Palo Alto Networks, Inc.

**Netzwerke**aus, klicken Sie bei den **Einstellungen** auf das Zahnradsymbol und wählen Sie das von Ihnen erstellte **Mastergerät** aus.




*Prisma Access füllt automatisch die Zuordnung von Benutzernamen zu Benutzergruppen für die Gerätegruppe aus, die nur mit dem Mastergerät verknüpft ist. In diesem Beispiel würde die automatische Auffüllung nur in der Gerätegruppe* ***Remote_Network_Device_Group*** *erfolgen und in keiner anderen Gerätegruppe.*

**STEP 3 |** Klicken Sie auf **OK**.

## Einträge mit der Langform ausgewählter Namen

Wenn weder eine Firewall der nächsten Generation als Mastergerät noch eine Cloud Identity Engine konfiguriert ist, um Sicherheitsrichtlinienregeln mit Benutzer und Gruppen auszufüllen, können Sie stattdessen in Panorama Einträge mit der Langform ausgewählter Namen verwenden. Prisma Access verwendet die Einträge ausgewählter Namen, um die in Panorama konfigurierten und auf der Benutzer-ID basierenden Richtlinien auszuwerten.

Wenn beispielsweise ein Benutzer mit dem Namen **Bob Alice** in der IT arbeitet und sich im ersten Stock befindet, kann eine übereinstimmende Sicherheitsrichtlinie `cn=first_floor, ou=it_staff, dc=dev, dc=example, dc=com` umfassen, wenn die Richtlinie auf alle IT-Mitarbeiter im ersten Stock angewendet werden soll, oder `cn=Bob Alice, ou=it_staff, dc=dev, dc=example, dc=com`, wenn die Richtlinie nur auf Bob Alice angewendet werden soll.

 ©2025 Palo Alto Networks, Inc.

# Identitätsweitergabe

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

Damit Sie Ihre Sicherheitsrichtlinien konsistent durchsetzen können, gibt Prisma Access Identitätsdaten, die GlobalProtect lokal in Ihrer gesamten Prisma Access-Umgebung entdeckt, frei. Prisma Access kann Identitätsdaten auch für lokale Geräte an Remote-Netzwerkstandorten oder Dienstverbindungsstandorten (Zentrale und Rechenzentren) freigeben.

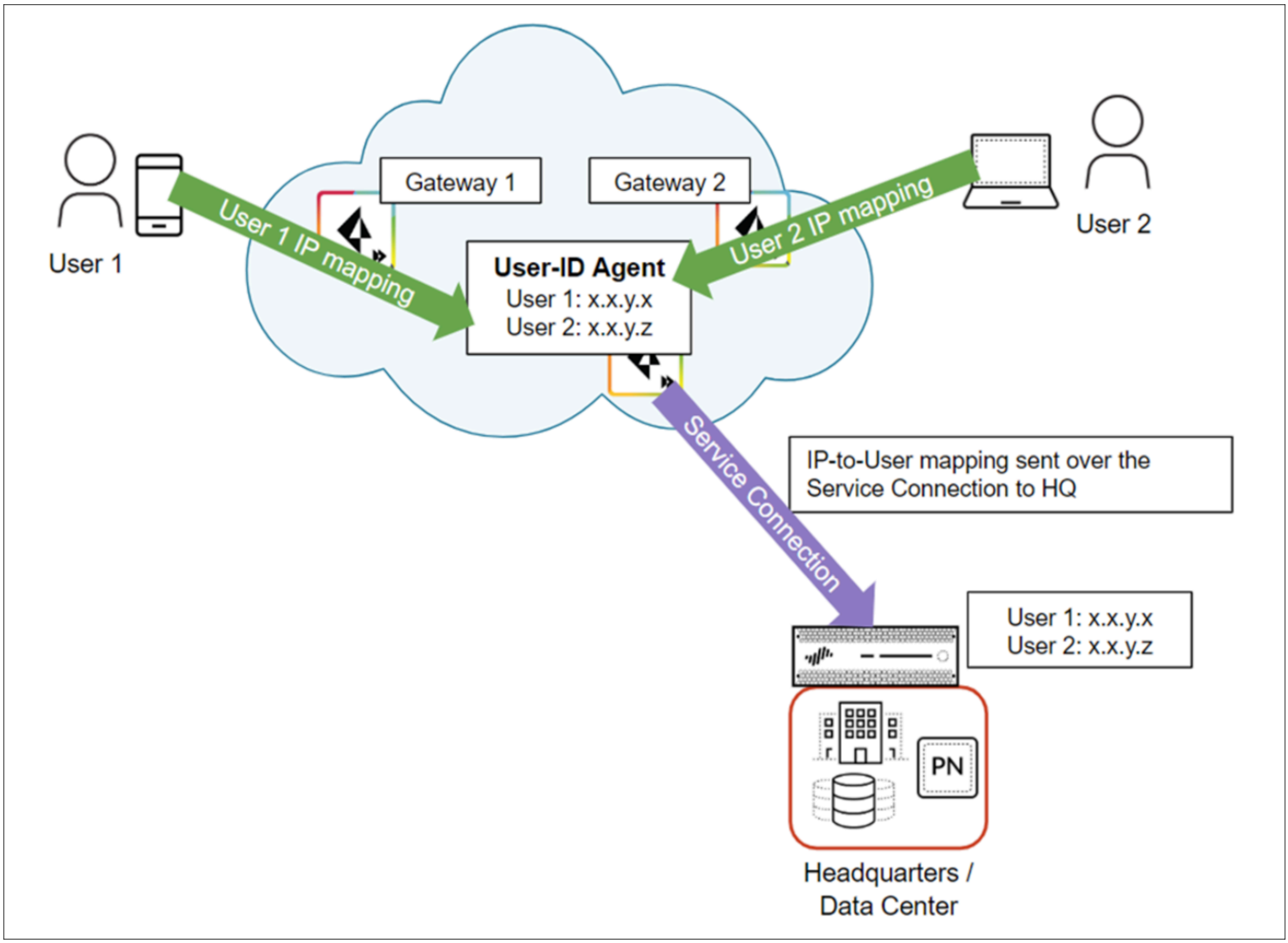
Damit mobile Benutzer auf eine Ressource an einem Remote-Netzwerkstandort oder am Standort einer Zentrale/eines Rechenzentrums zugreifen können, der durch ein Gerät mit benutzerbasierten Richtlinien gesichert ist, müssen Sie die Identitätsdaten der mobilen Prisma Access-Benutzer und der Remote-Netzwerk-Benutzer an dieses lokale Gerät weitergeben.

Wenn die Benutzer eine Verbindung mit Prisma Access herstellen, erfasst Prisma Access die Identitätsdaten der Benutzer und speichert diese.

Im folgenden Beispiel sind zwei mobile Benutzer dargestellt, für die eine Zuordnung von IP-Adresse und Benutzername in Prisma Access vorhanden ist. Prisma Access übernimmt dann die Umverteilung dieser Zuordnung über eine Dienstverbindung an die lokalen Geräte, die die Zentrale bzw. das Rechenzentrum sichern.

Prisma Access (Managed by Strata Cloud Manager) ermöglicht die automatische Aktivierung von Dienstverbindungen als Agents für die Identitätsweitergabe (auch als „User-ID-Agents“ bezeichnet).

 ©2025 Palo Alto Networks, Inc.




- Strata Cloud Manager
- Panorama

## Identitätsweitergabe (Strata Cloud Manager)

Damit Sie Ihre Sicherheitsrichtlinien konsistent durchsetzen können, gibt Prisma Access Identitätsdaten, die GlobalProtect lokal in Ihrer gesamten Prisma Access-Umgebung entdeckt, frei. Prisma Access kann Identitätsdaten auch für lokale Geräte an Remote-Netzwerkstandorten oder Dienstverbindungsstandorten (Zentrale und Rechenzentren) freigeben.

Für Prisma Access (Managed by Strata Cloud Manager) haben wir standardmäßig einige Weitergaben von Identitätsdaten aktiviert – und für die übrigen Daten haben wir die Konfiguration zur Aktivierung der Weitergabe sehr einfach gemacht (wählen Sie einfach ein Kontrollkästchen aus, um auszuwählen, welche Daten Sie teilen möchten).

Im Dashboard „Identitätsweitergabe“ können Sie sehen, wie Identitätsdaten gemeinsam genutzt werden, und die Datenweitergabe verwalten (**Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Identitätsdienste**).

 ©2025 Palo Alto Networks, Inc.

Zu den Identitätsdaten, die Sie weitergeben können, gehören:

- HIP-Daten
- IP-Adresse-zu-Tag-Zuordnungen
- IP-Adresse-zu-Benutzer-Zuordnungen
- Benutzer-zu-Tag-Zuordnungen
- Geräte in Quarantäne

Erste Schritte mit der Identitätsweitergabe:

- Einrichten der Identitätsweitergabe
- Identifizieren und Isolieren kompromittierter Geräte

## Einrichten der Identitätsweitergabe

**Einrichten der Identitätsweitergabe**

1. Bestätigen Sie die Einrichtung Ihrer Dienstverbindung.

   Wenn Sie noch keine Dienstverbindung für Ihren Hauptsitz oder Ihre Rechenzentren eingerichtet haben, konfigurieren Sie zunächst eine Dienstverbindung. Eine Dienstverbindung ist erforderlich, damit Prisma Access Identitätsdaten in Ihrer gesamten Umgebung austauschen kann. Prisma Access ermöglicht automatisch, dass Dienstverbindungen als Weitergabe-Agents fungieren. Ein neu erstellter Dienstverbindungsstandort kann als Weitergabe-Agent verwendet werden, wenn Sie sehen, dass ihm eine Benutzer-ID-Agent-Adresse zugewiesen wurde (Prisma Access macht dies automatisch, es dauert nur ein paar Minuten).

   > ***Verwaltung der Umverteilung von Benutzer-IDs*** *– Manchmal sind detaillierte Kontrollen für die Umverteilung von Benutzer-IDs bei besonders umfangreichen Prisma Access-Bereitstellungen erforderlich. Mithilfe der Verwaltung der Umverteilung von Benutzer-IDs können Sie das standardmäßige Identitätsweitergabeverhalten für bestimmte Dienstverbindungen manuell deaktivieren, indem Sie das Häkchen in der Spalte* ***Benutzer-ID*** *entfernen und dann bestimmte Dienstverbindungen auswählen, die für die Identitätsweitergabe verwendet werden sollen. Für die meisten Konfigurationen ist dieser Arbeitsschritt nicht erforderlich. Wenden Sie sich an den Support von Palo Alto Networks, um diese Funktionalität zu aktivieren.*

   Gehen Sie zu **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Identitätsdienste** > **Identitätsweitergabe** und legen Sie den Konfigurationsumfang auf **Dienstverbindungen** fest, um die Details des Benutzer-ID-Agents für die Dienstverbindung zu überprüfen.

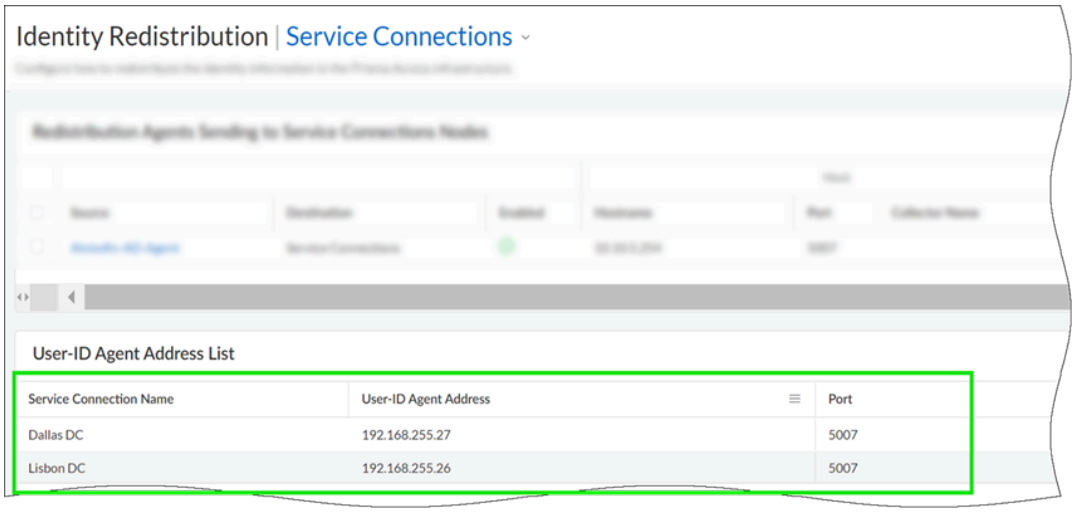
 ©2025 Palo Alto Networks, Inc.

- Senden Sie Identitätsdaten von Prisma Access an lokale -Geräte.

  Die Benutzer-ID-Agent-Informationen der Dienstverbindung sind alles, was Sie benötigen, um Prisma Access so zu konfigurieren, dass Identitätsdaten an lokale Geräte weitergegeben werden.

  Gehen Sie zu **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Identitätsdienste** > **Identitätsweitergabe** und legen Sie den Konfigurationsumfang auf **Dienstverbindungen** fest, um die Details des Benutzer-ID-Agents für die Dienstverbindung abzurufen.

  Verwenden Sie diese Angaben zur Konfiguration von Prisma Access als Datenweitergabe-Agent auf Panorama oder einer NGFW von Palo Alto Networks.

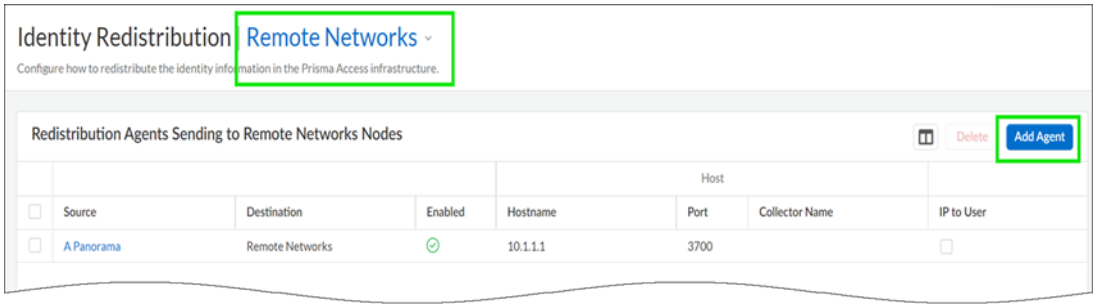



- Senden Sie Identitätsdaten von lokalen Geräten an Prisma Access.

  Fügen Sie lokale Geräte als Weitergabe-Agents zu Prisma Access hinzu. Die Geräte, die Sie hinzufügen, können Identitätsdaten an Prisma Access weitergeben.

  - **Über Geräte an Remote-Netzwerkstandorten:**

    Gehen Sie zum Dashboard zur **Identitätsweitergabe**, legen Sie den Konfigurationsumfang auf **Remote-Netzwerke** fest und wählen Sie **Agent hinzufügen** aus. Wählen Sie zusätzlich zur Angabe der Hostdetails den Datentyp aus, den das Gerät mit Prisma Access teilt. Zu den optionalen Einstellungen gehören der Name und ein Pre-Shared Key für das Gerät.

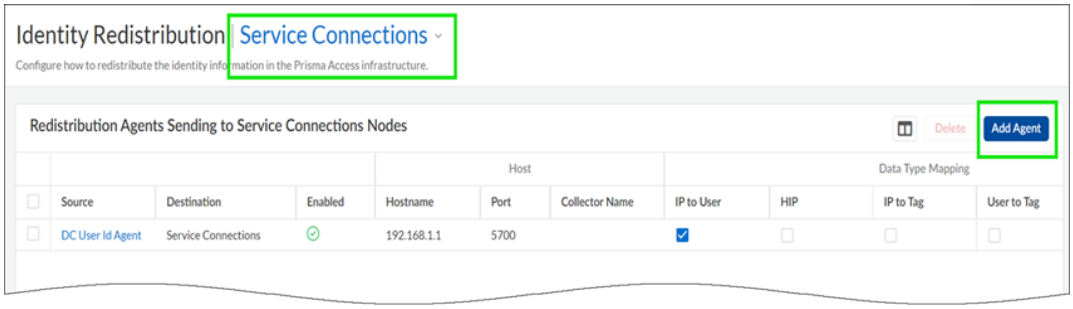



  - **Über Geräte an Dienstverbindungsstandorten:**

    Gehen Sie zum Dashboard für **Identitätsweitergabe**, legen Sie den Konfigurationsumfang auf **Dienstverbindungen** fest und wählen Sie **Agent hinzufügen** aus. Wählen Sie zusätzlich

 ©2025 Palo Alto Networks, Inc.

zur Angabe der Hostdetails den Datentyp aus, den das Gerät mit Prisma Access teilt. Zu den optionalen Einstellungen gehören der Name und ein Pre-Shared Key für das Gerät.

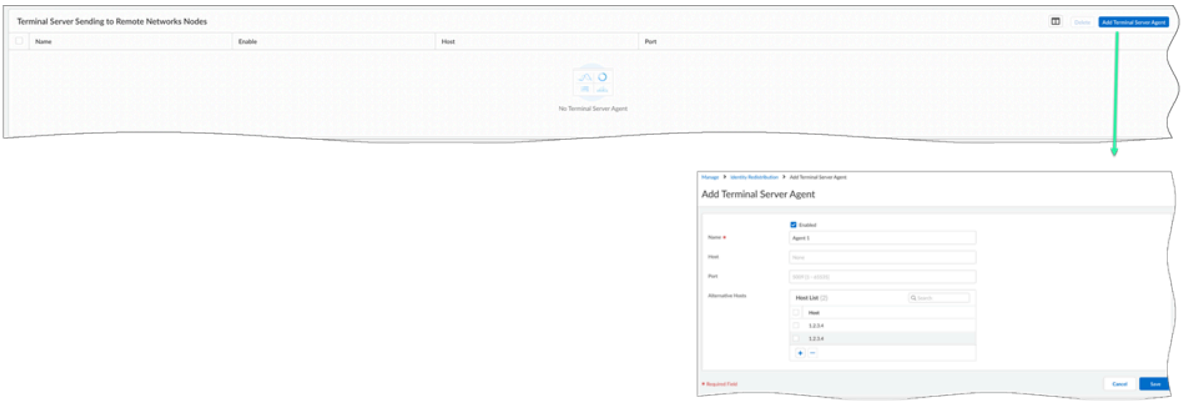



- Konfigurieren Sie den Terminalserver-Agent für die Benutzerzuordnung.

  Der Terminalserver-Agent (oder „TS-Agent“) weist jedem Benutzer einen Portbereich zu, um bestimmte Benutzer auf Windows-basierten Terminalservern zu identifizieren. Der TS-Agent benachrichtigt Prisma Access über die zugewiesenen Portbereiche, sodass Prisma Access Richtlinien auf der Grundlage von Benutzern und Benutzergruppen durchsetzen kann.

  Stellen Sie im Dashboard zur **Identitätsweitergabe** den Konfigurationsumfang auf **Remote-Netzwerke** ein und nutzen Sie **Terminalserver-Agent hinzufügen**, um unter **Terminalserver, die an Remote-Netzwerk-Knoten senden** einen TS-Agent hinzuzufügen.

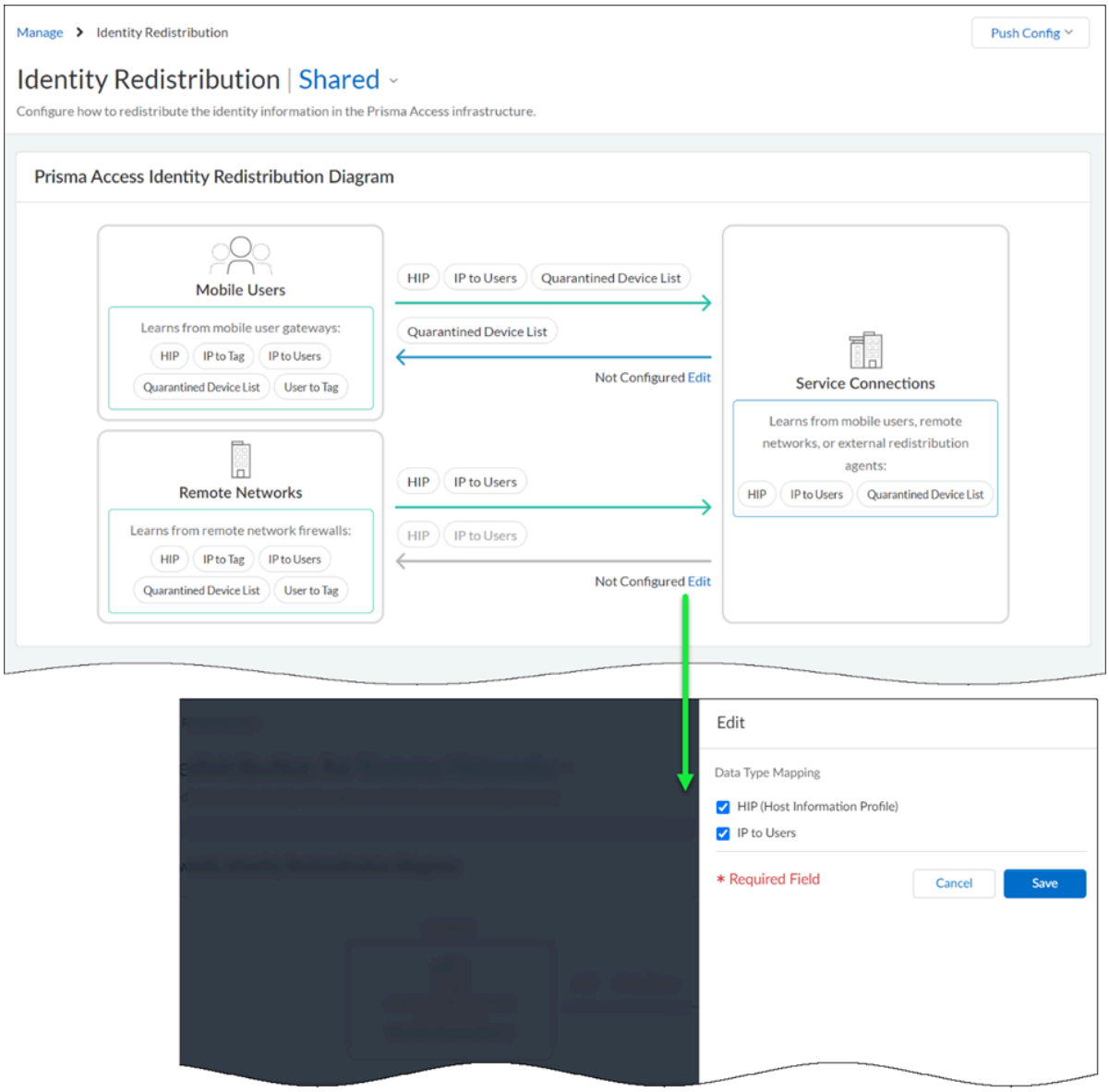
  - Die Konfiguration ist standardmäßig **aktiviert**.
  - Geben Sie einen **Namen** für den TS-Agent ein.
  - Geben Sie die IP-Adresse des Windows-**Hosts** ein, auf dem der TS-Agent installiert ist.
  - Geben Sie die Nummer des **Ports** ein, an dem der Agent auf Benutzerzuordnungsanfragen wartet. Der Port ist standardmäßig auf 5009 festgelegt.
  - **Save (Speichern)** Sie Ihre Änderungen.




 ©2025 Palo Alto Networks, Inc.

- Verteilen Sie Identitätsdaten in IhrerPrisma Access-Umgebung:

  **Bearbeiten** Sie im Dashboard zur **Identitätsweitergabe** das Diagramm, um die Identitätsdaten anzugeben, die Sie aus jeder Quelle sammeln und in Prisma Access teilen möchten.




- Übertragen Sie die Konfiguration an Prisma Access, um Ihre Änderungen zu aktivieren.

## Identitätsweitergabe (Panorama)

Nachdem Sie die Benutzer-ID konfiguriert haben, setzen Sie die benutzerbasierte Richtlinie für alle mobilen Benutzer und Benutzer an Remote-Netzwerkstandorten konsequent durch, indem Sie die Zuordnung von IP-Adresse zu Benutzername von Prisma Access zu allen Firewalls der nächsten Generation weitergeben, die den Zugriff auf Netzwerkressourcen sichern. Verwenden Sie eine der folgenden Methoden, um die Zuordnung von IP-Adresse zu Benutzername von einer lokalen Firewall der nächsten Generation an mobile Benutzer und Benutzer in Remote-Netzwerken weiterzugeben und umgekehrt:

 ©2025 Palo Alto Networks, Inc.

- Benutzer-ID-Informationen von Prisma Access an eine lokale Firewall weitergeben
- Benutzer-ID-Informationen von einer lokalen Firewall an Prisma Access weitergeben


## Benutzer-ID-Informationen von Prisma Access an eine lokale Firewall weitergeben

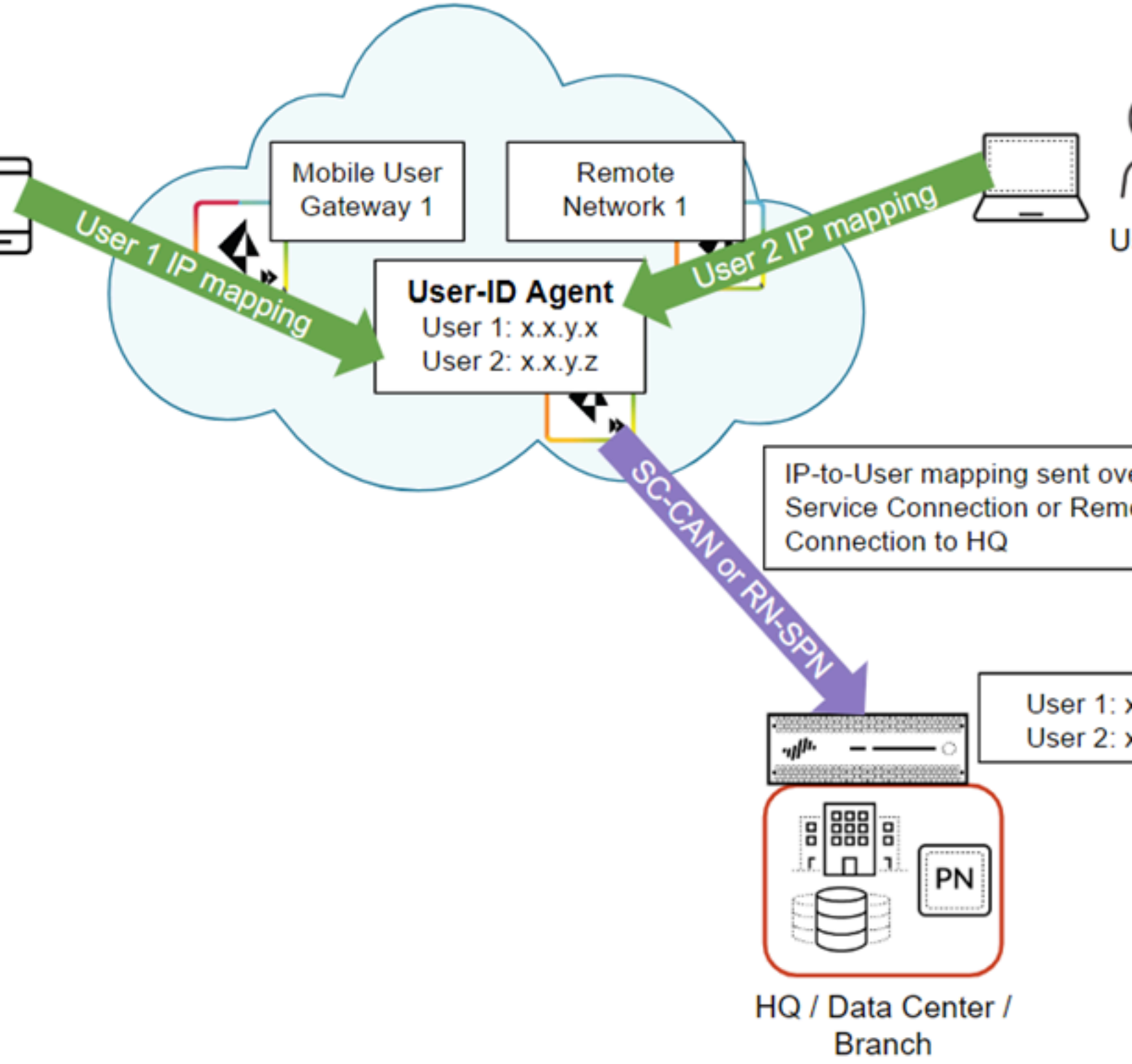
**Geben Sie Benutzer-ID-Informationen von Prisma Access an eine lokale Firewall weiter.**

In Fällen, in denen mobile Benutzer auf eine Ressource an einem Remote-Netzwerkstandort oder einer Zentrale / einem Rechenzentrum zugreifen müssen und die Ressource durch eine lokale Firewall der nächsten Generation mit benutzerbasierten Richtlinien gesichert ist, müssen Sie die Zuordnung von IP-Adresse zu Benutzername von den mobilen Prisma Access-Benutzern und Benutzern an Remote-Netzwerken an die lokale Firewall weitergeben. Wenn der Benutzer eine Verbindung zu Prisma Access herstellt, erfasst er diese Zuordnung von Benutzer zu IP-Adresse und speichert sie.

Die folgende Abbildung zeigt zwei mobile Benutzer, die über eine bestehende Zuordnung von IP-Adresse zu Benutzername in Prisma Access verfügen. Prisma Access gibt diese Zuordnung dann über eine Dienstverbindung (SC-CAN) oder Remote-Netzwerkverbindung (RN-SPN) an die lokale Firewall weiter, die das Zentrum/Rechenzentrum sichert.

*Prisma Access verwendet die Dienstverbindung oder Remote-Netzwerkverbindung als IPSec-Tunnel, der als Underlay-Pfad zum Layer-3-Netzwerk dient. Sie können einen beliebigen Routenpfad über einen vertrauenswürdigen IPSec-Tunnel für privat adressierte Ziele verwenden, um diese Zuordnung weiterzugeben.*

 ©2025 Palo Alto Networks, Inc.



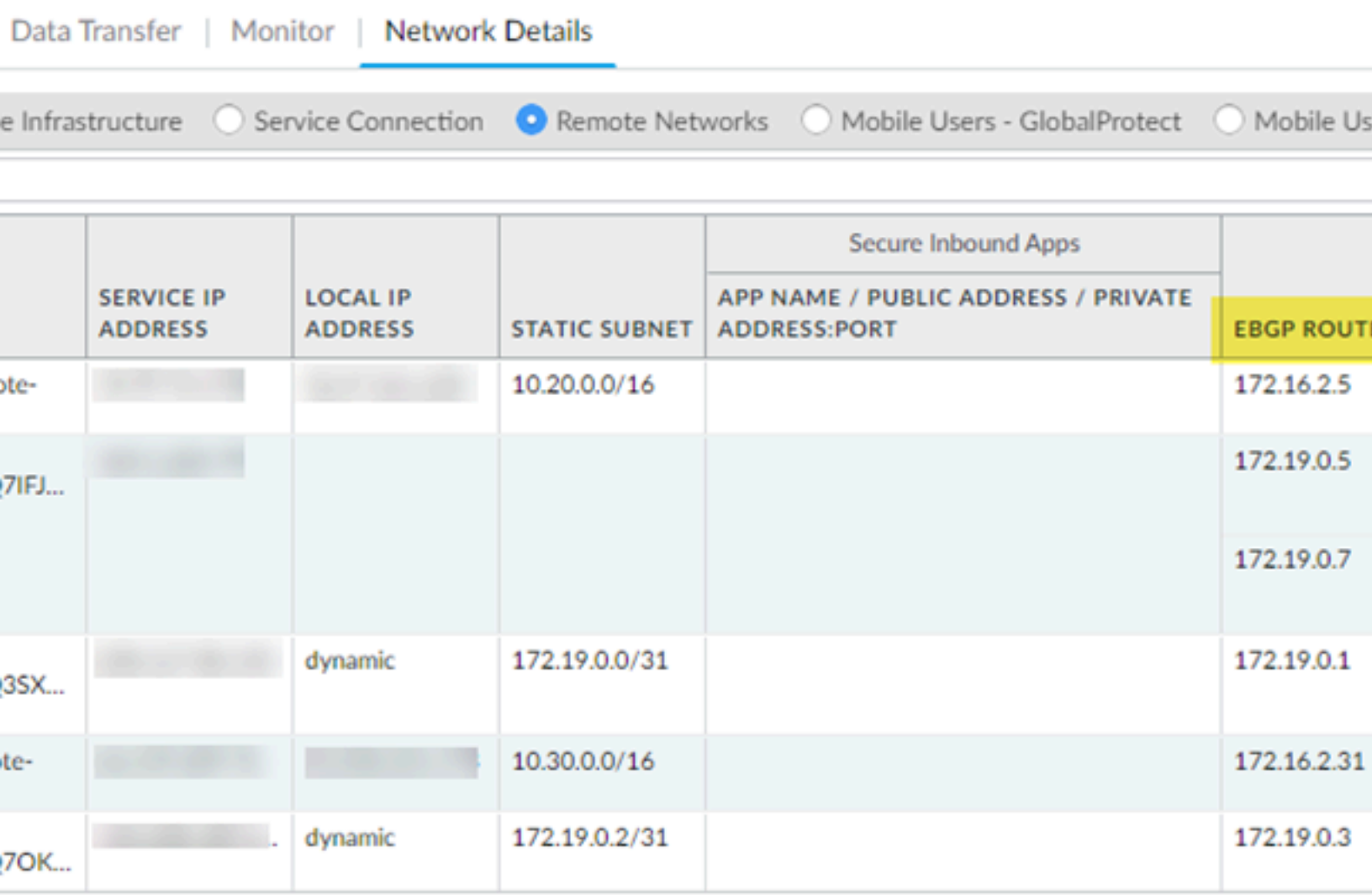

Führen Sie die folgenden Schritte aus, um Benutzer-ID-Zuordnungen von Prisma Access an eine lokale Firewall weiterzugeben.

 ©2025 Palo Alto Networks, Inc.

*Stellen Sie sicher, dass Sie keine SSL-Entschlüsselung auf eine Verbindung anwenden, die die Benutzeridentität an die lokale Firewall (SC-CAN oder RN-SPN) weitergibt, einschließlich aller Firewalls, die sich im Weitergabepfad befinden. Alternativ können Sie einen Ausschluss der Entschlüsselung auf den Datenverkehr für die Weitergabe anwenden.*

**STEP 1 |** Notieren Sie sich die IP-Adresse, die Sie beim Konfigurieren des Datenweitergabe-Agents verwenden sollen.

- Für Remote-Netzwerkverbindungen finden Sie die **EBGP-Routeradresse** (**Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Remote-Netzwerke** > **EBGP-Router**).



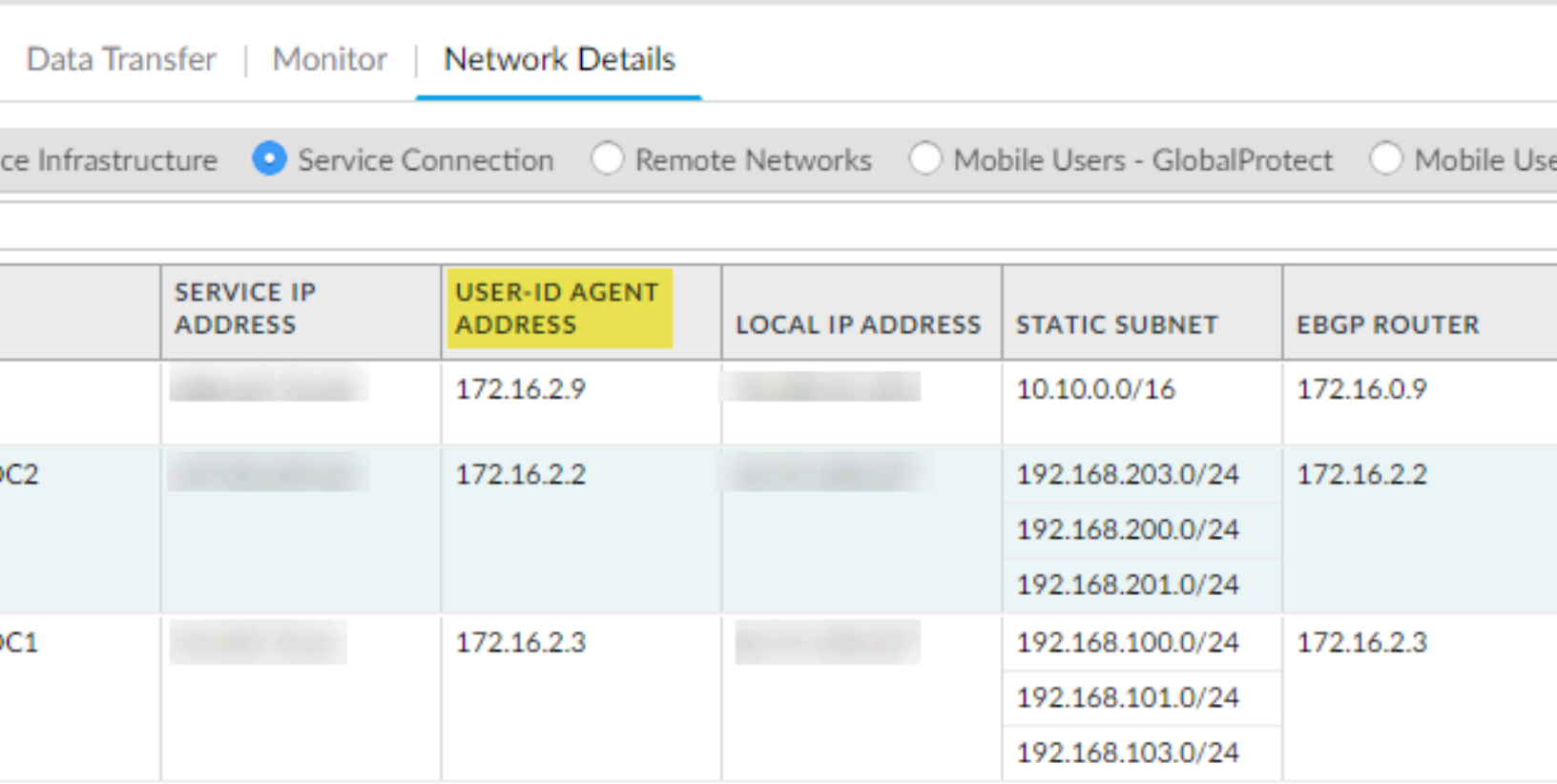

- Für Dienstverbindungen finden Sie die **Benutzer-ID-Agent-Adresse** (**Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Dienstverbindung** > **Benutzer-ID-Agent-Adresse**).

  Wenn Sie noch keine Dienstverbindung für Ihre Zentrale oder Rechenzentren eingerichtet haben, beginnen Sie mit der Konfiguration einer Dienstverbindung.Prisma Access gibt mithilfe von Dienstverbindungen Identitätsdaten in Ihrem Unternehmen frei. Prisma Access aktiviert automatisch Dienstverbindungen als Weitergabe-Agents. Ein neu erstellter Dienstverbindungsstandort ist bereit zur Verwendung als Weitergabe-Agent, wenn Sie

 ©2025 Palo Alto Networks, Inc.

sehen, dass ihm eine User-ID-Agent-Adresse zugewiesen wurde (Prisma Access erledigt dies automatisch, es dauert nur einige Minuten).

***Verwaltung der Weitergabe von Benutzer-IDs*** *– In bestimmten Fällen sind bei der Weitergabe von Benutzer-IDs in besonders umfangreichen Prisma Access-Bereitstellungen detaillierte Kontrollen erforderlich. Mithilfe der Verwaltung der Umverteilung von Benutzer-IDs können Sie das standardmäßige Identitätsweitergabeverhalten für bestimmte Dienstverbindungen manuell deaktivieren, indem Sie das Häkchen in der Spalte* ***Benutzer-ID*** *entfernen und dann bestimmte Dienstverbindungen auswählen, die für die Identitätsweitergabe verwendet werden sollen. Für die meisten Konfigurationen ist dieser Arbeitsschritt nicht erforderlich. Wenden Sie sich an den Support von Palo Alto Networks, um diese Funktionalität zu aktivieren.*




**STEP 2 |** Konfigurieren Sie Prisma Access als Benutzer-ID-Agent, der Benutzerzuordnungsinformationen weitergibt.

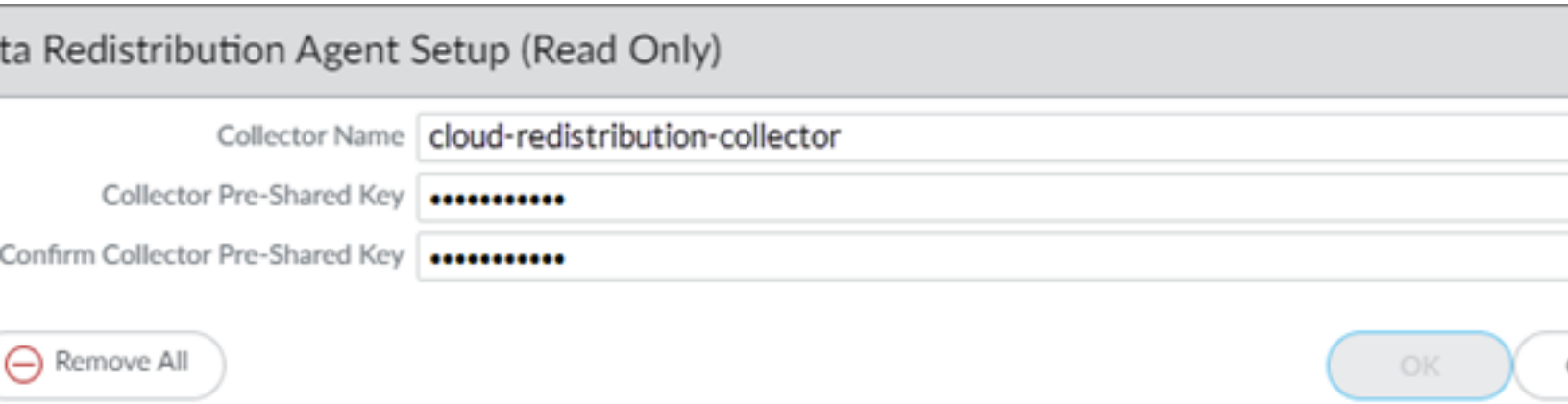
1. Wählen Sie im Panorama, das Prisma Access verwaltet, **Gerät** > **Datenweitergabe** > **Kollektor-Einstellungen** aus.

   Wenn Sie den Kollektor für eine Dienstverbindung konfigurieren möchten, wählen Sie die Vorlage **Service_Conn_Template** aus. Wenn Sie den Kollektor für eine

 ©2025 Palo Alto Networks, Inc.

Remote-Netzwerkverbindung konfigurieren möchten, wählen Sie die Vorlage **Remote_Network_Template** aus.

2. Klicken Sie auf das Zahnradsymbol, um die Einstellungen zu bearbeiten.
3. Geben Sie einen **Kollektornamen** und einen **Kollektor-PSK (Pre-Shared Key)** an, um Prisma Access als Benutzer-ID-Agent zu identifizieren.
4. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

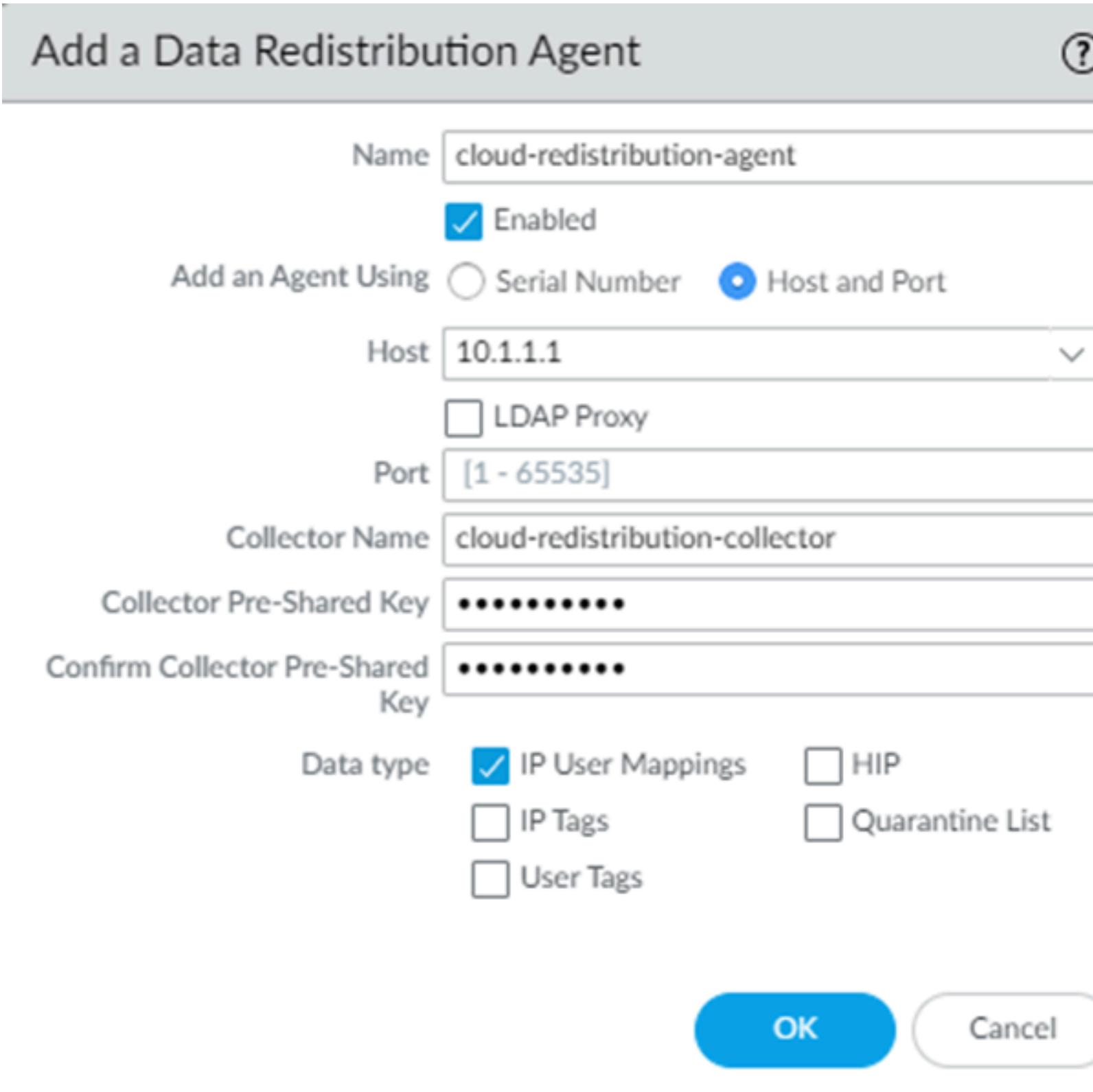



 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Konfigurieren Sie die lokale Firewall, um die Benutzer-ID-Zuordnung von Prisma Access zu erfassen.

1. Wählen Sie in der lokalen Firewall **Gerät** > **Datenweitergabe** > **Agents** aus.
2. **Fügen** Sie einen Benutzer-ID-Agent hinzu und geben Sie ihm einen **Namen**.
3. Wählen Sie einen **Host und Port** aus.
4. Geben Sie im Feld **Host** die **Benutzer-ID-Agent-Adresse** (bei einer Dienstverbindung) oder **EBGP-Routeradresse** (bei einer Remote-Netzwerkverbindung) von Prisma Access ein.
5. Geben Sie den **Kollektornamen** und den **Kollektor-PSK (Pre-Shared Key)** für den Prisma Access-Collector ein, den Sie zuvor im Verfahren erstellt haben.
6. Wählen Sie **IP-Benutzerzuordnungen** aus.
7. Klicken Sie auf **OK**.
8. Wiederholen Sie diese Schritte für jede Dienstverbindung oder Remote-Netzwerkverbindung, für die Sie Zuordnungen weitergeben möchten.

 ©2025 Palo Alto Networks, Inc.




## Benutzer-ID-Informationen von einer lokalen Firewall an Prisma Access weitergeben

**Geben Sie Benutzer-ID-Informationen von einer lokalen Firewall an Prisma Access weiter.**

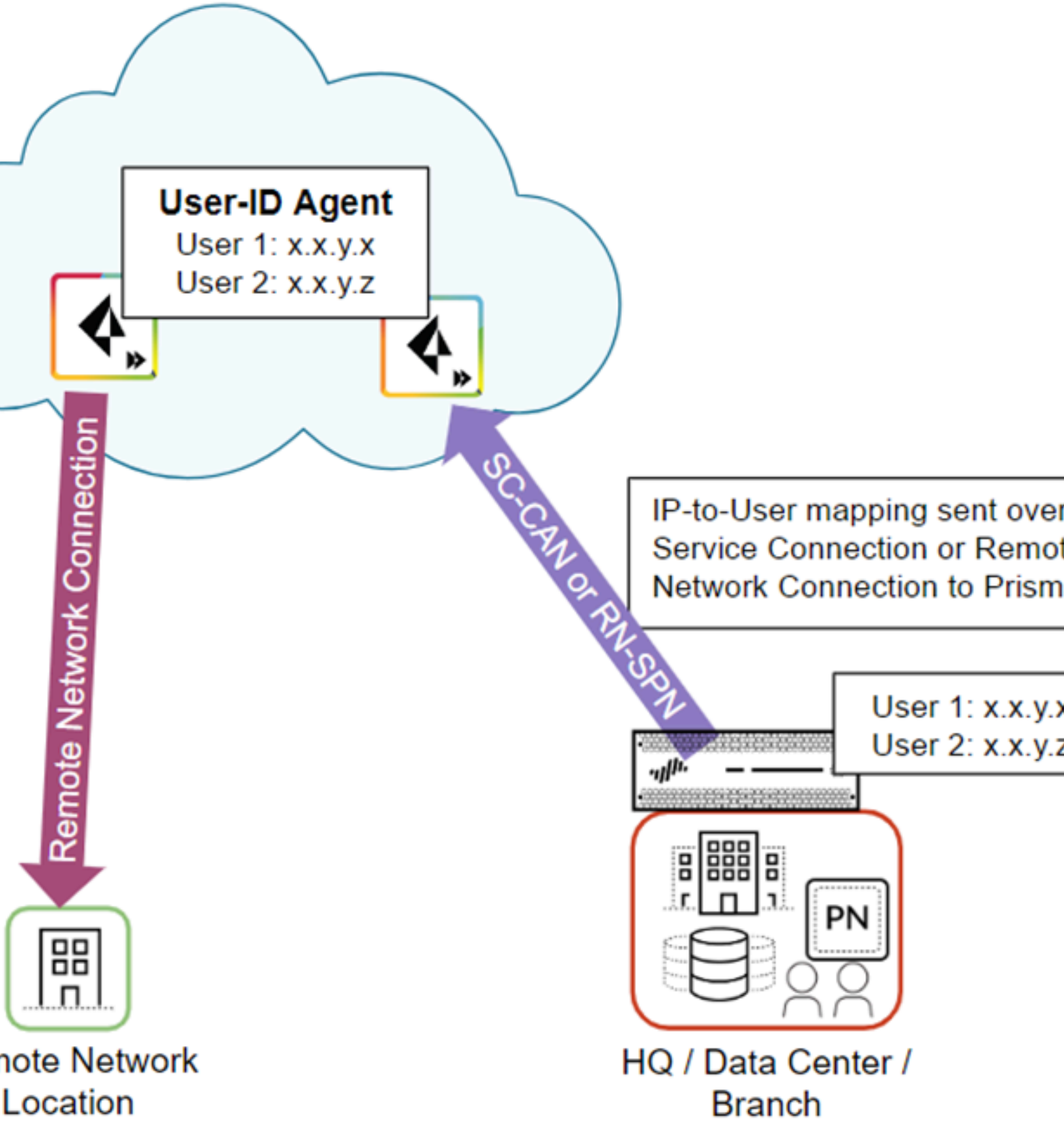

©2025 Palo Alto Networks, Inc.

Wenn sich Benutzer in einer Zweigstelle oder Zentrale befinden, die durch eine lokale Firewall der nächsten Generation mit benutzerbasierten Richtlinien gesichert ist, und sie an einer anderen Zweigstelle, die Sie mit Prisma Access gesichert haben, auf Ressourcen zugreifen müssen, müssen Sie Zuordnungen von IP-Adresse zu Benutzernamen von der lokalen Firewall an Prisma Access weitergeben.

Die folgende Abbildung zeigt eine Zentrale / ein Rechenzentrum mit einer lokalen Firewall der nächsten Generation mit vorhandener Zuordnung von IP-Adresse zu Benutzernamen. Prisma Access stellt entweder über eine Dienstverbindung (SC-CAN) oder über eine Remote-Netzwerkverbindung (RN-SPN) eine Verbindung mit der Firewall her und die lokale Firewall gibt die Zuordnung an Prisma Access weiter.

Die folgende Abbildung zeigt, wie eine Prisma Access-Dienstverbindung oder -Remote-Netzwerkverbindung zur Weitergabe der Zuordnung verwendet wird. Sie können einen beliebigen Routenpfad über einen vertrauenswürdigen IPSec-Tunnel für privat adressierte Ziele verwenden, um diese Zuordnung weiterzugeben.

 ©2025 Palo Alto Networks, Inc.




 ©2025 Palo Alto Networks, Inc.

Führen Sie die folgenden Schritte aus, um Benutzer-ID-Zuordnungen von einer lokalen Firewall an Prisma Access weiterzugeben.

**STEP 1 |** Konfigurieren Sie die lokale Firewall, um Benutzer-ID-Informationen an Prisma Access weiterzugeben.

1. Wählen Sie in der lokalen Firewall **Gerät** > **Datenweitergabe** > **Kollektor-Einstellungen** aus.
2. Klicken Sie auf das Zahnradsymbol, um die Einstellungen zu bearbeiten.
3. Geben Sie einen **Kollektornamen** und einen **Kollektor-PSK (Pre-Shared Key)** an, um die lokale Firewall als Benutzer-ID-Agent zu identifizieren.
4. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

**STEP 2 |** Konfigurieren Sie Prisma Access, um die Benutzer-ID-Zuordnung von der lokalen Firewall zu erfassen.

1. Wählen Sie im Panorama, das Prisma Access verwaltet, **Gerät** > **Datenweitergabe** > **Agents** aus.

   Stellen Sie sicher, dass Sie oben auf der Seite die Vorlage **Service_Conn_Template** (bei Dienstverbindungen) oder die Vorlage **Remote_Network_Template** (bei Remote-Netzwerkverbindungen) im Dropdown-Menü **Vorlagen** ausgewählt haben.
2. **Fügen** Sie einen Benutzer-ID-Agent hinzu und geben Sie ihm einen **Namen**.
3. Wählen Sie einen **Host und Port** aus.
4. Geben Sie im Feld **Host** die IP-Adresse der MGT-Schnittstelle oder Dienstroute ein, über die die Firewall Benutzerzuordnungen sendet.

   Für die MGT-Schnittstelle können Sie anstelle der IP-Adresse einen Hostnamen eingeben.
5. Geben Sie den **Kollektornamen** und den **Kollektor-PSK (Pre-Shared Key)** ein. Verwenden Sie dabei die Werte für den Kollektor, den Sie für die lokale Firewall in Schritt 1 verwendet haben.
6. Wählen Sie **IP-Benutzerzuordnungen** aus.
7. Klicken Sie auf **OK**.

 ©2025 Palo Alto Networks, Inc.

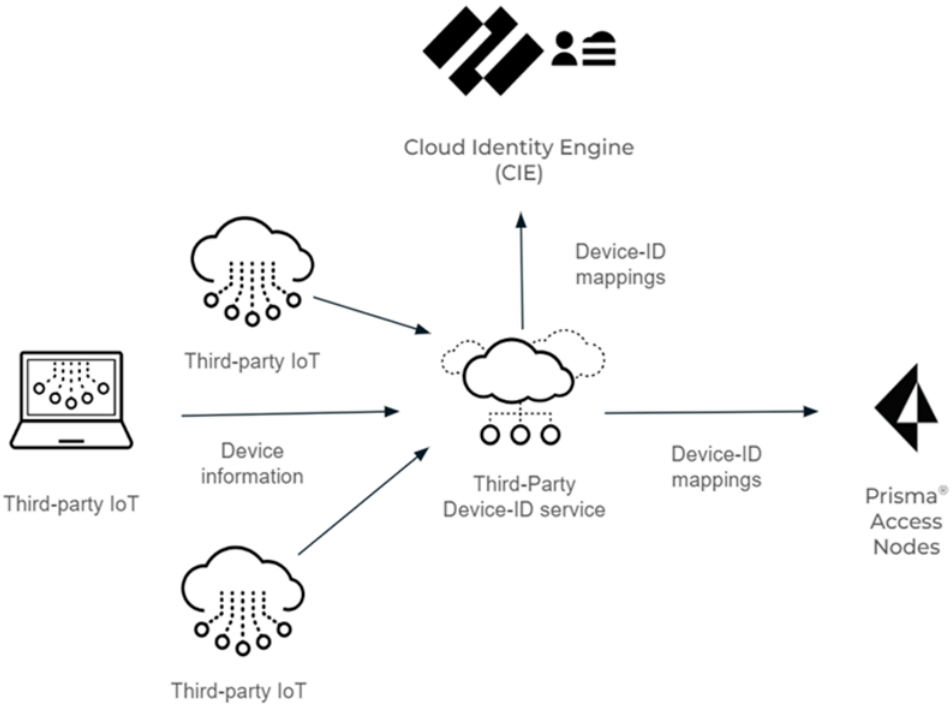
# Konfigurieren der Geräte-ID von Drittanbietern in Prisma Access

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama)<br>Wenn Sie diese Funktion in Ihrer Prisma Access-Umgebung nutzen möchten, dann wenden Sie sich an Ihr Account-Team, um weiterführende Informationen zu erhalten. | ❑ Prisma Access-Lizenz mit aktivierter Cloud Identity Engine-Funktion |

Sie können die Cloud Identity Engine zusammen mit Prisma Access verwenden, um Informationen aus IoT-Erkennungsquellen von Drittanbietern anzuwenden und die Erkennung und Schließung von Sicherheitslücken für Geräte in Ihrem Netzwerk zu vereinfachen. Nachdem Sie die Geräte-ID eines Drittanbieters in der Cloud Identity Engine mithilfe einer API eingerichtet haben, können Sie ein Geräteobjekt und eine Sicherheitsrichtlinienregel in Prisma Access einrichten, um Informationen von IoT-Sichtbarkeitslösungen eines Drittanbieters über die Cloud Identity Engine für die Gerätetransparenz und -steuerung abzurufen und zu verwenden.

In der folgenden Abbildung empfängt der Geräte-ID-Dienst eines Drittanbieters die Geräteinformationen von den Drittanbieter-IoT-Lösungen, die er dann als Zuordnungen von IP-Adressen zu Geräten an die Cloud Identity Engine und die Prisma Access-Security Processing Nodes (SPNs) übermittelt.

 ©2025 Palo Alto Networks, Inc.




- Strata Cloud Manager
- Panorama

## Konfigurieren der Geräte-ID eines Drittanbieters in Prisma Access (Strata Cloud Manager)

Gehen Sie zum Konfigurieren der Geräte-ID eines Drittanbieters wie folgt vor.

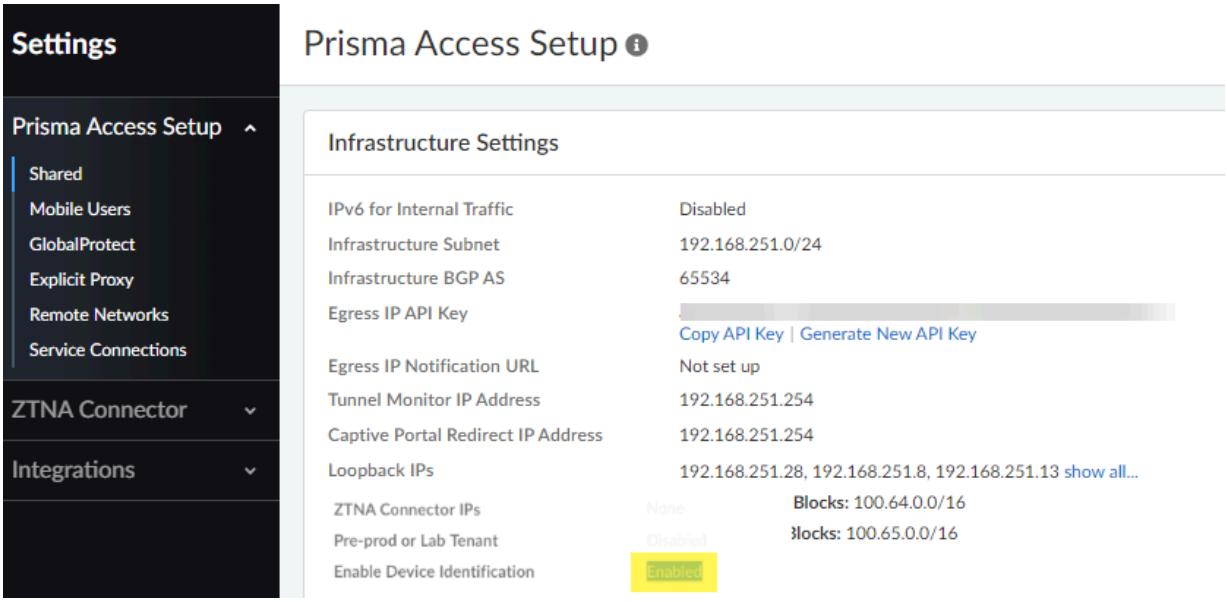
**STEP 1 |** Aktivieren Sie die Geräte-ID von Drittanbietern in der Cloud Identity Engine.

Bei dieser Vorgehensweise muss ein signiertes Zertifikat hochgeladen werden, um damit über eine API mit dem IoT-Drittanbieter zu kommunizieren und von diesem Informationen zur Geräte-ID herunterzuladen.

**STEP 2 |** Aktivieren Sie die Geräte-ID eines Drittanbieters in Prisma Access, indem Sie zu **Einstellungen** > **Einrichtung Prisma Access** > **Freigegeben** oder **Workflows** > **Einrichtung**

 ©2025 Palo Alto Networks, Inc.

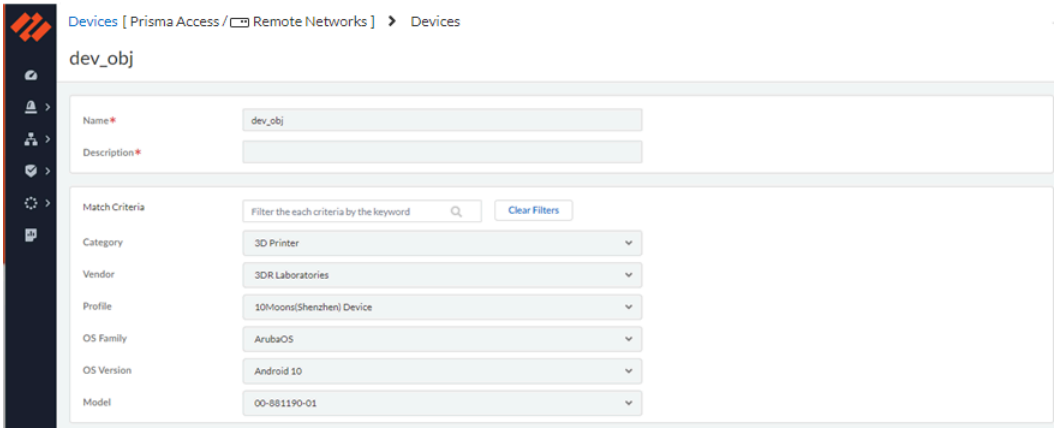
**Prisma Access** > **Prisma Access**wechseln und **Geräteidentifikation aktivieren** auf **Aktiviert** setzen.




**STEP 3 |** Konfigurieren Sie ein Geräteobjekt und geben Sie Geräteattribute ein. Wählen Sie **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** aus, legen Sie den Konfigurationsumfang auf **Remote-Netzwerke** fest und wählen Sie **Objekte** > **Geräte** und **Geräte hinzufügen** aus. Stellen Sie sicher, dass Sie sich in der Gerätegruppe „Remote-Netzwerke“ befinden.

1. Fügen Sie ein Geräteobjekt hinzu, das mit den Attributen für die Drittanbieterobjekte übereinstimmt.

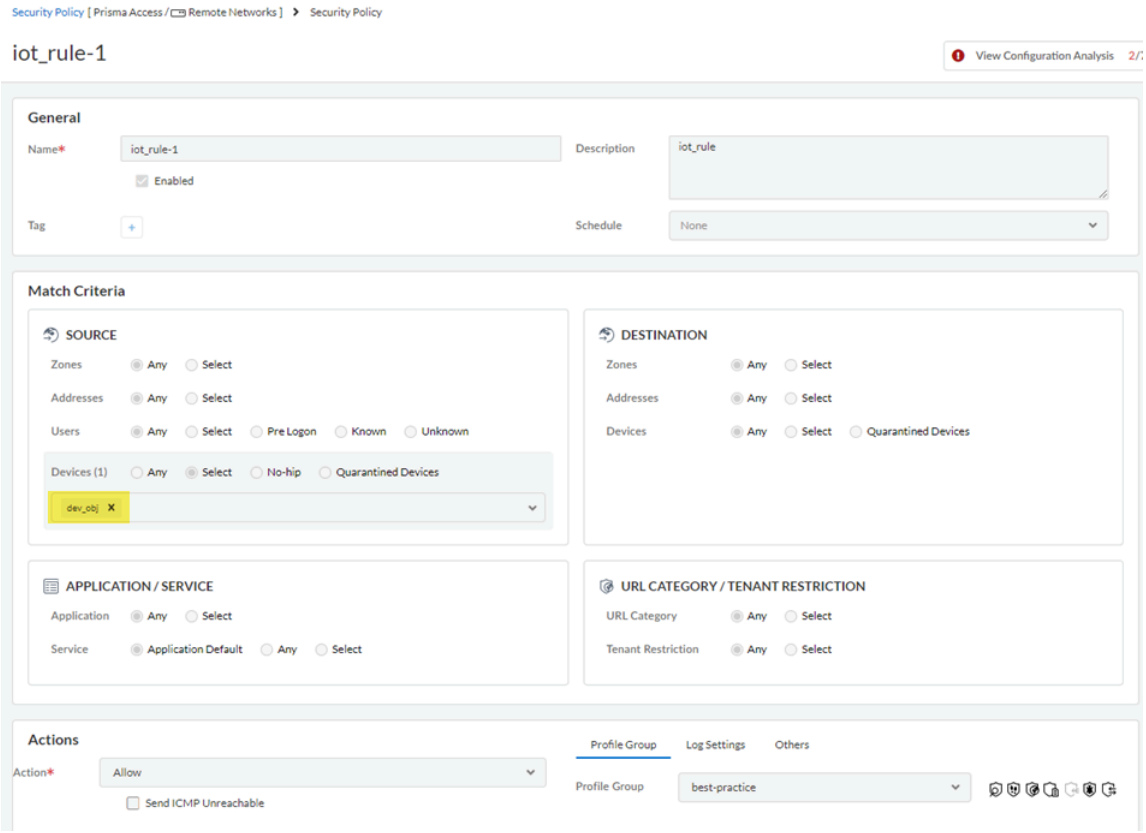
   Im Bereich **Zuordnungen** der Cloud Identity Engine werden die Attribute der Drittanbietergeräte angezeigt. Sie können alle von dort abgerufenen Attribute verwenden.




**STEP 4 |** Gehen Sie zu **Verwalten** > **Konfiguration** > **NGFW und Prisma Access**, legen Sie den Konfigurationsumfang auf **Remote-Netzwerke** fest und wählen Sie **Sicherheitsdienste**

 ©2025 Palo Alto Networks, Inc.

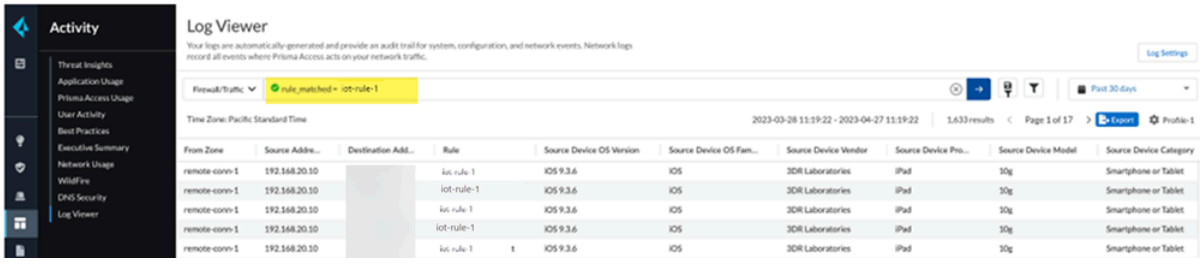
> **Sicherheitsrichtlinie** aus, um eine Sicherheitsrichtlinie **hinzuzufügen**, indem Sie die Geräteobjekte hinzufügen, die Sie im Bereich **Geräte** erstellt haben.




**STEP 5 |** Wählen Sie **Konfiguration übertragen** aus, um Ihre Änderungen an der Prisma Access-Konfiguration zu speichern, und wählen Sie im Übertragungsumfang die Option **Remote-Netzwerke** aus.

**STEP 6 |** Vergewissern Sie sich, dass Prisma Access die Geräte-ID-Protokolle empfängt, indem Sie unter **Vorfälle und Benachrichtigungen** > **Protokoll-Viewer** die Option **Firewall/ Datenverkehr** auswählen und gemäß der von Ihnen erstellten Regel nach Datenverkehr suchen, indem Sie `rule_matched = Regelname` eingeben, wobei *Regelname* der Sicherheitsrichtlinienregel entspricht, die Sie für die IoT-Drittanbietergeräte erstellt haben.

Die Zuordnungen von Geräte-IDs zu IP-Adressen werden in den Protokollen angezeigt.




 ©2025 Palo Alto Networks, Inc.

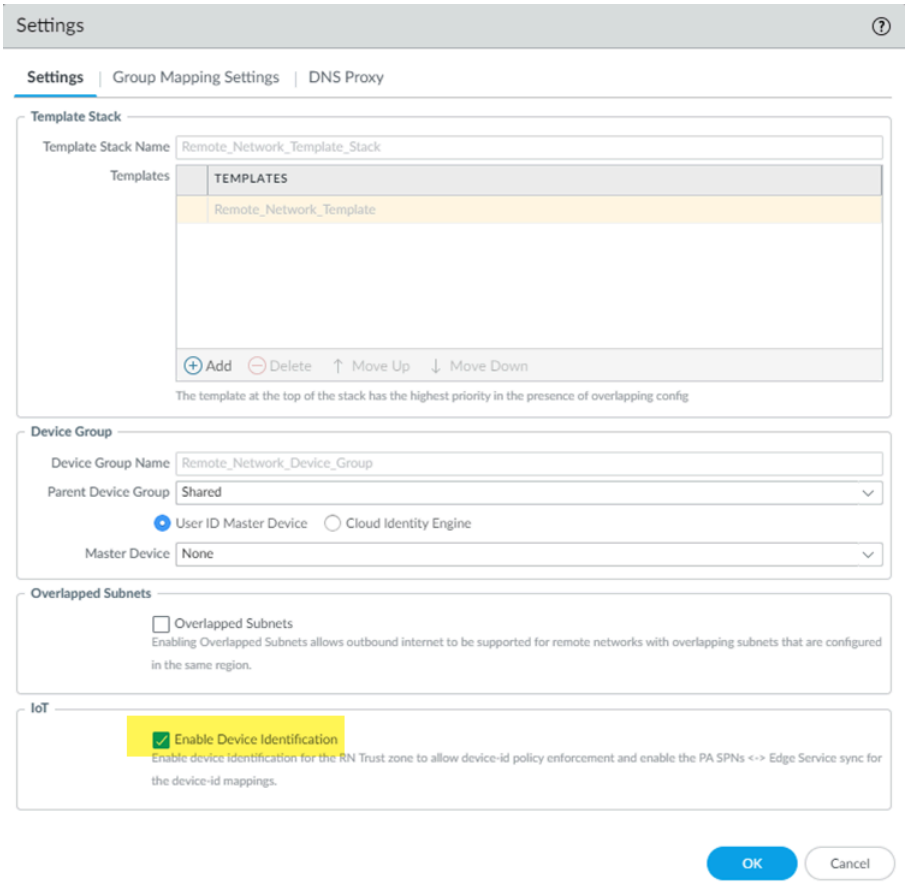
# Konfigurieren der Geräte-ID eines Drittanbieters in Prisma Access (Panorama)

Gehen Sie zum Konfigurieren der Geräte-ID eines Drittanbieters wie folgt vor.

**STEP 1 |** Aktivieren Sie die Geräte-ID von Drittanbietern in der Cloud Identity Engine.

Bei dieser Vorgehensweise muss ein signiertes Zertifikat hochgeladen werden, um damit über eine API mit dem IoT-Drittanbieter zu kommunizieren und von diesem Informationen zur Geräte-ID herunterzuladen.

**STEP 2 |** Aktivieren Sie die Geräte-ID von Drittanbietern in Prisma Access, indem Sie unter **Panorama** > **Cloud Services** > **Konfiguration** > **Remote-Netzwerke** > **Einstellungen** auf das Zahnrad klicken, um die **Einstellungen** zu bearbeiten, und **Geräteidentifikation aktivieren** auswählen.



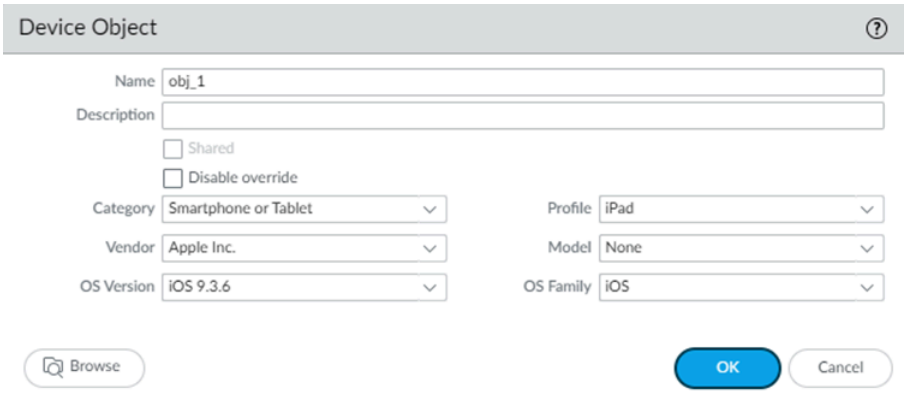

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Konfigurieren Sie ein Geräteobjekt und geben Sie Geräteattribute ein.

1. Wählen Sie unter **Objekte** > **Geräte** die Option **Hinzufügen** aus, um ein Geräteobjekt hinzuzufügen, das allen Geräte-ID-Attributen entspricht.

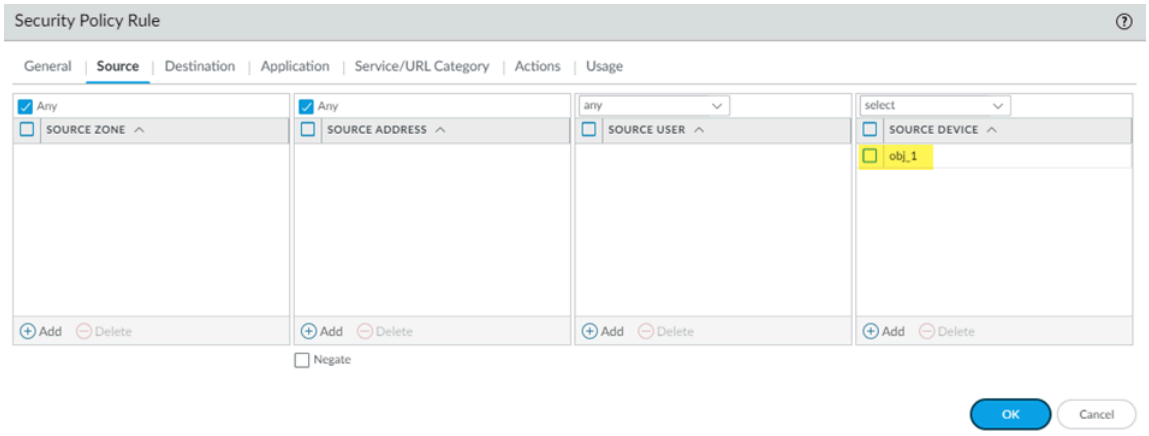
   Stellen Sie sicher, dass Sie sich in der Gerätegruppe für Remote-Netzwerke (**Remote_Network_Device_Group**) oder in der Gerätegruppe **Freigegeben** befinden.
2. Sie müssen ein Geräteobjekt **hinzufügen**, das mit Attributen für die Drittanbieterobjekte übereinstimmt.

   *Im Bereich **Zuordnungen** der Cloud Identity Engine werden die Attribute der Drittanbietergeräte angezeigt. Sie können alle von dort abgerufenen Attribute verwenden.*




**STEP 4 |** Wählen Sie unter **Richtlinien** > **Sicherheit** > **Vor-Regeln** die Option **Hinzufügen** aus, um eine Sicherheitsrichtlinie hinzuzufügen. Anschließend fügen Sie die im Bereich **Geräte** erstellte Geräteobjekte als **Quellgerät** hinzu.

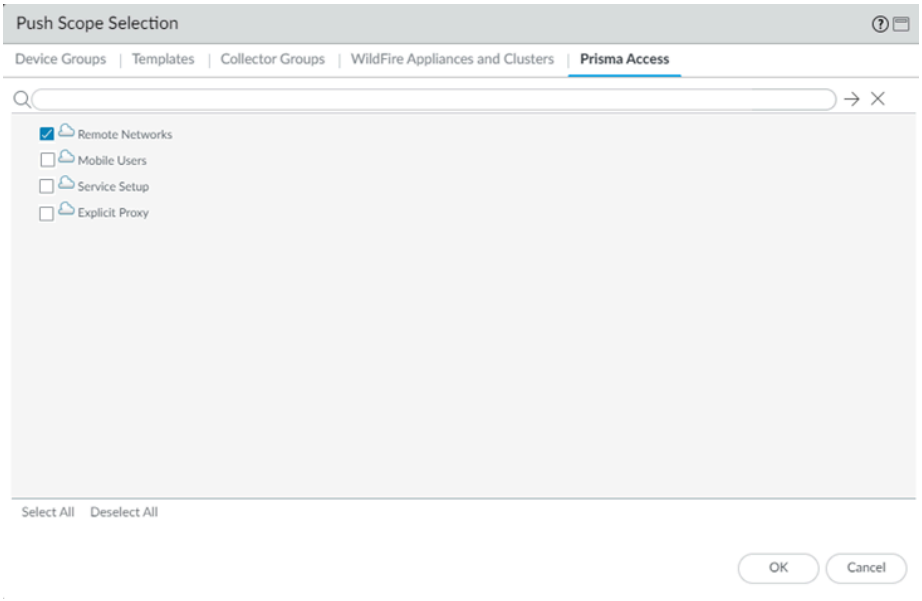
Stellen Sie sicher, dass Sie sich in der Gerätegruppe für Remote-Netzwerke (**Remote_Network_Device_Group**) oder in der Gerätegruppe **Freigegeben** befinden.




 ©2025 Palo Alto Networks, Inc.

**STEP 5 |** Führen Sie einen Commit aus und übertragen Sie Ihre Änderungen per Push. Vergewissern Sie sich dabei, dass **Remote-Netzwerke** im **Übertragungsumfang** ausgewählt ist.

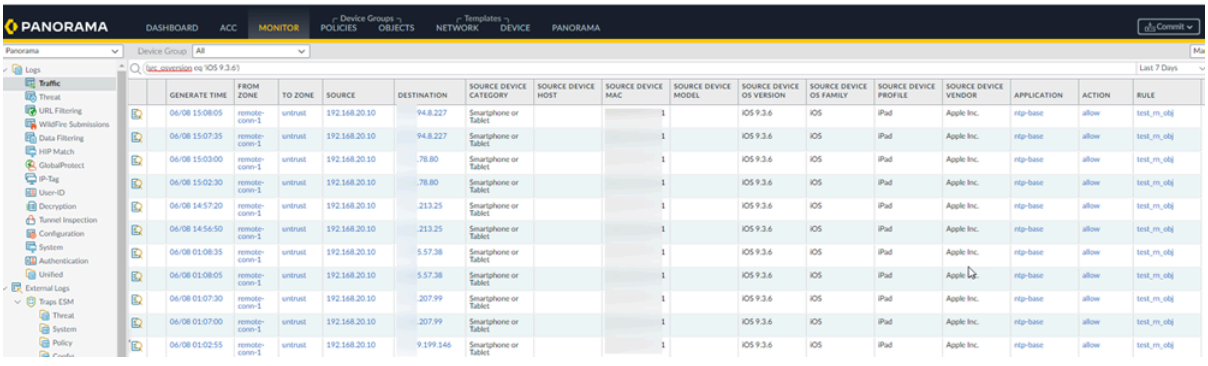
1. Klicken Sie auf **Commit** > **Commit und Push**.
2. Wählen Sie **Auswahl bearbeiten** aus und vergewissern Sie sich, dass auf der Registerkarte **Prisma Access** für **Übertragungsumfang** die Option **Remote-Netzwerke** ausgewählt ist, und klicken Sie anschließend auf **OK**.




3. Klicken Sie auf **Commit und Push**.

**STEP 6 |** Vergewissern Sie sich, dass Prisma Access die Geräte-ID-Protokolle empfängt, indem Sie unter **Überwachen** > **Protokolle** die **Datenverkehrsprotokolle** nach Datenverkehr gemäß der von Ihnen erstellten Regel durchsuchen. Geben Sie `rule_matched` =*Regelname* ein. Dabei entspricht *Regelname* der Sicherheitsrichtlinienregel, die Sie für die IoT-Drittanbietergeräte erstellt haben.

Die Zuordnungen von Geräte-IDs zu IP-Adressen werden in den Protokollen angezeigt.




 ©2025 Palo Alto Networks, Inc.

# APIs für Geräte-IDs von Drittanbietern

Nachdem Sie über die Benutzeroberfläche der Cloud Identity Engine in den Geräte-ID-Dienst eines Drittanbieters eingebunden wurden, können Sie mithilfe dieser APIs die *Urteile*, oder Zuordnungen von IP-Adressen zu Geräten, die in Ihrem Netzwerk erkannt und im Geräte-ID-Dienst des Drittanbieters gespeichert wurden, verwalten. Diese Zuordnungen informieren Prisma Access darüber, welche Attribute zu einem Gerät mit einer bestimmten IP-Adresse gehören, sodass Sie eine Sicherheitsrichtlinie definieren können, die auf Geräte mit bestimmten Attributen abzielen.

Diese APIs greifen nicht direkt auf die in Ihrem Cloud Identity Engine-Mandanten gespeicherten Daten zu. Vielmehr interagieren die APIs mit den Zuordnungen von IP-Adressen zu Geräten im Geräte-ID-Dienst eines Drittanbieters, der diese Zuordnungen mit der Cloud Identity Engine gemeinsam verwendet.

Die APIs für Geräte-IDs von Drittanbietern verwenden ein Zertifikat, einen API-Schlüssel und eine Basis-URL für API-Anfragen. Um Anfragen von APIs für Geräte-IDs von Drittanbietern zu authentifizieren, müssen Sie das signierte Zertifikat und das API-Token verwenden, das Sie während des Onboardings in der Benutzeroberfläche der Cloud Identity Engine erhalten haben.

Wenn Sie über ein Zertifikat und einen API-Schlüssel verfügen, können Sie Anfragen an den Geräte-ID-Dienst eines Drittanbieters stellen. Geben Sie das Zertifikat in jeder Anfrage mit seinem öffentlichen Schlüssel, dem API-Schlüssel und der Basis-URL an. Beispiel:

```
curl --cert onida1.crt --key onida.key "https://device-identity-
broker-beta.service-edge.panservicetest.com/:443/api/v1/token/
{apiKey}/verdicts"
```

- Urteile aktualisieren
- Alle Urteile löschen
- Abfrageurteile
- Abfrageurteile nach IP-Adresse
- Abfrageurteil Statistiken

## Urteile aktualisieren

Fügt Zuordnungen einer IP-Adresse zu einem Gerät hinzu, ändert oder löscht sie.

**Übersicht**

| | |
|---|---|
| URI | `/api/v1/token/{apiKey}/verdicts:update` |
| HTTP-Methode | POST |

**Beschreibung**

Die Geräte-ID von Drittanbietern erfasst Daten aus IoT-Erkennungsquellen von Drittanbietern in Ihrem Netzwerk und erstellt Zuordnungen einer IP-Adresse zu einem Gerät, mit denen Prisma

 ©2025 Palo Alto Networks, Inc.

Access gerätespezifische Sicherheitsrichtlinienregeln durchsetzen kann. Verwenden Sie diese API, um eine neue Zuordnung hinzuzufügen, eine vorhandene Zuordnung zu ändern oder eine Zuordnung zu löschen.

Sie fügen eine Zuordnung über das Feld `Aktualisieren` hinzu oder ändern sie. Gelöscht werden Zuordnungen über das Feld `Löschen`.

Wenn die Zuordnung bereits vorhanden ist, überschreibt `Aktualisieren` vorhandene Geräteattribute mit den im Anfragetext angegebenen Attributen. Ist keine Zuordnung vorhanden, wird mit „Aktualisieren“ eine neue Zuordnung erstellt.

Diese API unterstützt keine teilweisen Updates. Wenn Sie bestimmte Attribute einer Zuordnung aktualisieren möchten, müssen Sie auch die vorherigen Werte für die Attribute, die Sie nicht aktualisieren möchten, erneut eingeben. Wenn Sie Attribute leer lassen, werden vorhandene Werte gelöscht.

Sie können bis zu 10.000 Zuordnungen gleichzeitig aktualisieren oder löschen. Die Anfrage ist atomar: Eine Erfolgsmeldung bedeutet, dass das System alles verarbeitet hat, eine Fehlermeldung bedeutet, dass das System nichts verarbeitet hat.

**Felder**

| Feld | Beschreibung |
|---|---|
| Aktualisieren | Ein JSON-Objekt, das die Attribute einer Zuordnung einer IP-Adresse zu einem Gerät bereitstellt, das Sie aktualisieren oder erstellen möchten. Muss „ip“ und mindestens ein anderes Attribut enthalten. |
| Löschen | Ein JSON-Objekt, das die IP-Adresse der zu löschenden Zuordnung angibt. |

Beispiel:

```
{ "update": [ { "ip": "string", "serialNo": "string", "mac":
 "string", "category": "string", "vendor": "string", "model":
 "string", "os": "string", "osFamily": "string", "hostname":
 "string", "profile": "string", } ], "delete": [ { ip: "string" } ] }
```

**Erfolg**

Wenn die Aktion erfolgreich war, lautet der HTTP-Antwortcode 200. Zusätzlich enthält die Antwort ein JSON-Objekt mit dem folgenden Feld:

| Feld | Beschreibung |
|---|---|
| `updateTime` | Ein Unix-Zeitstempel, der angibt, wann die Anforderung erfolgreich war. |

 ©2025 Palo Alto Networks, Inc.

Beispiel:

```
{ "updateTime": unix-timestamp }
```

**Fehler**

Wenn Fehler auftreten, wird einer der HTTP-Antwortcodes angegeben:

| Antwortcode | Beschreibung |
|---|---|
| 400 | Ungültige Anfrage. Die Anfrage war unvollständig oder fehlerhaft. Korrigieren Sie die Anfrage, bevor Sie es erneut versuchen. |
| 401 | Nicht autorisiertes Token. Versuchen Sie, Ihr API-Token neu zu generieren. Sollte dies fehlschlagen, wenden Sie sich an den Support. |
| 409 | Konflikt. Die Anfrage konnte nicht verarbeitet werden, da derzeit ein anderer Aktualisierungs- oder Löschvorgang ausgeführt wird. Versuchen Sie es erneut, wenn der andere Vorgang abgeschlossen wurde. |
| 429 | Zu viele Anfragen. Die Anfrage konnte nicht verarbeitet werden, da das System in einem bestimmten Zeitraum zu viele Anfragen gestellt hat. Überschreiten Sie nicht den Grenzwert von mehr als einer Anfrage pro Sekunde. Warten Sie und versuchen Sie es erneut. |

Darüber hinaus enthält der Antworttext die folgenden Felder:

| Feld | Beschreibung |
|---|---|
| Code | Der Fehlercode. |
| Nachricht | Die Fehlermeldung. |

## update-Objekt

Enthält die zum Aktualisieren der Zuordnungen von IP-Adressen zu Geräten erforderlichen Informationen. Dieses JSON-Objekt umfasst die folgenden Felder:

| Feld | Beschreibung |
|---|---|
| ip | IP-Adresse des Geräts. |
| updateTime | Unix-Timestamp, der angibt, wann die letzte Aktualisierung der Zuordnung stattg |
| category | Gerätetyp. Beispiel: Drucker |
| vendor | Geräteanbieter. Beispiel: SHARP Corporation |

 ©2025 Palo Alto Networks, Inc.

| | |
|---|---|
| model | Gerätemodell. Beispiel: MX-6070N |
| os | Betriebssystem des Geräts. Beispiel: ThreadX 5 |
| osFamily | Familie, zu der das Betriebssystem des Geräts gehört. Beispiel: ThreadX RTOS |
| profile | Geräteprofil. Beispiel: Sharp Printer |

## Alle Urteile löschen

Löscht alle Zuordnungen von IP-Adressen zu Geräten aus dem Geräte-ID-Dienst eines Drittanbieters.

**Übersicht**

| | |
|---|---|
| URI | /api/v1/token/{apiKey}/verdicts:all |
| HTTP-Methode | LÖSCHEN |

**Beschreibung**

Fordert den Geräte-ID-Dienst eines Drittanbieters auf, alle Zuordnungen von IP-Adressen und Geräten im Geräte-ID-Dienst des Drittanbieters zu löschen. Wenn die Aktion erfolgreich war und eine entsprechende Antwort zurückgegeben wird, bedeutet dies, dass der Dienst alle Zuordnungen gelöscht hat. Wird ein Fehler zurückgegeben, bedeutet dies, dass keine Zuordnungen gelöscht werden konnten.

**Erfolg**

Wenn die Aktion erfolgreich war, lautet der HTTP-Antwortcode 200. Die Antwort enthält keinen Text.

**Fehler**

Wenn Fehler auftreten, wird einer der folgenden HTTP-Antwortcodes ausgegeben:

| Antwortcode | Beschreibung |
|---|---|
| 401 | Nicht autorisiertes Token. Versuchen Sie, Ihr API-Token neu zu generieren. Wenn das nicht funktioniert, kontaktieren Sie den Support. |
| 409 | Konflikt. Das System konnte die Anfrage nicht verarbeiten, da derzeit ein anderer Aktualisierungs- oder Löschvorgang ausgeführt wird. Versuchen Sie es erneut, wenn der andere Vorgang abgeschlossen wurde. |
| 429 | Zu viele Anfragen. Das System konnte die Anfrage nicht verarbeiten, da das System in einem bestimmten Zeitraum zu viele Anfragen gestellt hat. |

 ©2025 Palo Alto Networks, Inc.

| Antwortcode | Beschreibung |
|---|---|
| | Überschreiten Sie nicht den Grenzwert von mehr als einer Anfrage pro Sekunde. Warten Sie und versuchen Sie es erneut. |

Darüber hinaus wird in der Antwort Text in den folgenden Feldern ausgegeben:

| Feld | Beschreibung |
|---|---|
| Code | Der Fehlercode. |
| Nachricht | Die Fehlermeldung. |

## Abfrageurteile

Ruft die Zuordnungen von IP-Adressen zu Geräten beim Geräte-ID-Dienst eines Drittanbieters ab.

**Übersicht**

| | |
|---|---|
| URI | /api/v1/token/{apiKey}/verdicts?<br>bookmark={STRING}&pageLen={INTEGER} |
| HTTP-Methode | GET |

**Beschreibung**

Gibt entweder alle Zuordnungen oder eine Teilmenge zurück.

Wenn Sie alle Zuordnungen zurückgeben möchten, senden Sie die Anfrage einmal ohne Parameter. Beachten Sie den Wert `nextBookmark` in der Antwort. Senden Sie eine weitere Anfrage mit diesem Wert für den Wert `bookmark`, der an den URI angehängt ist. Der Anrufer wiederholt die Abfrage, bis `count` in der Antwort leer ist. Dies deutet darauf hin, dass alle Zuordnungen zurückgegeben wurden.

Wenn Sie eine Teilmenge von Zuordnungen zurückgeben möchten, geben Sie die Anzahl der Zuordnungen an, die Sie mit `pageLen` abrufen möchten (max. 10.000).

**Parameter**

Diese API akzeptiert folgende Parameter:

| Parameter | Beschreibung |
|---|---|
| bookmark | (Optional) Wird nach der ersten Anfrage verwendet, um alle Zuordnungen zurückzugeben. |

 ©2025 Palo Alto Networks, Inc.

| | |
|---|---|
| pageLen | (Optional) Die Anzahl der abzurufenden Zuordnungen. Der Bereich ist 1 bis 10.000. Falls kein Wert angegeben ist, beträgt der Standardwert 10.000. |

**Erfolg**

Wenn die Aktion erfolgreich war, lautet der HTTP-Antwortcode 200. Zusätzlich enthält die Antwort ein JSON-Objekt mit folgenden Feldern:

| Feld | Beschreibung |
|---|---|
| nextBookmark | Der Wert, den Sie im Lesezeichenparameter verwenden, um so lange wiederholt durchzuführen, bis alle Zuordnungen zurückgegeben werden. |
| count | Ganzzahl, die die Anzahl der Zuordnungen darstellt, die in der Antwort zurückgeg |
| verdicts | Objekt, das die Zuordnungen enthält, die in der Anfrage angegeben sind. |

Beispiel:

```
{ "nextBookmark": CkcKVxdWVuY2USAggEEjFqCHN, "count": 1, "verdicts" :
 [ { "ip": "10.10.10.10", "updateTime": 1623974506, "mac":
 "0a:d4:5f:e9:96:10", "category": "Smartphone oder Tablet",
 "Anbieter": "Apple Inc.", "model": "iPad2", "os": "iOS 9.3.6",
 "osFamily": "iOS", "profile": "iPad" } ] } }
```

**Fehler**

Wenn Fehler auftreten, wird einer der HTTP-Antwortcodes angegeben:

| Antwortcode | Beschreibung |
|---|---|
| 400 | Ungültige Anfrage. Die Anfrage war unvollständig oder fehlerhaft.<br>Sie sollten die Anfrage korrigieren, bevor Sie es erneut versuchen. |
| 401 | Nicht autorisiertes Token. |
| 429 | Zu viele Anfragen. Die Anfrage konnte nicht bearbeitet werden, da in einem best zu viele Anfragen gestellt wurden. Es ist nicht mehr als eine Anfrage pro Sekunde Sie und versuchen Sie es erneut. |

Darüber hinaus enthält der Antworttext die folgenden Felder:

 ©2025 Palo Alto Networks, Inc.

| Feld | Beschreibung |
|---|---|
| Code | Der Fehlercode. |
| Nachricht | Die Fehlermeldung. |

### Objekt „verdicts“ (Urteile)

Dieses Objekt wird nach erfolgreicher Abfrage einer IP-Adresse-zu-Gerät-Zuordnung zurückgegeben. Es enthält folgende Informationen:

| Feld | Beschreibung |
|---|---|
| ip | IP-Adresse des Geräts |
| updateTime | Unix-Zeitstempel, der angibt, wann die letzte Aktualisierung des Mappings stattg |
| category | Gerätetyp Beispiel: Drucker |
| vendor | Geräteanbieter Beispiel: SHARP Corporation |
| model | Gerätemodell Beispiel: MX-6070N |
| os | Betriebssystem des Geräts Beispiel: ThreadX 5 |
| osFamily | Familie, zu der das Betriebssystem des Geräts gehört Beispiel: ThreadX RTOS |
| profile | Geräteprofil Beispiel: Sharp-Drucker |

## Abfrageurteile nach IP-Adresse

Ruft Zuordnungen von IP-Adressen zu Geräten basierend auf der IP-Adresse ab.

**Übersicht**

| | |
|---|---|
| URI | /api/v1/token/{apiKey}/verdicts?ip={STRING} |
| HTTP-Methode | GET |

**Beschreibung**

Verwendet IP-Adressen, um entsprechende Gerätezuordnungen zurückzugeben. Sie können mehrere Zuordnungen abrufen, indem Sie eine Liste von bis zu 10 IP-Adressen bereitstellen, die durch Kommas getrennt und an den URI angehängt sind.

Wenn der Dienst keine Zuordnung finden kann, die einer IP-Adresse zugeordnet ist, gibt er keine Zuordnung für diese IP-Adresse zurück.

 ©2025 Palo Alto Networks, Inc.

**Erfolg**

Wenn die Aktion erfolgreich war, lautet der HTTP-Antwortcode 200. Zusätzlich enthält die Antwort ein JSON-Objekt mit folgenden Feldern:

| Feld | Beschreibung |
|---|---|
| count | Ganzzahl, die die Anzahl der Zuordnungen darstellt, die in der Antwort zurückge |
| verdicts | Objekt, das die Zuordnungen enthält, die in der Anfrage angegeben sind. |

Beispiel:

```
{ "count": 1, "verdicts" : [ { "ip": "10.10.10.10", "updateTime":
 1623974506, "mac": "0a:d4:5f:e9:96:10", "category": "Smartphone
 oder Tablet", "Anbieter": "Apple Inc.", "model": "iPad2", "os": "iOS
 9.3.6", "osFamily": "iOS", "profile": "iPad" } ] } }
```

**Fehler**

Wenn Fehler auftreten, wird einer der HTTP-Antwortcodes angegeben:

| Antwortcode | Beschreibung |
|---|---|
| 400 | Ungültige Anfrage. Die Anfrage war unvollständig oder fehlerhaft.<br>Korrigieren Sie die Anfrage, bevor Sie es erneut versuchen. |
| 401 | Nicht autorisiertes Token. |
| 429 | Zu viele Anfragen. Das System konnte die Anfrage nicht verarbeiten, da das Syst bestimmten Zeitraum zu viele Anfragen gestellt hat. Überschreiten Sie nicht den mehr als einer Anfrage pro Sekunde. Warten Sie und versuchen Sie es erneut. |

Darüber hinaus enthält der Antworttext die folgenden Felder:

| Feld | Beschreibung |
|---|---|
| Code | Der Fehlercode. |
| Nachricht | Die Fehlermeldung. |

## Abfrageurteil Statistiken

Ruft Statistiken über den Geräte-ID-Dienst von Drittanbietern ab.

 ©2025 Palo Alto Networks, Inc.

### Übersicht

| | |
|---|---|
| URI | /api/v1/token/{apiKey}/verdicts:statistics |
| HTTP-Methode | GET |

### Antwort bei Erfolg

Wenn die Aktion erfolgreich war, lautet der HTTP-Antwortcode 200. Zusätzlich enthält die Antwort ein JSON-Objekt mit folgenden Feldern:

| Feld | Beschreibung |
|---|---|
| Urteile | Objekt, das Statistiken über die Zuordnungen von IP-Adresse zu Gerät in Ihrem M enthält. Enthält folgende Felder:<br>• totalCount – Die Gesamtzahl der Zuordnungen von IP-Adressen zu Geräten ir<br>• totalUpdate – Die Anzahl der Zuordnungen von IP-Adressen zu Geräten, die s Erstellung aktualisiert wurden.<br>• totalDelete – Die Anzahl der Zuordnungen von IP-Adressen zu Geräten, die s Ihres Mandanten gelöscht wurden. |
| requestRcvd | Objekt, das die Anzahl der Male enthält, in denen der Mandant jede Art von Anfr<br>• update – Die Anzahl der eingegangenen Anfragen zu Urteile aktualisieren.<br>• deleteAll – Die Anzahl der eingegangenen Anfragen zu Alle Urteile löschen.<br>• query – Die Anzahl der eingegangenen Anfragen zu Abfrageurteile und Abfrag Adresse.<br>• statistics – Die Anzahl der eingegangenen Anfragen zu Abfrageurteil Statistike |

Beispiel:

```
{ "verdicts: { "totalCount": 1, "totalUpdate": 0, "totalDelete":
 0, }, "requestRcvd": { "update": 1, "deleteAll": 0, "query": 0,
 "statistics": 1 } }
```

### Antwort bei Fehler

Wenn Fehler auftreten, wird einer der HTTP-Antwortcodes angegeben:

| Antwortcode | Beschreibung |
|---|---|
| 401 | Nicht autorisiertes Token. |


©2025 Palo Alto Networks, Inc.

| | |
|---|---|
| 429 | Zu viele Anfragen. Die Anfrage konnte nicht bearbeitet werden, da in einem best<br>zu viele Anfragen gestellt wurden. Es ist nicht mehr als eine Anfrage pro Sekunde<br>Sie und versuchen Sie es erneut. |

Darüber hinaus wird in der Antwort Text in den folgenden Feldern angegeben:

| Feld | Beschreibung |
|---|---|
| Code | Der Fehlercode. |
| Nachricht | Die Fehlermeldung. |


©2025 Palo Alto Networks, Inc.

# Mehrmandantenfähigkeit von Prisma Access

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Panorama)<br>• Informationen zum Verwalten mehrerer Mandanten in Prisma Access (Managed by Strata Cloud Manager) finden Sie unter Prisma SASE. | ❑ Prisma Access-Lizenz |

Dieser Abschnitt enthält nur Informationen zur Verwaltung mehrerer Mandanten in Prisma Access (Panorama). Informationen zum Verwalten mehrerer Mandanten in Prisma Access (Managed by Strata Cloud Manager) finden Sie unter Prisma SASE.

Damit Sie mehrere Prisma Access-Instanzen erstellen und verwalten können, bietet Prisma Access Mehrmandantenfähigkeit, mit der Sie bis zu 200 Instanzen (Mandanten) auf einer einzigen Panorama-Appliance (oder auf zwei Appliances im Hochverfügbarkeitsmodus) erstellen können, wobei jeder Mandant über eigene separate Vorlagen und Vorlagenstacks, Gerätegruppen und Zugriffsdomänen verfügt.

Auf bestehende oder zukünftige Bereitstellungen, die nicht über mehrere Mandanten verfügen, hat die Mehrmandantenfähigkeit keinen Einfluss, sodass diese weiterhin normal funktionieren. Die Aktivierung der Mehrmandantenfähigkeit wird nur dann empfohlen, wenn Ihre Organisation mehrere Mandanten in Prisma Access verwalten muss.

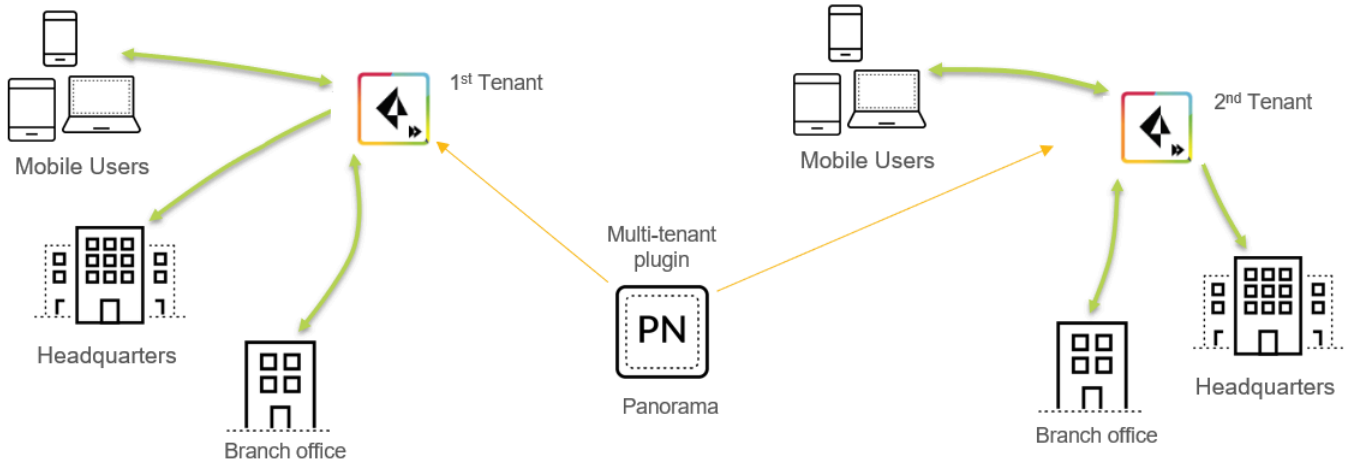
Dieser Abschnitt enthält nur die Aufgaben, die Sie ausführen, um Mandanten für Remote-Netzwerke, mobile Benutzer oder eine Kombination aus Bereitstellungen für Remote-Netzwerke und mobile Benutzer zu konfigurieren. Informationen zum Konfigurieren des Clean Pipe-Dienstes finden Sie unter Prisma Access für Clean Pipe.

# Konfiguration mit Mehrmandantenfähigkeit – Übersicht

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama)<br>• Informationen zum Verwalten mehrerer Mandanten in Prisma Access (Managed by Strata Cloud Manager) finden Sie unter Prisma SASE. | ❑ Prisma Access-Lizenz |

Mit der Aktivierung der Mehrmandantenfähigkeit können Sie mehrere Prisma Access-Instanzen auf einer einzigen Panorama-Appliance hosten. Jede Instanz wird als *Mandant* bezeichnet.

Prisma Access-Mandanten erhalten ihre eigenen dedizierten Prisma Access-Instanzen, die unter den Mandanten nicht gemeinsam verwendet werden.




Verwenden Sie den folgenden Workflow, um die Möglichkeit zu konfigurieren, mehrere Mandanten in einer einzigen Panorama-Appliance zu verwalten:

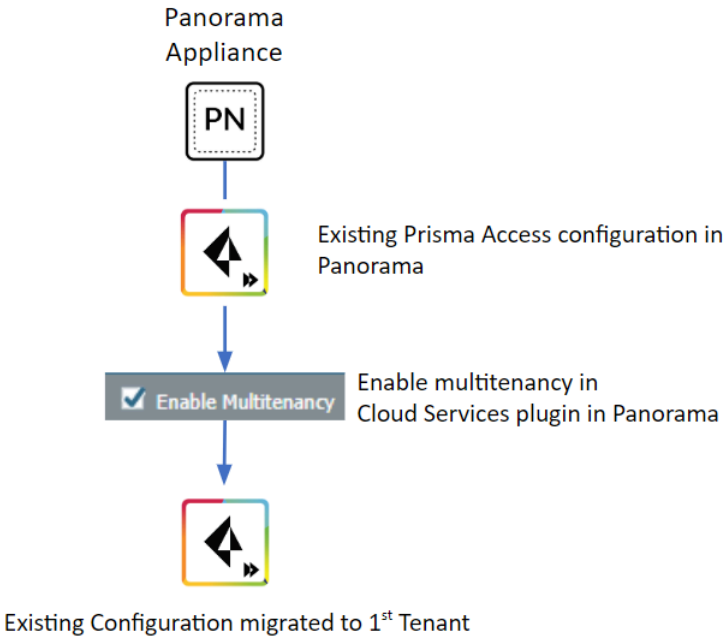
**STEP 1 |** Aktivieren Sie die Mehrmandantenfähigkeit. Wenn bereits eine Prisma Access-Instanz vorhanden ist, wird durch die Aktivierung der Mehrmandantenfähigkeit Ihre vorhandene Prisma Access-Konfiguration automatisch zum ersten Mandanten migriert.

Sie geben dem ersten (migrierten) Mandanten einen Namen und geben eine Zugriffsdomäne an. Prisma Access migriert die Vorlagen, Vorlagenstacks und Gerätegruppen, die der

 ©2025 Palo Alto Networks, Inc.

vorhandenen Konfiguration zugeordnet sind, und ordnet sie der von Ihnen erstellten Zugriffsdomäne zu.

Nachdem Sie Ihre ursprüngliche Konfiguration migriert haben, wird der administrative Benutzer in Panorama zu einem Superuser mit der Möglichkeit, alle Prisma Access-Mandanten zu erstellen und zu verwalten.




**STEP 2 |** Anschließend können Sie Mandanten zu Prisma Access hinzufügen.

Um mehrere Mandanten bereitzustellen, stellen Sie sicher, dass die folgenden Mindestanforderungen für Lizenzen erfüllt sind:

*Um den Typ der Prisma Access-Lizenz von Panorama zu bestimmen, wählen Sie **Panorama** > **Lizenzen** aus.*

- Wenn Sie über eine **Business-**, **Business Premium-**, **Zero Trust Network Access(ZTNA)-Secure Internet Gateway(SIG)-** oder **Enterprise**-Lizenz verfügen, verwenden Sie die folgenden Mindestanforderungen als Richtlinie:

  **Prisma Access für Netzwerke** und **Prisma Access für Benutzer**:

  Wenn Sie mit einer **lokalen** Edition arbeiten, ist für jeden Mandanten eine Mindestmenge von 200 Einheiten erforderlich und alle Mandanten werden lokal sein.

  Wenn Sie mit einer **weltweiten** Edition arbeiten, benötigen Sie mindestens 1.000 Einheiten, um einen **weltweiten** Mandanten zu erstellen. Wenn Sie einem Mandanten zwischen 200 und 999 Einheiten zuweisen, erstellt Prisma Access einen **lokalen** Mandanten. Wenn

 ©2025 Palo Alto Networks, Inc.

Sie einem Mandanten 1.000 oder mehr Einheiten zuweisen, erstellt Prisma Access einen **weltweiten** Mandanten.

Die *Einheiten* entsprechen der Bandbreite in Mbit/s für Prisma Access für Remote-Netzwerke und der Anzahl mobiler Benutzer für Prisma Access für Benutzer.

- Wenn Ihr Lizenztyp mit **GlobalProtect Cloud Service** beginnt, verwenden Sie die folgenden Mindestanforderungen als Richtlinie:

  **Prisma Access für Netzwerke** – Für jeden Mandanten müssen mindestens 200 Mbit/s in Ihrer Lizenz verfügbar sein.

  **Prisma Access für Benutzer** – Für jeden Mandanten müssen mindestens 200 mobile Benutzer in Ihrer Lizenz verfügbar sein.

  In beiden Prisma Access-Konfigurationstypen können Sie zusätzliche Lizenzen (oberhalb dieser Mindestanforderungen) beider Typen hinzufügen. Sie können die Bandbreite oder die Zuweisung mobiler Benutzer für beliebige Mandanten nach dem Onboarding erhöhen oder verringern, solange Sie die erforderliche Mindestzuweisung pro Mandant beibehalten und die lizenzierte Gesamtkapazität nicht überschritten wird.

Sie können eine Mehrmandantenkonfiguration nur für Remote-Netzwerke und/oder nur für mobile Benutzer einrichten. Wenn Sie Mehrmandantenfähigkeit aktivieren, weisen Sie jedem Mandanten entsprechende Lizenzen zu.

Wenn Sie eine Lizenz für Remote-Netzwerke und mobile Benutzer haben, können Sie einen individuellen Mandanten nur mit mobilen Benutzern oder nur mit Remote-Netzwerken einrichten. Wenn Ihre Prisma Access-Bereitstellung beispielsweise über eine Lizenz für die **weltweite** Edition für mobile Benutzer und Remote-Netzwerke verfügt, können Sie einen Mandanten nur für mobile Benutzer einrichten, sofern Sie für den Mandanten mindestens 1.000 mobile Benutzer angeben.

Für jeden Mandanten, den Sie nach dem ersten Mandanten erstellen, werden von Prisma Access automatisch Vorlagen, Vorlagenstacks und Gerätegruppen erstellt und der von Ihnen erstellten Zugriffsdomäne zugeordnet. Prisma Access erstellt diese Umgebung, damit Sie einen administrativen Benutzer auf Mandantenebene mithilfe einer administrativen Rolle erstellen können, die auf den Gerätegruppen und Vorlagen des Mandanten basiert, um anschließend einen administrativen Benutzer basierend auf dieser Rolle zu erstellen. Auf diese Weise erstellen Sie einen administrativen Benutzer, der Zugriff auf einen einzelnen Mandanten

 ©2025 Palo Alto Networks, Inc.

hat, ohne diesem Benutzer Zugriff auf die anderen Mandanten zu gewähren, die von der Panorama-Appliance verwaltet werden.

Prisma Access erstellt Vorlagenstacks, Vorlagen und Gerätegruppen mithilfe der folgenden Namenskonvention:

- Ein Dienstverbindungs-Vorlagenstack mit dem Namen des **sc-stk-***Mandant*, wobei *Mandant* der Name des Mandanten ist.
- Eine Dienstverbindungsvorlage mit dem Namen **sc-tpl-***Mandant*.
- Eine Dienstverbindungs-Gerätegruppe mit dem Namen **sc-dg-***Mandant*.
- Ein Vorlagenstack für mobile Benutzer mit dem Namen **mu-stk-***Mandant*.
- Eine Vorlage für mobile Benutzer mit dem Namen **mu-tpl-***Mandant*.
- Eine Gerätegruppe für mobile Benutzer mit dem Namen **mu-dg-***Mandant*.
- Ein Vorlagenstack für Remote-Netzwerke mit dem Namen **rn-stk-***Mandant*.
- Eine Vorlage für Remote-Netzwerke mit dem Namen **rn-tpl-***Mandant*.
- Eine Gerätegruppe für Remote-Netzwerkgeräte mit dem Namen **rn-dg-***Mandant*.
- Ein Vorlagenstack für expliziten Proxy mit dem Namen **ep-stk-***Mandant*.
- Eine Vorlage für expliziten Proxy mit dem Namen **ep-tpl-***Mandant*.
- Eine Gerätegruppe für expliziten Proxy mit dem Namen **ep-dg-***Mandant*.
- Ein Vorlagenstack für Clean Pipe mit dem Namen **cp-stk-***Mandant*.
- Eine Vorlage für Clean Pipe mit dem Namen **cp-tpl-***Mandant*.
- Eine Gerätegruppe für Clean Pipe mit dem Namen **cp-dg-***Mandant*.

Vorlagenstack, Vorlagen und Gerätegruppen werden für alle Prisma Access-Typen erstellt, auch für diejenigen, für die Sie möglicherweise keine Lizenz besitzen. Wenn Sie beispielsweise eine Lizenz für Remote-Netzwerke erwerben, erstellt Prisma Access automatisch Vorlagenstacks, Vorlagen und Gerätegruppen für Remote-Netzwerke, mobile Benutzer und Clean Pipe.

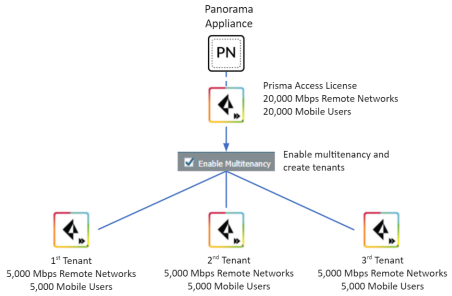
Wenn Sie benutzerdefinierte Vorlagen hinzufügen, können diese keinen Vorrang vor den von Prisma Access erstellten Vorlagen haben.

Sie weisen jedem Mandanten Lizenzressourcen für Remote-Netzwerk- und mobile Benutzer basierend auf der Lizenz zu, die dem Cloud Services-Plug-in in Panorama zugeordnet ist.

In der folgenden Abbildung ist ein Beispiel für die Prisma Access-Bereitstellung mithilfe einer Lizenz mit einem Pool mit 20.000 Mbit/s Bandbreite für Remote-Netzwerke und 20.000 mobilen Benutzern dargestellt. Der Administrator hat für die bestehende Konfiguration 5.000 Mbit/s Bandbreite für Remote-Netzwerke und 5.000 mobile Benutzer zugewiesen. Nachdem der Administrator Mehrmandantenfähigkeit aktiviert hat, wurde die Lizenzzuweisung zusammen mit allen anderen Konfigurationen zum ersten Mandanten migriert. Anschließend erstellte der Administrator weitere Mandanten, jeweils mit einem Pool von 5.000 Mbit/s Bandbreite für Remote-Netzwerke und 5.000 mobilen Benutzern für jeden Mandanten. Prisma Access weist die Lizenzressourcen aus der gesamten Lizenzzuweisung zu. Am Ende dieser

 ©2025 Palo Alto Networks, Inc.

Konfiguration stehen in der Lizenz 5.000 Mbit/s Bandbreite für Remote-Netzwerke und 5.000 mobile Benutzer zur Verfügung.




 ©2025 Palo Alto Networks, Inc.

# Mehrmandantenbereitstellung planen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama)<br>• Informationen zum Verwalten mehrerer Mandanten in Prisma Access (Managed by Strata Cloud Manager) finden Sie unter Prisma SASE. | • Prisma Access-Lizenz |

Bevor Sie Mehrmandantenfähigkeit aktivieren, müssen Sie den ersten Mandanten migrieren und zusätzliche Mandanten erstellen. Vergewissern Sie sich, dass Sie hierfür über alle erforderlichen Informationen und Ressourcen verfügen, indem Sie wie folgt vorgehen:

- Wenn Sie die Migration für eine vorhandene Einzelmandantenbereitstellung zu einer Mehrmandantenbereitstellung durchführen, notieren Sie sich die folgenden Prisma Access-Funktionen, die nicht unterstützt werden. Die Liste der nicht unterstützten Funktionen finden Sie in der Palo Alto Networks Kompatibilitätsmatrix.
- Wenn keine Prisma Access-Konfiguration vorhanden ist, wählen Sie **Mehrmandantenfähigkeit aktivieren** aus und fügen Sie Ihre Mandanten hinzu. Konfigurieren Sie anschließend die Mandanten, nachdem Sie sie erstellt haben. Weitere Informationen finden Sie unter Von Grund auf neue Bereitstellung mit mehreren Mandanten erstellen.
- Notieren Sie sich Ihre Lizenzzuordnung für Remote-Netzwerke und mobile Benutzer.

  Öffnen Sie Ihre Lizenz (**Panorama** > **Lizenzen**) und suchen Sie nach den Prisma Access-Konfigurationswerten **Mbit/s gesamt** (Bandbreitenpool für Remote-Netzwerke) für Remote-Netzwerke und **Benutzerlimit** (Gesamtanzahl lizenzierter Benutzer) für mobile Benutzer.

  Wenn Sie Mandanten erstellen, weisen Sie Ressourcen für Remote-Netzwerke und mobile Benutzer aus dieser Lizenzzuweisung zu. Wenn Sie die Mindestanforderungen an lizenzierter Bandbreite (Mbit/s) für Remote-Netzwerke oder mobile Benutzer nicht mehr erfüllen, können Sie keine zusätzlichen Mandanten erstellen.

  *Notieren Sie sich auch die Bandbreitenzuweisung und die Zuweisung mobiler Benutzer für Ihre bestehende Konfiguration. Nachdem Sie Ihre Konfiguration zum ersten Mandanten migriert haben, überprüfen Sie diese Werte, um sicherzustellen, dass der erste Mandant korrekt migriert wurde.*
- Erstellen Sie eine Liste der Namen, die Sie zum Identifizieren der einzelnen Mandanten verwenden möchten.

  *Wenn Sie Mandantennamen erstellen, vermeiden Sie es, Namen wie Mandant-1, Mandant-2, Mandant-3 usw. zu verwenden. Die Systemprotokolle reservieren eine kleine Anzahl von Zeichen für den Mandantennamen in der Protokollausgabe, und wenn Mandanten ähnliche Namen haben, kann es schwierig sein, den Mandanten den Protokollen zuzuordnen. Es wird empfohlen, für Mandanten einen eindeutigen und kurzen Namen zu verwenden (z. B. Acme oder Hooli).*


©2025 Palo Alto Networks, Inc.

- Erstellen Sie eine Liste der administrativen Benutzer, die Sie für jeden Mandanten erstellen und zuweisen werden, und notieren Sie die maximale Anzahl administrativer Benutzer, die gleichzeitig angemeldet sein können.

  Wenn administrative Benutzer normale Mehrmandantenvorgänge wie Konfigurationsänderungen und Commit-Vorgänge durchführen, wird empfohlen, die Anzahl der gleichzeitig bei Panorama angemeldeten administrativen Benutzer auf maximal 12 zu begrenzen.

  Ein administrativer Benutzer, der in der Lage ist, mehrere Mandanten zu verwalten, kann bis zu 200 Mandanten gleichzeitig mit einem einzigen Commit-Vorgang bereitstellen.
- Stellen Sie sicher, dass Sie über ausreichende Lizenzressourcen verfügen, um mehrere Mandanten zu aktivieren.

  Die Mindestlizenzzuweisung für jeden Mandanten beträgt 200 Mbit/s für jedes Remote-Netzwerk oder 200 mobile Benutzer. Sie können einen Mandanten auch nur mit Remote-Netzwerken oder mobilen Benutzern erstellen und Mandanten in verschiedenen Konfigurationen auf derselben Panorama-Instanz konfigurieren. Sie können beispielsweise einen Mandanten nur mit Remote-Netzwerken, einen Mandanten nur mit mobilen Benutzern oder einen Mandanten sowohl mit mobilen Benutzern als auch mit Remote-Netzwerken erstellen, sofern jeder Mandant die Mindestlizenzzuweisung erfüllt und die relevanten Lizenzen aktiviert und der Panorama-Instanz zugeordnet sind, in der Sie die Mandanten konfigurieren.
- Wenn Sie einen Mandanten im Mehrmandantenmodus konfigurieren, erstellen Sie für jeden IPSec-Tunnel und jedes IKE-Gateway einen eindeutigen Namen für Dienstverbindungen und Remote-Netzwerkverbindungen. Verwenden Sie nach Möglichkeit einen Namen, der nicht von einem anderen Mandanten dupliziert wird. Sie können einen IPSec-Tunnel oder ein IKE-Gateway nicht löschen, wenn ein anderer Mandant einen Tunnel oder ein Gateway mit demselben Namen verwendet.

  Dieser Vorbehalt gilt für alle Objekte, einschließlich QoS-Profile (Sie können Objekte mit doppelten Namen in einer Mehrmandantenbereitstellung nicht löschen, wenn eines der Objekte von einem anderen Mandanten referenziert wird).
- Einzelmandantenbenutzer können keine Systemprotokolle anzeigen. Dies ist Superusern vorbehalten. Sie können jedoch Protokolle nach Mandanten sortieren.
- Wenn sich ein mobiler Benutzer bei einem einzelnen Prisma Access-Mandanten anmeldet, verbraucht der Benutzer eine Lizenzeinheit. Wenn sich ein Benutzer bei weiteren Mandanten im Rahmen einer einzelnen Mehrmandantenbereitstellung anmeldet, verbraucht der Benutzer für jeden Mandanten, bei dem er angemeldet ist, eine Lizenzeinheit. Wenn beispielsweise ein einzelner Benutzer bei fünf Mandanten angemeldet ist, verbraucht der Benutzer insgesamt fünf Lizenzeinheiten für mobile Benutzer.
- Wenn Sie die Mehrmandantenfähigkeit verwenden und als administrativer Benutzer auf Mandantenebene angemeldet sind, werden beim Öffnen des Panorama-Task-Managers (klicken Sie unten in der Panorama-Weboberfläche auf **Aufgaben**) alle Aufgaben für alle Mandanten angezeigt, einschließlich aller Aufgaben, die auf Superuser-Ebene (Admin) ausgeführt wurden.
- Einige Prisma Access-Funktionen werden für die Verwendung mit Mehrmandantenfähigkeit nicht unterstützt. Weitere Informationen finden Sie unter Nicht unterstützte Funktionen für Mehrmandantenfähigkeit in der Palo Alto Networks Kompatibilitätsmatrix.

 ©2025 Palo Alto Networks, Inc.

- Wenn Sie eine Panorama-Konfiguration sichern und sie anschließend auf eine frühere gespeicherte Konfiguration zurücksetzen, kann Panorama nicht zur gespeicherten Konfiguration zurückkehren, wenn Sie die folgenden Aktionen in der folgenden Reihenfolge ausführen:

  1. Sichern Sie eine Panorama-Konfiguration.
  2. Löschen Sie einen Mandanten.
  3. Speichern Sie die Konfiguration.

  Wenn Sie einen Mandanten löschen, können Sie keine der vorherigen Sicherungen verwenden, die Sie vor dem Löschen des Mandanten gespeichert haben. Sie können jedoch alle Backups verwenden, die Sie nach dem Löschen des Mandanten erstellen.

 ©2025 Palo Alto Networks, Inc.

# Von Grund auf neue Bereitstellung mit mehreren Mandanten erstellen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama)<br>• Informationen zum Verwalten mehrerer Mandanten in Prisma Access (Managed by Strata Cloud Manager) finden Sie unter Prisma SASE. | ❑ Prisma Access-Lizenz |

Wenn Sie eine Bereitstellung mit mehreren Mandanten erstellen möchten und keine Prisma Access-Konfiguration vorhanden ist, können Sie **Mehrmandantenfähigkeit aktivieren** auswählen und Ihre Mandanten hinzufügen. Anschließend konfigurieren Sie die Mandanten.

*Wenn Sie über eine bestehende Bereitstellung mit eine Mandanten verfügen und zu einer Bereitstellung mit mehreren Mandanten migrieren möchten, verwenden Sie den Workflow, um* Mehrmandantenfähigkeit zu aktivieren und den ersten Mandanten zu migrieren.

Wenn Sie den ersten Mandanten ohne vorhandene Konfiguration erstellen, beachten Sie die folgenden Unterschiede und Richtlinien:

- Da keine Konfiguration zum Verschieben vorhanden ist, erstellt Prisma Access Vorlagen, Vorlagenstacks und Gerätegruppen für jeden Mandanten und ordnet sie der Zugriffsdomäne zu, die Sie beim Erstellen der Mandanten erstellen. Informationen zur Namenskonvention, die Prisma Access verwendet, finden Sie unter Konfiguration mit Mehrmandantenfähigkeit – Übersicht.
- Optional können Sie nach dem Erstellen der Zugriffsdomäne auf Mandantenebene einen administrativen Benutzer erstellen, der die Verwaltung für einen einzelnen Mandanten ermöglicht, indem Sie der Zugriffsdomäne einen Administrator zuordnen.
- Wenn Sie über vorhandene Vorlagen oder Gerätegruppen verfügen (z. B. Vorlagen von einem lokalen Gerät, das von Panorama verwaltet wird und auch von Prisma Access verwendet werden soll), fügen Sie diese Gerätegruppen und Vorlagendomänen beim Erstellen und Konfigurieren der **Zugriffsdomäne** hinzu. Wenn Sie der Zugriffsdomäne keine Gerätegruppen und Vorlagen hinzufügen, können Sie diese beim Konfigurieren der Prisma Access-Komponenten im Cloud Services-Plug-in nicht anzeigen oder auswählen.

 ©2025 Palo Alto Networks, Inc.

# Mehrmandantenfähigkeit aktivieren und den ersten Mandanten migrieren

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama)<br>• Informationen zum Verwalten mehrerer Mandanten in Prisma Access (Managed by Strata Cloud Manager) finden Sie in Prisma SASE. | ❑ Prisma Access-Lizenz |

Verwenden Sie den folgenden Workflow, um Mehrmandantenfähigkeit zu aktivieren und Ihre vorhandene Konfiguration auf den ersten Mandanten zu migrieren, den Sie erstellen. Wenn Sie keine vorhandene Konfiguration haben, können Sie Mehrmandantenfähigkeit aktivieren und Ihre Mandanten hinzufügen und diese dann konfigurieren.

Wenn Sie Mehrmandantenfähigkeit aktivieren, migriert Prisma Access die folgenden Komponenten Ihrer Konfiguration:

- Alle Onboarding-Informationen zu Dienstverbindungen und Remote-Netzwerktunneln, einschließlich Tunnelkonfiguration.
- Onboarding-Informationen zu vorhandenen mobilen Benutzern.
- Strata Logging Service-Informationen.
- Vorhandene Autonomous DEM (ADEM)-Konfiguration
- Die Vorlagen, Vorlagenstacks und Gerätegruppen für Dienstverbindungen, Remote-Netzwerke und mobile Benutzer.

Sie müssen die Anzahl der Benutzer (für eine Bereitstellung für mobile Benutzer), die Bandbreite (für eine Bereitstellung für Remote-Netzwerke) und Autonomous DEM (ADEM) angeben, die für jede Bereitstellung zugewiesen werden sollen (wenn Sie eine ADEM-Lizenz erworben haben).

Aufgrund dieser Gerätegruppenänderungen erstellen Sie eine Zugriffsdomäne und fügen die migrierten Gerätegruppen, Vorlagen und Vorlagenstacks hinzu, wie im folgenden Workflow gezeigt.

*Wenn Sie keine vorhandene Prisma Access-Konfiguration haben und eine völlig neue Mehrmandantenbereitstellung erstellen, verwenden Sie diesen Workflow nicht. Führen Sie stattdessen die Schritte in Mandanten zu Prisma Access hinzufügen aus, um den ersten Mandanten zu erstellen.*


©2025 Palo Alto Networks, Inc.

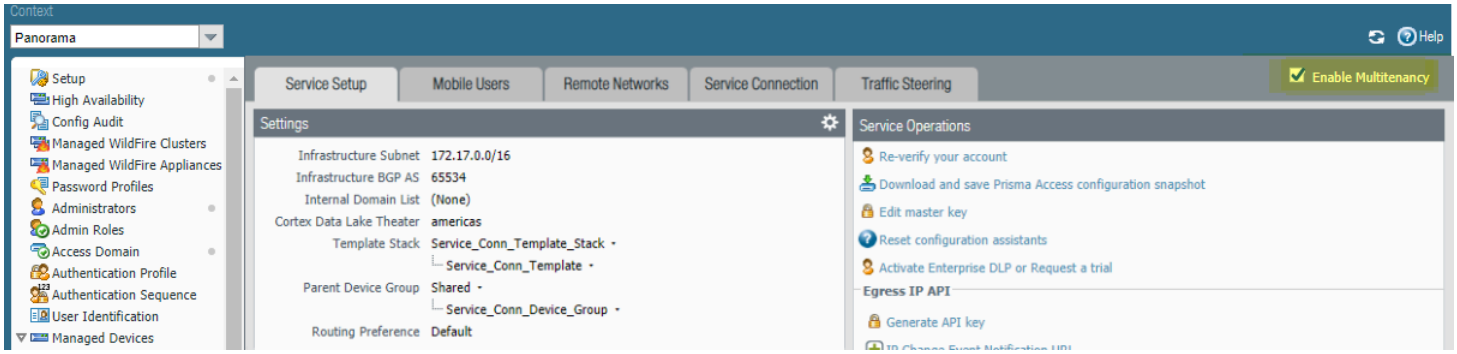
**STEP 1 |** Bestimmen Sie die Anzahl der lizenzierten Einheiten, die Sie dieser Bereitstellung zuweisen möchten.

Während Prisma Access Ihre Konfiguration zum ersten Mandanten migriert, müssen Sie Folgendes angeben:

- Die **Bandbreite**, die für die Bereitstellung für Remote-Benutzer des Mandanten zugewiesen werden soll (falls zutreffend).
- Die **Benutzer**, die für die Bereitstellung für mobile Nutzer des Mandanten zugewiesen werden sollen (falls zutreffend).
- Anzahl der ADEM-Einheiten, die für mobile Nutzungen und Remote-Netzwerke (falls zutreffend) zugewiesen werden sollen.

**STEP 2 |** Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** aus.

**STEP 3 |** Wählen Sie **Mehrmandantenfähigkeit aktivieren** aus (oben rechts auf der Seite).




Nachdem Sie Mehrmandantenfähigkeit aktiviert haben, zeigt Panorama eine Benachrichtigung an, in der Sie darüber informiert werden, dass die vorhandene Prisma Access-Konfiguration zum ersten Mandanten wechselt.

*Nachdem Sie Mehrmandantenfähigkeit aktiviert haben, ändert sich Ihre Bereitstellung dauerhaft in eine Mehrmandantenbereitstellung und Sie können nicht in den Einzelmandantenmodus zurückkehren.*

**STEP 4 |** Klicken Sie auf **OK**, um die vorhandene Konfiguration zum ersten Mandanten zu migrieren.

Die Seite **Mandanten** wird angezeigt, mit Tortendiagrammen in der Mitte des Fensters.

- Wenn Sie über eine Lizenz für Remote-Netzwerke oder mobile Benutzer verfügen, werden die verfügbare Menge an lizenzierter Remote-Netzwerkbandbreite und mobilen Benutzern angezeigt.
- (Nur Bereitstellungen für Remote-Netzwerke und mobile Benutzer) Wenn Sie eine Autonomous DEM-Lizenz erworben haben, wird die verfügbare Anzahl von Einheiten für ADEM-Verwendungen angezeigt.
- Wenn Sie eine Clean Pipe-Bereitstellung haben, wird die Bandbreite für den Mandanten angezeigt.

 ©2025 Palo Alto Networks, Inc.

**STEP 5 |** Wählen Sie den Typ der Bereitstellung aus, die Sie für den Mandanten verwenden möchten.

- Wählen Sie für eine Bereitstellung für Remote-Netzwerke/mobile Benutzer oder zum Konfigurieren beider Bereitstellungstypen für einen Mandanten **Remote-Netzwerke/ Mobile Benutzer** aus.
- Wählen Sie für eine Clean Pipe-Bereitstellung **Clean Pipe** aus.

  In diesem Abschnitt wird nur beschrieben, wie Sie Mandanten für Bereitstellungstypen für Remote-Netzwerke, für mobile Benutzer oder sowohl für Remote-Netzwerke als auch für mobile Benutzer konfigurieren. Informationen zum Konfigurieren des Clean Pipe-Dienstes finden Sie unter Prisma Access für Clean Pipe.

 ©2025 Palo Alto Networks, Inc.

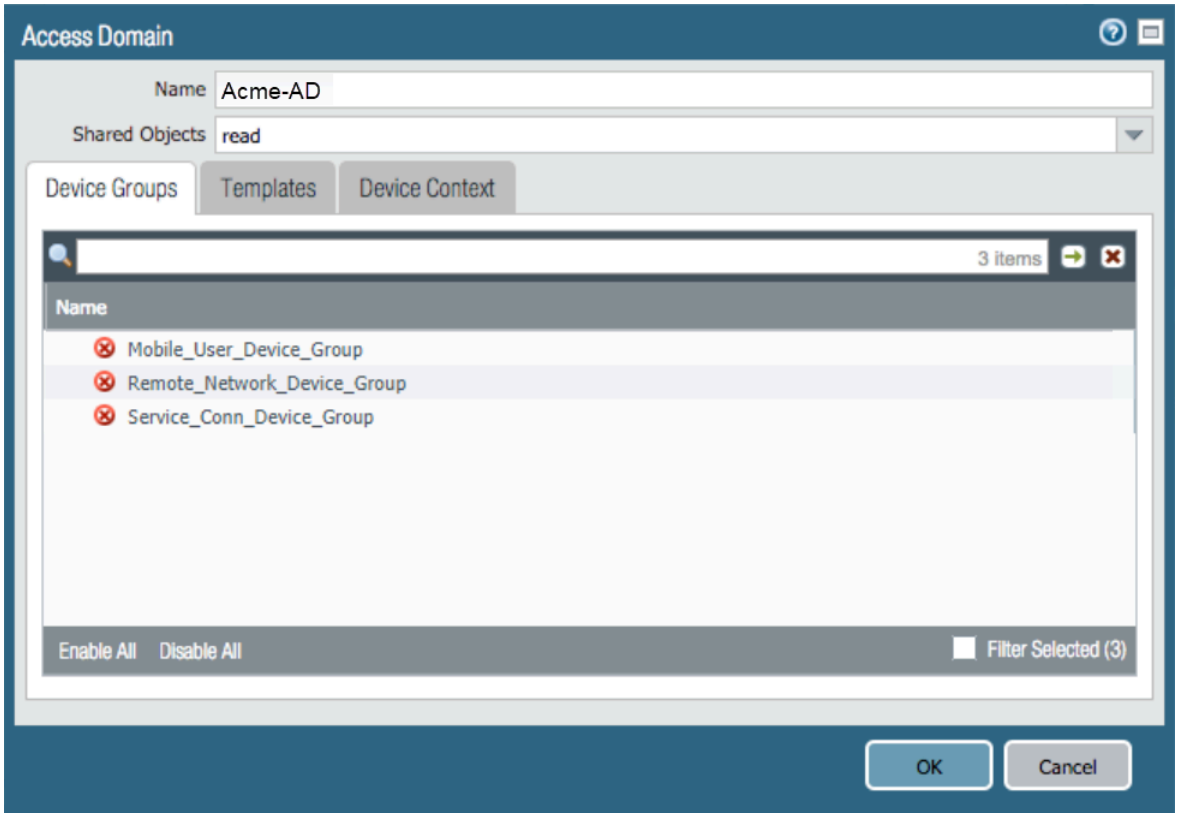
**STEP 6 |** Migrieren Sie die vorhandene Konfiguration zum ersten Mandanten.

Der Name des ersten migrierten Untermandanten wird automatisch vom Mandanten ausgefüllt, den Sie migrieren, und kann nicht bearbeitet werden.

1. Erstellen Sie eine neue **Zugriffsdomäne**, indem Sie auf den Abwärtspfeil klicken und **Neue Zugriffsdomäne** auswählen.
2. Geben Sie einen **Namen** für die Zugriffsdomäne ein und klicken Sie auf **OK**.

   Prisma Access fügt der neuen Zugriffsdomäne die **Gerätegruppen Mobile_User_Device_Group**, **Remote_Network_Device_Group** und **Service_Conn_Device_Group** hinzu.

   Ordnen Sie die Standardgerätegruppen und #vorlagen keinen anderen Untermandanten als dem ersten migrierten Untermandanten zu.

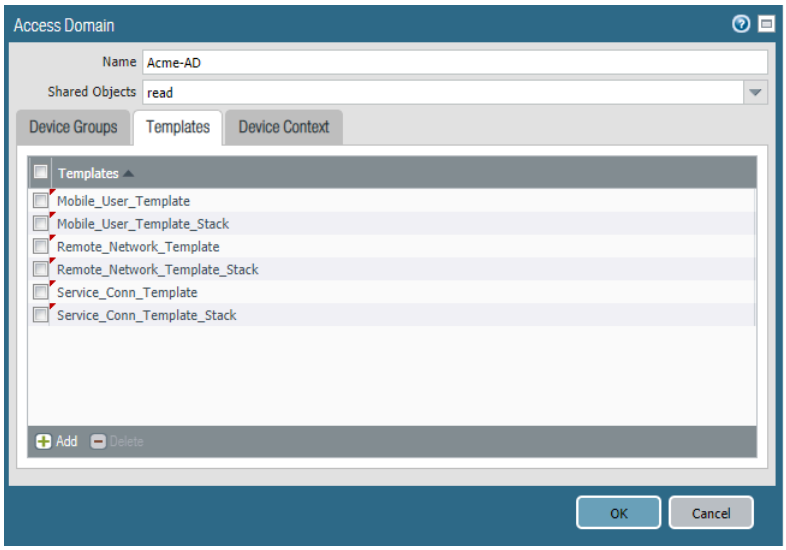



3. (Optional) Klicken Sie auf **Vorlagen**, um zu überprüfen, ob Prisma Access die folgenden Vorlagen und Vorlagenstacks hinzugefügt hat:
   - **Explicit_Proxy_Template**
   - **Explicit_Proxy_Template_Stack**
   - **Mobile_User_Template**
   - **Mobile_User_Template_Stack**
   - **Remote_Network_Template**
   - **Remote_Network_Template_Stack**
   - **Service_Conn_Template**

 ©2025 Palo Alto Networks, Inc.

- **Service_Conn_Template_Stack**

  Dies sind die Standardvorlagenstacks und #vorlagen für eine Standardbereitstellung von Prisma Access. Wenn Sie andere Vorlagen hinzugefügt haben, stellen Sie sicher, dass Prisma Access diese hinzugefügt hat.



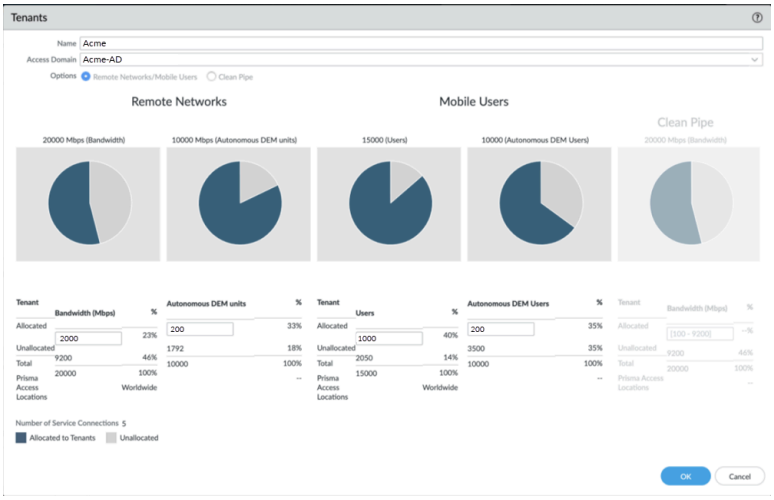

4. (Optional) Wenn Sie andere Vorlagen haben, die dieser Konfiguration zugeordnet sind, wählen Sie sie aus.
5. Klicken Sie auf **OK**, um die Seite **Zugriffsdomäne** zu schließen und zur Seite **Mandanten** zurückzukehren.

 ©2025 Palo Alto Networks, Inc.

**STEP 7 |** Geben Sie die Werte in **Bandbreite (Mbit/s)** für Remote-Netzwerke, **Benutzer** für mobile Benutzer und die Anzahl der **Autonomous DEM-Benutzer** ein, die Sie für jeden Bereitstellungstyp zuweisen möchten.

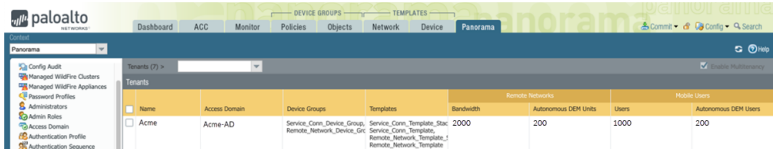
Verwenden Sie bei der Zuweisung von ADEM-Einheiten für einen Mandanten die folgenden Richtlinien:

- Die Anzahl der ADEM-Einheiten, die Sie für mobile Benutzer und Remote-Netzwerke zuweisen können, muss kleiner oder gleich der Angaben der Basislizenz sein.
- Die Mindestanzahl der Einheiten, die Sie zuweisen können, liegt bei 200.
- Nachdem Sie die ADEM-Einheiten für einen Mandanten zugewiesen haben, können Sie diese Einheiten bearbeiten oder entfernen.
- Wenn Sie keine ADEM-Lizenz für Ihren Bereitstellungstyp (Mobile Benutzer oder Remote-Netzwerke) erworben haben, wird diese Option abgeblendet dargestellt.




**STEP 8 |** Klicken Sie auf **OK**.

Auf der Seite **Panorama** > **Cloud Services** > **Konfiguration** wird der erste Mandant angezeigt, der erfolgreich migriert wurde, und über dem Bereich **Mandanten** wird das Dropdown-Menü **Mandanten** hinzugefügt.




 ©2025 Palo Alto Networks, Inc.

**STEP 9 |** Stellen Sie sicher, dass alle Vorlagen und Gerätegruppen für den Mandanten ausgefüllt wurden.

1. Wählen Sie den Mandanten aus der Dropdown-Liste aus.
2. Gehen Sie zu **Panorama** > **Cloud Services** > **Konfiguration**.
3. Wählen Sie **Diensteinrichtung** aus.
4. Klicken Sie auf das Zahnrad, um die **Einstellungen** zu bearbeiten.
5. Stellen Sie sicher, dass der richtige Vorlagenstack, die richtige Vorlage und die richtige Gerätegruppe (Service_Conn_Template_Stack, Service_Conn_Template bzw. Service_Conn_Device_Group) in den Einstellungen eingegeben wurden.
6. Wechseln Sie zu den Registerkarten, für die Sie bereits eine Konfiguration haben (z. B. **Mobile Benutzer – GlobalProtect**, **Mobile Benutzer – Expliziter Proxy**, **Remote-Netzwerke** oder **Dienstverbindung**), klicken Sie auf das Zahnrad, um die **Einstellungen** zu bearbeiten, und stellen Sie sicher, dass der richtige Vorlagenstack, die richtige Vorlage und die richtige Gerätegruppe eingegeben wurden.

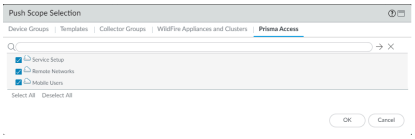
**STEP 10 |** Schreiben Sie Ihre Änderungen lokal in Panorama fest (**Commit** > **Commit in Panorama**).

**STEP 11 |** Wählen Sie **Commit** > **Commit in Panorama** aus, um Ihre Änderungen lokal auf dem Panorama zu speichern, das Prisma Access verwaltet.

Wenn Sie keinen lokalen Commit durchführen, werden Prisma Access-Komponenten beim Commit und Push Ihrer Änderungen nicht im Übertragungsumfang angezeigt.

**STEP 12 |** Führen Sie die Aktion „Commit und Push“ aus, um Ihre Änderungen festzuschreiben und zu übertragen und sie so in Prisma Access zu aktivieren.

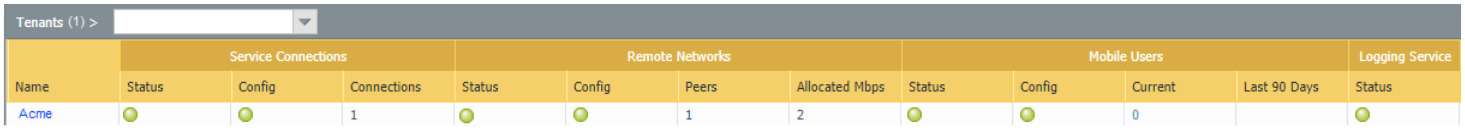
1. Wählen Sie **Commit** > **Commit und Push** und **Auswahl bearbeiten** im Übertragungsumfang aus.
2. Wählen Sie **Prisma Access**, dann den von Ihnen erstellten Mandanten und **Diensteinrichtung**, **Remote-Netzwerke** und **Mobile Benutzer** aus.




3. Klicken Sie auf **OK**, um Ihre Änderungen im Übertragungsumfang zu speichern.
4. Führen Sie einen **Commit** aus und übertragen Sie die Änderung per **Push**.

**STEP 13 |** Wählen Sie **Panorama** > **Cloud Services** > **Status** aus.

Die Statusseite zeigt den Status aller Mandanten. Da Sie nur einen Mandanten erstellt haben, wird nur dieser Mandant angezeigt. Wenn Sie diesen Mandanten aus dem Dropdown-Menü auswählen, sehen Sie einen detaillierten Status dieses Mandanten.




| | Service Connections | | | Remote Networks | | | | Mobile Users | | | | Logging Service |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Name | Status | Config | Connections | Status | Config | Peers | Allocated Mbps | Status | Config | Current | Last 90 Days | Status |
| Acme | | | 1 | | | 1 | 2 | | | 0 | | |

Wenn Sie einen Mandanten aus dem Dropdown-Menü auswählen, gelangen Sie zur Statusseite für diesen Mandanten.

 ©2025 Palo Alto Networks, Inc.

**STEP 14 |** Fügen Sie weitere Mandanten zu Prisma Access hinzu.

 ©2025 Palo Alto Networks, Inc.

# Mandanten zu Prisma Access hinzufügen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama)<br>• Informationen zum Verwalten mehrerer Mandanten in Prisma Access (Managed by Strata Cloud Manager) finden Sie in Prisma SASE. | ❑ Prisma Access-Lizenz |

Nachdem Sie die vorhandenen Informationen für den ersten Mandanten migriert haben, können Sie weitere Mandanten erstellen und konfigurieren. Für jeden Mandanten, den Sie nach dem ersten Mandanten erstellen, erstellt Prisma Access eine separate Zugriffsdomäne mit eigenen Gruppen von Vorlagenstacks und Vorlagen sowie eigenen Domänengruppen.

Verwenden Sie diesen Workflow, um weitere Mandanten zu Prisma Access hinzuzufügen.

*Wenn Sie eine völlig neue Bereitstellung mit mehreren Mandanten erstellen, verwenden Sie diesen Workflow, um den ersten Mandanten sowie weitere Mandanten hinzuzufügen. Weitere Informationen finden Sie unter* Von Grund auf neue Bereitstellung mit mehreren Mandanten erstellen.

**STEP 1 |** Melden Sie sich bei Panorama als Superuser an.

**STEP 2 |** Fügen Sie den Mandanten hinzu und konfigurieren Sie ihn.

1. Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** aus und dann die Option **Hinzufügen**, um einen neuen Mandanten hinzuzufügen.

   Vergewissern Sie sich, dass **Remote-Netzwerke/Mobile Benutzer** ausgewählt wurde; zum Erstellen und Konfigurieren einer Clean Pipe-Bereitstellung siehe Prisma Access für Clean Pipe.
2. Geben Sie unter **Name** einen aussagekräftigen Namen für den Mandanten an.
3. Fügen Sie durch Auswahl von **Hinzufügen** eine neue **Zugriffsdomäne** hinzu, ordnen Sie ihr unter **Name** einen aussagekräftigen Namen zu und klicken Sie dann auf **OK**, um zum Fenster **Mandanten** zurückzukehren.

   Nachdem Sie auf **OK** geklickt haben, erstellt Prisma Access automatisch Vorlagen, Vorlagenstacks und Gerätegruppen und ordnet diese der von Ihnen erstellten Zugriffsdomäne zu.

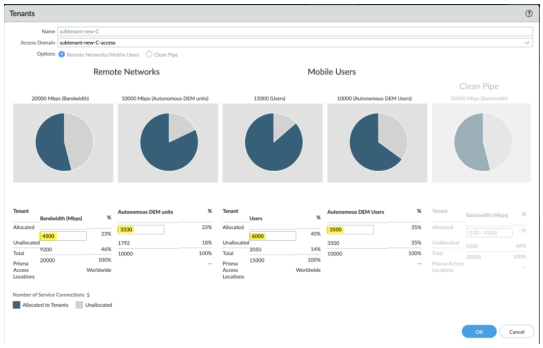
**STEP 3 |** Geben Sie die **Bandbreite (Mbit/s)** an, die den **Remote-Netzwerken** zugewiesen werden soll. Geben Sie außerdem unter **Benutzer** die Anzahl der Benutzer an, die für **Mobile Benutzer** zugewiesen werden sollen.

 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** (Nur Bereitstellungen mit Autonomous DEM) Wenn Sie eine Lizenz für Autonomous DEM (ADEM) erworben haben, wählen Sie die Anzahl der Einheiten aus, die für ADEM zugewiesen werden sollen.

Verwenden Sie bei der Zuweisung von ADEM-Einheiten für einen Mandanten die folgenden Richtlinien:

- Die Anzahl der ADEM-Einheiten, die Sie für mobile Benutzer und Remote-Netzwerke zuweisen können, muss kleiner oder gleich der Angaben der Basislizenz sein.
- Die Mindestanzahl der Einheiten, die Sie zuweisen können, beträgt 200.
- Nachdem Sie die ADEM-Einheiten für einen Mandanten zugewiesen haben, können Sie diese Einheiten bearbeiten oder entfernen.
- Wenn Sie keine ADEM-Lizenz für Ihren Bereitstellungstyp (Mobile Benutzer oder Remote-Netzwerke) erworben haben, wird diese Option abgeblendet dargestellt.

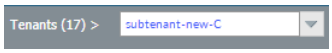



**STEP 5 |** Klicken Sie auf **OK**, um den ersten Mandanten zu erstellen.

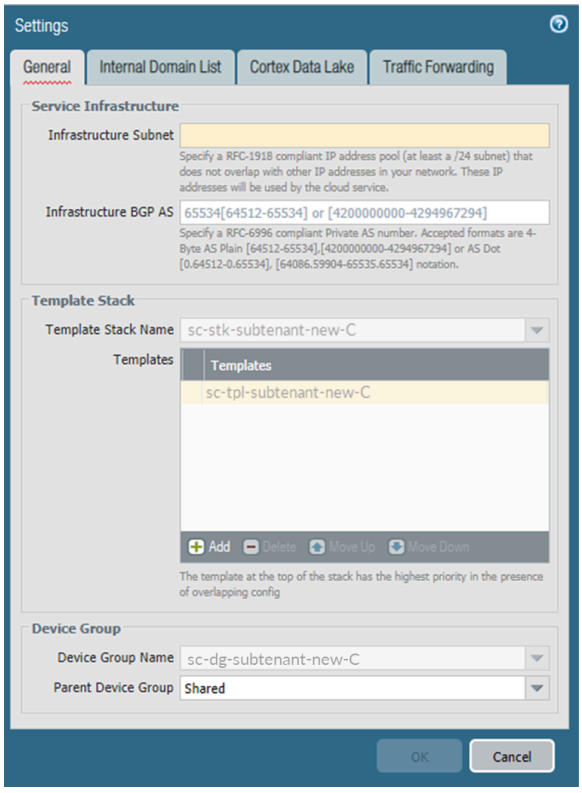
 ©2025 Palo Alto Networks, Inc.

**STEP 6 |** Stellen Sie sicher, dass Prisma Access die Angaben für den Vorlagenstack, die Vorlage und die Diensteinstellungen der Gerätegruppe auf die Dienstverbindungseinstellungen des soeben erstellten Mandanten angewendet hat.

1. Wählen Sie im Dropdown-Menü **Mandant** den Mandanten aus, den Sie erstellt haben.



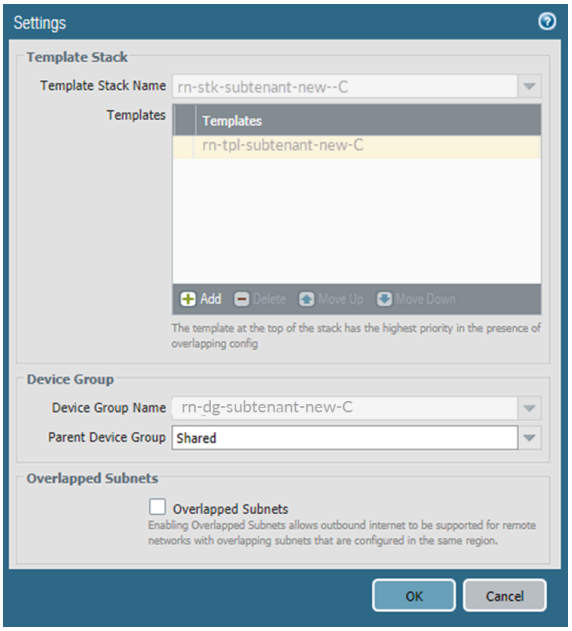

2. Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Diensteinrichtung** aus.
3. Klicken Sie auf das Zahnradsymbol rechts neben dem Bereich **Einstellungen**, um die Einstellungen zu bearbeiten.
4. Vergewissern Sie sich, dass Prisma Access den Vorlagenstack (**sc-stk-***mandant*), die Vorlage (**sc-tpl-***mandant*) und die Gerätegruppe (**sc-dg-***mandant*) Ihren Dienstverbindungseinstellungen zugeordnet hat.
5. Überprüfen Sie, ob die **Übergeordnete Gerätegruppe** auf **Freigegeben** eingestellt ist, und klicken Sie dann auf **OK**.




 ©2025 Palo Alto Networks, Inc.

**STEP 7 |** Stellen Sie sicher, dass Prisma Access den Vorlagenstack, die Vorlage und die Gerätegruppe auf die Einstellungen des Remote-Netzwerks angewendet hat.

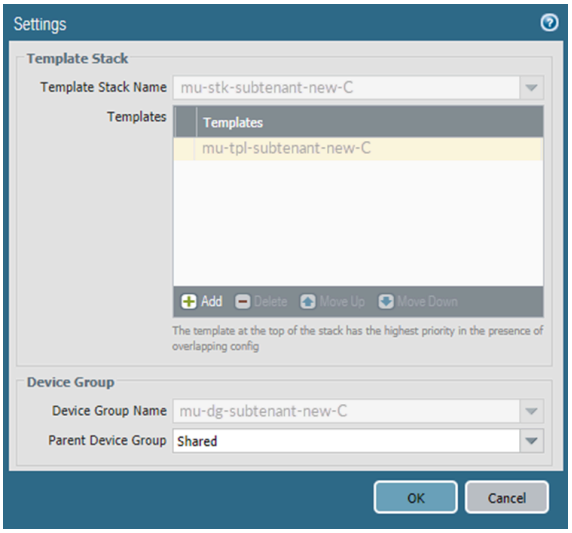
1. Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Remote-Netzwerke** aus und klicken Sie dann auf das Zahnradsymbol rechts neben dem Bereich **Einstellungen**, um die Einstellungen zu bearbeiten.
2. Stellen Sie sicher, dass Prisma Access den Vorlagenstack (**rn-stk-***mandant*), die Vorlage (**rn-tpl-***mandant*) und die Gerätegruppe (**rn-dg-***mandant*) den Einstellungen Ihres Remote-Netzwerks zugeordnet hat.
3. Überprüfen Sie, ob die **Übergeordnete Gerätegruppe** auf **Freigegeben** eingestellt ist, und klicken Sie dann auf **OK**.




 ©2025 Palo Alto Networks, Inc.

**STEP 8 |** Stellen Sie sicher, dass Prisma Access den Vorlagenstack, die Vorlage und die Gerätegruppe auf die Einstellungen des mobilen Benutzers angewendet hat.

1. Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Mobile Benutzer** aus und klicken Sie dann auf das Zahnradsymbol rechts neben dem Bereich **Einstellungen**, um die Einstellungen zu bearbeiten.
2. Überprüfen Sie, ob Prisma Access den Vorlagenstack (**mu-stk-***mandant*), die Vorlage (**mu-tpl-***mandant*) und die Gerätegruppe (**mu-dg-***mandant*) den Einstellungen Ihres Remote-Netzwerks zugeordnet hat.
3. Überprüfen Sie, ob die **Übergeordnete Gerätegruppe** auf **Freigegeben** eingestellt ist, und klicken Sie dann auf **OK**.




**STEP 9 |** Schreiben Sie Ihre Änderungen lokal in Panorama fest (**Commit** > **Commit in Panorama**).

**STEP 10 |** (Nur Bereitstellungen für mobile Benutzer) – Fügen Sie ein Infrastruktursubnetz hinzu, schreiben Sie anschließend Ihre Änderungen fest und übertragen Sie sie mit „Commit und Push“, um sie in Prisma Access zu aktivieren.

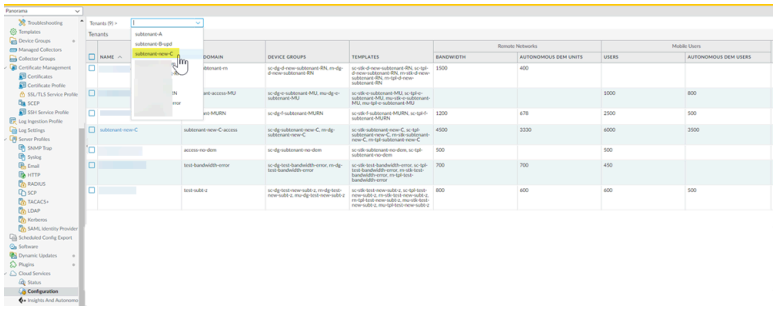
Diese Schritte sind erforderlich, damit die Änderungen für mobile Benutzer wirksam werden.

1. Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Diensteinrichtung** aus und klicken Sie dann auf das Zahnradsymbol, um die Einstellungen zu bearbeiten und ein Infrastruktursubnetz zu konfigurieren.
2. Wählen Sie **Commit** > **Commit und Push**, **Ausgewählte Optionen bearbeiten** im Übertragungsumfang aus und vergewissern Sie sich, dass **Mobile Benutzer** ausgewählt wurde.
3. Klicken Sie auf **OK**, um Ihre Änderungen im Übertragungsumfang zu speichern.
4. Führen Sie die Aktion **Commit** und **Push** aus, um Ihre Änderungen festzuschreiben und zu übertragen.

 ©2025 Palo Alto Networks, Inc.

**STEP 11 |** Wählen Sie den neuen Mandanten aus, indem Sie **Panorama** > **Cloud Services** > **Konfiguration** > ***Mandantenname*** auswählen, und setzen Sie die Konfiguration Ihres Mandanten fort.

1. Konfigurieren der Serviceinfrastruktur.
2. Erstellen Sie eine Dienstverbindung, um den Zugriff auf private Apps zu ermöglichen.
3. Führen Sie für die Remote-Netzwerke ein Onboarding und eine Konfiguration durch, wenn Sie über eine Lizenz für Remote-Netzwerke verfügen.
4. Richten Sie für Prisma Access (Managed by Panorama) Global Protect ein, wenn Sie über eine Lizenz für Remote-Benutzer verfügen.



 ©2025 Palo Alto Networks, Inc.

# Mandanten löschen

Löschen Sie einen Mandanten in einer Prisma Access (Managed by Panorama)-Bereitstellung, indem Sie die folgenden Schritte ausführen.

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Panorama)<br>• Informationen zum Verwalten mehrerer Mandanten in Prisma Access (Managed by Strata Cloud Manager) finden Sie unter Prisma SASE. | ❑ Prisma Access-Lizenz |

- *Während Sie alle Mandanten in einer Bereitstellung mit mehreren Mandanten löschen können, ist es nicht möglich, die Prisma Access-Konfiguration auf Administratorebene zu löschen, in der Sie Mandanten hinzufügen oder löschen.*
- *Wenn Sie einen Mandanten löschen, löscht Prisma Access die Vorlagen- und Gerätegruppe, für die Sie lizenziert sind, nicht jedoch den nicht lizenzierten Satz. Wenn Sie z. B. über eine Prisma Access-Lizenz für Benutzer verfügen und einen Mandanten löschen, löscht Prisma Access die auf die mobilen Benutzer bezogenen Vorlagenstacks, Vorlagen und Gerätegruppen, nicht jedoch den Satz, der für das nicht lizenzierte Prisma Access für Netzwerke erstellt wurde. Sie können diese nicht verwendeten Vorlagen- und Gerätegruppensätze manuell löschen, nachdem Sie den Mandanten gelöscht haben.*

**STEP 1 |** Wählen Sie in der Panorama-Instanz, die Prisma Access verwaltet, **Panorama** > **Cloud Services** > **Konfiguration** aus.

**STEP 2 |** Wählen Sie den Mandanten aus und löschen Sie alle ihm zugeordneten Konfigurationen.

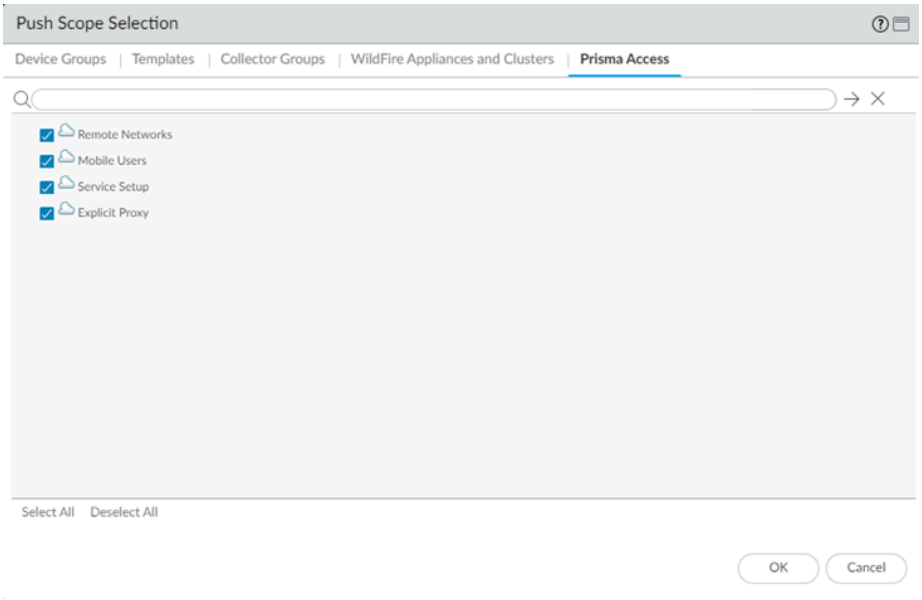
Führen Sie diesen Schritt als bewährte Methode aus, um sicherzustellen, dass alle Konfigurationen aus dem Mandanten gelöscht werden – einschließlich aller Konfigurationen für Dienstverbindungen, mobile Benutzer, Remote-Netzwerke oder Clean Pipe.

**STEP 3 |** Führen Sie einen Commit aus, und übertragen Sie die Änderungen per Push an Prisma Access.

1. Wählen Sie **Commit** > **An Geräte übertragen** aus.
2. Wählen Sie **Auswahl bearbeiten** aus und stellen Sie sicher, dass alle Komponenten, die Sie gelöscht haben (einschließlich „Remote-Netzwerke“, „Mobile Benutzer“,

 ©2025 Palo Alto Networks, Inc.

„Diensteinrichtung“, „Expliziter Proxy“ und „Clean Pipe“, je nach Bereitstellung), ausgewählt sind.




3. Klicken Sie auf **Push**.

**STEP 4 |** Wählen Sie einen oder mehrere Mandanten aus, und klicken Sie dann auf **Löschen**.

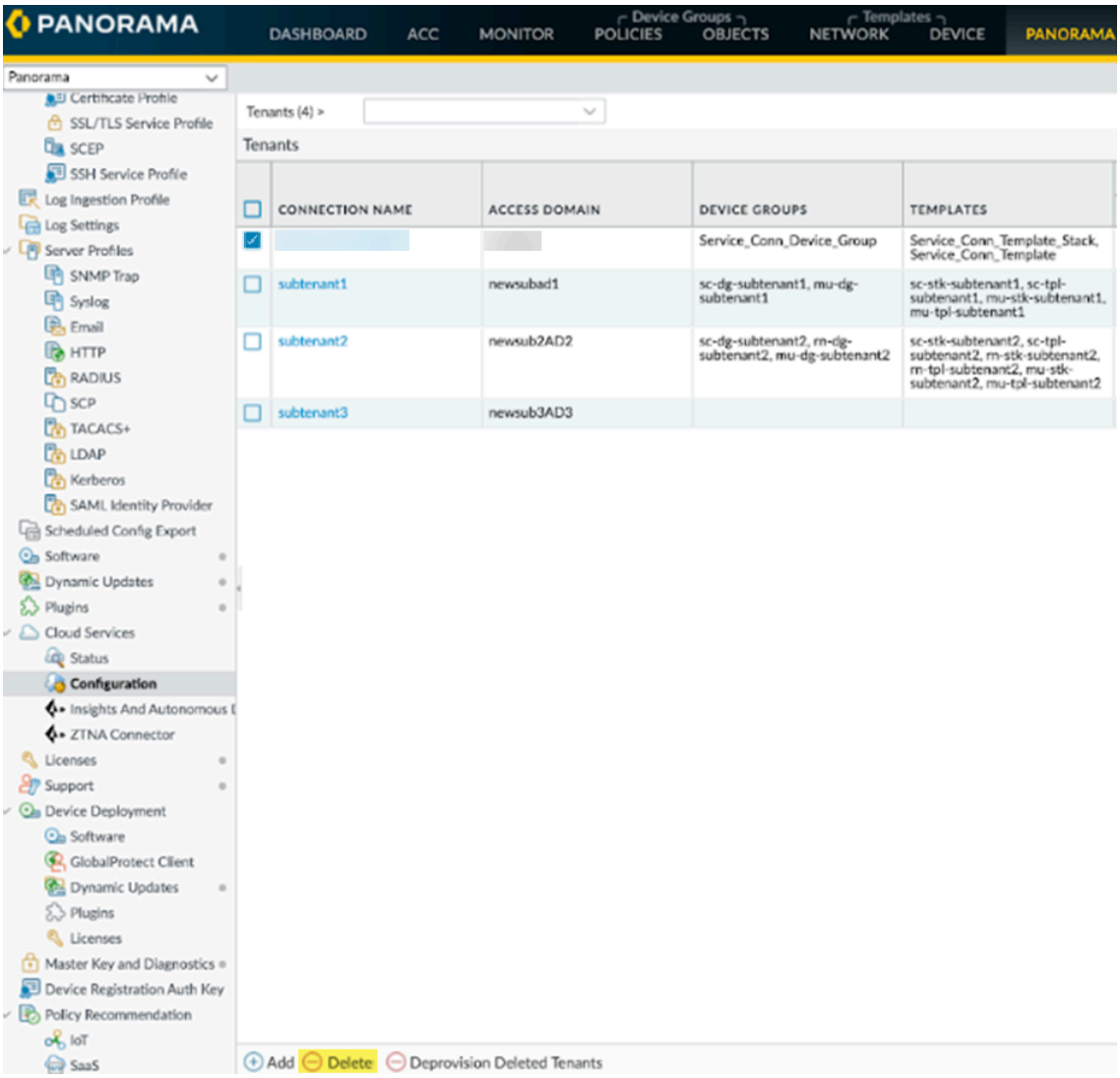
Durch das Löschen eines Mandanten wird der Mandant aus Panorama entfernt, nicht jedoch aus der Infrastruktur von Prisma Access. Um einen Mandanten zu löschen und aus der

 ©2025 Palo Alto Networks, Inc.

Infrastruktur zu entfernen, müssen Sie ihn löschen, einen lokalen Commit ausführen und anschließend die Bereitstellung aufheben, wie in den folgenden Schritten veranschaulicht.

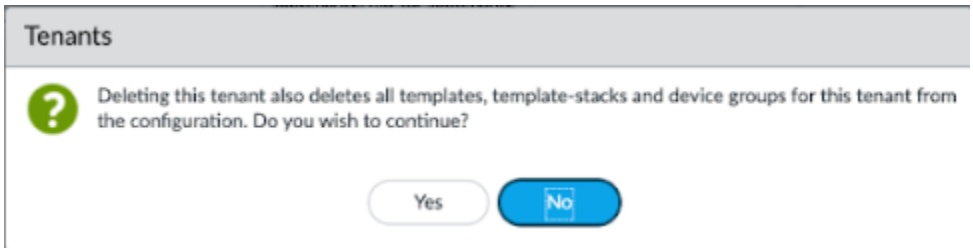
Wenn Sie den Mandanten löschen, aber die Bereitstellung nicht aufheben, können Sie ihn weiterhin abrufen, indem Sie sich an den Support von Palo Alto Networks wenden.

*Wenn Sie Ihre Panorama-Instanzen in einer HA-Konfiguration eingerichtet haben, führen Sie die Aktionen zum Löschen und Aufheben der Bereitstellung aus der aktiven Panorama-Instanz nur in einem HA-Paar aus.*



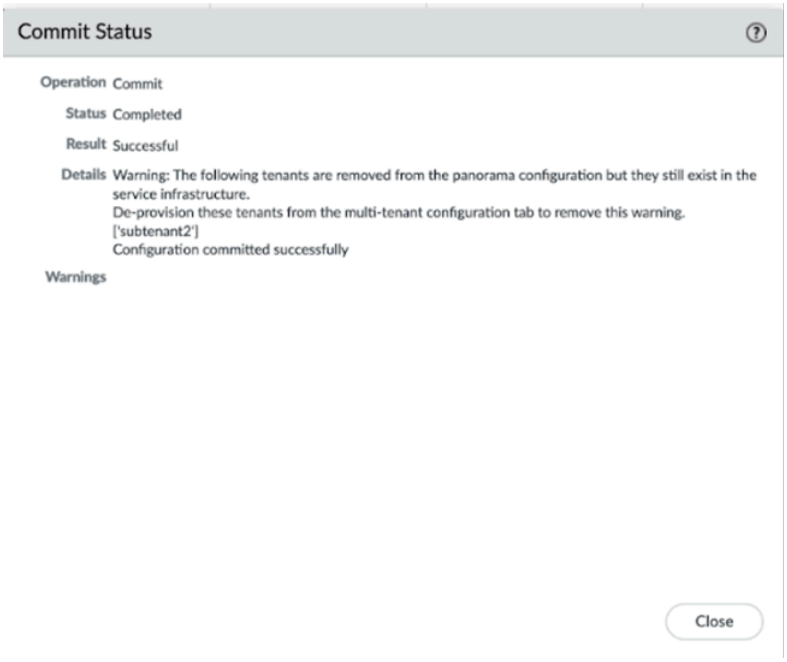

Es wird ein Popup-Fenster angezeigt, in dem der Löschvorgang für den Mandanten bestätigt werden muss. Klicken Sie auf **Ja**, um fortzufahren, oder klicken Sie auf **Nein**, um den Löschvorgang abzubrechen.

 ©2025 Palo Alto Networks, Inc.




**STEP 5 |** Schreiben Sie Ihre Änderungen lokal in Panorama fest, indem Sie **Commit** > **Commit in Panorama** auswählen und einen **Commit** für Ihre Änderungen ausführen.

Nach dem lokalen Commit werden die Mandanten zum Löschen markiert und aus der Liste der Mandanten (nicht jedoch aus der Infrastruktur von Prisma Access) entfernt. Es wird ein Pop-up-Fenster geöffnet, in dem die zu löschenden Mandanten angezeigt werden.




**STEP 6 |** (Optional) Um die Mandanten vollständig aus der Infrastruktur von Prisma Access zu entfernen, wählen Sie **Bereitstellung gelöschter Mandanten aufheben** aus.

Aufheben der Bereitstellung eines Mandanten:

- Mit dieser Aktion wird ein Mandant aus Ihrer Konfiguration und aus der Infrastruktur von Prisma Access gelöscht und Sie können sie nicht abrufen.
- Die dem Mandanten zugewiesene Lizenz wird wiederhergestellt.

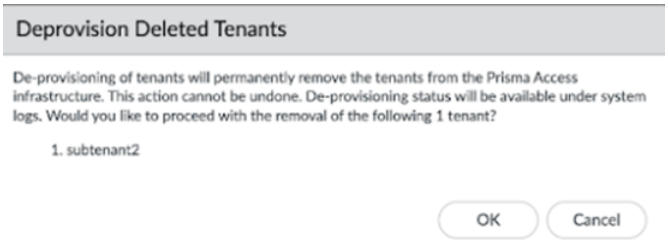



Es wird eine Bestätigungsmeldung mit den Namen der Mandanten angezeigt, deren Bereitstellung aufgehoben werden soll. Klicken Sie auf **OK**, um die Aufhebung der

 ©2025 Palo Alto Networks, Inc.

Bereitstellung des Mandanten fortzusetzen, oder klicken Sie auf **Abbrechen**, um den Vorgang abzubrechen.

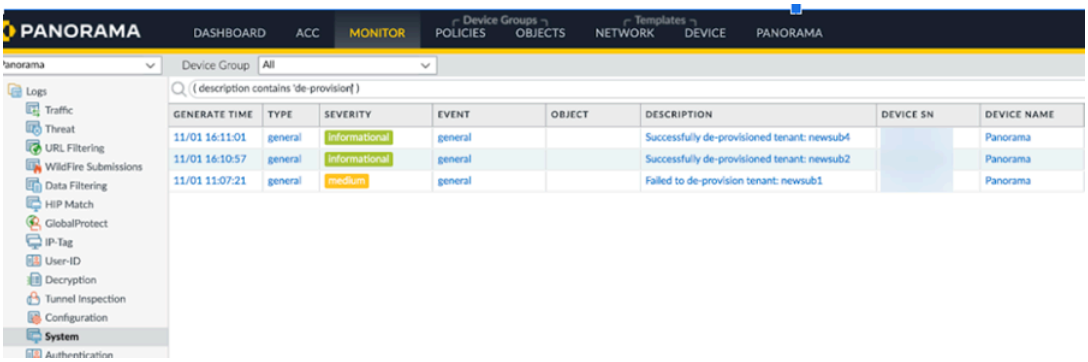
Wenn Sie die Bereitstellung eines Mandanten aufheben, löschen Sie den Mandanten und alle ihm zugewiesenen Ressourcen vollständig. Die Lizenzen, die diesen Mandanten zugeordnet waren, erhalten Sie zurück. Der Mandant kann nicht abgerufen werden.




Wenn die Bereitstellung für keinen Mandanten aufgehoben werden muss, wird die folgende Meldung angezeigt.




**STEP 7 |** (Optional) Überprüfen Sie den Status des Bereitstellungsaufhebungsvorgangs, indem Sie zu **Überwachen** > **Protokolle** > **System** wechseln. Der Vorgang zum Aufheben der Bereitstellung und der Name des Mandanten werden in den Protokollen angezeigt.




 ©2025 Palo Alto Networks, Inc.

# Administrative Benutzer auf Mandantenebene erstellen

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Panorama)<br>• Informationen zum Verwalten mehrerer Mandanten in Prisma Access (Managed by Strata Cloud Manager) finden Sie unter Prisma SASE. | ❑ Prisma Access-Lizenz |

Sie sollten für jeden Mandanten einen administrativen Benutzer erstellen. Auf diese Weise kann ein Administrator auf Mandantenebene seine Mandantenkonfiguration einsehen und ändern, hat aber keinen Zugriff auf andere Mandanten. Um einen administrativen Benutzer für einen bestimmten Mandanten zu erstellen, führen Sie die folgende Aufgabe aus. Weitere Informationen zur rollenbasierten Zugriffssteuerung (Role-Based Access Control, RBAC) für administrative Benutzer auf Mandantenebene finden Sie unter Steuern des rollenbasierten Zugriffs für administrative Benutzer auf Mandantenebene.

*Benutzer, die einzelne Mandanten verwalten, können die Systemprotokolle nicht sehen, da die Option **Überwachen** > **Protokolle** > **System** nicht verfügbar ist. Diese Einschränkung gilt für alle Administratoren, die eine administrative Rolle des Typs **Gerätegruppe und Vorlage** haben. Nur Superuser können Systemprotokolle im Modus für mehrere Mandanten anzeigen.*

 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** Erstellen Sie eine administrative Rolle des Typs **Gerätegruppe und Vorlage**.

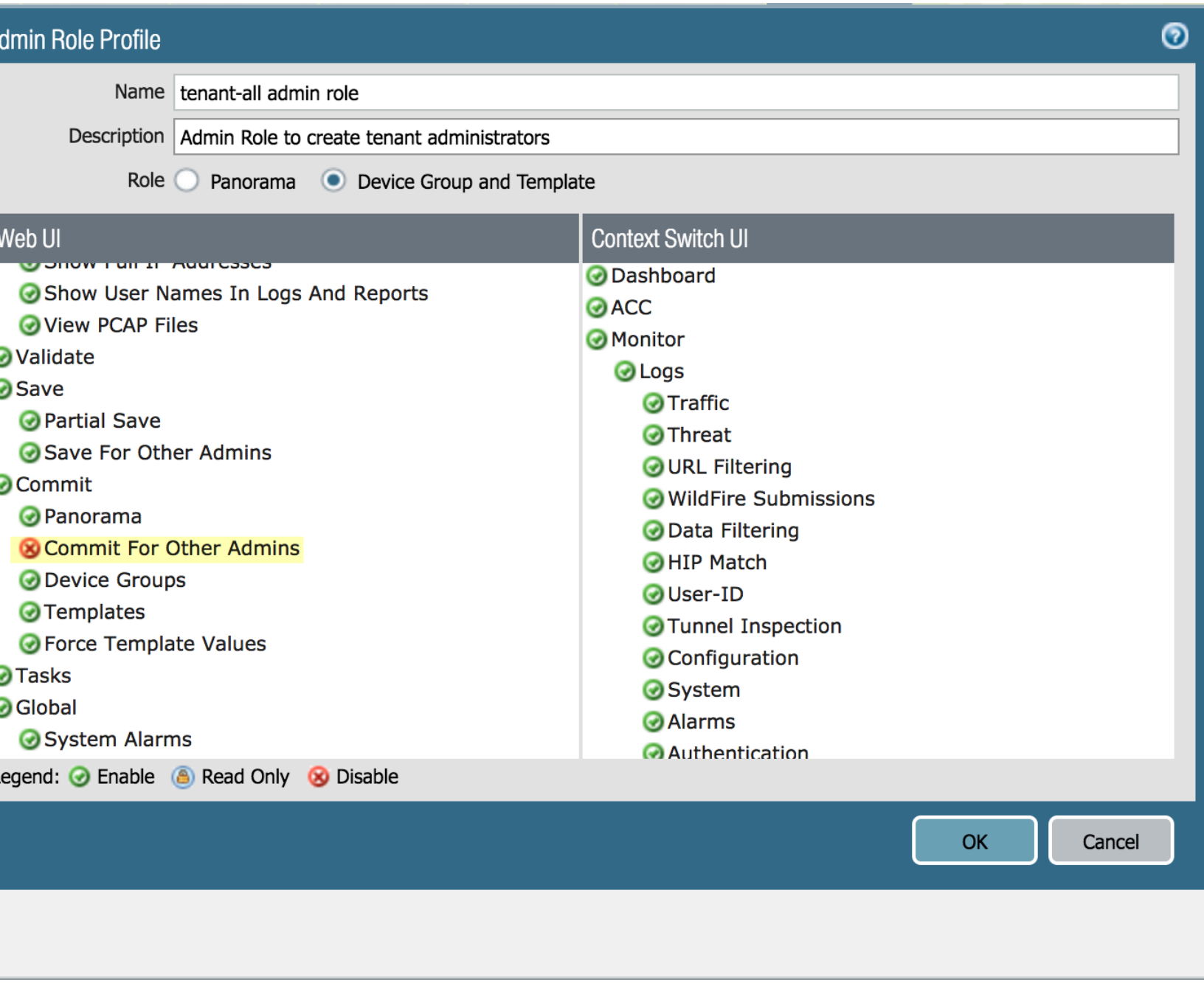
1. Wählen Sie **Panorama** > **Administratorrollen** aus.
2. Wählen Sie **Hinzufügen** aus, um ein Administratorrollenprofil mit der **Rollengruppe Gerätegruppe und Vorlage** hinzuzufügen.
3. Klicken Sie auf **OK**.

Sie können ein einzelnes Administratorrollenprofil erstellen und es für mehrere Mandanten freigeben. Allerdings müssen Sie für jeden Mandanten einen separaten Administrator erstellen.



*Wir empfehlen, während der Anpassung der administrativen Rolle an die Bedürfnisse Ihrer Organisation, die Option **Commit für andere Admins** zu deaktivieren. Wenn Sie diese Option deaktivieren, kann ein Benutzer auf Mandantenebene nur Commits für solche Änderungen durchführen, die er selbst vorgenommen hat. So wird verhindert, dass er unbeabsichtigt andere Änderungen übernimmt, die andere administrative Benutzer auf Mandantenebene vorgenommen haben und für die noch kein Commit durchgeführt wurde.*

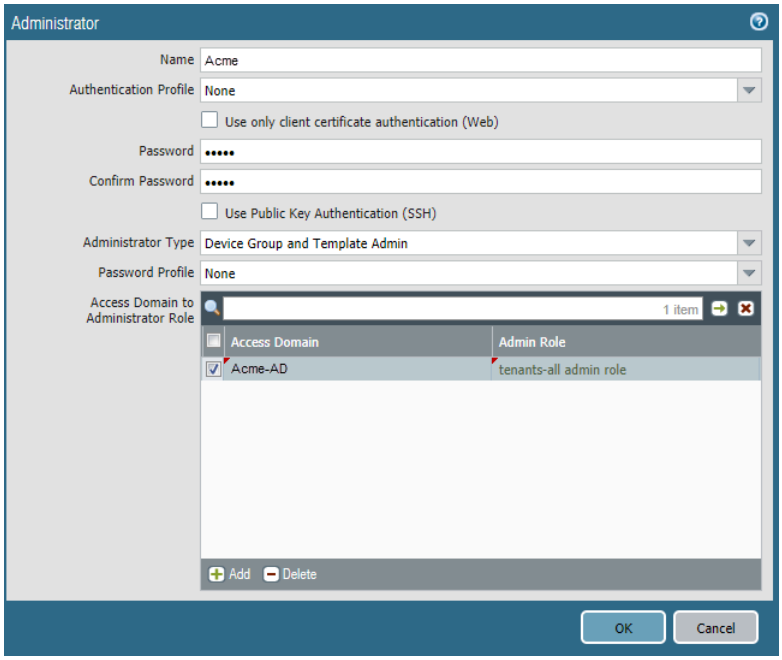
 ©2025 Palo Alto Networks, Inc.




 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Erstellen und konfigurieren Sie einen Administrator für den Mandanten.

1. Wählen Sie **Panorama** > **Administratoren** aus.
2. Wählen Sie **Hinzufügen** aus und fügen Sie einen Administrator hinzu.
3. Geben Sie ein **Passwort** für den neuen Administrator ein und bestätigen Sie es.
4. Geben Sie für **Administratortyp** den Wert **Gerätegruppe und Vorlagenadministrator** an.
5. Geben Sie die **Zugriffsdomäne** an, die den Gerätegruppen für diesen Mandanten zugeordnet ist.
6. Geben Sie die **Administratorrolle** an, die Sie in Schritt 1 für den Mandanten erstellt haben.




**STEP 3 |** Klicken Sie auf **OK**.

**STEP 4 |** Wiederholen Sie die Schritte 2 und 3, um weitere Benutzer hinzuzufügen, sodass Ihre Mandanten wie erforderlich verwaltet werden können.

**STEP 5 |** Wählen Sie **Commit** > **Commit in Panorama** aus, um ein **Commit** für Ihre Änderungen durchzuführen.

 ©2025 Palo Alto Networks, Inc.

# Steuern des rollenbasierten Zugriffs für administrative Benutzer auf Mandantenebene

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama)<br>• Informationen zum Verwalten mehrerer Mandanten in Prisma Access (Managed by Strata Cloud Manager) finden Sie unter Prisma SASE. | ❑ Prisma Access-Lizenz |

Wenn Sie eine Bereitstellung mit mehreren Mandanten verwalten, können Sie rollenbasierte Zugriffssteuerung (RBAC) zum Erstellen administrativer Benutzer auf Mandantenebene verwenden.

Zum Ändern des RBAC-Zugriffs für administrative Benutzer auf Mandantenebene in Panorama erstellen Sie einen administrativen Benutzer auf Mandantenebene, verwenden ein Administratorrollenprofil mit der **Rolle Gerätegruppe und -vorlage** und **aktivieren**, **deaktivieren** oder gewähren Sie **Lesezugriff** auf Bereiche der Panorama-**Weboberfläche**. Verwenden Sie diese Methode, um den Zugriff auf alle Panorama-Komponenten für Benutzer auf Mandantenebene zu verwalten, mit Ausnahme des Zugriffs auf das Cloud Services-Plug-in, in dem Sie Prisma Access verwalten.

Wenn Sie einen Benutzer auf Mandantenebene daran hindern möchten, die Prisma Access-Komponenten in Panorama zu konfigurieren, können Sie keine Administratorrollen verwenden. Damit Benutzer keine Prisma Access-spezifischen Konfigurationsaufgaben konfigurieren können, müssen Sie verhindern, dass ein Benutzer auf das Cloud Services-Plug-in zugreift, wodurch er es auch nicht anzeigen kann. Mit dieser Methode können Sie einen administrativen Benutzer für einen Sicherheitsfachmann erstellen, der die Berechtigungen hat, Änderungen an Sicherheitsrichtlinien vorzunehmen und diese Änderungen per Push an Panorama zu übertragen, aber Änderungen an Prisma Access weder anzeigen noch vornehmen kann.

*Sie können den Zugriff auf das Cloud Services-Plug-in für einen Benutzer entweder aktivieren oder deaktivieren, einem Benutzer jedoch keinen Lesezugriff gewähren. Wenn ein Benutzer Zugriff auf das Cloud Services-Plug-in hat, kann der Benutzer auch Konfigurationsänderungen an den Komponenten, einschließlich Prisma Access, vornehmen.*

In der folgenden Tabelle sind beispielhafte administrative Rollen auf Mandantenebene und die Schritte zum Erstellen dieser Rollen aufgeführt.

| Beispielkonfiguration auf Mandantenebene | Konfigurationsaufgabe |
|---|---|
| Erstellen Sie einen netzwerkorientierten Benutzer, der: | Erstellen Sie einen administrativen Benutzer auf Mandantenebene, aktivieren Sie die Berechtigungen **Speichern** und **Commit** im **Administratorrollenprofil** und deaktivieren Sie alle Berechtigungen, über die der |

 ©2025 Palo Alto Networks, Inc.

| Beispielkonfiguration auf Mandantenebene | Konfigurationsaufgabe |
|---|---|
| • Plug-in-Konfigurationen bearbeiten kann,<br>• Änderungen per Push an Panorama übertragen kann,<br>• eine Konfiguration per Push an Prisma Access übertragen kann. | administrative Benutzer auf Mandantenebene nicht verfügen soll, bzw. setzen Sie diese auf **Nur lesen**. |
| Erstellen Sie einen sicherheitsorientierten Benutzer, der:<br>• Sicherheitsrichtlinien anzeigen und durchführen kann,<br>• Daten per Commit in Panorama festschreiben kann,<br>• das Cloud Services-Plug-in nicht anzeigen oder Änderungen daran vornehmen kann,<br>• eine Konfiguration nicht per Push an Prisma Access übertragen kann (erfordert, dass der Superuser die Konfiguration per Push überträgt). | Um zu verhindern, dass ein administrativer Benutzer auf Mandantenebene das Plug-in einsehen oder darauf zugreifen kann, deaktivieren Sie den Plug-in-Zugriff für einen Administrator auf Mandantenebene. Ändern Sie für alle anderen Panorama-Berechtigungen die Berechtigungen der Administratorrolle für den Benutzer. |
| Erstellen Sie einen Hybridbenutzer, der:<br>• Lesezugriff auf das Cloud Services-Plug-in hat,<br>• Lese- und Schreibzugriff auf die Sicherheitsrichtlinie hat,<br>• die Konfiguration nicht per Push an Prisma Access übertragen kann (erfordert, dass der Superuser die Konfiguration per Push überträgt). | Diese Konfiguration ist nicht möglich. Sie können für das Cloud Services-Plug-in den Nur-Lesen-Modus nicht aktivieren. Sie können nur Administratorbenutzern Zugriff gewähren, damit sie es anzeigen und zum Vornehmen von Konfigurationsänderungen verwenden können, oder sie können diesen Benutzern die Anzeige des Plug-ins verwehren. |

## Entfernen des Plug-in-Zugriffs für einen administrativen Benutzer auf Mandantenebene

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama)<br>• Informationen zum Verwalten mehrerer Mandanten in Prisma Access (Managed by Strata Cloud Manager) finden Sie unter Prisma SASE. | ☐ Prisma Access-Lizenz |

 ©2025 Palo Alto Networks, Inc.

In normalen Konfigurationen mit mehreren Mandanten verwenden Sie Zugriffsdomänen Mandanten zu Prisma Access hinzufügen und ordnen jeder Zugriffsdomäne einen Mandanten zu. Damit verhindert wird, dass ein administrativer Benutzer auf Mandantenebene Konfigurationsänderungen an Prisma Access anzeigen oder vornehmen kann, erstellen Sie eine Zugriffsdomäne, die Sie jedoch keinem Mandanten zuordnen.

Da Sie die Zugriffsdomäne den Gerätegruppen und Vorlagenstacks für den Mandanten zugeordnet haben, verfügt der administrative Benutzer auf Mandantenebene über RBAC-Zugriff auf Mandantenebene und kann die Konfiguration nur für diesen Mandanten durchführen. Da Sie die Zugriffsdomäne nicht mit einem Mandanten in Prisma Access verknüpft haben, kann die Zugriffsdomäne das Cloud Services-Plug-in nicht anzeigen, das den Zugriff auf Prisma Access bietet. Auf diese Weise erstellen Sie einen Benutzer, der Konfigurationsaufgaben auf Mandantenebene ausführen kann, ohne auf Konfigurationsänderungen an Prisma Access zugreifen, sie anzeigen oder vornehmen zu können.

Führen Sie die folgende Aufgabe aus, um Prisma Access für einen Benutzer auf Verwaltungsebene zu entfernen.

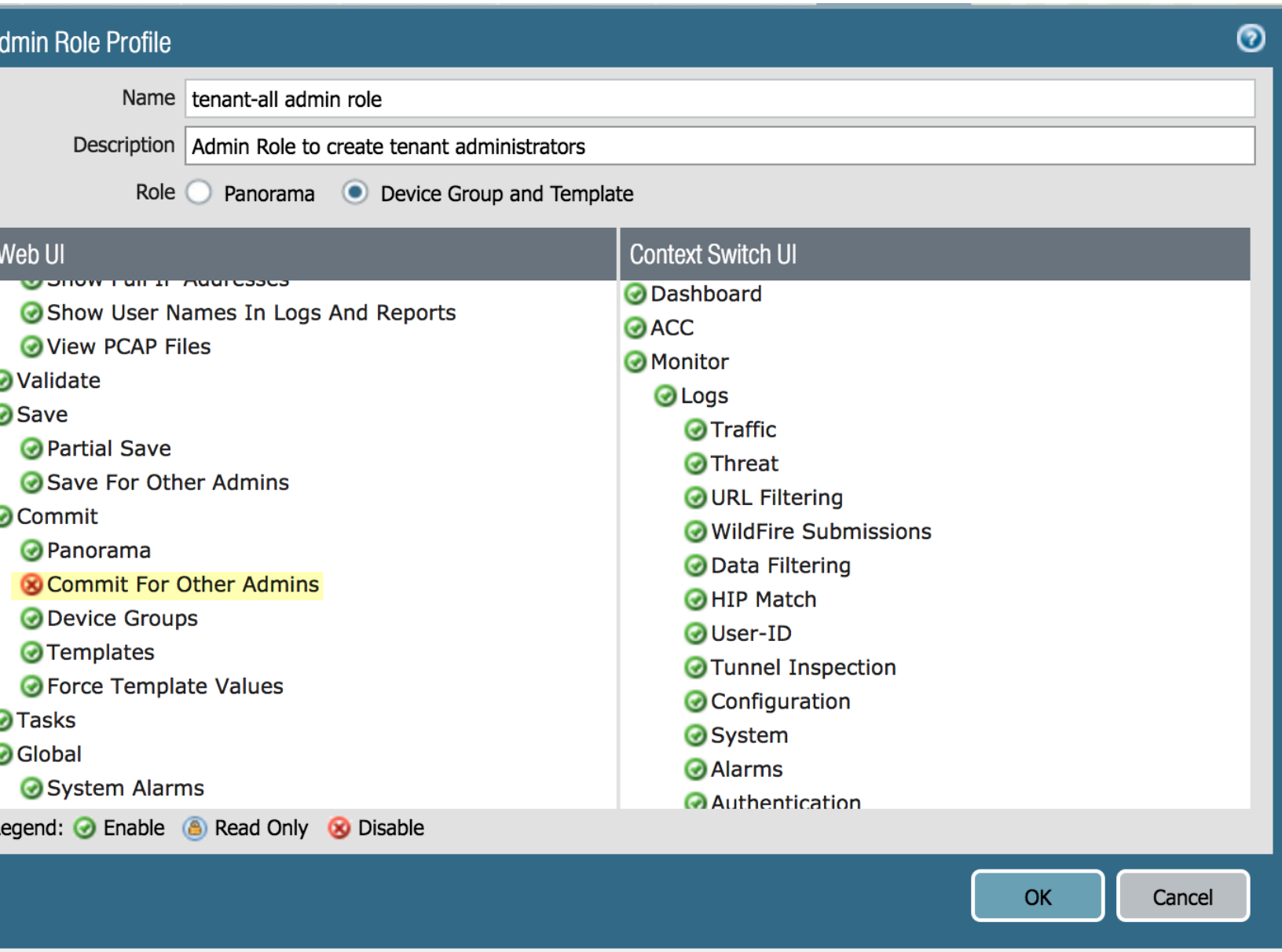
*Diese Aufgabe setzt voraus, dass Sie über Vorlagen zu* Mandanten zu Prisma Access hinzufügen, *Vorlagenstacks und Gerätegruppen für den Mandanten verfügen. Sie ordnen diese dem administrativen Benutzer auf Mandantenebene zu.*

 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** Erstellen Sie eine administrative Rolle des Typs **Gerätegruppe und Vorlage**.

1. Wählen Sie **Panorama** > **Administratorrollen** aus.
2. Wählen Sie **Hinzufügen** aus, um ein Administratorrollenprofil mit der **Rolle Gerätegruppe und Vorlage** hinzuzufügen.
3. Klicken Sie auf **OK**.

   Sie können ein einzelnes Administratorrollenprofil erstellen und es für mehrere Mandanten freigeben.

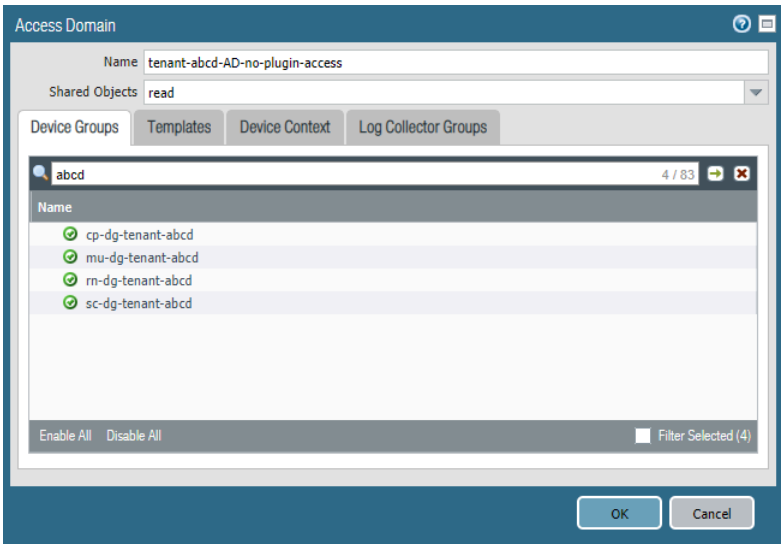


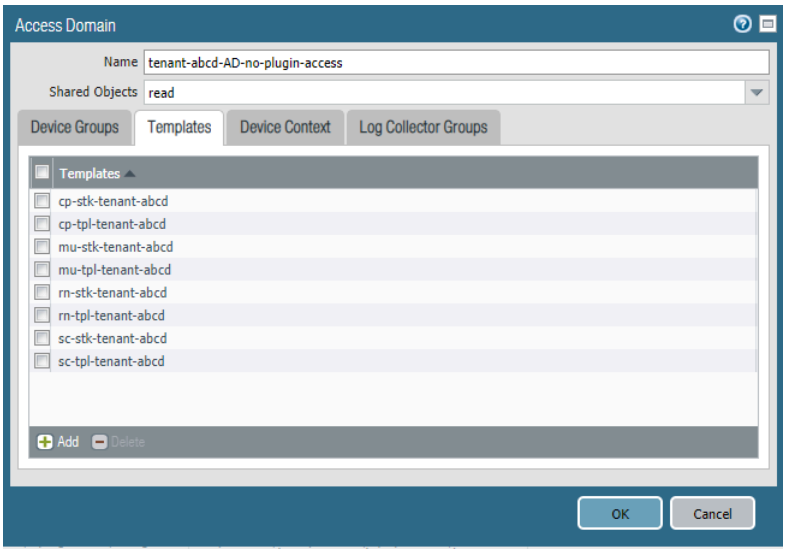

**STEP 2 |** Wählen Sie **Panorama** > **Zugriffsdomäne** aus. Anschließend können Sie eine Zugriffsdomäne **hinzufügen**.

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Geben Sie die dem Mandanten zugeordneten **Gerätegruppen** und **Vorlagen** an.

*Wenn Sie Gerätegruppen erstellt haben, bei denen es sich um untergeordnete Elemente anderer Gerätegruppen handelt, wählen Sie unter der übergeordneten Gerätegruppe **Freigegeben** nur die Gerätegruppe auf der untersten Hierarchieebene (untergeordnetes Element auf zweiter oder dritter Ebene) aus. Wählen Sie das übergeordnete Gerät nicht aus, andernfalls werden Fehler beim Übertragen angezeigt.*



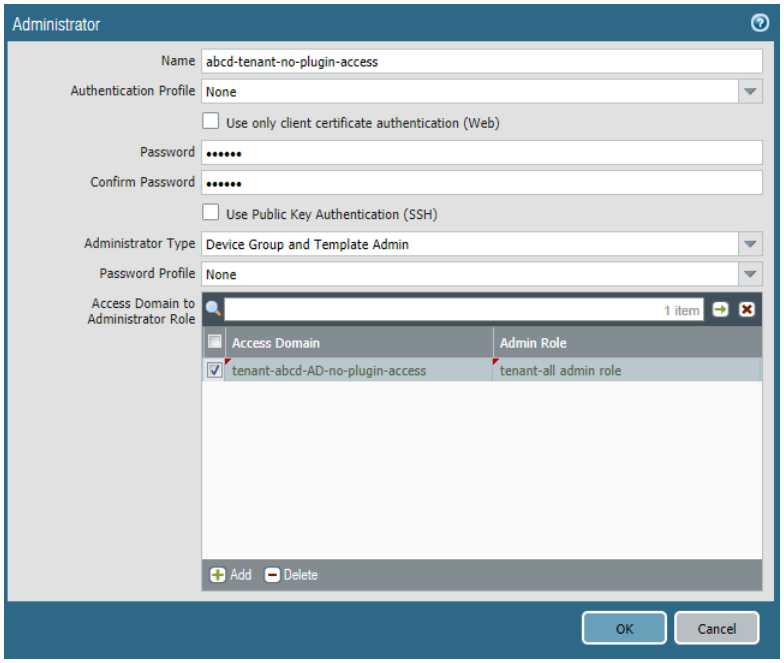




 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** Erstellen und konfigurieren Sie einen Administrator für den administrativen Benutzer auf Mandantenebene und geben Sie dabei die Zugriffsdomäne an, die Sie gerade erstellt haben.

1. Wählen Sie **Panorama** > **Administratoren** aus.
2. Wählen Sie **Hinzufügen** aus und fügen Sie einen Administrator hinzu.
3. Geben Sie ein **Passwort** für den neuen Administrator ein und bestätigen Sie es.
4. Geben Sie für **Administratortyp** den Wert **Gerätegruppe und Vorlagenadministrator** an.
5. Geben Sie die **Zugriffsdomäne** an, die den Gerätegruppen für diesen Mandanten zugeordnet ist.
6. Geben Sie die **Administratorrolle** an, die Sie in Schritt 1 für den Mandanten erstellt haben.

   Wenn Sie dieses Beispiel ausführen, verfügt der administrative Benutzer **abcd-tenant-no-plugin-access** über Berechtigungen, die auf den im Administratorrollenprofil definierten Berechtigungen basieren, kann das Cloud Services-Plug-in (einschließlich Prisma Access) jedoch nicht anzeigen oder konfigurieren. Beachten Sie jedoch, dass er keine vorgenommenen Änderungen in die Cloud übertragen kann.




**STEP 5 |** Wählen Sie **Commit** > **Commit in Panorama** aus, um ein **Commit** für Ihre Änderungen durchzuführen.

 ©2025 Palo Alto Networks, Inc.

# Protokolle nach Gerätegruppen-ID in einer Mehrmandantenbereitstellung sortieren

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama)<br>• Informationen zur Verwaltung mehrerer Mandanten in Prisma Access (Managed by Strata Cloud Manager) finden Sie in Prisma SASE. | ❑ Prisma Access- Lizenz |

Zum manuellen Sortieren der Protokolle in Panorama nach Mandanten wählen Sie **Überwachen > Protokolle** sowie die mit dem Mandanten verknüpfte **Gerätegruppe** aus, um die Protokolle für diese Gerätegruppe anzuzeigen. Wenn Sie Ihre Protokolle jedoch an ein externes Gerät weiterleiten, müssen Sie diese Protokolle möglicherweise auf Mandantenebene sortieren. Suchen Sie dazu in den Protokollen nach der Gerätegruppen-ID, die der Gerätegruppe zugeordnet ist, und verwenden Sie diese Zuordnung von Gruppen-ID und Gerätegruppe, um die Protokolle einem Mandanten zuzuordnen.

In den Protokollen sind der Gerätegruppe vier Felder zugeordnet: **Gerätegruppen-Hierarchieebene 1**, **Gerätegruppen-Hierarchieebene 2**, **Gerätegruppen-Hierarchieebene 3**und **Gerätegruppen-Hierarchieebene 4**. Diese Felder zeigen die Gerätegruppen-IDs in ihrer Hierarchie an. Die gemeinsam genutzte Gerätegruppe (Ebene 0) ist in dieser Struktur nicht enthalten.

**Gerätegruppen-Hierarchieebene 1** bezieht sich auf die erste Gerätegruppenebene in der Hierarchie. Wenn Sie untergeordnete Gerätegruppen auf zweiter oder dritter Ebene hinzugefügt haben, wird in den Feldern **Gerätegruppen-Hierarchieebene 2** bis **Gerätegruppen-Hierarchieebene 4** jeweils die Hierarchie von der untergeordneten Gruppe auf zweiter Ebene bis zur untergeordneten Gruppe auf vierter Ebene angezeigt.

Gehen Sie wie folgt vor, um Protokolle nach Mandant zu suchen.

**STEP 1 |** Suchen Sie die mit der Gerätegruppe verknüpften Gerätegruppen-IDs.

- Um diese Informationen mit einem CLI-Befehl zu finden, melden Sie sich als Superuser (Benutzer auf Administratorebene) bei Panorama an, geben Sie im Konfigurationsmodus den Befehl `show readonly` ein und betrachten Sie die Werte in der Überschrift **device-group**. Die IDs für die Gerätegruppen werden unter dem Gerätegruppennamen angezeigt. Das folgende Beispiel verdeutlicht, dass für die Gerätegruppe **acme-sc** die Geräte-ID **20** lautet.

  Beachten Sie, dass sich diese Gerätegruppen auf der ersten Ebene der Hierarchie befinden (**Gerätegruppen-Hierarchieebene 1**). Sie verwenden diese Information in der Abfrage im nächsten Schritt.

```
admin# show readonly ... device-group { acme-sc { id 20; } acme-
rn { id 39; } acme-mu { id 40; } hooli-rn { id 56; } hooli-sc
 { id 57; } hooli-mu {
```

 ©2025 Palo Alto Networks, Inc.

- Wenn Sie eine API-Abfrage verwenden möchten, geben Sie den folgenden API-Befehl ein:

```
/api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>
```

*Weitere Informationen zur Verwendung von APIs mit Protokollen finden Sie unter* Protokolle abrufen (API).

**STEP 2 |** Verwenden Sie die Zuordnung der Gerätegruppen-ID zum Gerätegruppennamen, um die Protokolle einem Mandanten zuzuordnen.

**STEP 3 |** Wählen Sie **Hinzufügen** aus, um die Parameter zur **Weiterleitung** hinzuzufügen, mit denen die weiterzuleitenden Protokolle ausgewählt werden.

 ©2025 Palo Alto Networks, Inc.

 ©2025 Palo Alto Networks, Inc.

# Prisma Access in einer FedRAMP-Umgebung

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz<br>❑ Cloud Services-Plug-in-Version 3.2.1-h94+, 4.0.0-h88+, 4.1.0-h58+, 5.0.0-h31+ |

Das Federal Risk and Authorization Management Program (FedRAMP) ist ein regierungsweites Programm der Vereinigten Staaten, das einen standardisierten Ansatz zur Sicherheitsbewertung, Autorisierung und kontinuierlichen Überwachung von Cloud-Produkten und -Diensten für behördliche Benutzer bietet. Palo Alto Networks hat die Compliance mit FedRAMP Moderate für Prisma Access (Managed by Panorama) demonstriert. Lesen Sie die folgenden Themen, um mehr darüber zu erfahren, wie Sie Prisma Access einrichten, um die Einhaltung von FedRAMP Moderate sicherzustellen.

Für cloudbasierte Dienste wie Prisma Access verlangt die Regierung der Vereinigten Staaten ein besonderes Maß an Sicherheit, das als *moderat* bezeichnet wird und bei dem der Verlust von Vertraulichkeit, Integrität und Verfügbarkeit schwerwiegende negative Auswirkungen auf den Betrieb, die Sachwerte oder Einzelpersonen einer Behörde hätte. Zu den schwerwiegenden negativen Auswirkungen könnten erhebliche betriebliche Schäden an Sachwerten der Behörde, finanzielle Verluste oder individuelle Schäden gehören, ausgenommen Todesfälle oder körperliche Schäden.

Prisma Access erfüllt die FedRAMP Moderate-Anforderungen und hat von der US-Bundesregierung eine Authorization to Operate (ATO) erhalten. Um die Konformität mit FedRAMP Moderate sicherzustellen, müssen Sie Prisma Access mithilfe der in den folgenden Themen aufgeführten Anforderungen und Richtlinien installieren und konfigurieren.

# FedRAMP-Anforderungen für Prisma Access

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz<br>❑ Cloud Services-Plug-in-Version 3.2.1-h94+, 4.0.0-h88+, 4.1.0-h58+, 5.0.0-h31+ |

FedRAMP ist das von der Regierung der Vereinigten Staaten verwendete Programm, das einen Standardansatz hinsichtlich der Compliance von Cloud-Service-Angeboten (Cloud Service Offerings, CSOs) bietet. Um sicherzustellen, dass Ihr Prisma Access (Managed by Panorama) Access mit „FedRAMP Moderate“ konform ist, verwenden Sie diese Richtlinien und Anforderungen, wenn Sie Prisma Access installieren, aktivieren, zum ersten Mal einrichten und konfigurieren.

## Installationsvorbereitung und Produktaktivierung – Anforderungen

Um sicherzustellen, dass Ihre Prisma Access-Bereitstellung konform bleibt, beachten Sie diese Installations- und Produktaktivierungsanforderungen.

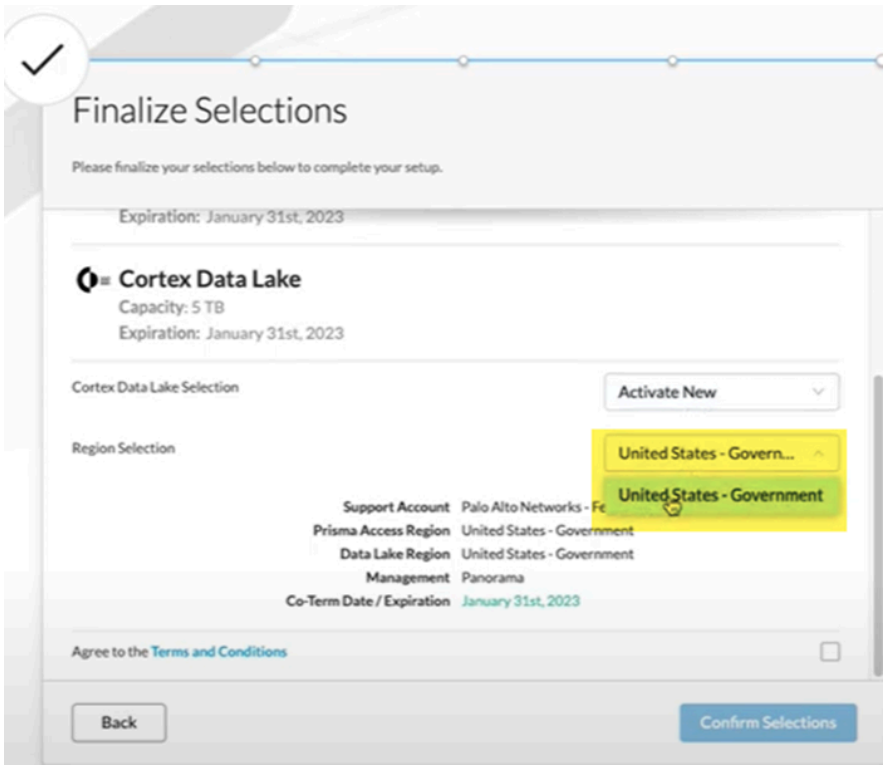
- **Anforderungen hinsichtlich der Installationsvorbereitung:**
  - **Bereitstellungstyp (neu oder vorhanden)** – Neue Prisma Access-Bereitstellungen werden in einer „FedRAMP Moderate“-Umgebung unterstützt. Upgrades von einer bestehenden Prisma Access-Bereitstellung auf eine „FedRAMP Moderate“-Bereitstellung von Prisma Access werden nicht unterstützt.
  - **Erforderliche SKUs** – Wenn Sie Prisma Access für eine „FedRAMP Moderate“-Bereitstellung erwerben, benötigt Prisma Access spezielle SKUs für die FedRAMP-Umgebung. Bestimmen Sie mit Ihrem autorisierten Palo Alto Networks Vertreter oder Partner, welche SKUs Sie für Ihre „FedRAMP Moderate“-Bereitstellung erwerben müssen.
  - Verwenden Sie nur die in Erforderliche Panorama-, Plug-in- und PAN-OS-Dataplane-Versionen aufgeführten Panorama-Versionen, GlobalProtect-Versionen und Cloud Services-Plug-in-Versionen.
  - **Aufnehmen öffentlicher IP-Adressen von Strata Logging Service in Zulassungslisten** – Der IP-Adressblock, der von der Bundesregion für den Strata Logging Service verwendet wird, lautet 34.67.50.64/28. Wenn Ihr Unternehmen Zulassungslisten verwendet, nehmen Sie diese IP-Adressen unbedingt in Ihre Zulassungslisten auf, um sicherzustellen, dass der Strata Logging Service die Protokolle von Prisma Access empfangen kann.
  - **Änderungen an API-URLs** – Wenn Sie das API-Skript ausführen, um die von Prisma Access verwendeten öffentlichen IP-Adressen abzurufen, ändern Sie die URL für die API von **`https://api.gpcloudservice.com/GetPrismaAccessIP/v2`** in **`https://api.fed.prismaaccess.com/GetPrismaAccessIP/v2`**.

    Wenn Ihre Panorama-Appliance einen Proxyserver verwendet (**Panorama** > **Einrichtung** > **Dienst** > **Proxyserver**) oder wenn Sie die SSL-Weiterleitungs-Proxy-Entschlüsselung mit Prisma Access verwenden, fügen Sie unbedingt die URL api.fed.prismaaccess.com zu Ihrer Zulassungsliste auf dem Proxy oder Proxyserver hinzu.

 ©2025 Palo Alto Networks, Inc.

- **GlobalProtect-Portalnamenänderung** – Der standardmäßige Portal-Hostname für eine FedRAMP-konforme Prisma Access-Bereitstellung des Typs „Mobile Benutzer – GlobalProtect“ unterscheidet sich von einer Nicht-FedRAMP-Bereitstellung. Der Portalname lautet *<portal-name>*.fed.prismaaccess.com. und nicht *<portal-name>*.gpcloudservice.com.
- **Supportanforderungen** – Prisma Access FedRAMP Moderate benötigt Palo Alto Networks US Government Support Services, die rund um die Uhr Unterstützung für Beamte der US-Behörden auf dem Territorium der USA beinhalten.

- **Aktivierungsanforderungen** – Wenn Sie Ihre Prisma Access-Bereitstellung aktivieren und installieren, ähneln die Aufgaben zur Aktivierung und Installation einer Nicht-FedRAMP-Bereitstellung. Sie müssen jedoch während der Produktaktivierung eine Region des **Strata-Protokollierungsdienstes** in **Vereinigte Staaten – Regierung** auswählen.




## Erforderliche Panorama-, Plug-in- und PAN-OS-Dataplane-Versionen

Um sicherzustellen, dass Prisma Access mit den Anforderungen von „FedRAMP Moderate“ konform bleibt, müssen Sie sicherstellen, dass Ihre Prisma Access (Managed by Panorama)-Bereitstellung die folgenden Versionen von Panorama, Cloud Services und GlobalProtect verwendet.

| Komponente | Erforderliche Version |
|---|---|
| Panorama PAN-OS-Version | 10.2.8-h3 oder eine neuere 10.2.8-Hotfix-PAN-OS-Version |

 ©2025 Palo Alto Networks, Inc.

| Komponente | Erforderliche Version |
|---|---|
| | 10.2.9-h1 oder eine neuere 10.2.9-Hotfix PAN-OS-Version<br><br>Die Aktivierung des FIPS-CC-Modus in der Panorama-Instanz, von der Prisma Access verwaltet wird, ist die empfohlene Best Practice, die auch mit FedRAMP-Kontrollen vereinbar ist. Wenn Sie FIPS-CC-Unterstützung in Panorama aktivieren möchten, müssen Sie auf das Maintenance Recovery Tool (MRT) zugreifen.<br><br>*Um den Installations- und Aktivierungsprozess zu vereinfachen, können Sie eine vorhandene Panorama-Instanz auswählen, die Sie bereits im FIPS-Modus konfiguriert haben, sofern Sie Panorama registriert, die Lizenzen installiert und die Supportlizenz im Kunden-Support-Portal (CSP) aktiviert haben. Wenn Sie die Seriennummer von Panorama demselben CSP-Konto hinzugefügt haben, auf dem Sie Prisma Access bereitstellen möchten, können Sie die Seriennummer dieser Panorama-Appliance während der Installation auswählen.*<br><br>Sie können keine Panorama-Instanz verwenden, die bereits für die Verwaltung einer anderen Prisma Access- oder Strata Logging Service-Bereitstellung verwendet wurde. |
| Version des Cloud Services-Plug-ins | • 3.2.1-h94+<br>• 4.0.0-h88+<br>• 4.1.0-h58+<br>• 5.0.0-h31+ |
| GlobalProtect-Version | 5.1.4+ und 6.0.7+<br><br>5.1.4 ist FIPS-zertifiziert und die Standardversion für auf den Vorgaben der US-Bundesregierung basierende Bereitstellungen. Wenn Sie eine andere |

 ©2025 Palo Alto Networks, Inc.

| Komponente | Erforderliche Version |
| --- | --- |
| | GlobalProtect-Standardversion als 5.1.4 festlegen, können Sie Version 5.1.4 in der Panorama-Benutzeroberfläche nicht auswählen und müssen einen Supportfall beim technischen Support von Palo Alto Networks einleiten, um die Version wieder hinzuzufügen. |

## Unterstützte Prisma Access-FedRAMP-Standorte

Die folgenden Standorte sind für die Verwendung mit Prisma Access in einer „FedRAMP Moderate“-Umgebung zugelassen, die Unterstützung für CONUS- und OCONUS-Standorte der Vereinigten Staaten umfasst:

- Australien (Südost)
- Belgien
- Brasilien (Süd)
- Kanada (Ost)
- Finnland
- Deutschland (Mitte)
- Indien (West)
- Japan (Mitte)
- Japan (Süd)
- Niederlande (Mitte)
- Singapur
- Schweiz
- Taiwan
- Vereinigtes Königreich
- USA (Mitte)
- USA (Ost)
- USA (Nordwest)
- USA (Südost)
- USA (Südwest)

## Unterstützte und nicht unterstützte Funktionen in einer FedRAMP-Bereitstellung von Prisma Access

IPv6-Unterstützung für Zugriff auf private Apps wird in einer Prisma Access-Umgebung des Typs „FedRAMP Moderate“ unterstützt.

Die folgenden Apps und Funktionen werden für die Verwendung in einer Prisma Access-Umgebung des Typs „FedRAMP Moderate“ nicht unterstützt:

 ©2025 Palo Alto Networks, Inc.

- Prisma Access Insights
- Autonomous DEM
- Expliziter Proxy
- Prisma Access für Clean Pipe
- Enterprise DLP
- IoT Security
- SaaS Security Inline-Unterstützung – Sichtbarkeit

 ©2025 Palo Alto Networks, Inc.

# Konfigurieren von Prisma Access in einer FedRAMP-Umgebung

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz<br>❑ Cloud Services-Plug-in Version 3.2.1-h94+ , 4.0.0-h88+, 4.1.0-h58+, 5.0.0-h31+ |

Nachdem Sie die Anforderungen erfüllt haben, schließen Sie die Einrichtung der Prisma Access-Bereitstellung für eine FedRAMP Moderate-Umgebung ab, indem Sie die folgenden Schritte ausführen.

*Bevor Sie beginnen, notieren Sie die Anforderungen und Richtlinien, die speziell für eine Prisma Access FedRAMP-Bereitstellung gelten, einschließlich der Konfiguration der Panorama-Anwendungen im FIPS-CC-Modus und der spezifischen Versionen, die für Panorama, das Cloud Services-Plug-in und GlobalProtect erforderlich sind.*

**STEP 1 |** Stellen Sie sicher, dass Sie über ein Konto beim Kunden-Support-Portal (CSP) verfügen, das Sie exklusiv für Ihre FedRAMP-Bereitstellungen verwenden können.

Sie können FedRAMP- und Nicht-FedRAMP-Bereitstellungen nicht in einem einzigen CSP-Konto verwenden. Aus diesem Grund empfiehlt Palo Alto Networks die Erstellung eines neuen CSP-Kontos, das ausschließlich für FedRAMP-Konten verwendet wird.

**STEP 2 |** Bereiten Sie Ihre Panorama-Anwendungen auf die Verwendung in der Prisma Access FedRAMP-Umgebung vor.

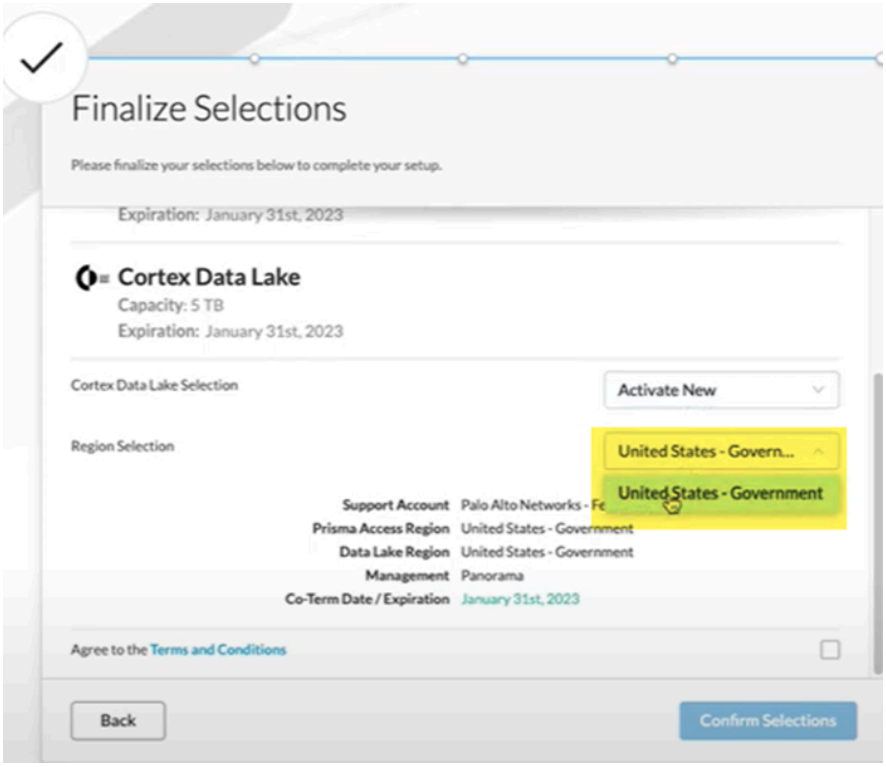
1. Installieren Sie die Panorama-Anwendungen (entweder Anwendungen der M-Serie oder virtuelle Anwendungen).
2. (Optional, empfohlen) Aktivieren Sie die Unterstützung von Federal Information Processing Standard und Common Criteria (FIPS-CC) für die Panorama-Anwendungen.

   Um die FIPS-Unterstützung zu aktivieren, muss auf das Maintenance Recovery Tool (MRT) zugegriffen werden.
3. Aktualisieren Sie Ihre Panorama-Version auf die in Erforderliche Panorama-, Plug-in- und PAN-OS-Dataplane-Versionen aufgelistete Version.

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Ermitteln Sie Ihre Lizenzanforderungen und aktivieren und installieren Sie dann die Prisma Access-Lizenzkomponenten.

Wählen Sie während der Produktaktivierung für den **Strata-Protokollierungsdienst** die Region **Vereinigte Staaten – Regierung** aus.




**STEP 4 |** Fügen Sie die folgenden URLs, IP-Adressen und Ports zu einer Zulassungsliste in allen Sicherheitsanwendungen hinzu, die Sie mit den Panorama-Anwendungen benutzen, die Prisma Access verwalten.

Wenn Ihre Panorama-Anwendungen Proxyserver benutzen (**Panorama** > **Einrichtung** > **Dienst** > **Proxyserver**) oder wenn Sie den SSL-Forward-Proxy mit Prisma Access verwenden, fügen Sie die folgenden URLs, IP-Adressen und Ports zu einer Zulassungsliste auf dem Proxy oder Proxyserver hinzu.

- api.gpcloudservice.com (für Prisma Access)
- api.paloaltonetworks.com (für Prisma Access)
- api.fed.prismaaccess.com (für Prisma Access)
- apitrusted.paloaltonetworks.com (für Prisma Access)
- Die für den Strata-Protokollierungsdienst erforderlichen FQDNs und Ports
- 34.67.50.64/28

  Der IP-Adressblock, der von der Strata Logging Service-Bundesregion verwendet wird, lautet 34.67.50.64/28. Fügen Sie diese IP-Adressen Ihrer Zulassungsliste hinzu, damit Strata Logging Service die Protokolle von Prisma Access empfangen kann.
- Die Ports, die von Panorama benutzt werden.

 ©2025 Palo Alto Networks, Inc.

**STEP 5 |** Öffnen Sie einen Fall im Kunden-Support-Portal (CSP), damit die Quell- und Zielports für Strata Logging Service von Palo Alto Networks in die Zulassungsliste aufgenommen werden können.

Um Strata Logging Service in einer Prisma Access-Umgebung verwenden zu können, müssen Sie einen Fall erstellen, damit Palo Alto Networks die Quell- und Zielports intern in die Zulassungsliste aufnehmen kann.

**STEP 6 |** Wählen Sie **Gerät** > **Einrichtung** > **WildFire** aus und geben Sie dann **`wildfire.gov.paloaltonetworks.com`** ein.

Für FedRAMP-Bereitstellungen müssen Sie WildFire U.S. verwenden. Regierungscloud .

**STEP 7 |** Binden Sie mobile Benutzer ein und sichern Sie sie mit GlobalProtect, falls dies für Ihre Bereitstellung erforderlich ist.

Wir empfehlen die Verwendung der lokalen Authentifizierung als ersten Schritt, um zu überprüfen, ob der Dienst eingerichtet ist und Ihre Benutzer über Internetzugriff verfügen. Später können Sie zur Verwendung Ihrer unternehmensspezifischen Authentifizierungsmethoden wechseln.

1. GlobalProtect für mobile Benutzer einrichten.
2. Konfigurieren Sie Zonen für mobile Benutzer.
   1. Erstellen Sie zwei Zonen in der Vorlage für mobile Benutzer. Zum Beispiel „Mobile-Users“ und „Internet“.
   2. Ordnen Sie die Zonen zu. Ordnen Sie jede Zone, die weder verbundenen Prisma Access-Benutzern noch der Zentrale bzw. den Zweigstellen entspricht, die Option „Nicht vertrauenswürdig“ zu.

      Ordnen Sie unter **Panorama** > **Cloud Services** > **Konfiguration** > **Mobile Benutzer** der Zone „Internet“ die Option „Nicht vertrauenswürdig“ und der Zone „Mobile-Users“ die Option „Vertrauenswürdig“ zu.
3. Konfigurieren Sie Sicherheitsrichtlinien für die Gerätegruppe.

   Zum Erstellen einer Sicherheitsrichtlinie, mit der der Datenverkehr zum Internet zugelassen werden kann, wählen Sie die Gerätegruppe Mobile_User_Device_Group

 ©2025 Palo Alto Networks, Inc.

**Richtlinien** > **Sicherheit** > **Vor-Regeln** > **Hinzufügen** einer Regel aus. Beispiel: „Mobile-Users“ zu „Internet“.

4. Verwenden Sie „Commit und Push“, um Ihre Änderungen festzuschreiben und zu übertragen, damit die Nutzung des Dienstes gestartet werden kann.
   1. Führen Sie **Commit** lokal in Panorama durch.
   2. Führen Sie **Commit und Push** zu Prisma Access durch.
   3. Wählen Sie **Panorama** > **Cloud Services** > **Status** > **Überwachen** > **Mobile Benutzer** aus, um den **Status** anzuzeigen und zu überprüfen, ob Sie den FQDN des Portals mit einem Ping-Signal erreichen können.
5. Vergewissern Sie sich, dass Prisma Access den Internet-Verkehr für mobile Benutzer sichert.
   1. Laden Sie die GlobalProtect-App herunter und installieren Sie sie.
   2. Verwenden Sie die App, um als mobiler Benutzer (lokaler Benutzer) eine Verbindung zum Portal herzustellen.
   3. Navigieren Sie zu verschiedenen Websites im Internet und überprüfen Sie, ob der Datenverkehr in Panorama protokolliert wird.

**STEP 8 |** (Mobile Benutzer – nur GlobalProtect-Bereitstellungen) Erstellen Sie ein Zertifikat für die Authentifizierungsüberschreibung in Ihrer GlobalProtect-Bereitstellung für mobile Benutzer,

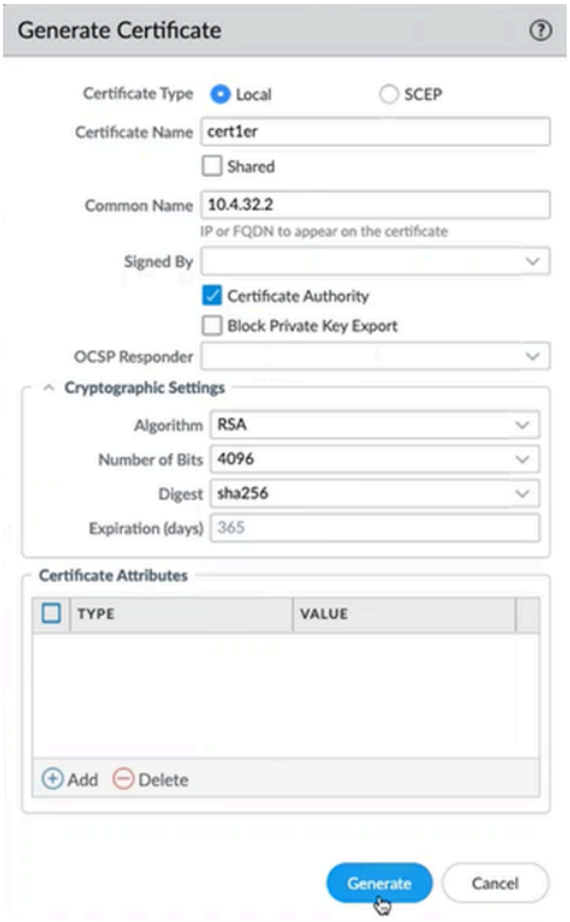
 ©2025 Palo Alto Networks, Inc.

das die Anforderungen einer Panorama-Anwendung erfüllt, die im FIPS-Modus ausgeführt wird. Wenden Sie dieses Zertifikat dann auf Ihre Bereitstellung an.

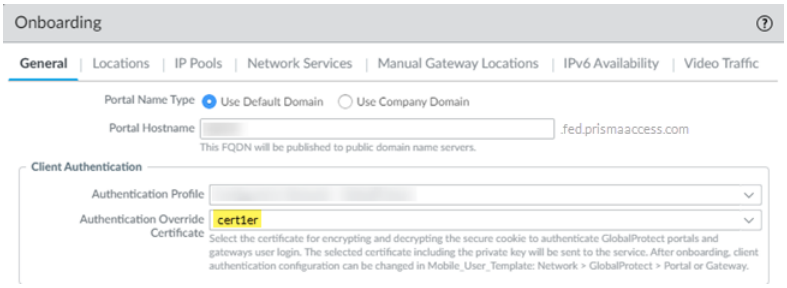
Generieren Sie ein neues Zertifikat, da das Standardzertifikat für GlobalProtect für mobile Benutzer (**Authentifizierungscookie CA**) nicht die Mindestanforderungen der Cipher Suite für eine Panorama-Anwendung erfüllt, die im FIPS-CC-Modus ausgeführt wird.

1. Wählen Sie in der Panorama-Anwendung, die Prisma Access verwaltet, **Gerät** > **Zertifikatverwaltung** > **Zertifikate** > **Gerätezertifikate** aus.

   Stellen Sie sicher, dass Sie sich in der Vorlage **Mobile_User_Template** befinden.
2. Generieren Sie ein Zertifikat, das die Mindestanforderungen für die Cipher Suite für eine Panorama-Anwendung im FIPS-CC-Modus erfüllt.




3. Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Mobile Benutzer – GlobalProtect** und dann den **Hostnamen** und im Bereich **Clientauthentifizierung** das von Ihnen erstellte **Authentifizierungsüberschreibungszertifikat** aus.




 ©2025 Palo Alto Networks, Inc.

*Wenn Sie Ihre GlobalProtect-Konfiguration für mobile Benutzer bereits erstellt haben, wird dieser Bereich ausgegraut dargestellt. Um das Zertifikat für die Authentifizierungsüberschreibung zu ändern, wählen Sie* ***Netzwerk*** *>* ***GlobalProtect*** *>* ***Portale*** *>* ***<portal-config>*** *>* ***Agent*** *>* ***STANDARD*** *>* ***Authentifizierung*** *und dann dieses Zertifikat unter dem* ***Zertifikat zum Ver-/Entschlüsseln von Cookies*** *aus.*

**STEP 9 |** Aktivieren Sie die Dienstinfrastruktur und die Dienstverbindungen, die die Kommunikation zwischen Prisma Access-Elementen ermöglichen.

1. Planen Sie, die Dienstinfrastruktur und die Dienstverbindungen zu aktivieren.
2. Aktivieren Sie die Dienstinfrastruktur.
3. Erstellen Sie eine Dienstverbindung für den Zugriff auf Ihre Unternehmensressourcen.

   Wenn Sie keinen Zugriff auf Ihre Unternehmensressourcen benötigen, sollten Sie dennoch eine Dienstverbindung erstellen, um den Zugriff zwischen mobilen Benutzern und Remote-Netzwerken zu ermöglichen.

**STEP 10 |** Planen, erstellen und konfigurieren Sie Remote-Netzwerkverbindungen.

1. Fügen Sie einzelne oder mehrere Remote-Netzwerke zu Prisma Access hinzu.

   Sie können einen Standort einbinden und dann mithilfe der Massenimportfunktion weitere Standorte hinzufügen.
2. Erstellen Sie eine Sicherheitsrichtlinienregel, um beispielsweise den Datenverkehr von den Remote-Netzwerken zur Zentrale zuzulassen. (Beispiel: „Vertrauenswürdig“ zu „Vertrauenswürdig“).
3. Vergewissern Sie sich, dass Konnektivität zwischen der Dienstverbindung, der Remote-Netzwerkverbindung und den mobilen Benutzern besteht.

**STEP 11 |** Rufen Sie die öffentlichen und privaten IP-Adressen für Prisma Access ab.

Sie fügen diese Adressen einer Zulassungsliste im Netzwerk Ihrer Organisation hinzu, um den Inbound Access auf Ihr Unternehmensnetzwerk und Ihre Unternehmensanwendungen zu begrenzen.

*Wenn Sie über eine GlobalProtect-Bereitstellung für mobile Benutzer verfügen, können Sie anstelle dieser API die Prisma Access-Benutzeroberfläche verwenden, um die Zuweisung öffentlicher IP-Adressen zu verwalten und zu bestätigen, dass die IP-Adressen Ihren Zulassungslisten hinzugefügt wurden, bevor Prisma Access die IP-Adressen freigibt. Auf diese Weise stellt Prisma Access nur die IP-Adressen bereit, die Sie der Zulassungsliste hinzugefügt haben.*

 ©2025 Palo Alto Networks, Inc.

**STEP 12 |** (Optional) Ändern Sie die Authentifizierungsmethode von der lokalen Authentifizierung in die Authentifizierungsmethode Ihrer Organisation.

Verwenden Sie eine der folgenden Methoden, um die SAML-Authentifizierung für mobile Benutzer einzurichten:

- Konfigurieren Sie die Azure AD SAML-Authentifizierung für Bereitstellungen für mobile Benutzer

  Konfigurieren Sie nur die GlobalProtect-Komponenten dieser Konfiguration und stellen Sie die Konfiguration des expliziten Proxys zurück.
- Konfigurieren Sie die SAML-Authentifizierung mit Okta als IdP für mobile Benutzer
- Konfigurieren Sie ADFS als SAML-Anbieter für mobile Benutzer

Sie können die Cloud Identity Engine verwenden, um Benutzer- und Gruppeninformationen mithilfe der Cloud Identity Engine abzurufen, nachdem Sie die Authentifizierung eingerichtet haben. Sie können Benutzer jedoch nicht ausschließlich mithilfe der Cloud Identity Engine authentifizieren.

**STEP 13 |** (Optional) Leiten Sie Protokolle von Strata Logging Service an einen externen Syslog-Empfänger weiter, indem Sie die App für die Protokollweiterleitung einrichten.

 ©2025 Palo Alto Networks, Inc.

 ©2025 Palo Alto Networks, Inc.

# Prisma Access – Erweiterte Bereitstellungen

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Einige Routing- und Netzwerkbereitstellungen von Prisma Access erfordern umfassende Kenntnisse der Topologie und Routinggeräte Ihrer Organisation sowie ein Verständnis der Funktionsweise von Prisma Access. In diesem Abschnitt erfahren Sie mehr über diese erweiterten Bereitstellungen und wie Sie diese konfigurieren.

Erweiterte Bereitstellungen für Dienstverbindungen, mobile Benutzer und Remote-Netzwerke:

- Neuen Compute-Standort für einen bereitgestellten Prisma Access-Standort hinzufügen
- IPv6-Unterstützung
- DNS-Auflösung für Bereitstellungen für mobile Benutzer – GlobalProtect und Remote-Netzwerke
- Wie BGP IP-Adresspools mobiler Benutzer für Dienstverbindungen und Remote-Netzwerkverbindungen ankündigt
- Proxy-Unterstützung für Prisma Access und Strata Logging Service
- Blockieren Sie eingehende Verbindungen aus bestimmten Ländern
- Sicherer Internet-Verkehr aus AWS WorkSpace
- Prisma Access für Netzwerke ohne Standardroute

Dienstverbindungen – Erweiterte Bereitstellungen:

- Multicloud-Redundanz für Dienstverbindungen
- Internetgebundenen Datenverkehr mittels Datenverkehrslenkung an Dienstverbindungen weiterleiten
- Routing für Dienstverbindungsverkehr
- Benutzer-ID- und Geräte-ID-Zuordnung für Dienstverbindungen mit Quell-NAT beibehalten

Mobile Benutzer – GlobalProtect – Erweiterte Bereitstellungen:

- Mehrere Portale in Prisma Access konfigurieren
- Dynamische DNS-Registrierungsunterstützung für Remote-Fehlerbehebung und Updates
- Unterstützung der Registrierung von dynamischem DNS für „Mobile Benutzer – GlobalProtect“
- Kompromittierte Geräte in einer GlobalProtect-Bereitstellung von Prisma Access identifizieren und unter Quarantäne stellen

- IPv6-Datenverkehr in Bereitstellungen von „Mobile Benutzer – GlobalProtect“ gezielt umleiten oder blockieren
- HIP-Informationen mit Prisma Access weitergeben
- Anzeigen von HIP-Berichten
- Unterstützung für Gzip-Codierung in clientlosem VPN
- Replikation des Datenverkehrs in Prisma Access

Remote-Netzwerk – Erweiterte Bereitstellungen:

- Sicheren eingehenden Zugriff auf Remote-Netzwerkstandorte gewähren
- Netzwerk mit hoher Bandbreite für einen Remote-Standort erstellen

 ©2025 Palo Alto Networks, Inc.

# Neuen Compute-Standort für einen bereitgestellten Prisma Access-Standort hinzufügen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Um die Leistung zu optimieren und die Latenz zu verbessern, kann Prisma Access neue Compute-Standorte für Standorte einführen, die Sie bereits im Rahmen eines Plug-in-Upgrades bereitgestellt haben. Wenn Sie das Plug-in aktualisieren, ändert sich die vorhandene Zuordnung von Compute-Standort zu Standort nicht, aber Sie können den neuen Compute-Standort nutzen. Wenn Sie den Compute-Standort ändern, ändert Prisma Access die IP-Adressen des Gateways und des Portals (für mobile Benutzer) sowie die Dienst-IP-Adressen (für Remote-Netzwerke) für die Standorte, denen der neue Compute-Standort zugeordnet ist. Wenn Sie Zulassungslisten in Ihrem Netzwerk verwenden, um Benutzern Zugriff auf Internetressourcen wie SaaS-Anwendungen oder öffentlich zugängliche Partneranwendungen zu gewähren, müssen Sie diese neuen IP-Adressen zu Ihren Zulassungslisten hinzufügen.

Führen Sie die folgende Aufgabe aus, um ein Upgrade auf einen neuen Compute-Standort durchzuführen, wenn dieser verfügbar wird.

Da Sie Zeit einplanen müssen, um den vorhandenen Standort zu löschen und hinzuzufügen und Ihre Zulassungslisten (für mobile Benutzer) oder die IP-Adresse des Peer-IPSec-Tunnels (für Remote-Netzwerkbereitstellungen) zu ändern, empfiehlt Palo Alto Networks, dass Sie eine Änderung des Compute-Standorts während eines Wartungsfensters oder außerhalb der Spitzenbedarfszeiten planen.



*Um Ausfallzeiten für Bereitstellungen mobiler Benutzer zu reduzieren, verwenden Sie die API, um das neue Gateway und die IP-Adresse für mobile Benutzer vorab zuzuweisen, bevor Sie diese Schritte ausführen.*

**STEP 1 |** Fügen Sie Bandbreite für die neuen Compute-Standorte des Remote-Netzwerks hinzu.

1. (Remote-Netzwerkbereitstellungen, die Remote-Netzwerkbandbreite nur nach Compute-Standorten zuweisen) Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Remote-Netzwerke** aus.
2. Klicken Sie auf das Zahnradsymbol in der **Bandbreitenzuweisung** und fügen Sie **Bandbreitenzuweisung (Mbit/s)** für den neuen Compute-Standort hinzu.
3. Warten Sie, bis die Bandbreite im Feld „Gesamt zugewiesen“ oben auf der Seite angezeigt wird. Klicken Sie dann auf **OK**.

**STEP 2 |** (Nur Bereitstellungen für mobile Benutzer) Rufen Sie die neuen Gateway- und Portal-IP-Adressen mithilfe des API-Skripts ab und fügen Sie sie Ihren Zulassungslisten hinzu.

**STEP 3 |** Löschen Sie den Standort „Dienstverbindung“, „Remote-Netzwerkverbindung“ oder „Mobiler Benutzer“, der dem neuen Compute-Standort zugeordnet ist.

**STEP 4 |** Führen Sie einen Commit aus und übertragen Sie die Änderung per Push.

 ©2025 Palo Alto Networks, Inc.

**STEP 5 |** Fügen Sie die soeben gelöschten Standorte erneut hinzu.

**STEP 6 |** Führen Sie einen Commit aus und übertragen Sie die Änderung per Push.

**STEP 7 |** (Nur Bereitstellungen der Typen „Remote-Netzwerk“ und „Dienstverbindungen“) Ändern Sie Ihr CPE so, dass es auf die neuen IP-Adressen für den IPSec-Tunnel für die Remote-Netzwerk- oder Dienstverbindung verweist.

Wählen Sie für Remote-Netzwerkverbindungen **Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Remote-Netzwerke** aus, notieren Sie sich die **Dienst-IP-Adresse** und konfigurieren Sie die neue **Dienst-IP-Adresse** als Peer-Adresse für den IPSec-Tunnel des Remote-Netzwerks auf Ihrem CPE.

Wählen Sie für Dienstverbindungen **Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Dienstverbindung** aus, notieren Sie sich die **Dienst-IP-Adresse** und konfigurieren Sie die neue **Dienst-IP-Adresse** als Peer-IP-Adresse für den IPSec-Tunnel der Dienstverbindung auf Ihrem CPE.

**STEP 8 |** Wählen Sie **Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Remote-Netzwerke** aus, notieren Sie sich die **Dienst-IP-Adresse** und konfigurieren Sie die neue **Dienst-IP-Adresse** als Peer-Adresse für den IPSec-Tunnel des Remote-Netzwerks auf Ihrem CPE.

Wenn Sie eine Remote-Netzwerkverbindung löschen und erneut hinzufügen, ändert sich die IP-Adresse des IPSec-Tunnels auf der Prisma Access-Seite.

**STEP 9 |** (Nur Bereitstellungen des Typs „Mobile Benutzer“) Nachdem ein Standort neu zugeordnet wurde, rufen Sie den neuen Gateway-FQDN ab, und fügen Sie ihn der Authentifizierungskonfiguration Ihres SAML-Anbieters hinzu.

Wenn der Standort eines mobilen Benutzers neu zugeordnet wird, ändert sich der Gateway-FQDN möglicherweise nach dem Upgrade der Infrastruktur, das die Neuzuordnung verursacht, was zu Problemen mit der SAML-Authentifizierung führen kann. So finden Sie den Gateway-Namen:

- Wählen Sie in Prisma Access (Managed by Strata Cloud Manager) die Optionen **Workflows** > **Einrichtung Prisma Access** > **GlobalProtect** > **GlobalProtect-Einrichtung** > **Infrastruktur** > **Infrastruktureinstellungen** aus, klicken Sie auf das Zahnrad, um die Infrastruktureinstellungen anzuzeigen, und kopieren Sie das umbenannte Gateway in den Bereich „Gateway-FQDNs“.
- Wählen Sie in Prisma Access (Managed by Panorama) die Optionen **Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Mobile Benutzer – GlobalProtect** aus und kopieren Sie das umbenannte Gateway in den Bereich „Gateways“.

 ©2025 Palo Alto Networks, Inc.

# IPv6-Unterstützung

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access Lizenzversion 2.2 Preferred und höher<br>❑ Der native IPv6-Zugriff auf öffentliche und private Apps erfordert die folgenden Mindestreleases:<br>• Prisma Access (Managed by Strata Cloud Manager): Juni 2024 Release<br>• Prisma Access (Managed by Panorama): Prisma Access 5.1.1 nur für neue Bereitstellungen.<br>Alle anderen Bereitstellungen (einschließlich vorhandener Prisma Access (Managed by Panorama)-Bereitstellungen) unterstützen nur den Zugriff auf private Apps. |

Wenn Ihre Organisation IPv6-Adressierung verwendet, ermöglicht Ihnen Prisma Access den Zugriff auf interne (private) Apps, die sich hinter IPv6-Adressen verbergen. Abhängig von Ihrer Prisma Access-Version können Sie entweder auf private (interne) Apps über IPv6 oder sowohl auf interne als auch auf öffentliche (externe) Apps für GlobalProtect und Remote-Netzwerke zugreifen.

*Für den Zugriff auf externe Apps ist bei manchen Prisma Access-Komponenten die IPv6-Funktionalität nicht standardmäßig aktiviert. Bevor Sie natives IPv6 für den Zugriff auf öffentliche Apps aktivieren, wenden Sie sich an Ihr Palo Alto Networks Account-Team und öffnen Sie ein TAC-Ticket, um den Aktivierungsprozess zu starten.*

Ein Vorteil der nativen IPv6-Unterstützung ist die Möglichkeit für mobile Benutzer, an reinen IPv6- und Dual-Stack-Endpunkten über IPv6-Verbindungen mithilfe von GlobalProtect eine Verbindung mit Prisma Access herzustellen. Ein weiterer Vorteil ist die Möglichkeit für GlobalProtect- und Remote-Netzwerke, über das Internet auf Internet- und öffentliche SaaS-Anwendungen zuzugreifen, wenn diese Internetziele IPv6-Verbindungen erfordern.

IPv6 bietet im Vergleich zu IPv4 einen erheblich größeren Adressraum und ermöglicht eine nahezu unbegrenzte Anzahl eindeutiger IP-Adressen. Gleichzeitig ist Dual Stack ein Übergangsansatz, der den gleichzeitigen Betrieb von Netzwerken und Geräten mithilfe von IPv4 und IPv6 ermöglicht. Dank nativer IPv6-Unterstützung ist Prisma Access kompatibel mit IPv6- und Dual-Stack-Verbindungen, um den Migrationsprozess von IPv4 auf IPv6 zu erleichtern, Abwärtskompatibilität sicherzustellen und Ihre Umstellung auf die Cloud und IPv6-fähige Netzwerke zu unterstützen.

Sie konfigurieren IPv6 in folgenden Prisma Access-Netzwerkkomponenten:

 ©2025 Palo Alto Networks, Inc.

- Aktivieren Sie IPv6 und geben Sie ein IPv6-Subnetz in Ihrem Infrastruktursubnetz an, um eine IPv6-Netzwerkinfrastruktur einzurichten, die die Kommunikation zwischen Ihren Remote-Netzwerken (Zweigstellen), mobilen Benutzern und Dienstverbindungen (Rechenzentrum oder Zentrale) ermöglicht.

  *Die besten Ergebnisse erzielen Sie, wenn Sie Ihren eigenen IPv6-Adresspool (öffentlich oder privat) mit einer Präfixlänge von /64 bereitstellen, z. B. 3005:10:209:55::/64.*

- Geben Sie für eine Bereitstellung des Typs „Mobile Benutzer – GlobalProtect“ an, ob IPv6-Netzwerke für die Compute-Standorte verwendet werden sollen, die mit den Standorten Ihrer mobilen Benutzer verknüpft sind.

  Sie können nach Bedarf IP-Adresspools für mobile IPv6-Benutzer und IPv6-DNS-Serveradressen angeben.

  *Die besten Ergebnisse erzielen Sie, wenn Sie Ihren eigenen IPv6-Adresspool (öffentlich oder privat) mit einer Präfixlänge von /64 bereitstellen, z. B. 3001:192:168:32::/64, angewendet auf weltweiter Ebene.*

  *Prisma Access weist jeder Compute-Region einen Pool aus einem /80-Subnetz und jedem Standort (Gateway) einen Pool aus einem /112-Subnetz zu. Da jede GlobalProtect-Verbindung eine IP-Adresse aus dem Pool verwendet, können durch diese Zuordnung pro Standort über 65.000 verfügbare IPv6-Adressen (/128) den Endpunkten der Benutzer zugewiesen werden.*

- Für Dienstverbindungen und Remote-Netzwerkverbindungen können Sie die IPv6-Adressierung für den Routingtyp angeben, den die Verbindung verwendet (entweder statische oder BGP-Routen).
  - Geben Sie für statische Routen eine IPv6-Adresse für die Subnetze an, die für die statischen Routen verwendet werden.
  - Geben Sie für BGP-Routen eine IPv6-**Peer-Adresse** und eine **lokale Adresse** an.

    Sie können auch die Transportmethode angeben, die zum Austausch von BGP-Peering-Informationen verwendet wird. Sie können angeben, dass IPv4 zum Austausch aller BGP-Peering-Informationen (einschließlich IPv4 und IPv6) verwendet werden soll, dass IPv6 zum Austausch aller BGP-Peering-Informationen verwendet werden soll oder dass IPv4 zum Austausch von IPv4-BGP-Peering-Informationen und IPv6 zum Austausch von IPv6-BGP-Peering-Informationen verwendet werden soll.

    *Die besten Ergebnisse erzielen Sie, wenn Sie Ihren eigenen IPv6-Adresspool (öffentlich oder privat) mit einer maximalen Präfixlänge von /64 bereitstellen, z. B. 2005:10:209:79::/64.*

- Für Remote-Netzwerke können Sie IPv6-Adressen für DNS-Server hinzufügen.

  *Um optimale Ergebnisse zu erzielen, stellen Sie Ihren eigenen IPv6-Adresspool (öffentlich oder privat) mit einer maximalen Präfixlänge von /64 bereit, z. B. 2001:10:209:65::/64.*

  *Jede Zweigstelle sollte ein eindeutiges /112-Subnetz (maximale Länge) verwenden, das mehr als 65.000 eindeutige Hosts zulässt.*

 ©2025 Palo Alto Networks, Inc.

- *Die von Ihnen angegebenen IPv6-Adressen dürfen sich nicht mit dem öffentlichen BYOIP-IPv6-Adressraum von Prisma Access überschneiden.*
- *Ihr IP-Pool, die Subnetze Ihrer Zweigstelle (Remote-Netzwerk), die Unternehmenssubnetze (Dienstverbindung) und das Infrastruktursubnetz dürfen sich nicht überschneiden (sie sollten sich gegenseitig ausschließen).*

Die folgenden Compute-Standorte unterstützen IPv6 nicht:

- Südkorea
- Asien (Nordost)
- Südamerika (Ost)
- Bahrain
- Südafrika (West)
- Europa Nord (Stockholm)
- Naher Osten (Mitte) (VAE)

Die folgenden Standorte unterstützen IPv6 nicht:

- Alle Standorte der lokalen Zonen
- Kanada (West)
- Südafrika (Mitte)

Die folgenden Bereitstellungen unterstützen keine IPv6-Adressierung:

- Remote-Netzwerke – Hohe Leistung
- IP-Optimierung

  Bereitstellungen mit IP-Optimierung unterstützen IPv6 nicht für den Zugriff auf öffentliche (externe) Apps. Der Zugriff auf private Apps wird unterstützt. Um IPv6 für Ihre neue Prisma Access-Bereitstellung zu aktivieren, wenden Sie sich an Ihr Palo Alto Networks Account-Team, das einen TAC-Fall zur Bearbeitung Ihrer Anfrage eröffnen wird.
- Clean Pipe-Bereitstellungen
- Datenverkehrslenkung (Verwendung von Datenverkehrslenkungsregeln zur Umleitung des internetgebundenen Datenverkehrs über eine Dienstverbindung)
- Outboundrouten für den Dienst für Dienstverbindungen und Remote-Netzwerkverbindungen

*Prisma Access kündigt keine IPv6-Standardrouten an.*

## Unterstützung von nativem IPv6 – Übersicht

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | ☐ Prisma Access Lizenzversion 2.2 Preferred und höher |

 ©2025 Palo Alto Networks, Inc.

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Panorama) | ❑ Der native IPv6-Zugriff auf öffentliche und private Apps erfordert die folgenden Mindestreleases:<br>• Prisma Access (Managed by Strata Cloud Manager): Juni 2024 Release<br>• Prisma Access (Managed by Panorama): Prisma Access 5.1.1 nur für neue Bereitstellungen.<br>Alle anderen Bereitstellungen (einschließlich vorhandener Prisma Access (Managed by Panorama)-Bereitstellungen) unterstützen nur den Zugriff auf private Apps. |

Prisma Access erweitert die Unterstützung für IPv6 über den Zugriff auf private Anwendungen hinaus, um IPv6 für GlobalProtect sowie Remote-Netzwerke nativ zu unterstützen.

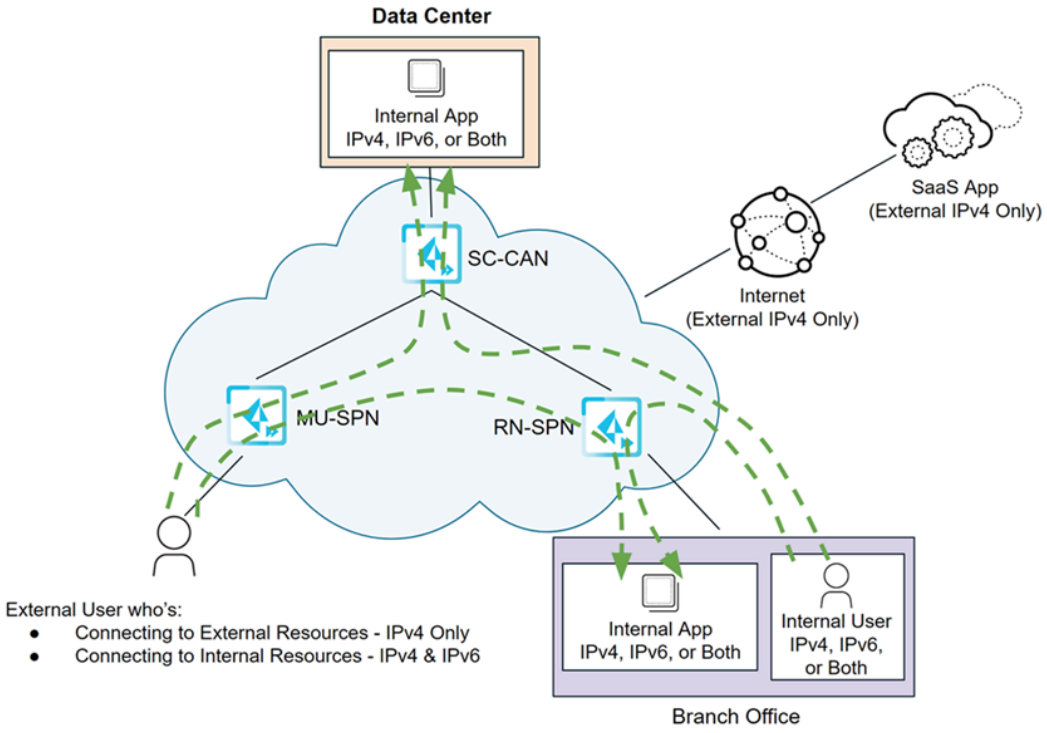
Ein Vorteil der nativen IPv6-Unterstützung ist die Möglichkeit für mobile Benutzer, an reinen IPv6- und Dual-Stack-Endpunkten über IPv6-Verbindungen mithilfe von GlobalProtect eine Verbindung mit Prisma Access herzustellen. Ein weiterer Vorteil ist die Möglichkeit für GlobalProtect- und Remote-Netzwerke, über das Internet auf Internet- und öffentliche SaaS-Anwendungen zuzugreifen, wenn diese Internetziele IPv6-Verbindungen erfordern.

IPv6 bietet im Vergleich zu IPv4 einen erheblich größeren Adressraum und ermöglicht eine nahezu unbegrenzte Anzahl eindeutiger IP-Adressen. Gleichzeitig ist Dual Stack ein Übergangsansatz, der den gleichzeitigen Betrieb von Netzwerken und Geräten mithilfe von IPv4 und IPv6 ermöglicht. Dank nativer IPv6-Unterstützung ist Prisma Access kompatibel mit IPv6- und Dual-Stack-Verbindungen, um den Migrationsprozess von IPv4 auf IPv6 zu erleichtern, Abwärtskompatibilität sicherzustellen und Ihre Umstellung auf die Cloud und IPv6-fähige Netzwerke zu unterstützen.

## Unterstützung privater Apps

Einige Prisma Access-Bereitstellungen unterstützen IPv6-Verbindungen zu internen „privaten“ Apps. Prisma Access stellt mithilfe von Underlay Verbindungen mit Rechenzentren (Dienstverbindungen) und Zweigstellen (Remote-Netzwerke) her, in denen IPv6-Datenverkehr durch einen IPv4-Tunnel geleitet wird.

 ©2025 Palo Alto Networks, Inc.



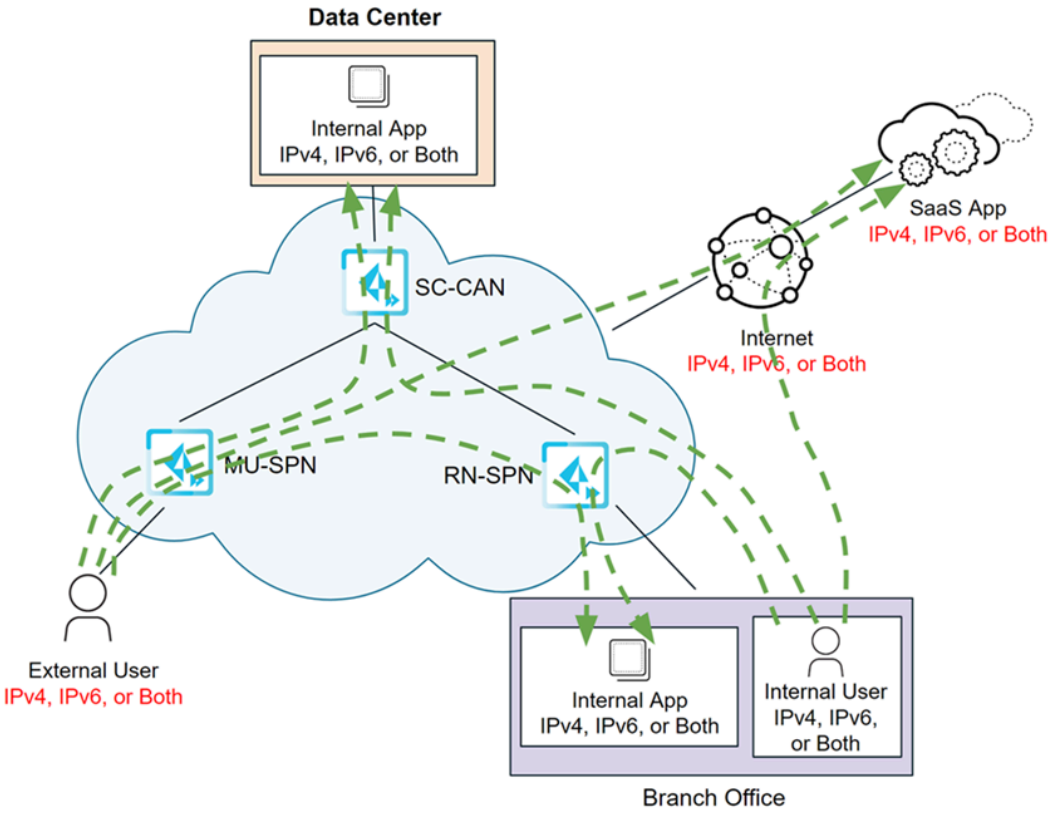

## Natives IPv6 in Prisma Access

Prisma Access

- Eingehende Dual-Stack-Verbindungen über IPv4/IPv6 mit Prisma Access
- Ausgehende Dual-Stack-Verbindungen über IPv4/IPv6 ins Internet und zu SaaS-Apps über das Internet

Jetzt können Benutzer mithilfe von IPv6 eine Verbindung mit dem Internet herstellen und „öffentliche“ SaaS-Apps über das Internet verwenden.

 ©2025 Palo Alto Networks, Inc.




*Externe Benutzer (mobile Benutzer) müssen mit einer der folgenden unterstützten GlobalProtect-Versionen arbeiten, damit natives IPv6 funktioniert:*

- *5.2.13-c418 (Win/Mac)*
- *6.0.7-c378 (Win/Mac)*
- *6.0.7-c20 (Linux)*
- *6.1.2 (Win/Mac/Linux)*
- *6.2.0-c89 (Win/Mac)*

In der folgenden Tabelle ist die Konnektivität aufgeführt, die bei Prisma Access-Bereitstellungen mit IPv4 und IPv6 unterstützt wird. Ein Häkchen zeigt an, dass diese Verbindung unterstützt wird, und ein Bindestrich zeigt an, dass sie nicht unterstützt wird.

 ©2025 Palo Alto Networks, Inc.

### IPv6 Not Enabled

| Mobile User IP Version | GlobalProtect IP Version | Internet Destination Gateway ➞ Internet | | Private App Access Service Connection ➞ Internet | | GlobalProtect Tunnel | NAT Gateway ➞ Internet |
|---|---|---|---|---|---|---|---|
| | | IPv4 | IPv6 | IPv4 | IPv6 | ESP | IPv4 ➞ IPv4 |
| IPv4 | IPv4 | ✓ | — | ✓ | — | IPv4 | NAT44 |
| Dual Stack | Dual Stack | ✓ | ✓ Sinkhole | ✓ | ✓ | IPv4 | NAT44 |
| IPv6 | — | — | — | — | — | — | — |

### IPv6 Enabled

| Mobile User IP Version | GlobalProtect IP Version | Internet Destination Gateway ➞ Internet | | Private App Access Service Connection ➞ Internet | | GlobalProtect Tunnel | NAT Gateway ➞ Internet | |
|---|---|---|---|---|---|---|---|---|
| | | IPv4 | IPv6 | IPv4 | IPv6 | ESP | IPv6 ➞ IPv4 | IPv6 ➞ IPv6 |
| IPv4 | IPv4 | ✓ | — | ✓ | — | IPv4 | NAT64 | NPTv6 |
| Dual Stack | Dual Stack | ✓ | ✓ | ✓ | ✓ | IPv6 | NAT64 | NPTv6 |
| IPv6 | Dual Stack | ✓ (DNS64 & NAT64 Req'd) | ✓ | ✓ (Custom DNS64 + NAT64) | ✓ | IPv6 | NAT64 | NPTv6 |

Folgen Sie diesen Workflows, um IPv6 in Ihrer Konfiguration zu aktivieren.

- ❑ IPv6-Netzwerke und -IP-Pools in Ihrer Prisma Access-Infrastruktur aktivieren und konfigurieren
- ❑ IPv6-Netzwerke für die Bereitstellung des Typs „Mobile Benutzer – GlobalProtect“ aktivieren
- ❑ IPv6-Netzwerke für Dienstverbindungen aktivieren
- ❑ IPv6-Netzwerke für Remote-Netzwerke aktivieren

## IPv6-Networking und #IP-Pools in Ihrer Prisma Access-Infrastruktur aktivieren und konfigurieren

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz Version 2.2 bevorzugt und höher |


©2025 Palo Alto Networks, Inc.

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| | ❑ Der native IPv6-Zugriff auf öffentliche und private Apps erfordert die folgenden Releases:<br>• Prisma Access (Managed by Strata Cloud Manager): Juni 2024 Release<br>• Prisma Access (Managed by Panorama): Prisma Access 5.1.1 nur für neue Bereitstellungen.<br>Alle anderen Bereitstellungen (einschließlich vorhandener Prisma Access (Managed by Panorama)-Bereitstellungen) unterstützen nur den Zugriff auf private Apps. |

Für jede Prisma Access-Bereitstellung müssen Sie IPv6 global aktivieren und ein IPv6-Subnetz in Ihrem Infrastruktursubnetz angeben, damit Prisma Access eine IPv6-Netzwerkinfrastruktur zwischen Ihren Remote-Netzwerkstandorten, mobilen Benutzern und Dienstverbindungen aufbauen kann. Führen Sie dazu die folgenden Schritte aus.

- Strata Cloud Manager
- Panorama

## IPv6-Netzwerke und IP-Pools in Ihrer Prisma Access-Infrastruktur aktivieren und konfigurieren (Strata Cloud Manager)

**STEP 1 |** Wählen Sie **Workflows** > **Einrichtung Prisma Access** > **Prisma Access** und dann das Zahnradsymbol aus, um die Einstellungen zu bearbeiten.

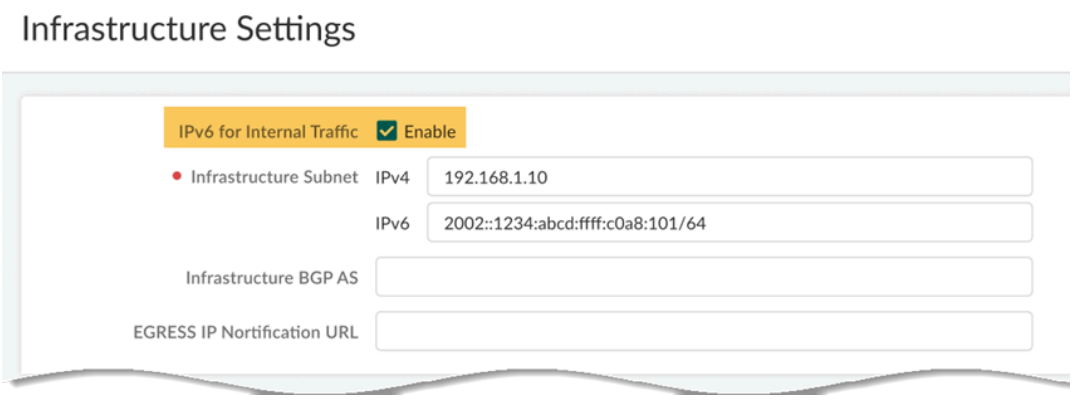
**STEP 2 |** Aktivieren Sie das Kontrollkästchen **IPv6 für internen Datenverkehr**.

Das Aktivieren oder Deaktivieren von IPv6 führt zu einer kurzen Datenverkehrsunterbrechung (bis zu 120 Sekunden), während das Dataplane sich darauf vorbereitet, IPv6-Routen auf dem Prisma Access-Backbone zu akzeptieren oder abzulehnen. Wir empfehlen, dass Sie diese

 ©2025 Palo Alto Networks, Inc.

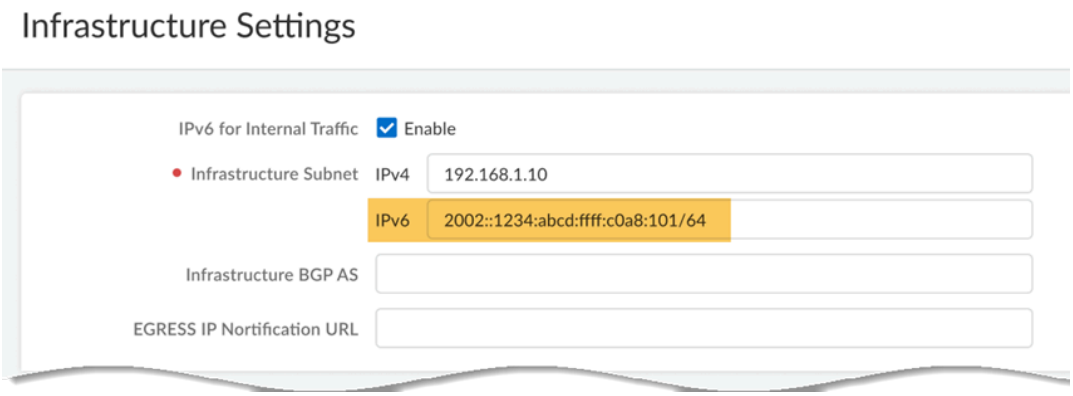
Konfigurationsänderung während eines Wartungsfensters oder außerhalb der Spitzenzeiten per Push übertragen.

*Wenn Sie IPv6 löschen müssen, löschen Sie alle Konfigurationen (ggf. auch für mobile Benutzer, Remote-Netzwerke und Dienstverbindungen), bevor Sie das Kontrollkästchen **IPv6 für internen Datenverkehr** deaktivieren.*




**STEP 3 |** Geben Sie ein **IPv6**-Infrastruktursubnetz und eine **Infrastruktur-BGP-AS** an.

- Geben Sie ein minimales Subnetz von /96 an.
- Sie müssen auch ein IPv4-Subnetz eingeben; Prisma Access benötigt IPv4- und IPv6-Subnetze in seiner Netzwerkinfrastruktur, um IPv6 zu verwenden. Weitere Einzelheiten finden Sie unter Prisma Access-Infrastrukturverwaltung.
- Palo Alto Networks empfiehlt, private (nicht öffentliche) IPv4- und IPv6-Adressen zu verwenden.
- Verwenden Sie keine IPv6-Local-Link-Adressen (fe80::/10).




**STEP 4 |** Geben Sie die **Infrastruktur-BGP-AS** ein, den Sie innerhalb der Prisma Access-Infrastruktur verwenden möchten.

Wenn Sie dynamisches Routing verwenden möchten, damit Prisma Access Routen zu Ressourcen in Ihren Remote-Netzwerken und Standorten des Hauptsitzes/Rechenzentrums dynamisch ermitteln können, geben Sie die AS-Nummer (Autonomes System) an. Wenn Sie keine AS-Nummer angeben, wird die Standard-AS-Nummer 65534 verwendet.

 ©2025 Palo Alto Networks, Inc.

**STEP 5 |** Falls Sie dies noch nicht getan haben, sollten Sie erwägen, interne DNS-Server hinzuzufügen, damit Prisma Access Ihre internen Domänen auflösen kann, um auf Dienste wie LDAP- und DNS-Server in Ihrem Unternehmensnetzwerk zuzugreifen.

Weitere Einzelheiten finden Sie unter Prisma Access-Infrastrukturverwaltung.

**STEP 6 |** (Nur Bereitstellungen für mobile Benutzer) Fügen Sie IPv6-IP-Adresspools für Ihre Bereitstellung für mobile Benutzer – GlobalProtect hinzu.

Eine Bereitstellung für mobile Benutzer – GlobalProtect erfordert IP-Adresspools. Sowohl IPv4- als auch IPv6-IP-Adresspools sind erforderlich, um die IPv6-Funktionalität zu aktivieren. Sie wenden IPv4-Adressen auf regionaler oder weltweiter Ebene und IPv6-Adressen auf weltweiter Ebene an. Geben Sie ein minimales Subnetz von /80 an.

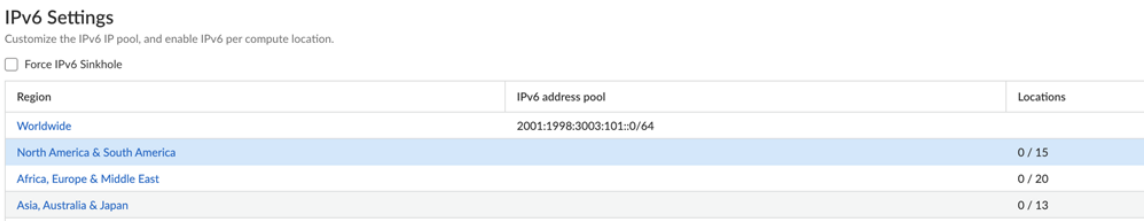
Prisma Access unterteilt die weltweiten IPv6-Adressen wie folgt:

- Prisma Access weist jedem Standort (Gateway) einen Pool aus einem /112-Subnetz zu. Da jede GlobalProtect-Verbindung eine IP-Adresse aus dem Pool verwendet, können durch diese Zuordnung pro Standort über 65.000 verfügbare IPv6-Adressen den Endpunkten der Benutzer zugewiesen werden.

  Wenn ein automatisches Skalierungsereignis auftritt (wenn sich eine große Anzahl von Benutzern an einem einzelnen Prisma Access-Standort anmeldet), kann Prisma Access einen anderen Standort mit einem anderen /112-Subnetz hinzufügen.
- Wenn an einem Standort IPv6 verwendet werden soll, weist Prisma Access der Region, zu der der Standort gehört, einen IPv6-Adresspool zu und teilt den Pool auf die Gesamtzahl der Regionen auf, in denen IPv6 aktiviert ist.

*Verwenden Sie keine Local-Link-Adressen (fe80::/10) in einem IP-Adresspool.*

1. Wählen Sie **Workflows** > **Einrichtung Prisma Access** > **GlobalProtect** und wählen dann Sie das Zahnradsymbol aus, um die Infrastruktureinstellungen zu bearbeiten.
2. Wählen Sie im Abschnitt „Client-IP-Pools“ eine **Region** oder **IP-Portal hinzufügen** aus.
3. Geben Sie einen **IPv6-Adresspool** ein.
   - Sie müssen sowohl IPv4- als auch IPv6-IP-Adressen für mobile Benutzer eingeben. Prisma Access benötigt IPv4- und IPv6-Adressen, um seine interne Infrastruktur zu unterstützen, wenn IPv6 verwendet wird.
   - Geben Sie ein minimales IPv6-Subnetz von /80 ein.
   - Prisma Access unterteilt jedes Subnetz pro Region.



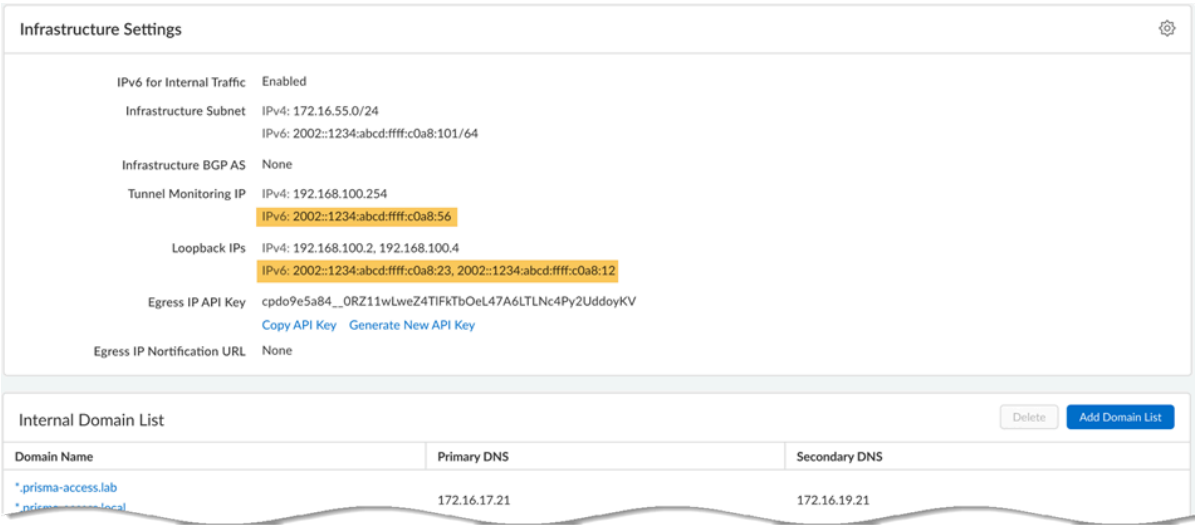

**STEP 7 |** Wählen Sie **Speichern** und **Konfiguration übertragen** aus.

 ©2025 Palo Alto Networks, Inc.

**STEP 8 |** Wählen Sie **Workflows** > **Einrichtung Prisma Access** > **Prisma Access** aus und notieren Sie sich die folgenden IPv6-Adressen in Ihren Infrastruktureinstellungen:

- **Umleitungs-IP-Adressen für Captive Portal** – Verwendet bei der auf dem Authentifizierungsportal basierenden Benutzer-ID-Adresszuordnung
- **IP-Adressen für Tunnelüberwachung** – Verwendet für die Tunnelüberwachung

Da mobile GlobalProtect-Benutzer eine IPv4-Adresse für die VPN-Tunnel benötigen, verwenden Loopback-Adressen, deren IP-Adressen aus dem Infrastruktursubnetz stammen, weiterhin IPv4-Adressen.




## IPv6-Networking und #IP-Pools in Ihrer Prisma Access-Infrastruktur aktivieren und konfigurieren (Panorama)

**STEP 1 |** Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Diensteinrichtung** aus und klicken Sie auf das Zahnradsymbol, um die Einstellungen zu bearbeiten.

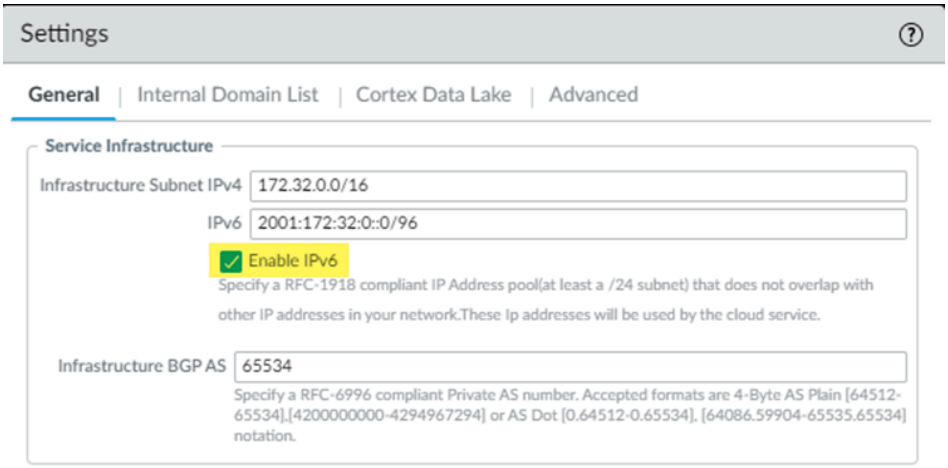
**STEP 2 |** Wählen Sie auf der Registerkarte **Allgemein** die Option **IPv6 aktivieren** aus.

Das Aktivieren oder Deaktivieren von IPv6 führt zu einer kurzen Datenverkehrsunterbrechung (bis zu 120 Sekunden), während sich das Dataplane darauf vorbereitet, IPv6-Routen auf dem Prisma Access-Backbone zu akzeptieren oder abzulehnen. Palo Alto Networks empfiehlt,

 ©2025 Palo Alto Networks, Inc.

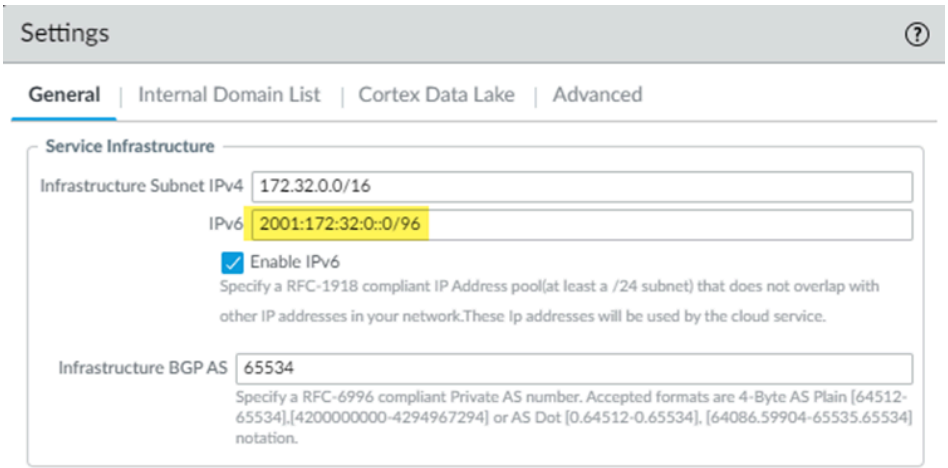
dass Sie diese Konfigurationsänderung während eines Wartungsfensters oder außerhalb der Spitzenzeiten vornehmen.

*Wenn Sie IPv6 löschen müssen, löschen Sie alle Konfigurationen (ggf. auch für mobile Benutzer, Remote-Netzwerke und Dienstverbindungen), bevor Sie das Kontrollkästchen **IPv6 aktivieren** deaktivieren.*




**STEP 3 |** Geben Sie ein **IPv6**-Infrastruktursubnetz und eine **Infrastruktur-BGP-AS** an.

- Geben Sie ein minimales Subnetz von /96 an.
- Sie müssen auch ein IPv4-Subnetz eingeben; Prisma Access benötigt IPv4- und IPv6-Subnetze in seiner Netzwerkinfrastruktur, um IPv6 zu verwenden. Weitere Einzelheiten finden Sie unter Konfigurieren Sie die Prisma Access-Dienstinfrastruktur (Panorama).
- Palo Alto Networks empfiehlt, private (nicht öffentliche) IPv4- und IPv6-Adressen zu verwenden.
- Verwenden Sie keine IPv6-Local-Link-Adressen (fe80::/10).




 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** Geben Sie die **Infrastruktur-BGP-AS** ein, die Sie innerhalb der Prisma Access-Infrastruktur verwenden möchten.

Wenn Sie dynamisches Routing verwenden möchten, damit Prisma Access Routen zu Ressourcen in Ihren Remote-Netzwerken und Standorten des Hauptsitzes/Rechenzentrums dynamisch ermitteln kann, geben Sie die AS-Nummer (Autonomes System) an. Wenn Sie keine AS-Nummer angeben, wird die Standard-AS-Nummer 65534 verwendet.

**STEP 5 |** Wenn Sie die Konfiguration der Diensteinrichtung noch nicht abgeschlossen haben, geben Sie die **Liste interner Domänen**, den **Strata-Protokollierungsdienst** und die **erweiterten** Einstellungen ein.

Weitere Einzelheiten finden Sie unter Konfigurieren Sie die Prisma Access-Dienstinfrastruktur (Panorama).

**STEP 6 |** (Nur Bereitstellungen für mobile Benutzer) Fügen Sie IPv6-IP-Adresspools für Ihre Bereitstellung für mobile Benutzer – GlobalProtect hinzu.

Eine Bereitstellung für mobile Benutzer – GlobalProtect erfordert IP-Adresspools. Sowohl IPv4- als auch IPv6-IP-Adresspools sind erforderlich, um die IPv6-Funktionalität zu aktivieren. Sie wenden IPv4-Adressen auf regionaler oder weltweiter Ebene und IPv6-Adressen auf weltweiter Ebene an. Geben Sie ein minimales Subnetz von /80 an.

Prisma Access unterteilt die weltweiten IPv6-Adressen wie folgt:

- Prisma Access weist jedem Standort (Gateway) einen Pool aus einem /112-Subnetz zu. Da jede GlobalProtect-Verbindung eine IP-Adresse aus dem Pool verwendet, können durch

 ©2025 Palo Alto Networks, Inc.

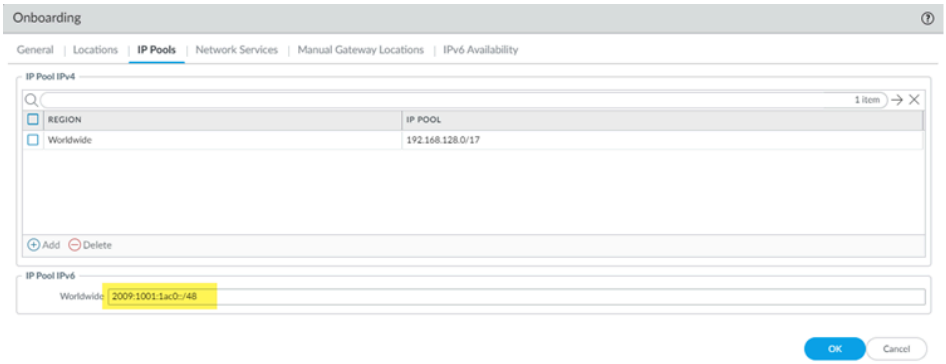
diese Zuordnung pro Standort über 65.000 verfügbare IPv6-Adressen den Endpunkten der Benutzer zugewiesen werden.

Wenn ein automatisches Skalierungsereignis auftritt (wenn sich eine große Anzahl von Benutzern an einem einzelnen Prisma Access-Standort anmeldet), kann Prisma Access einen weiteren Standort mit einem anderen /112-Subnetz hinzufügen.

- Wenn an einem Standort IPv6 verwendet werden soll, weist Prisma Access der Region, zu der der Standort gehört, einen IPv6-Adresspool zu und teilt den Pool auf die Gesamtzahl der Regionen auf, in denen IPv6 aktiviert ist.

*Verwenden Sie keine Local-Link-Adressen (fe80::/10) in einem IP-Adresspool.*

1. Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Mobile Benutzer – GlobalProtect** aus.
2. Wählen Sie im Abschnitt „Onboarding“ den **Hostnamen** des Portals oder **Konfigurieren** aus.
3. Wählen Sie die Registerkarte **IP-Pools** aus.
4. Geben Sie einen **IPv6-IP-Pool** ein.
   - Sie müssen sowohl IPv4- als auch IPv6-IP-Adressen für mobile Benutzer eingeben. Prisma Access benötigt IPv4- und IPv6-Adressen, um seine interne Infrastruktur zu unterstützen, wenn IPv6 verwendet wird.
   - Geben Sie ein minimales IPv6-Subnetz von /80 ein.
   - Prisma Access unterteilt jedes Subnetz pro Region.



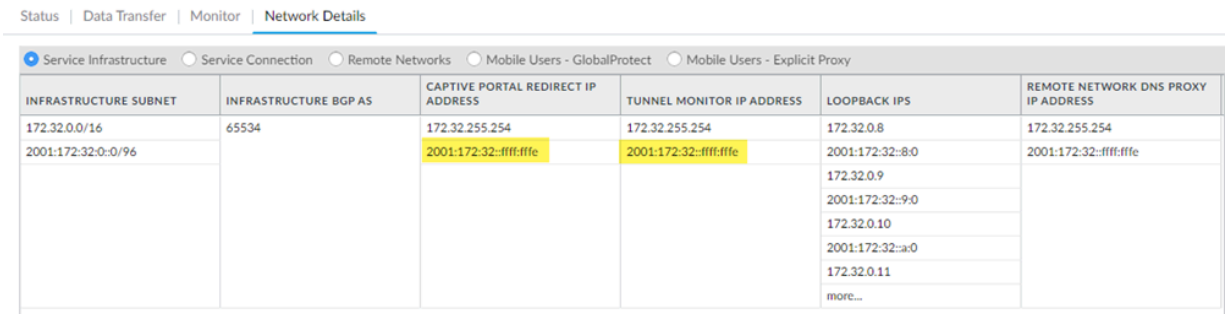

**STEP 7 |** Führen Sie für Ihre Änderungen die Aktion **Commit und Push** aus.

 ©2025 Palo Alto Networks, Inc.

**STEP 8 |** Wählen Sie **Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Dienstinfrastruktur** aus und notieren Sie sich die folgenden IPv6-Adressen:

- **Umleitungs-IP-Adressen für Captive Portal** – Verwendet bei der auf dem Authentifizierungsportal basierenden Benutzer-ID-Adresszuordnung
- **IP-Adressen für Tunnelüberwachung** – Verwendet für die Tunnelüberwachung

Da mobile GlobalProtect-Benutzer eine IPv4-Adresse für die VPN-Tunnel benötigen, verwenden Loopback-Adressen, deren IP-Adressen aus dem Infrastruktursubnetz stammen, weiterhin IPv4-Adressen.




# IPv6-Networking für die Bereitstellung für mobile Benutzer – GlobalProtect aktivieren

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz Version 2.2 bevorzugt und höher<br>❑ Der native IPv6-Zugriff auf öffentliche und private Apps erfordert die folgenden Releases:<br>• Prisma Access (Managed by Strata Cloud Manager): Juni 2024 Release<br>• Prisma Access (Managed by Panorama): Prisma Access 5.1.1 nur für neue Bereitstellungen.<br>Alle anderen Bereitstellungen (einschließlich vorhandener Prisma Access (Managed by Panorama)-Bereitstellungen) unterstützen nur den Zugriff auf private Apps. |

Zusätzlich zur Angabe von IP-Adresspools für mobile Benutzer müssen Sie die **IPv6-Verfügbarkeit** für Ihre Bereitstellungen für mobile Benutzer – GlobalProtect konfigurieren. Wenn Ihr Netzwerk IPv6-DNS-Server zur Auflösung interner Domänen verwendet, können Sie auch IPv6-Adressen für primäre und sekundäre DNS-Server angeben, wie im folgenden Abschnitt gezeigt.

- Strata Cloud Manager

 ©2025 Palo Alto Networks, Inc.

- Panorama

## IPv6-Networking für die Bereitstellung für mobile Benutzer – GlobalProtect Deployment aktivieren (Strata Cloud Manager)

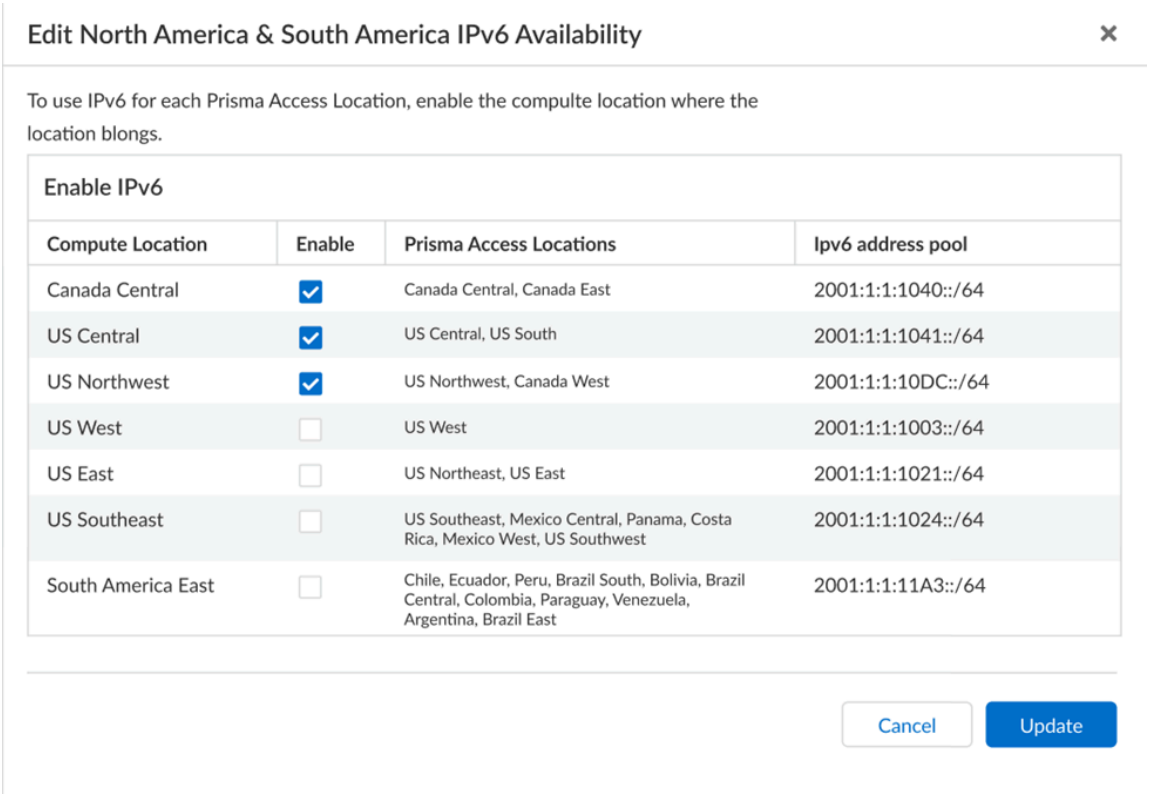
Zusätzlich zur Angabe von IP-Adresspools für mobile Benutzer müssen Sie die **IPv6-Verfügbarkeit** für Ihre Bereitstellungen für mobile Benutzer – GlobalProtect konfigurieren. Wenn Ihr Netzwerk IPv6-DNS-Server zur Auflösung interner Domänen verwendet, können Sie auch IPv6-Adressen für primäre und sekundäre DNS-Server angeben, wie im folgenden Abschnitt gezeigt.

**STEP 1 |** Planen Sie, ob Sie IPv6 für Ihre gesamte Prisma Access-Bereitstellung oder nur für eine bestimmte Anzahl von Compute-Standorten bereitstellen möchten.

**STEP 2 |** Konfigurieren Sie die IPv6-Verfügbarkeit für die Regionen, in denen Sie IPv6 bereitstellen möchten.

1. Wählen Sie **Workflows** > **Einrichtung Prisma Access** > **GlobalProtect** und dann das Zahnradsymbol aus, um die **Infrastruktureinstellungen** zu bearbeiten.
2. Wählen Sie im Abschnitt **IPv6-Einstellungen** die Standorte aus, für die Sie IPv6 **aktivieren** möchten.

   Alle Standorte sind einem Compute-Standort zugeordnet. Wenn an Standorten in einem Compute-Standort IPv6 nicht aktiviert ist, lassen Sie diesen Compute-Standort deaktiviert.




**STEP 3 |** (Optional) Wenn Ihre internen DNS-Server über IPv6-Adressen erreichbar sind, aktivieren Sie im Abschnitt **Client-DNS** die Option **Region hinzufügen**, aktivieren Sie das Kontrollkästchen **Interne Domänen auflösen**, **fügen** Sie eine Regel hinzu bzw. geben Sie

 ©2025 Palo Alto Networks, Inc.

die Standardregel an und geben Sie **benutzerdefinierte** DNS-Server-IPv6-Adressen für den **primären DNS**- und den **sekundären DNS**-Server an.

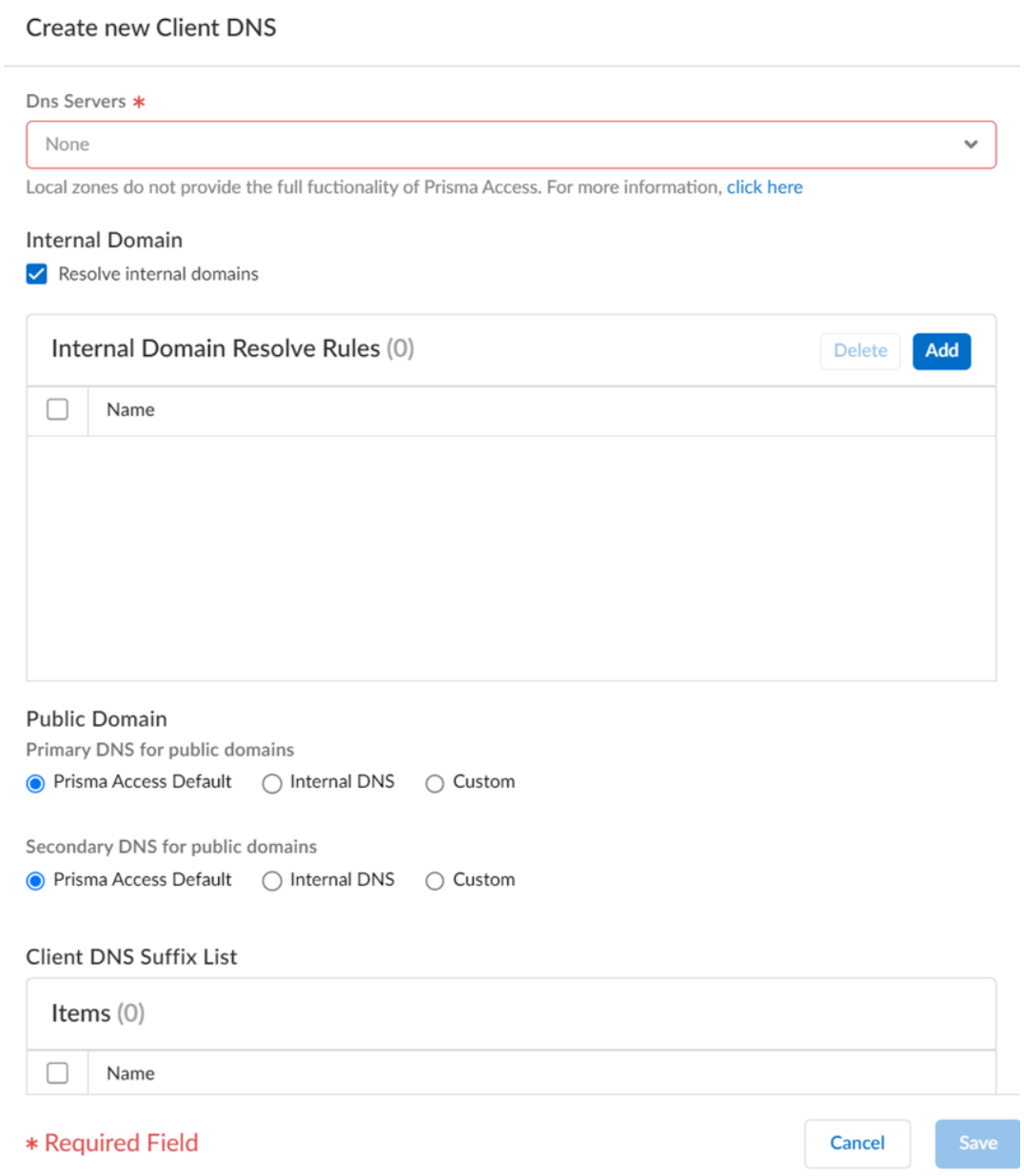
Wenn Sie IPv6-Adressen für DNS-Server eingeben, müssen Sie auch IPv6-Adressen in Ihrem IP-Adresspool für mobile Benutzer haben.

Sie können eine beliebige Kombination von IPv4- oder IPv6-Adressen für primäre und sekundäre DNS-Server eingeben. Wenn Sie eine IPv6-Adresse für den primären DNS-Server und eine IPv4-Adresse für den sekundären DNS-Server eingeben und eine DNS-Abfrage von

 ©2025 Palo Alto Networks, Inc.

einem Compute-Standort empfangen wird, an dem **IPv6-Verfügbarkeit** nicht aktiviert ist, verwendet Prisma Access den sekundären DNS-Server, da dieser eine IPv4-Adresse nutzt.

*IPv4-Adressen verwenden A-Einträge, während IPv6-Adressen AAAA-Einträge verwenden. Einige DNS-Server können AAAA-DNS-Lookups über IPv4-Transport durchführen; daher benötigen Sie möglicherweise keinen Server mit einer IPv6-IP-Adresse.*




**STEP 4 |** (Optional) Wenn Sie die Konfiguration für mobile Benutzer noch nicht abgeschlossen haben, schließen Sie sie jetzt ab. Weitere Informationen finden Sie unter Mobile GlobalProtect-Benutzer einrichten.

 ©2025 Palo Alto Networks, Inc.

**STEP 5 |** Klicken Sie auf **Konfiguration übertragen**, um die Änderungen in Ihrem Netzwerk bereitzustellen.

## IPv6-Networking für die Bereitstellung für mobile Benutzer – GlobalProtect Deployment aktivieren (Panorama)

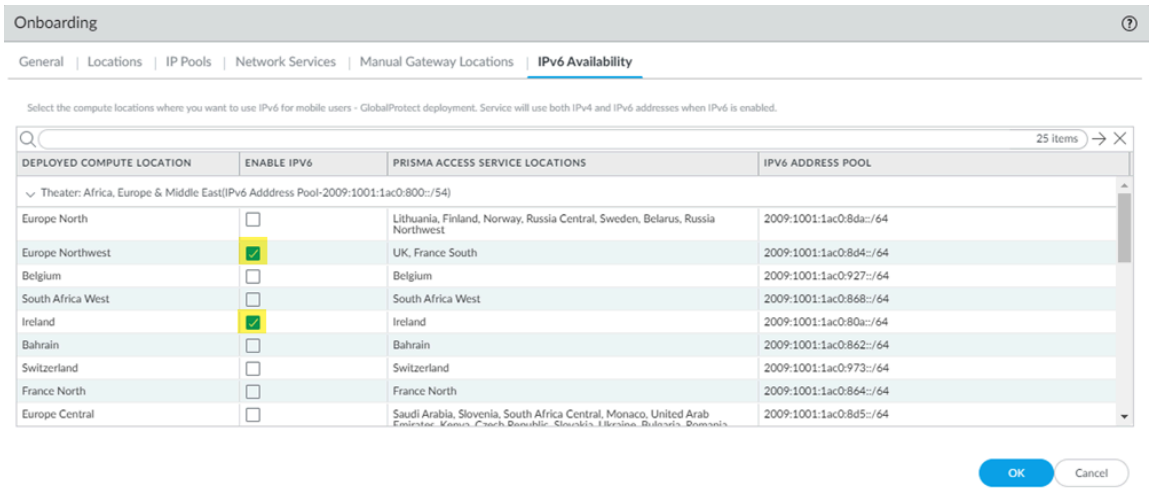
Zusätzlich zur Angabe von IP-Adresspools für mobile Benutzer müssen Sie die **IPv6-Verfügbarkeit** für Ihre Bereitstellungen für mobile Benutzer – GlobalProtect konfigurieren. Wenn Ihr Netzwerk IPv6-DNS-Server zur Auflösung interner Domänen verwendet, können Sie auch IPv6-Adressen für primäre und sekundäre DNS-Server angeben, wie im folgenden Abschnitt gezeigt.

**STEP 1 |** Planen Sie, ob Sie IPv6 für Ihre gesamte <ph keyref="pa"/>-Bereitstellung oder nur für eine bestimmte Anzahl von Compute-Standorten bereitstellen möchten.

**STEP 2 |** Konfigurieren Sie die IPv6-Verfügbarkeit für die Regionen, in denen Sie IPv6 bereitstellen möchten.

1. **Aktivieren Sie IPv6** auf der Registerkarte **IPv6-Verfügbarkeit** für die Standorte, für die Sie IPv6 aktivieren möchten.

   Alle Standorte sind einem Compute-Standort zugeordnet. Wenn an Standorten in einem Compute-Standort IPv6 nicht aktiviert ist, lassen Sie diesen Compute-Standort deaktiviert.




**STEP 3 |** (Optional) Wenn Ihre internen DNS-Server über IPv6-Adressen erreichbar sind, klicken Sie auf die Registerkarte **Netzwerkdienste**, **fügen** Sie eine Regel hinzu bzw. geben Sie die Standardregel an und geben Sie IPv6-Adressen des **benutzerdefinierten DNS-Servers** für den **primären DNS**- und den **sekundären DNS**-Server an.

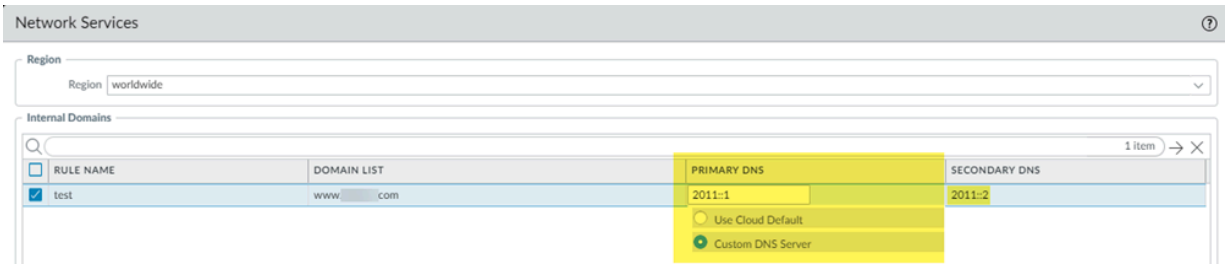
Wenn Sie IPv6-Adressen für DNS-Server eingeben, müssen Sie auch IPv6-Adressen in Ihrem IP-Adresspool für mobile Benutzer haben.

Sie können eine beliebige Kombination von IPv4- oder IPv6-Adressen für primäre und sekundäre DNS-Server eingeben. Wenn Sie eine IPv6-Adresse für den primären DNS-Server und eine IPv4-Adresse für den sekundären DNS-Server eingeben und eine DNS-Abfrage von

 ©2025 Palo Alto Networks, Inc.

einem Compute-Standort empfangen wird, an dem **IPv6-Verfügbarkeit** nicht aktiviert ist, verwendet <ph keyref="pa"/> den sekundären DNS-Server, da dieser eine IPv4-Adresse nutzt.

*IPv4-Adressen verwenden A-Einträge, während IPv6-Adressen AAAA-Einträge verwenden. Einige DNS-Server können AAAA-DNS-Lookups über IPv4-Transport durchführen; daher benötigen Sie möglicherweise keinen Server mit einer IPv6-IP-Adresse.*




**STEP 4 |** (Optional) Wenn Sie die Konfiguration für mobile Benutzer noch nicht abgeschlossen haben, schließen Sie sie jetzt ab. Weitere Informationen finden Sie unter Mobile GlobalProtect-Benutzer einrichten.

**STEP 5 |** Führen Sie für Ihre Änderungen die Aktion **Commit und Push** aus.

# IPv6-Networking für Dienstverbindungen aktivieren

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz Version 2.2 bevorzugt und höher<br>❑ Der native IPv6-Zugriff auf öffentliche und private Apps erfordert die folgenden Releases:<br>• Prisma Access (Managed by Strata Cloud Manager): Juni 2024 Release<br>• Prisma Access (Managed by Panorama): Prisma Access 5.1.1 nur für neue Bereitstellungen.<br>Alle anderen Bereitstellungen (einschließlich vorhandener Prisma Access (Managed by Panorama)-Bereitstellungen) unterstützen nur den Zugriff auf private Apps. |

Für Dienstverbindungen können Sie IPv6-Subnetze für statisches oder BGP-Routing verwenden. Für BGP-Routing können Sie IPv6-Peer-Adressen eingeben und IPv4- sowie IPv6-Routing-Optionen angeben.

 ©2025 Palo Alto Networks, Inc.

Führen Sie die folgende Aufgabe aus, um IPv6-Networking für Dienstverbindungen zu konfigurieren.

- Prisma Access (Managed by Strata Cloud Manager)
- Prisma Access (Managed by Panorama)

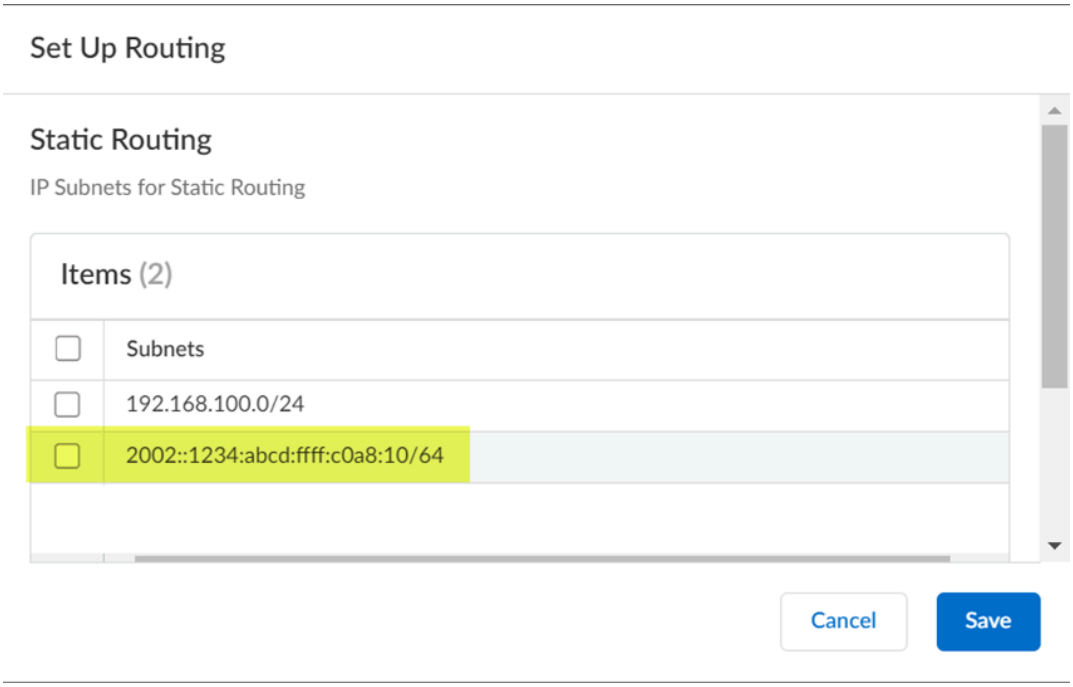
## IPv6-Networking für Dienstverbindungen aktivieren (Strata Cloud Manager)

**STEP 1 |** Wählen Sie **Workflows** > **Einrichtung Prisma Access** > **Dienstverbindungen** und **Dienstverbindung hinzufügen** aus.

**STEP 2 |** Fügen Sie eine neue Dienstverbindung hinzu oder wählen Sie eine vorhandene Dienstverbindung aus, um sie zu bearbeiten.

**STEP 3 |** Richten Sie IPv6-Routing für die Dienstverbindung ein.

1. (Nur Bereitstellungen für statisches Routing) Geben Sie auf der Registerkarte **Statisches Routing** ein oder mehrere **Unternehmenssubnetze** ein.




2. (Nur Bereitstellungen für BGP-Routing) Geben Sie die Methode zum Austausch von IPv4- und IPv6-BGP-Routen an. Geben Sie dann eine IPv6-**Peer-Adresse** und eine **lokale Adresse** ein.
   - Um eine einzelne IPv4-BGP-Sitzung zum Austausch von IPv4- und IPv6-BGP-Peering-Informationen zu verwenden, wählen Sie **IPv4- und IPv6-Routen über IPv4-Peering austauschen** aus.
   - Um eine IPv4-BGP-Sitzung zum Austausch von IPv4-BGP-Peering-Informationen und eine IPv6-Sitzung zum Austausch von IPv6-BGP-Peering-Informationen zu

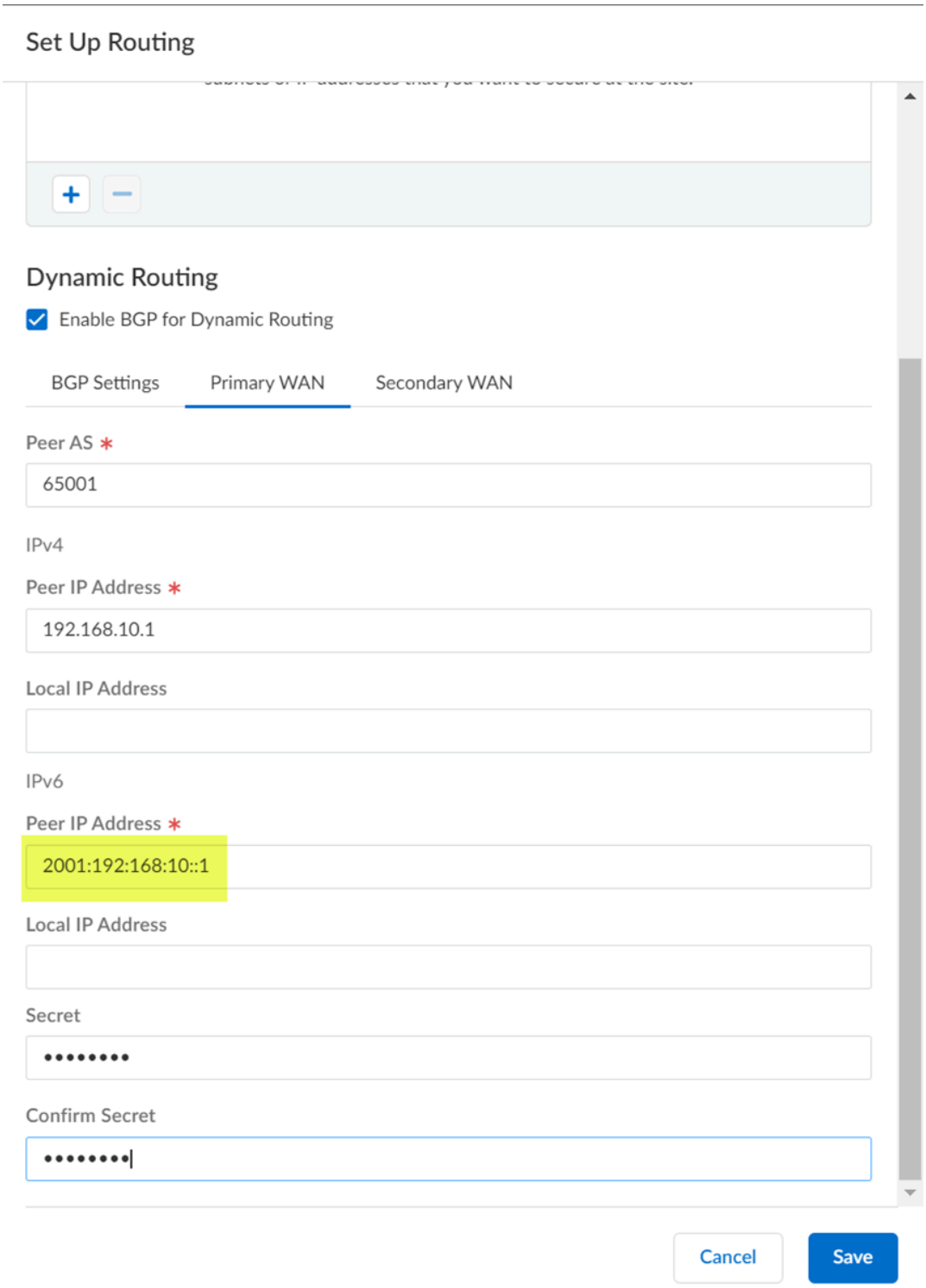
 ©2025 Palo Alto Networks, Inc.

verwenden, wählen Sie **IPv4-Routen über IPv4-Peering und IPv6-Routen über IPv6-Peering austauschen** aus.

- Um eine einzelne IPv6-BGP-Sitzung zum Austausch von IPv6-BGP-Peering-Informationen zu verwenden, wählen Sie **IPv6-Routen über IPv6-Peering austauschen** aus.

3. Wenn Ihr sekundäres WAN eine andere Peer-Adresse oder lokale Adresse verwendet, deaktivieren Sie **Wie primäres WAN** und geben Sie die IPv6-**Peer-Adresse** und die **lokale Adresse** für das sekundäre WAN ein.

 ©2025 Palo Alto Networks, Inc.




 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** Wenn Sie die Einrichtung Ihrer Dienstverbindung noch nicht abgeschlossen haben, schließen Sie sie jetzt ab. Weitere Details finden Sie unter Dienstverbindung in Prisma Access konfigurieren.

> *Der IPv6-Internetzugang für Dienstverbindungen wird durch eine Underlay-Verbindung ermöglicht, bei der der IPv6-Datenverkehr durch einen IPv4-Tunnel geleitet wird.*

**STEP 5 |** Klicken Sie auf **Konfiguration übertragen**, um die Änderungen in Ihrem Netzwerk bereitzustellen.

**STEP 6 |** Wenn Sie die Konfiguration der mobilen Benutzer noch nicht abgeschlossen haben, schließen Sie sie jetzt ab.

## IPv6-Networking für Dienstverbindungen aktivieren (Panorama)

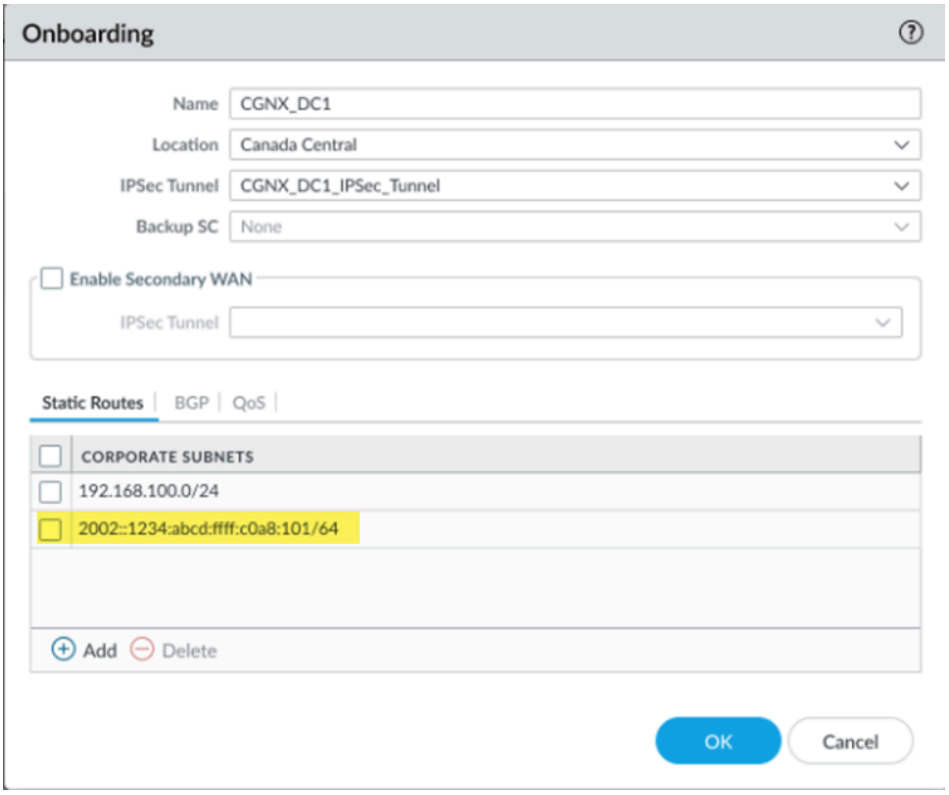
**STEP 1 |** Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Dienstverbindung** aus.

**STEP 2 |** **Fügen** Sie eine neue Dienstverbindung hinzu oder wählen Sie eine vorhandene Dienstverbindung aus, um diese zu bearbeiten.

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Richten Sie IPv6-Routing für die Dienstverbindung ein.

1. (Nur Bereitstellungen für statisches Routing) Geben Sie auf der Registerkarte **Statisches Routing** ein oder mehrere **Unternehmenssubnetze** ein.




2. (Nur Bereitstellungen für BGP-Routing) Geben Sie die Methode zum Austausch von IPv4- und IPv6-BGP-Routen an. Geben Sie dann eine IPv6-**Peer-Adresse** und eine **lokale Adresse** ein.

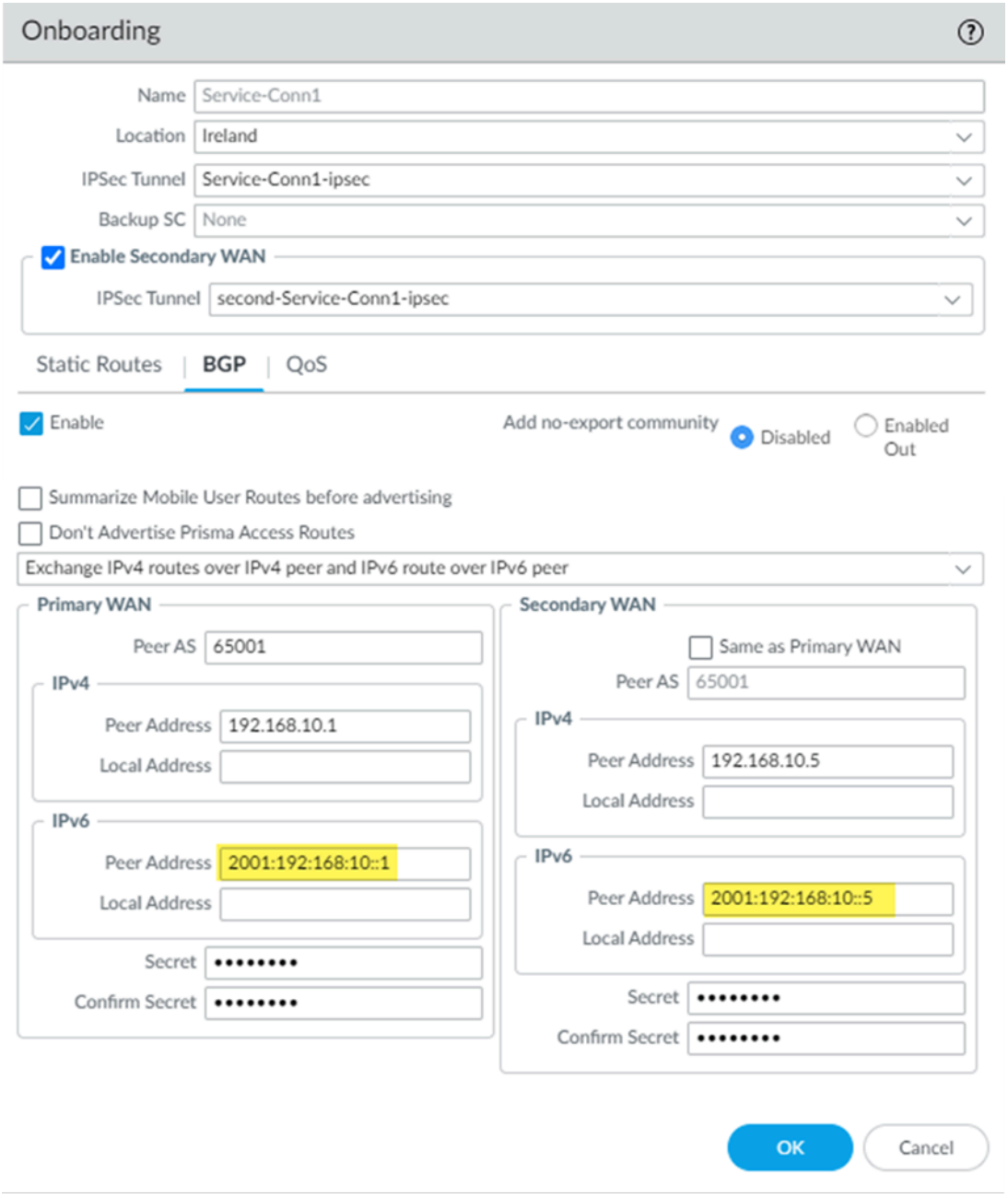
   - Um eine einzelne IPv4-BGP-Sitzung zum Austausch von IPv4- und IPv6-BGP-Peering-Informationen zu verwenden, wählen Sie **IPv4- und IPv6-Routen über IPv4-Peering austauschen** aus.
   - Um eine IPv4-BGP-Sitzung zum Austausch von IPv4-BGP-Peering-Informationen und eine IPv6-Sitzung zum Austausch von IPv6-BGP-Peering-Informationen zu

 ©2025 Palo Alto Networks, Inc.

verwenden, wählen Sie **IPv4-Routen über IPv4-Peering und IPv6-Routen über IPv6-Peering austauschen** aus.

- Um eine einzelne IPv6-BGP-Sitzung zum Austausch von IPv6-BGP-Peering-Informationen zu verwenden, wählen Sie **IPv6-Routen über IPv6-Peering austauschen** aus.

3. Wenn Ihr sekundäres WAN eine andere Peer-Adresse oder lokale Adresse verwendet, deaktivieren Sie **Wie primäres WAN** und geben Sie die IPv6-**Peer-Adresse** und die **lokale Adresse** für das sekundäre WAN ein.




**STEP 4 |** Wenn Sie die Einrichtung Ihrer Dienstverbindung noch nicht abgeschlossen haben, schließen Sie sie jetzt ab. Weitere Informationen finden Sie unter Dienstverbindung in Prisma Access konfigurieren.

 ©2025 Palo Alto Networks, Inc.

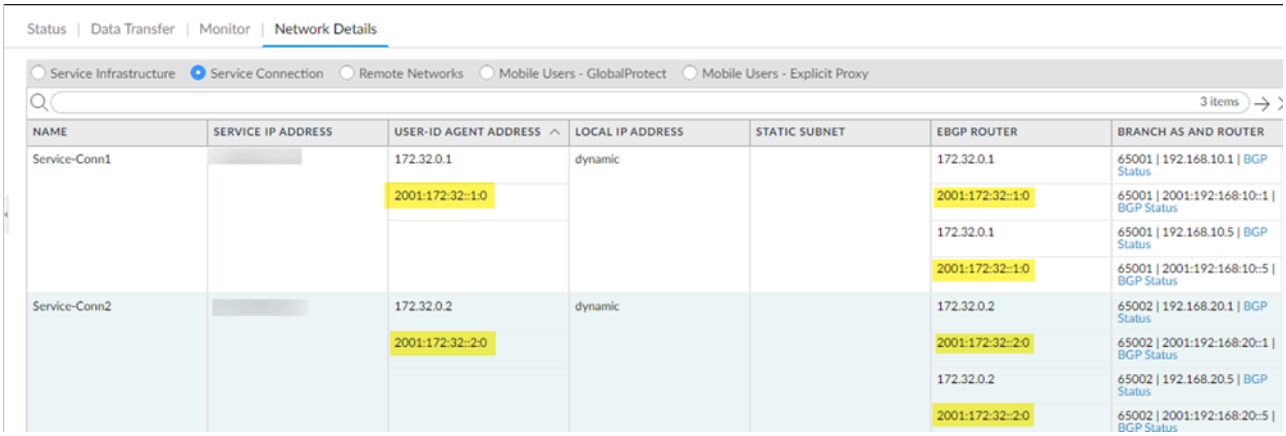
**STEP 5 |** Führen Sie für Ihre Änderungen die Aktion **Commit und Push** aus.

**STEP 6 |** Wählen Sie **Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Dienstverbindung** aus und notieren Sie sich die IPv6-**Benutzer-ID-Agent-Adresse** und Adressen vom **EBGP-Router**.

Nachdem Sie Ihre Änderungen übernommen haben, haben Sie eine IPv6-**Benutzer-ID-Agent-Adresse** (die für Benutzer-ID-Abruf und #Verteilung verwendet wird) und Adressen vom **EBGP-Router** für Dienstverbindungen.

Da der für die Dienstverbindung verwendete IPSec-Tunnel eine IPv4-Adressierung verwendet, ist die **Dienst-IP-Adresse** eine IPv4-Adresse.

Der IPv6-Internetzugang für Dienstverbindungen wird durch eine Underlay-Verbindung ermöglicht, bei der der IPv6-Datenverkehr durch einen IPv4-Tunnel geleitet wird.




**STEP 7 |** Wenn Sie die Konfiguration der mobilen Benutzer noch nicht abgeschlossen haben, schließen Sie sie jetzt ab.

# IPv6-Networking für Remote-Netzwerke aktivieren

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz Version 2.2 bevorzugt und höher<br>❑ Der native IPv6-Zugriff auf öffentliche und private Apps erfordert die folgenden Releases:<br>• Prisma Access (Managed by Strata Cloud Manager): Juni 2024 Release<br>• Prisma Access (Managed by Panorama): Prisma Access 5.1.1 nur für neue Bereitstellungen.<br>Alle anderen Bereitstellungen (einschließlich vorhandener Prisma Access (Managed by Panorama)-Bereitstellungen) |

 ©2025 Palo Alto Networks, Inc.

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| | unterstützen nur den Zugriff auf private Apps. |

Für Remote-Netzwerkverbindungen können Sie IPv6-Subnetze für statische Routen verwenden. Beim BGP-Routing können Sie IPv6-Peer-Adressen eingeben und festlegen, dass BGP nur IPv6-Routing oder sowohl IPv4- als auch IPv6-Routing verwendet.

Führen Sie die folgende Aufgabe aus, um IPv6-Networking für Remote-Netzwerkverbindungen zu konfigurieren.

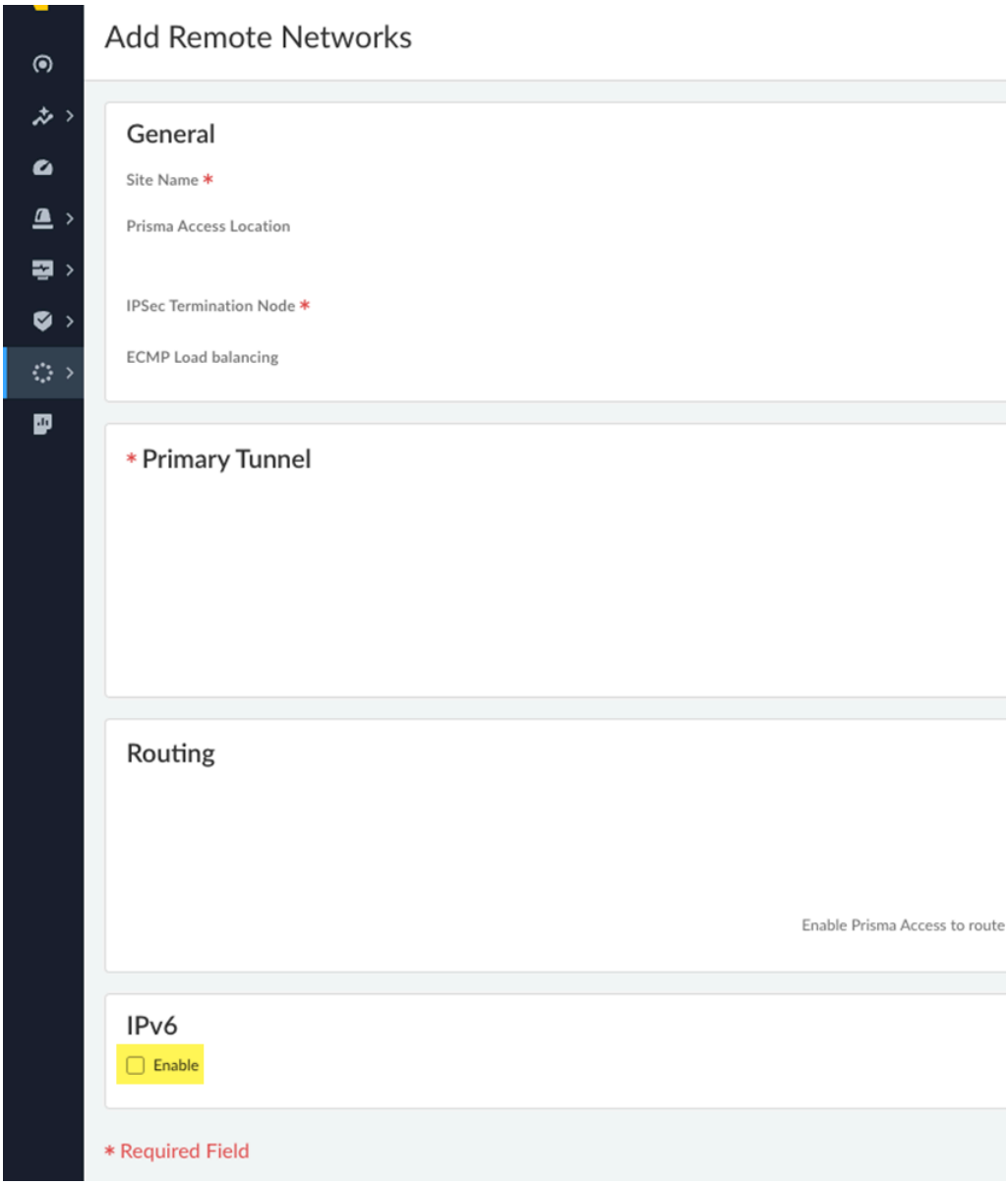
- Prisma Access (Managed by Strata Cloud Manager)
- Prisma Access (Managed by Panorama)

## IPv6-Networking für Remote-Netzwerke aktivieren (Strata Cloud Manager)

**STEP 1 |** Wählen Sie **Workflows** > **Einrichtung Prisma Access** > **Remote-Netzwerke**und **Remote-Netzwerke hinzufügen** aus.

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** **Aktivieren** Sie IPv6.

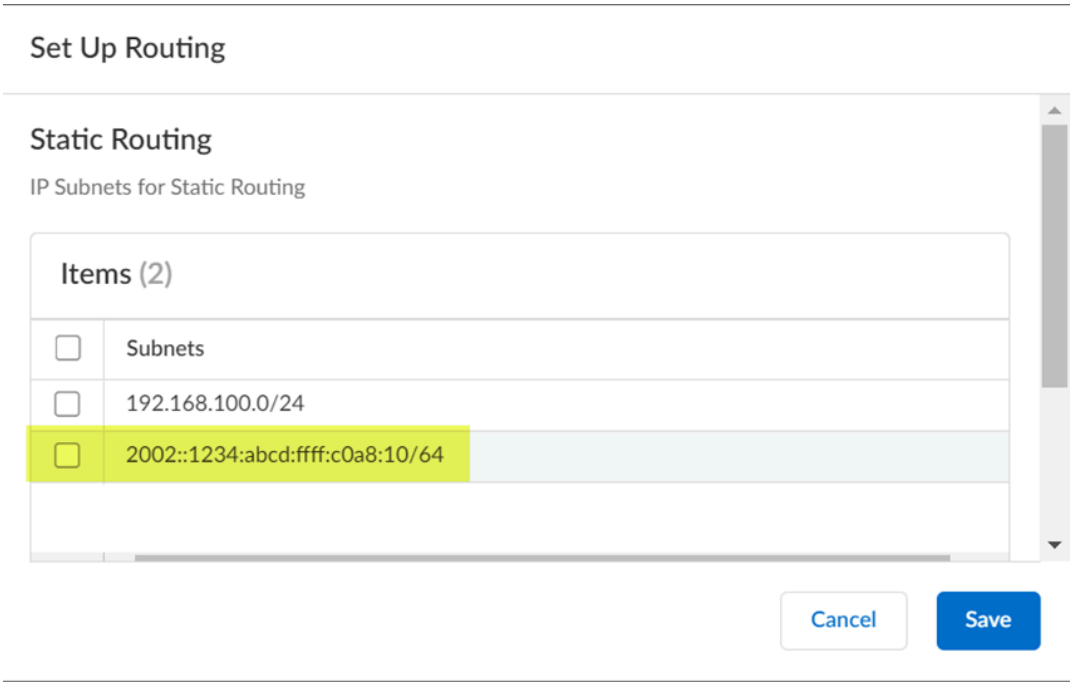



**STEP 3 |** Fügen Sie eine neue Remote-Netzwerkverbindung hinzu oder wählen Sie eine vorhandene Remote-Netzwerkverbindung aus, um sie zu bearbeiten.

 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** Richten Sie IPv6-Routing für Ihr Remote-Netzwerk ein.

1. (Nur Bereitstellungen für statisches Routing) Geben Sie auf der Registerkarte **Statisches Routing** ein oder mehrere **Unternehmenssubnetze** ein.




2. (Nur Bereitstellungen für BGP-Routing) Geben Sie die Methode zum Austausch von IPv4- und IPv6-BGP-Routen an. Geben Sie dann eine IPv6-**Peer-Adresse** und eine **lokale Adresse** ein.
   - Um eine einzelne IPv4-BGP-Sitzung zum Austausch von IPv4- und IPv6-BGP-Peering-Informationen zu verwenden, wählen Sie **IPv4- und IPv6-Routen über IPv4-Peering austauschen** aus.
   - Um eine IPv4-BGP-Sitzung zum Austausch von IPv4-BGP-Peering-Informationen und eine IPv6-Sitzung zum Austausch von IPv6-BGP-Peering-Informationen zu

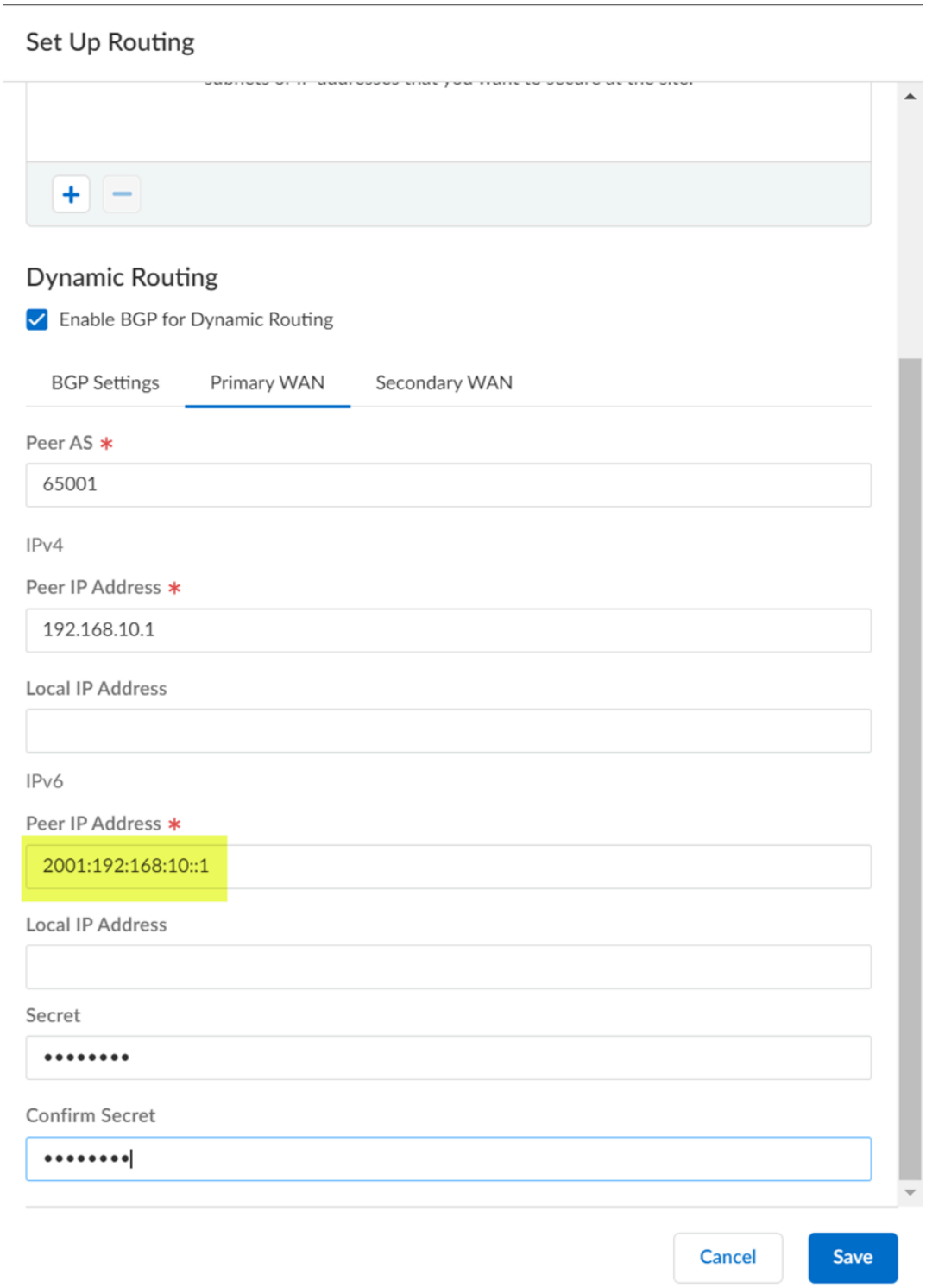
 ©2025 Palo Alto Networks, Inc.

verwenden, wählen Sie **IPv4-Routen über IPv4-Peering und IPv6-Routen über IPv6-Peering austauschen** aus.

- Um eine einzelne IPv6-BGP-Sitzung zum Austausch von IPv6-BGP-Peering-Informationen zu verwenden, wählen Sie **IPv6-Routen über IPv6-Peering austauschen** aus.

3. Wenn Ihr sekundäres WAN eine andere Peer-Adresse oder lokale Adresse verwendet, deaktivieren Sie **Wie primäres WAN** und geben Sie die IPv6-**Peer-Adresse** und die **lokale Adresse** für das sekundäre WAN ein.

 ©2025 Palo Alto Networks, Inc.




**STEP 5 |** (Optional) Wenn Ihre internen DNS-Server über IPv6-Adressen erreichbar sind, wählen Sie **Workflows** > **Einrichtung Prisma Access** > **Remote-Netzwerke** > **Erweiterte Einstellungen** aus. Suchen Sie **DNS-Proxy**, **fügen** Sie eine Regel hinzu bzw. geben Sie die Standardregel an

 ©2025 Palo Alto Networks, Inc.

und geben Sie IPv6-Adressen des **benutzerdefinierten DNS-Servers** für den **primären DNS**- und **sekundären DNS**-Server an.

Mit Prisma Access können Sie DNS-Server angeben, um sowohl unternehmensinterne als auch externe Domänen aufzulösen. Wenn Sie keine Einstellungen angeben, leitet Prisma Access DNS-Anfragen für Remote-Netzwerke nicht weiter. Sie müssen auch eine **Region** auswählen.

Sie können eine beliebige Kombination von IPv4- oder IPv6-Adressen für primäre und sekundäre DNS-Server eingeben.

- *IPv4-Adressen verwenden A-Einträge, während IPv6-Adressen AAAA-Einträge verwenden. Einige DNS-Server können AAAA-DNS-Lookups über IPv4-Transport durchführen; daher benötigen Sie möglicherweise keinen Server mit einer IPv6-IP-Adresse.*

**STEP 6 |** Wenn Sie die Einrichtung der Remote-Netzwerkverbindungen noch nicht abgeschlossen haben, schließen Sie sie jetzt ab.

*IPv6-Internetzugang für Remote-Netzwerkverbindungen wird durch eine Underlay-Verbindung ermöglicht, bei der IPv6-Datenverkehr durch einen IPv4-Tunnel geleitet wird.*

**STEP 7 |** Klicken Sie auf **Konfiguration übertragen**, um die Änderungen in Ihrem Netzwerk bereitzustellen.

## IPv6-Networking für Remote-Netzwerke aktivieren (Panorama)

**STEP 1 |** (Optional) Geben Sie IPv6-Adressen in die Proxy-Konfiguration Ihres benutzerdefinierten DNS-Servers ein.

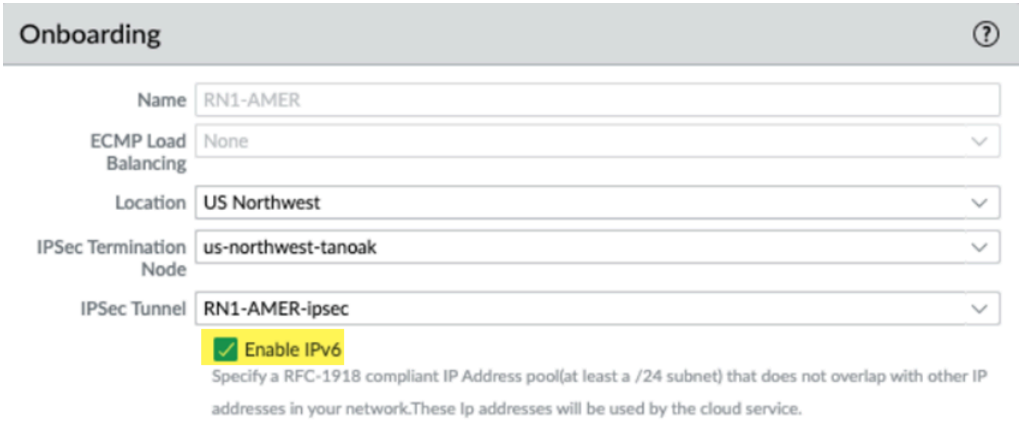
1. Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Remote-Netzwerke** aus und bearbeiten Sie die Einstellungen, indem Sie auf das Zahnradsymbol im Bereich **Einstellungen** klicken.
2. Geben Sie im Bereich **DNS-Proxy** IPv6-Adressen Ihres **benutzerdefinierten DNS-Servers** für Ihre DNS-Proxy-Einstellungen ein.

**STEP 2 |** Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Remote-Netzwerke** aus.

**STEP 3 |** **Fügen** Sie eine neue Remote-Netzwerkverbindung hinzu oder wählen Sie eine vorhandene Remote-Netzwerkverbindung aus, um sie zu bearbeiten.

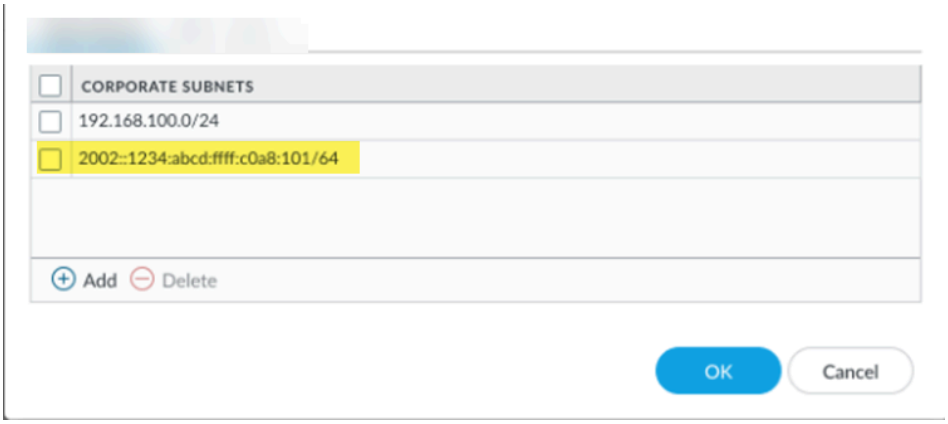
 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** **Aktivieren Sie IPv6.**




**STEP 5 |** Richten Sie IPv6-Routing für Ihr Remote-Netzwerk ein.

1. (Nur Bereitstellungen für statisches Routing) Geben Sie auf der Registerkarte **Statisches Routing** ein oder mehrere **Unternehmenssubnetze** ein.




2. (Nur Bereitstellungen für BGP-Routing) Geben Sie die Methode zum Austausch von IPv4- und IPv6-BGP-Routen an. Geben Sie dann eine IPv6-**Peer-Adresse** und eine **lokale Adresse** ein.

   - Um eine einzelne IPv4-BGP-Sitzung zum Austausch von IPv4- und IPv6-BGP-Peering-Informationen zu verwenden, wählen Sie **IPv4- und IPv6-Routen über IPv4-Peering austauschen** aus.
   - Um eine IPv4-BGP-Sitzung zum Austausch von IPv4-BGP-Peering-Informationen und eine IPv6-Sitzung zum Austausch von IPv6-BGP-Peering-Informationen zu

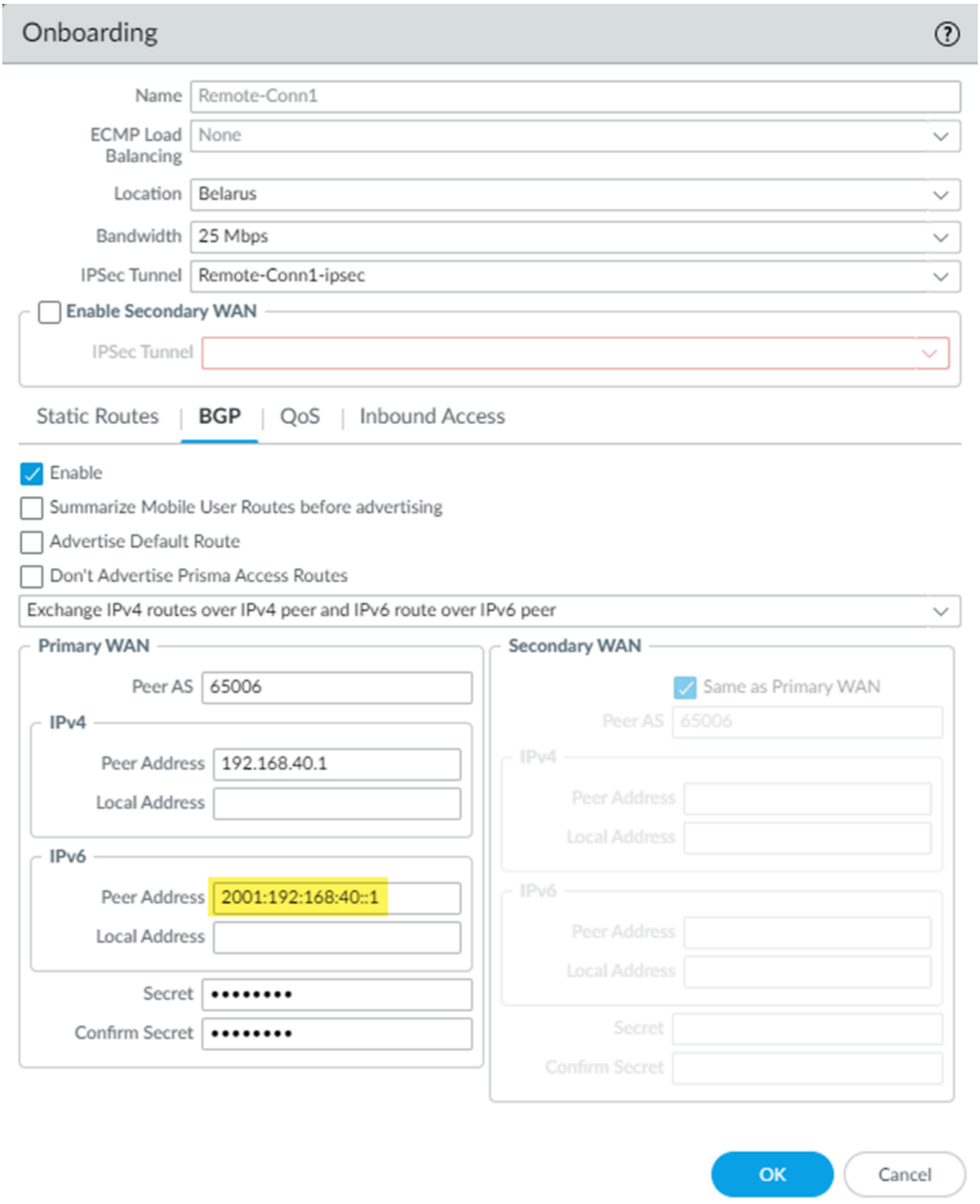
 ©2025 Palo Alto Networks, Inc.

verwenden, wählen Sie **IPv4-Routen über IPv4-Peering und IPv6-Routen über IPv6-Peering austauschen** aus.

- Um eine einzelne IPv6-BGP-Sitzung zum Austausch von IPv6-BGP-Peering-Informationen zu verwenden, wählen Sie **IPv6-Routen über IPv6-Peering austauschen** aus.

3. Wenn Ihr sekundäres WAN eine andere Peer-Adresse oder lokale Adresse verwendet, deaktivieren Sie **Wie primäres WAN** und geben Sie die IPv6-**Peer-Adresse** und die **lokale Adresse** für das sekundäre WAN ein.

 ©2025 Palo Alto Networks, Inc.




**STEP 6 |** (Optional) Wenn Ihre internen DNS-Server über IPv6-Adressen erreichbar sind, wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Remote-Netzwerke** > **Einstellungen** aus, klicken Sie auf das Zahnradsymbol, um die Einstellungen zu bearbeiten, wählen Sie die

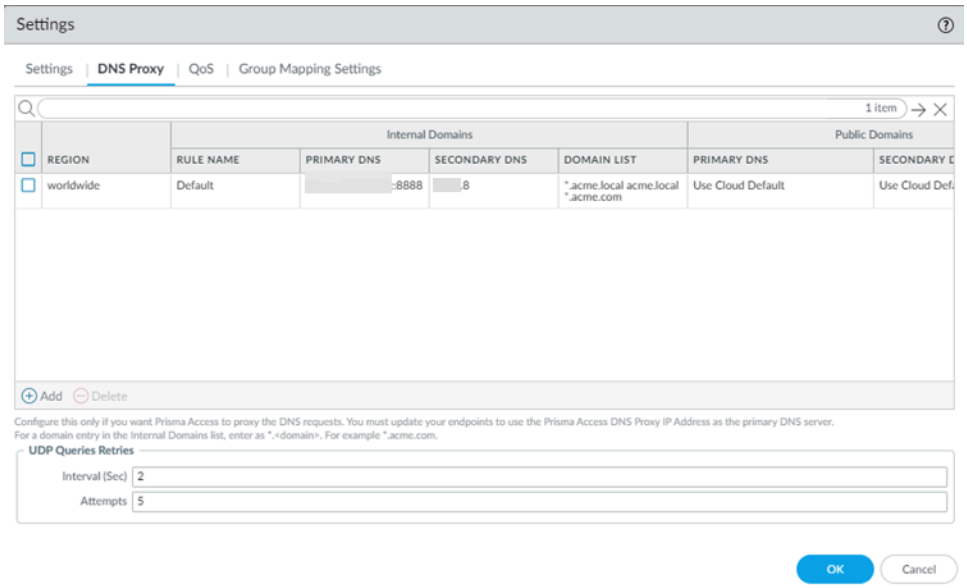
 ©2025 Palo Alto Networks, Inc.

Registerkarte **DNS-Proxy** aus, **fügen** Sie eine Regel hinzu bzw. geben Sie die Standardregel an und geben Sie IPv6-Adressen des **benutzerdefinierten DNS-Servers** für den **primären DNS**- und **sekundären DNS**-Server ein.

Mit Prisma Access können Sie DNS-Server angeben, um sowohl unternehmensinterne als auch externe Domänen aufzulösen. Wenn Sie keine Einstellungen angeben, leitet Prisma Access DNS-Anfragen für Remote-Netzwerke nicht weiter. Sie müssen auch eine **Region** auswählen.

Sie können eine beliebige Kombination von IPv4- oder IPv6-Adressen für primäre und sekundäre DNS-Server eingeben.

*IPv4-Adressen verwenden A-Einträge, während IPv6-Adressen AAAA-Einträge verwenden. Einige DNS-Server können AAAA-DNS-Lookups über IPv4-Transport durchführen; daher benötigen Sie möglicherweise keinen Server mit einer IPv6-IP-Adresse.*




**STEP 7 |** Wenn Sie die Einrichtung der Remote-Netzwerkverbindungen noch nicht abgeschlossen haben, schließen Sie sie jetzt ab.

**STEP 8 |** Führen Sie für Ihre Änderungen die Aktion **Commit und Push** aus.

**STEP 9 |** Wählen Sie **Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Remote-Netzwerke** aus und notieren Sie sich die Adressen vom **EBGP-Router**.

Nachdem Sie Ihre Änderungen übernommen haben, verfügen Sie über IPv6-Adressen vom **EBGP-Router** für Dienstverbindungen.

Da der IPSec-Tunnel, der für die Remote-Netzwerkverbindung genutzt wird, IPv4-Adressierung verwendet, bleibt die **Dienst-IP-Adresse** als IPv4-Adresse erhalten.

IPv6-Internetzugang für Remote-Netzwerkverbindungen wird durch eine Underlay-Verbindung ermöglicht, bei der IPv6-Datenverkehr durch einen IPv4-Tunnel geleitet wird.

 ©2025 Palo Alto Networks, Inc.

# DNS-Auflösung für Bereitstellungen für mobile Benutzer – GlobalProtect und Remote-Netzwerke

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz Version 2.2 bevorzugt und höher<br>❑ Der native IPv6-Zugriff auf öffentliche und private Apps erfordert die folgenden Releases:<br>• Prisma Access (Managed by Strata Cloud Manager): Juni 2024 Release<br>• Prisma Access (Managed by Panorama): Prisma Access 5.1.1 nur für neue Bereitstellungen.<br>Alle anderen Bereitstellungen (einschließlich vorhandener Prisma Access (Managed by Panorama)-Bereitstellungen) unterstützen nur den Zugriff auf private Apps. |

Mit Prisma Access können Sie DNS-Server angeben, um sowohl unternehmensinterne als auch externe Domänen aufzulösen. Prisma Access leitet die DNS-Anfrage basierend auf der Konfiguration Ihrer DNS-Server weiter. Die folgende Tabelle zeigt die unterstützten DNS-Auflösungsmethoden für interne und externe Domänen und gibt an, wann Prisma Access die DNS-Anfragen weiterleitet.

| Interne DNS-Auflösungsmethode | Externe DNS-Auflösungsmethode | Prisma Access leitet die DNS-Anfrage weiter (Ja/Nein) |
|---|---|---|
| Einzelregel, DNS-Server für interne Domänen konfiguriert | Cloud-Standard (Google Public DNS64 für IPv6) | Ja |
| Einzelregel, DNS-Server für interne Domänen konfiguriert | Wie interne Domänen | Nein |
| Einzelregel, DNS-Server für interne Domänen konfiguriert | Benutzerdefinierter DNS-Server (Google Public DNS64 für IPv6) | Ja |
| Einzelregel, Cloud-Standard für eine Domäne konfiguriert | Cloud-Standard (Google Public DNS64 für IPv6) | Ja |


©2025 Palo Alto Networks, Inc.

| Interne DNS-Auflösungsmethode | Externe DNS-Auflösungsmethode | Prisma Access leitet die DNS-Anfrage weiter (Ja/Nein) |
|---|---|---|
| Einzelregel, Cloud-Standard für eine Domäne konfiguriert | Wie interne Domänen (Google Public DNS64 für IPv6) | Ja |
| Einzelregel, Cloud-Standard für Domäne konfiguriert | Benutzerdefinierter DNS-Server (Google Public DNS64 für IPv6) | Ja |
| Mehrere Regeln, DNS-Server für interne Domänen konfiguriert | Cloud-Standard (Google Public DNS64 für IPv6) | Ja |
| Mehrere Regeln, DNS-Server für interne Domänen konfiguriert | Wie interne Domänen | Ja |
| Mehrere Regeln, DNS-Server für interne Domänen konfiguriert | Benutzerdefinierter DNS-Server (Google Public DNS64 für IPv6) | Ja |
| Keine Konfiguration | Benutzerdefinierter DNS-Server (Google Public DNS64 für IPv6) | Ja |
| Keine Konfiguration | Cloud-Standard (Für IPv6, Primär = Google Public DNS64, Sekundär = Cloud-Standard) | Nein |
| Keine Konfiguration | Keine Konfiguration | Nein |
| Keine DNS-Auflösung angegeben (Standardkonfiguration vorhanden, die Cloud-Standard verwendet) | Keine DNS-Auflösung angegeben | Nein |
| ZTNA-Connector (*unabhängig von der DNS-Auflösungsmethode*) | n. a. | Ja |
| Nachdem Sie ZTNA-Connector aktiviert haben, leitet Prisma Access alle DNS-Anfragen mithilfe der DNS-Regeln weiter, die für Remote-Netzwerke und Mobile Benutzer – GlobalProtect eingerichtet wurden. | | |

Die Quell-IP-Adresse der DNS-Anfrage hängt davon ab, ob Prisma Access die DNS-Anfrage weiterleitet oder nicht.


©2025 Palo Alto Networks, Inc.

- Wenn Prisma Access die DNS-Anfragen nicht weiterleitet, ändert sich die Quell-IP-Adresse der DNS-Anfrage in die IP-Adresse des Geräts, das die DNS-Lookup-Funktion angefordert hat. Mit dieser Quell-IP-Adresse können Sie auf die Quell-IP-Adresse basierte DNS-Richtlinien durchsetzen oder Endpunkte identifizieren, die mit bösartigen Domänen kommunizieren. Dieses Verhalten gilt für Bereitstellungen sowohl für mobile Benutzer als auch für Remote-Netzwerke.
- Wenn Prisma Access die DNS-Anfragen weiterleitet, ändert sich die Quell-IP-Adresse der DNS-Anfrage in die folgenden Adressen:
  - **Bereitstellungen für mobile Benutzer** – Die Quell-IP-Adresse der DNS-Anfrage ist eine IP-Adresse, die aus dem IP-Adresspool des mobilen Benutzers für interne Anfragen und der Gateway-IP-Adresse des Standorts des mobilen Benutzers für externe Anfragen entnommen wird.
  - **Bereitstellungen für Remote-Netzwerke** – Die Quell-IP-Adresse der DNS-Anfrage ist die **EBGP-Routeradresse** für interne Anfragen und die Dienst-IP-Adresse der Remote-Netzwerkverbindung für externe Anfragen.

Die folgenden Richtlinien und Einschränkungen gelten für die Verwendung der DNS-Auflösung mit Prisma Access:

- Die maximale Anzahl gleichzeitig anstehender TCP-DNS-Anfragen (**Max. ausstehende Anfragen**), die Prisma Access unterstützt, liegt bei 64.
- Bei UDP-Abfragen sendet der DNS-Proxy eine weitere Anfrage, wenn er in 2 Sekunden keine Antwort erhalten hat, und versucht es maximal fünf Mal, bevor er den nächsten DNS-Server versucht.
- Prisma Access speichert die DNS-Einträge mit einem Time-to-Live (TTL)-Wert von 300 Sekunden zwischen. EDNS-Antworten werden ebenfalls zwischengespeichert.

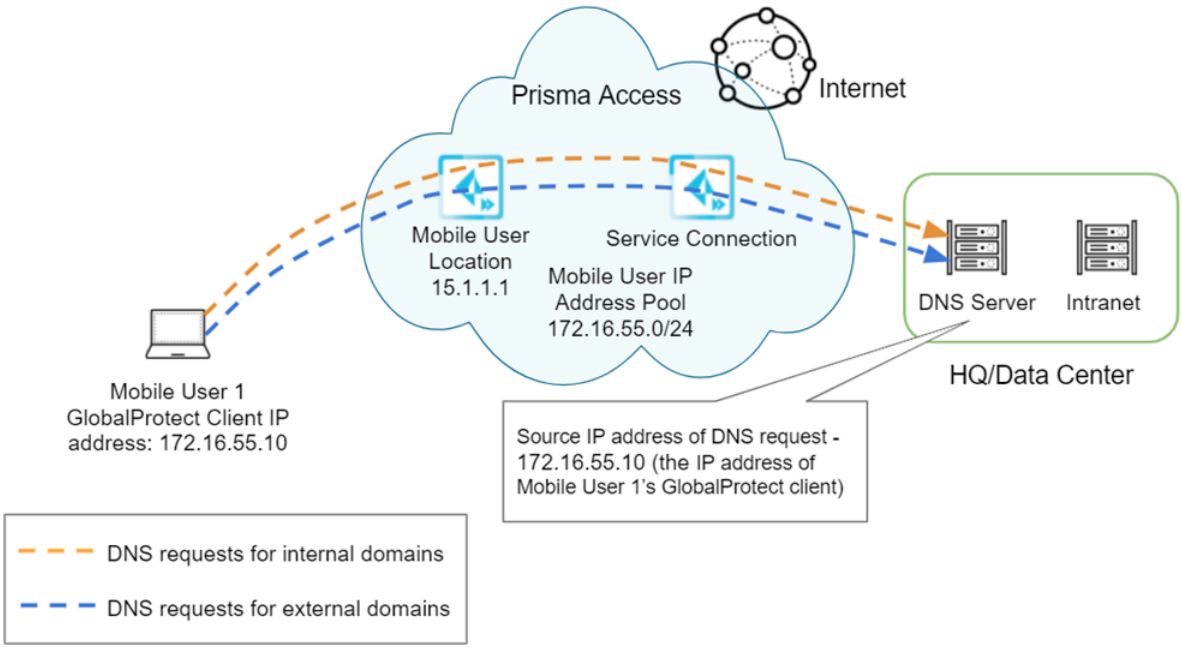
## DNS-Auflösung für Bereitstellungen für mobile Benutzer – GlobalProtect und Remote-Netzwerke

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Panorama | • Prisma Access-Lizenz |

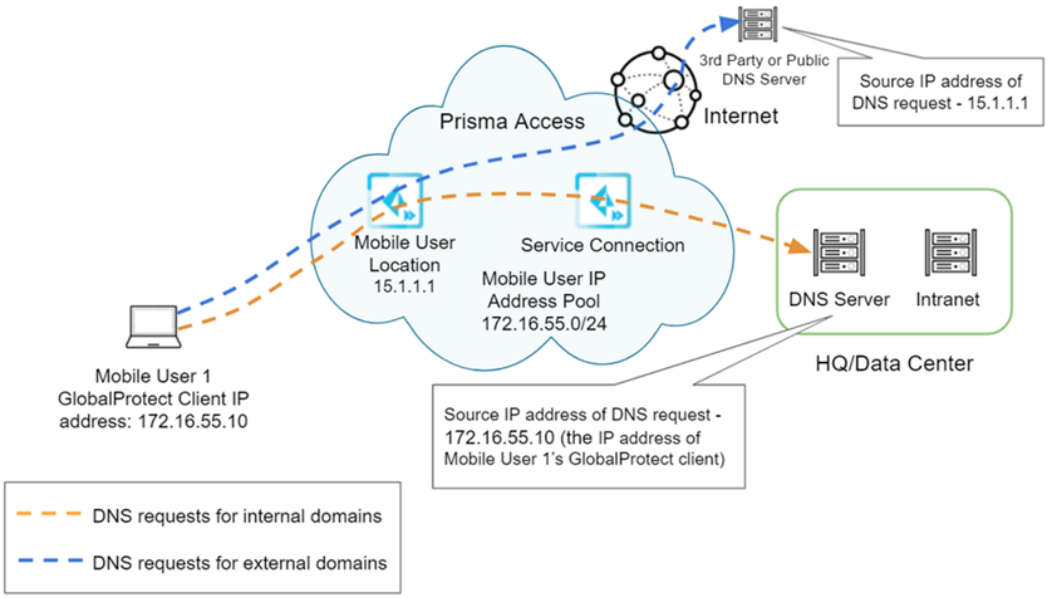
Der folgende Abschnitt enthält Beispiele dafür, wie Prisma Access die Quell-IP-Adresse der DNS-Anfragen verarbeitet, nachdem Sie die DNS-Auflösung für mobile Benutzer und für Remote-Netzwerke konfiguriert haben.

Die folgende Abbildung zeigt eine Bereitstellung, bei der Sie einen internen DNS-Server zugewiesen haben, um sowohl interne als auch externe Domänen aufzulösen. In diesem Fall leitet Prisma Access die DNS-Anfragen nicht weiter und die DNS-Anfrage stammt von der GlobalProtect-Client-IP-Adresse von „Mobiler Benutzer 1“. Der GlobalProtect-Client weist diese IP dem mobilen Benutzer zu und sie wird von der Gateway-IP-Adresse des Standorts des mobilen Benutzers übernommen.

 ©2025 Palo Alto Networks, Inc.

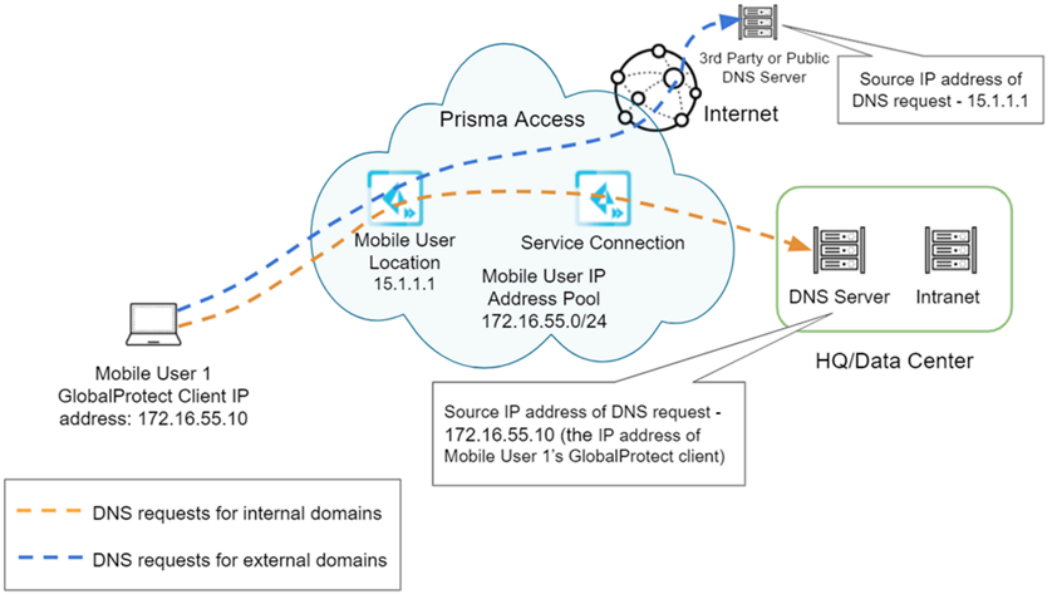



Die folgende Abbildung zeigt, dass die DNS-Anfragen für interne Domänen vom DNS-Server am Hauptsitz oder am Standort des Rechenzentrums aufgelöst werden, während Anfragen für externe Domains vom Cloud-Standard-DNS-Server von Prisma Access aufgelöst werden. In diesem Fall leitet Prisma Access die Anfragen für die externe Anfrage weiter und die Quell-IP-Adresse ist die Gateway-IP-Adresse von Prisma Access (15.1.1.1 in diesem Beispiel), während die interne Quell-IP die GlobalProtect-Client-IP-Adresse von „Mobiler Benutzer 1“ bleibt.




Die folgende Abbildung zeigt die Organisation, die einen Drittanbieter- oder öffentlichen DNS-Server verwendet, auf den für Anfragen an externe Domänen über das Internet zugegriffen werden kann. Prisma Access leitet diese Anfragen ebenfalls weiter.

 ©2025 Palo Alto Networks, Inc.



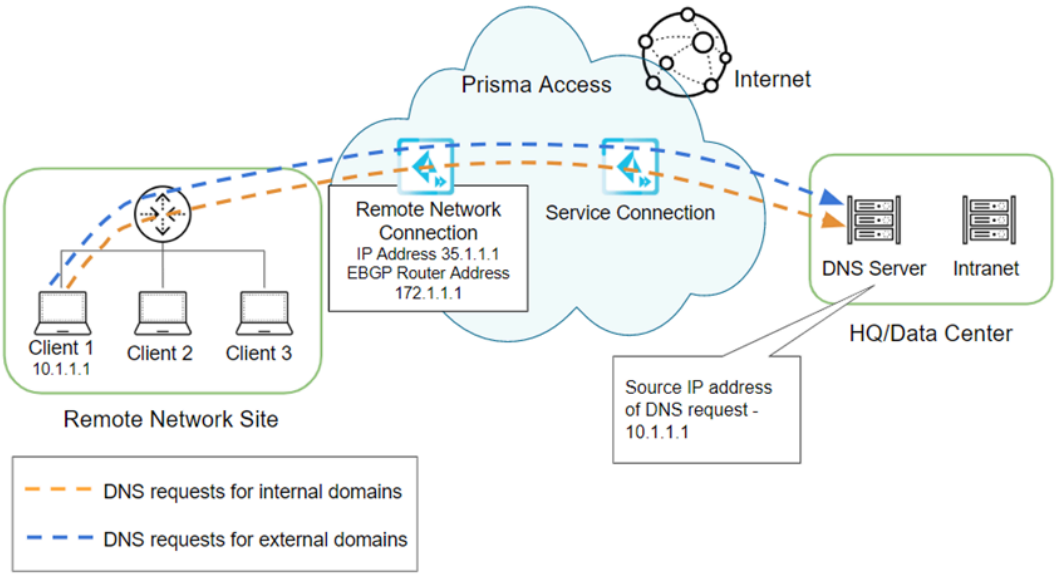

# DNS-Auflösung für Remote-Netzwerke

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Panorama | • Prisma Access-Lizenz |

Wenn Sie über eine vorhandene Bereitstellung für Remote-Netzwerke verfügen, können Sie die bereits vorhandenen DNS-Auflösungsmethoden weiterhin verwenden oder Sie können Prisma Access zum Weiterleiten der DNS-Anfrage verwenden. Durch das Weiterleiten der DNS-Anfragen können Sie DNS-Anfragen für öffentliche Domänen an einen Server senden und DNS-Anfragen für interne Domänen an einen anderen Server senden.

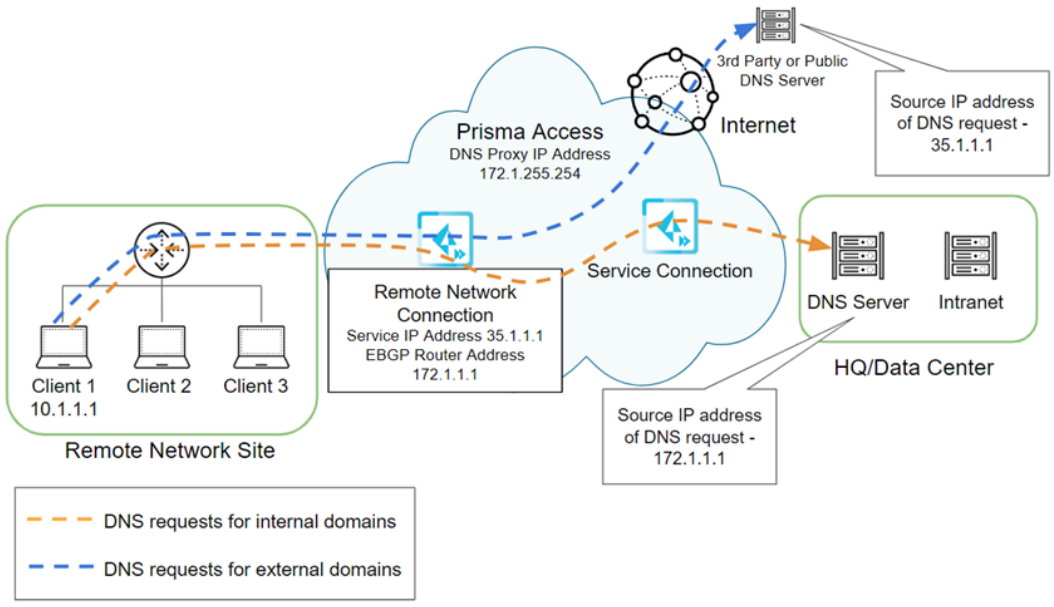
Die folgende Abbildung zeigt eine DNS-Anfrage an eine Bereitstellung, bei der ein interner DNS-Server verwendet wird, um Anfragen für interne und externe Domänen zu verarbeiten. Die IP-Adresse des Remote-Netzwerks ist 35.1.1.1 und die IP-Adresse des **EBGP-Routers** ist 172.1.1.1. In diesem Fall leitet Prisma Access die Anfragen nicht weiter, und wenn der interne DNS-Server NAT nicht verwendet, ist die Quell-IP der DNS-Anfrage 10.1.1.1 (die IP-Adresse des Geräts von Client 1 im Remote-Netzwerkstandort).

 ©2025 Palo Alto Networks, Inc.




Wenn Prisma Access die DNS-Anfrage weiterleitet, ändern sich die Quell-IP-Adressen der weitergeleiteten DNS-Anfragen in die **EBGP-Routeradresse** für interne Anfragen und in die Dienst-IP-Adresse der Remote-Netzwerkverbindung für externe Anfragen, wie in der folgenden Abbildung gezeigt.

*Wenn Sie die DNS-Adresse in Ihrem Netzwerk so konfigurieren, dass sie für weitergeleitete externe Anfragen von Prisma Access verwendet wird, geben Sie die IP-Adresse des DNS-Proxy für das **Remote-Netzwerk** (**Panorama** > **Cloud Services** > **Status** > **Dienstinfrastruktur** > ) **an**. Im folgenden Beispiel würden Sie 172.1.255.254 in Ihrem Netzwerk für den DNS-Server angeben.*



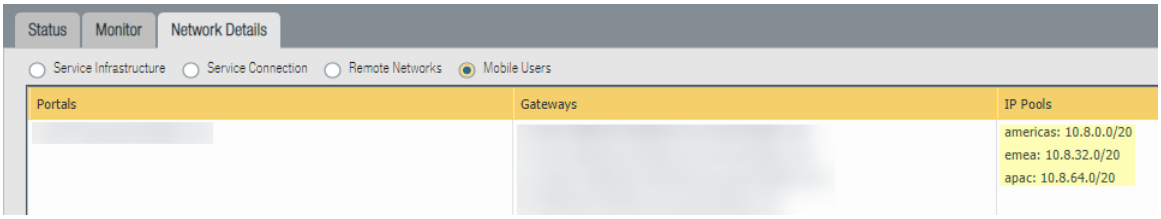

 ©2025 Palo Alto Networks, Inc.

# Wie BGP IP-Adresspools mobiler Benutzer für Dienstverbindungen und Remote-Netzwerkverbindungen ankündigt

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Panorama | • Prisma Access-Lizenz |

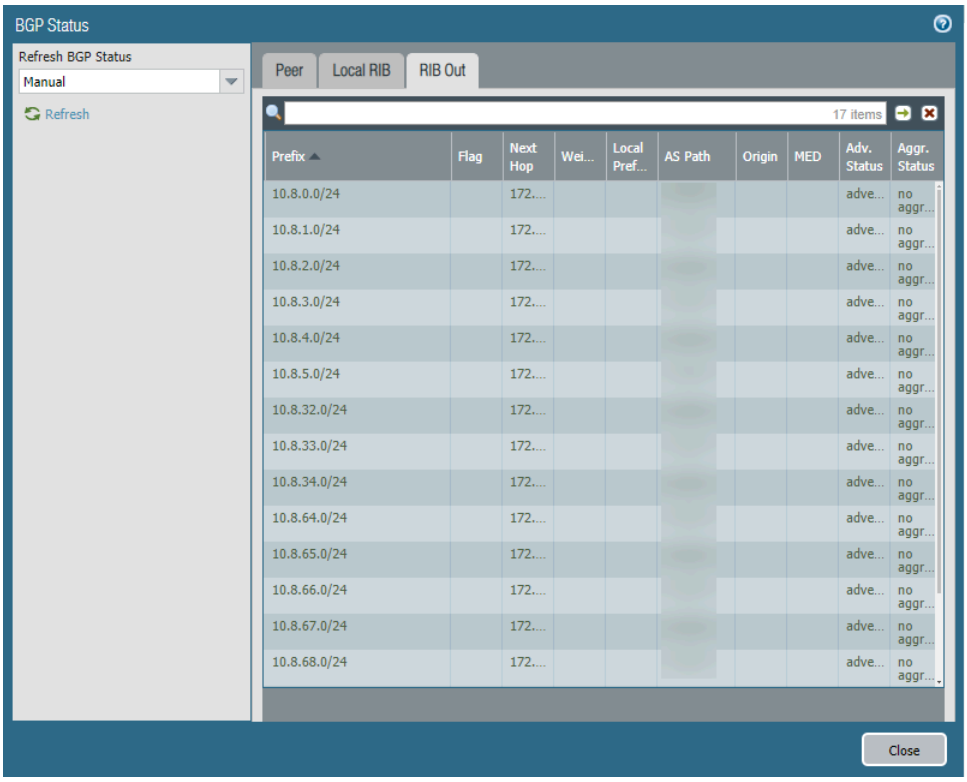
Wenn Sie BGP für Dienstverbindungen oder Remote-Netzwerkverbindungen aktivieren, nachdem Sie wie unter GlobalProtect für mobile Benutzer einrichten (Panorama) beschrieben vorgegangen sind, weist Prisma Access die IP-Adresspools mobiler Benutzer zu, die Sie mithilfe von Adressblöcken der Klasse C (/24) angegeben haben. BGP kündigt daher zugewiesene mobile Benutzersubnetze in Blöcken von /24 an und nicht die gesamten Pools, die dieser Region zugeordnet sind. Wenn Prisma Access ein /24-Subnetz für ein Prisma Access-Gateway hinzufügt, sendet es automatisch eine BGP-Ankündigung. Wenn Subnetze hinzugefügt und entfernt werden, aktualisiert Prisma Access seine BGP-Anzeigen automatisch. Diese Zuweisungsmethode bietet mehr Flexibilität bei der Ankündigung von BGP-Routen, insbesondere wenn Sie einen **weltweiten** Pool konfiguriert haben, anstatt Pools pro Region zuzuweisen. Durch die Aufteilung des IP-Adresspools in kleinere Subnetze kann ein Subnetz hinzugefügt, entfernt oder gelöscht und dann in verschiedenen Regionen wiederverwendet werden, wenn der zugewiesene Adressraum erschöpft ist.

Der folgende Screenshot von **Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Mobile Benutzer – GlobalProtect** zeigt drei /20-IP-Pools für mobile Benutzer, aufgeteilt nach Regionen.




Die Tabelle **RIB Out** von **Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Dienstverbindung** > **BGP Status anzeigen** (im Bereich **Zweigstellen-AS und -Router**) enthält den Adresspool mobiler Benutzer, aufgeteilt in Blöcke mit /24-Subnetzen für BGP-Routenankündigungen. Beachten Sie, dass nicht alle /20-Subnetze angekündigt werden.

 ©2025 Palo Alto Networks, Inc.




 ©2025 Palo Alto Networks, Inc.

# Proxy-Unterstützung für Prisma Access und Strata Logging Service

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Panorama | • Prisma Access-Lizenz |

Wenn Sie einen Proxyserver zwischen Panorama, der Prisma Access-Infrastruktur und Strata Logging Service bereitstellen, finden Sie in der folgenden Tabelle Details zum erwarteten Verhalten:

| Funktionalität | Unterstützung durch einen Proxyserver, der keine SSL-Entschlüsselung durchführt | Unterstützung durch einen Proxyserver, der SSL-Entschlüsselung durchführt |
|---|---|---|
| **Erstes Onboarding in Strata Logging Service mit Prüfungen des Zertifikatswiderrufsstatus mittels OCSP** | Unterstützt | Es werden nur Passthrough-Proxys unterstützt. Sämtliche Proxys, die SSL-Entschlüsselung verwenden, werden nicht unterstützt. |
| **Panoramaabfragen an Strata Logging Service für Berichte und Protokolle** | Wenn der Proxyserver die Standardroute auf Panorama ist, können Sie die Daten im ACC und auf den Seiten **Überwachen** > **Protokolle** nicht anzeigen.<br>Sie können Daten im ACC und auf den Seiten **Überwachen** > **Protokolle** anzeigen, wenn Panorama eine alternative Route zum Strata Logging Service hat und Sie den Proxyserver umgehen können. | |

 ©2025 Palo Alto Networks, Inc.

# Blockieren Sie eingehende Verbindungen aus bestimmten Ländern

Prisma Access ermöglicht Ihnen die Erstellung von Sicherheitsrichtlinien, um Anmeldeversuche für Bereitstellungen von Remote-Netzwerken, mobilen GlobalProtect-Benutzern und mobilen Benutzern des expliziten Proxy aus den von Ihnen angegebenen Ländern zu blockieren. Prisma Accessblockiert eingehende Verbindungen aus den von Ihnen angegebenen Ländern auf Grundlage der geografischen Standortinformationen aus der Quell-IP-Adresse des Clients.

Um eingehende Verbindungen aus diesen Ländern zu blockieren, führen Sie die folgende Aufgabe aus.

**STEP 1 |** Erstellen Sie eine Sicherheitsrichtlinien-Vor-Regel mit einem der spezifischen Regelnamen:

Stellen Sie sicher, dass Sie diese Regel als Vor-Regel konfigurieren.

- Um ein Land für Bereitstellungen für mobile GlobalProtect-Benutzer zu blockieren, erstellen Sie eine Regel mit dem Namen **Mobile_User_EMBG_Source_Countries**.
- Um ein Land für Bereitstellungen für mobile Benutzer des expliziten Proxy zu blockieren, erstellen Sie eine Regel mit dem Namen **Explicit_Proxy_EMBG_Source_Countries**.
- Um ein Land für Remote-Netzwerkbereitstellungen zu blockieren, erstellen Sie eine Regel mit dem Namen **Remote_Network_EMBG_Source_Countries**.

**STEP 2 |** Fügen Sie einen **Tag** für die Regel mit dem Namen **PA_predefined_embargo_rule** hinzu.

**STEP 3 |** Fügen Sie unter **Quelle** mindestens ein Land hinzu, das blockiert werden soll.

**STEP 4 |** Geben Sie als **Aktion** die Option **Löschen** an.

 ©2025 Palo Alto Networks, Inc.

# Sicherer Internet-Verkehr aus AWS WorkSpace

Organisationen müssen ihren Ansatz für die Sicherung ihrer Remote-Mitarbeiter, Auftragnehmer, Krankenhausmitarbeiter und Callcenter-Benutzer, die über cloudbasierte virtuelle Maschinen von Amazon WorkSpace auf das Internet zugreifen, überdenken. Diese Benutzer müssen in der Lage sein, sicher auf das Internet zuzugreifen und vor internetbasierten Bedrohungen geschützt zu bleiben, während der Internet-Verkehr, der durch diese in der Cloud gehosteten, virtuellen Maschinen generiert wird, für das Unternehmen vollumfänglich transparent bleibt.

Herkömmliche Netzwerkmodelle, die für Remote-Mitarbeiter und -Ressourcen entwickelt wurden, reichen in der heutigen komplexen und innovativen Wirtschaft, in der die Mitarbeiter-, Daten- und Cloud-Anwendungen mehr und mehr dezentral vorliegen, nicht mehr aus. Unternehmen benötigen die Flexibilität und Skalierbarkeit von Cloud-Diensten, aber diese Dienste erfordern Cloud-Sicherheitslösungen, die auf ihre einzigartigen Anforderungen zugeschnitten sind.

Erfahren Sie mehr über Prisma SASE und AWS WorkSpace.

Mit dem Strata Cloud Manager von Palo Alto Networks können Sie AWS WorkSpace mithilfe der folgenden Methoden sicheren Zugriff auf das Internet gewähren:

- Eine PAC-Datei auf AWS-WorkSpace-Clients konfigurieren
- Konfigurieren eines Standort-zu-Standort-Tunnels zwischen AWS und Prisma Access

## Eine PAC-Datei auf AWS-WorkSpace-Clients konfigurieren

Eine Methode zur Sicherung des Internetverkehrs von Amazon WorkSpaces ist die Verwendung einer PAC-Datei (Proxy Auto-Configuration). Eine PAC-Datei enthält JavaScript-Code, der einem Webbrowser mitteilt, wie er eine Verbindung zu einem Proxyserver herstellen kann. Unternehmensumgebungen verwenden PAC-Dateien, um den Webverkehr zu kontrollieren und Sicherheitsrichtlinienregeln durchzusetzen. Ein Webserver speichert normalerweise die PAC-Datei und der Webbrowser lädt die PAC-Datei herunter, wenn er gestartet wird.

**STEP 1 |** Wenn Sie diesen Schritt noch nicht ausgeführt haben, dann richten Sie den expliziten Proxy in Prisma SASE ein.

Sie können eine PAC-Datei entweder in Prisma SASE oder auf dem Webserver hosten. Stellen Sie sicher, dass der PAC-Server über Workspace-Clients erreichbar ist, indem Sie mit einem Webbrowser auf die PAC-URL zugreifen.

**STEP 2 |** Passen Sie die PAC-Datei des expliziten Proxy in Prisma SASE an, um den Proxy-FQDN zu aktualisieren und Ausschlüsse zu definieren.

1. Wählen Sie in Strata Cloud Manager **Workflows** > **Prisma Access-Einrichtung** > **Expliziter Proxy** > **Weiterleitungsregeln** aus.
2. Bearbeiten Sie die PAC-Datei gemäß den Richtlinien für PAC-Dateien.

**STEP 3 |** Laden Sie die Stammzertifikate des expliziten Proxy in Prisma SASE herunter, um sie in AWS WorkSpace zu installieren.

 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** Installieren Sie das Zertifikat auf dem AWS-WorkSpace-Client, um benutzerbasierte Richtlinienregeln, Datenverkehrsinspektionen und Berichte anzuwenden.

Dadurch kann der WorkSpace-Client mit dem expliziten Proxy in Prisma SASE kommunizieren.

**STEP 5 |** Konfigurieren Sie die PAC-Datei in AWS WorkSpace.

Die Vorgehensweise hängt vom verwendeten Browser ab.

- Google Chrome:
  1. Öffnen Sie Chrome.
  2. Wählen Sie die drei Punkte in der oberen rechten Ecke des Fensters aus.
  3. Wählen Sie **Einstellungen** aus.
  4. Wählen Sie **Erweitert** aus.
  5. Wählen Sie unter **System** die Option **Proxy-Einstellungen öffnen** aus.
  6. Wählen Sie im Fenster mit den Einstellungen für das Local Area Network (LAN) die Option **Automatisches Konfigurationsskript verwenden** aus.
  7. Geben Sie im Feld **Adresse** die URL Ihrer PAC-Datei ein.
  8. Wählen Sie dann **OK** aus, um Ihre Änderungen zu speichern.
- Firefox
  1. Öffnen Sie Firefox.
  2. Wählen Sie die drei Linien in der oberen rechten Ecke des Fensters aus.
  3. Wählen Sie **Optionen** aus.
  4. Wählen Sie **Erweitert** aus.
  5. Wählen Sie unter **Netzwerk** die Option **Einstellungen** aus.
  6. Wählen Sie im Fenster **Verbindungseinstellungen** die Option **URL für automatische Proxykonfiguration** aus.
  7. Geben Sie im Feld **URL** die URL Ihrer PAC-Datei ein.
  8. Wählen Sie **OK** aus, um Ihre Änderungen zu speichern.

Wenn Sie die PAC-Datei angewendet haben, verwenden Chrome und Firefox sie, um zu ermitteln, welcher Proxyserver für jede Website verwendet werden soll.

**STEP 6 |** Führen Sie einen Neustart des AWS-WorkSpace-Browsers durch.

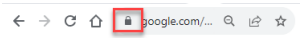
Nach dem Neustart des WorkSpace-Browsers erfasst er die neue PAC-Datei und beginnt mit der Weiterleitung des Datenverkehrs über den Prisma-SASE-Proxy.

 ©2025 Palo Alto Networks, Inc.

**STEP 7 |** Testen und verifizieren Sie den Datenverkehrsfluss.

Nachdem Sie die WorkSpace-Clients zur Verwendung des expliziten Proxy in Prisma SASE konfiguriert haben, können Sie den Datenverkehrsfluss testen, indem Sie das Zertifikat im Browser validieren und die Anzeige der Protokolle in Prisma Access aufrufen.

1. Wenn Sie Google Chrome verwenden, wählen Sie das Vorhängeschloss in der Adressleiste aus.




   1. Wählen Sie **Verbindung ist sicher** aus.
   2. Wählen Sie **Zertifikat ist gültig** aus.
   3. Überprüfen Sie die korrekten Zertifikatsdetails, die im Pop-up-Fenster angezeigt werden.
2. Wenn Sie Safari verwenden, wählen Sie das Vorhängeschlosssymbol in der Adressleiste aus.
   1. Wählen Sie **Sichere Verbindung** aus.
   2. Wählen Sie **Weitere Informationen** aus.
   3. Wählen Sie **Zertifikat anzeigen** aus.
   4. Überprüfen Sie die korrekten Zertifikatsdetails, die im Pop-up-Fenster angezeigt werden.

## Konfigurieren eines Standort-zu-Standort-Tunnels zwischen AWS und Prisma Access

Wenn Ihr Unternehmen wächst und auf Ihren Systemen mehrere AWS-WorkSpace-Clients ausgeführt werden, können Sie mit Prisma Access-Remote-Netzwerken Ihren WorkSpace rasch einbinden und Ihren Benutzern beste Sicherheit bieten. Das Produkt bietet eine komfortable Option, die das Konfigurieren und Verwalten von WorkSpace erheblich vereinfacht.

Unternehmen können AWS-WorkSpace-Benutzer in Prisma Access einbinden, indem sie einen IPSec-Tunnel zwischen AWS und Prisma Access einrichten.

Der Vorteil der Nutzung eines Remote-Netzwerks besteht darin, dass der ausgehende Internetverkehr für Benutzer gesichert wird, die über Prisma Access Verbindungen zum Internet herstellen.

**STEP 1 |** Konfigurieren Sie eine virtuelle private Cloud (VPC) für Ihren Amazon WorkSpace oder verwenden Sie die vorhandene VPC für Ihren Amazon WorkSpace.

**STEP 2 |** Verbinden Sie das AWS Transit Gateway mit der VPC, um den Standort-zu-Standort-IPSec-Tunnel zwischen AWS und Prisma Access zu konfigurieren.

**STEP 3 |** Konfigurieren Sie ein IPSec-VPN zwischen AWS Transit Gateway und dem Prisma Access-Remote-Netzwerk.

**STEP 4 |** Im Prisma Access-Remote-Netzwerk können Sie Sicherheitsregeln definieren, um den Internetverkehr zum Schutz von AWS-WorkSpace-Benutzern einzuschränken.

 ©2025 Palo Alto Networks, Inc.

# Prisma Access für Netzwerke ohne Standardroute

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access | ❑ Prisma Access-Lizenz |

## Was ist ein Netzwerk ohne Standardroute?

Ein Netzwerk ohne Standardroute ist ein Netzwerk, für das keine Standardroute konfiguriert ist. Wenn in einem Netzwerk keine Standardroute konfiguriert ist, werden Pakete an unbekannte Ziele gelöscht. Unternehmen verwenden häufig Netzwerke ohne Standardroute, um den Zugriff für ihre Benutzer einzuschränken. Wenn ein Gerät in einem Netzwerk ohne Standardroute auf ein bestimmtes Ziel (IP-Adresse oder Subnetz) zugreifen soll, muss der Administrator eine Route für dieses Ziel manuell konfigurieren. Unternehmen benötigen außerdem einen eingeschränkten und sicheren Internetzugang für Benutzer, Server und Geräte in einem Zweigstellennetzwerk ohne Standardroute.

Für die Konfiguration eines Netzwerks ohne Standardroute gibt es einige wenige Gründe:

- Verbesserung der Sicherheit, indem ausgehender bösartiger und DDoS-Datenverkehr zu zufälligen Zielen von kompromittierten Endpunkten im Netzwerk blockiert wird, was vor Denial-of-Service-Angriffen und anderem bösartigen Datenverkehr schützt.
- Verbesserung der Leistung von Routinggeräten, indem die Anzahl der zu verarbeitenden Routen reduziert wird.
- Implementieren der Routingrichtlinien, die den spezifischen Anforderungen der Benutzer entsprechen, indem bestimmte Routen für bestimmte Ziele konfiguriert werden.

## Überlegungen zu Netzwerken ohne Standardroute

Bei der Sicherung von Internetdatenverkehr aus einem Netzwerk ohne Standardroute müssen Unternehmen Benutzer, Endpunkte, Server und Geräte im Zweigstellennetzwerk, die mit dem Internet kommunizieren könnten, eindeutig evaluieren.

In Zweigstellen ohne Standardroute können Geräte mit einer Vielzahl unterschiedlicher Betriebssysteme, Endpunkte für mehrere Benutzer oder gemeinsam genutzte Endpunkte wie VDIs und monitorlose Geräte wie Server und IoT-Geräte vorhanden sein. Internetdatenverkehr von diesen Geräten erfordert Sicherheit. Es ist entscheidend, mit einer Lösung zu arbeiten, die alle diese Anwendungsfälle abdeckt, Flexibilität mit verschiedenen Konnektivitätsmethoden sowie eine einheitliche Plattform bietet, um den Internetzugang unabhängig vom Gerätetyp durchgängig zu sichern.

## Bereitstellungsempfehlungen zur Absicherung des Internetzugangs für Netzwerke ohne Standardroute

Wenn Sie kein Netzwerk mit Standardroute haben, wird von Palo Alto Networks Folgendes zur Absicherung des Internetdatenverkehrs empfohlen:

 ©2025 Palo Alto Networks, Inc.

| Geräte | Empfehlung |
|---|---|
| Windows, macOS | GlobalProtect Agent im Proxy-Modus |
| ChromeOS, VDIs | Agentenlose PAC-Dateien |
| iOS, Android | Agentenlose PAC-Dateien |
| Linux | Agentenlose PAC-Dateien |
| Server | Agentenlose PAC-Dateien |
| IoT-Geräte (proxyfähig) | Agentenlose PAC-Dateien |
| IoT-Geräte (nicht proxyfähig) | Remote-Netzwerke (IPSec) |

## Wichtige Überlegungen

Beachten Sie bei der Bereitstellung von GlobalProtect in einem Netzwerk ohne Standardroute folgende Punkte:

- Fügen Sie eine Route auf dem Perimetergerät hinzu, um den Internetdatenverkehr des Benutzers an die Prisma Access IP-Adresse des expliziten Proxy zu leiten.
- Hosten Sie die PAC-Datei intern, um die IdP-URL und die URL des Prisma Access-Portals an den expliziten Proxy weiterzuleiten, damit GlobalProtect eine Verbindung zum Portal und zum IdP herstellen kann.
- Fügen Sie interne DNS-Einträge hinzu, um den FQDN des expliziten Proxy, der PAC-Datei und des Prisma Access-Portals aufzulösen, wenn der DNS-Server im Netzwerk ohne Standardroute externe FQDNs nicht auflösen kann.
- Konfigurieren Sie DNAT für die interne IP-Adresse der Prisma Access-Bereitstellung des Typs „Expliziter Proxy“ und die IP-Adresse des Prisma Access-Portals zur IP-Adresse des expliziten Proxy und zur Portal-IP-Adresse.

*Bei PAC-basierten Bereitstellungen muss die URL des Prisma Access-Portals nicht an einen expliziten Proxy weitergeleitet und von den Authentifizierungseinstellungen in den Einstellungen des expliziten Proxy für Prisma Access nicht ausgeschlossen werden.*

 ©2025 Palo Alto Networks, Inc.

# Prisma Access-Dienstverbindungen – Erweiterte Bereitstellungen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Panorama | • Prisma Access-Lizenz |

In den folgenden Abschnitten sind die erweiterten Bereitstellungen aufgeführt, die für Prisma Access-Dienstverbindungen verfügbar sind:

- Multicloud-Redundanz für Dienstverbindungen
- Internetgebundenen Datenverkehr mittels Datenverkehrslenkung an Dienstverbindungen weiterleiten
- Routing für Dienstverbindungsverkehr
- Netzwerk mit hoher Bandbreite mithilfe mehrerer Dienstverbindungen erstellen

## Multicloud-Redundanz für Dienstverbindungen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

*Die Multicloud-Redundanz für Dienstverbindungen wird ab Prisma Access Version 3.1 Innovation unterstützt.*

Wenn Sie Prisma Access-Dienstverbindungen verwenden, um mobilen Benutzern und Benutzern an Remote-Standorten Zugriff auf interne Ressourcen und Apps in einer Zentrale oder in einem Rechenzentrum zu gewähren, können Sie einen belastbareren Zugriff auf diese Ressourcen gewährleisten, indem Sie aktive und Back-up-Dienstverbindungen bei verschiedenen Cloud-Anbietern erstellen. Sie können diese aktiven und Back-up-Dienstverbindungen am selben Standort oder an verschiedenen Standorten in verschiedenen geografischen Regionen angeben, wodurch Sie auch dann auf Ressourcen über Dienstverbindungen zugreifen können, wenn ein Cloud-Anbieter oder eine Region nicht mehr verfügbar ist.

Sie geben aktive und Back-up-Dienstverbindungen an einem *Standort* an. Ein Standort ist ein Kundenrechenzentrum oder eine Zentrale (lokal oder in der öffentlichen Cloud), an dem bzw. der eine oder mehrere Dienstverbindungen enden. Nachdem Sie Dienstverbindungen erstellt haben, erstellen Sie einen Standort, fügen Sie diesem Standort Dienstverbindungen hinzu und geben Sie dann die Dienstverbindungen an, die Sie entweder als aktiv oder als Backup hinzugefügt haben.

Wenn ein Ausfall bei einem Cloud-Anbieter oder ein regionaler Ausfall dazu führt, dass eine aktive Dienstverbindung an einem Standort ausfällt, leitet Prisma Access den Datenverkehr mithilfe dieser Regeln um, sodass Ihre mobilen Benutzer weiterhin auf die Ressourcen in dieser Zentrale oder in diesem Rechenzentrum zugreifen können:

 ©2025 Palo Alto Networks, Inc.

- Wenn an einem Standort nur eine einzige aktive Dienstverbindung vorhanden ist, wählt Prisma Access die Back-up-Dienstverbindung an diesem Standort aus, um den Datenverkehr weiterzuleiten.
- Wenn mehrere aktive Dienstverbindungen an einem Standort vorhanden sind, wählt Prisma Access eine der anderen aktiven Dienstverbindungen aus, um den Datenverkehr weiterzuleiten. Die Back-up-Dienstverbindung wird nur verwendet, um Datenverkehr weiterzuleiten, wenn alle aktiven Dienstverbindungen ausfallen.

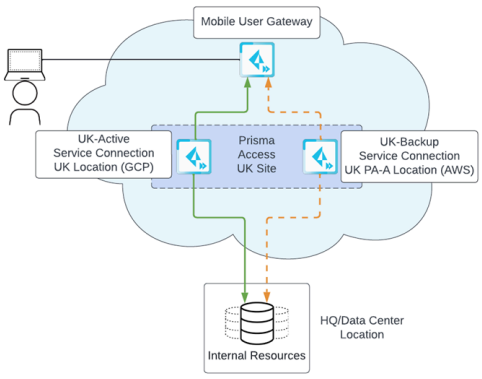
Um einen Standort zu nutzen, der aktive und Back-up-Standorte im selben Land verwendet, binden Sie Dienstverbindungen mithilfe bevorzugter und alternativer Standorte im Land ein, erstellen Sie dann einen Standort und fügen Sie diese landesinternen Standorte diesem Standort hinzu.

Prisma Access stellt Ihnen auch Statusmeldungen zu den Dienstverbindungen bereit, die Sie an einem Standort eingebunden haben (z. B. wenn alle Dienstverbindungen an einem Standort in einer einzigen Region bereitgestellt werden).

Die folgenden Beispiele veranschaulichen, welche Vorteile es hat, wenn Sie Standorte erstellen und diesen Dienstverbindungen hinzufügen:

- **Verschiedene Cloud-Anbieter in der gleichen geografischen Region** – Wenn Sie eine Organisation (z. B. eine Bank) sind und Zugriff auf Ihre Daten in einem bestimmten Land benötigen, können Sie einen bevorzugten Standort aus diesem Land und einen alternativen Standort aus demselben Land auswählen. Im folgenden Beispiel ist eine Organisation in Großbritannien (UK) dargestellt, die ihre Dienstverbindungen in Großbritannien einbindet, um die Vorschriften zum Datenstandort einzuhalten. In diesem Fall bindet der Administrator der Organisation zwei Dienstverbindungen in Großbritannien ein: „UK-Active“ am Standort „UK“ und „UK-Backup“ am Standort „UK PA-A“. Der Standort „UK“ wird vom bevorzugten Cloud-Anbieter (GCP) in Großbritannien gehostet, und der Standort „UK PA-A“ wird vom alternativen Cloud-Anbieter (AWS) in diesem Land gehostet. In der Liste der Standorte im Land sind die bevorzugten und alternativen Cloud-Anbieter für ein Land enthalten. Der Administrator erstellt dann einen Standort und bestimmt „UK-Active“ als aktiven Standort und „UK-Backup“ als Back-up-Standort an diesem Standort.

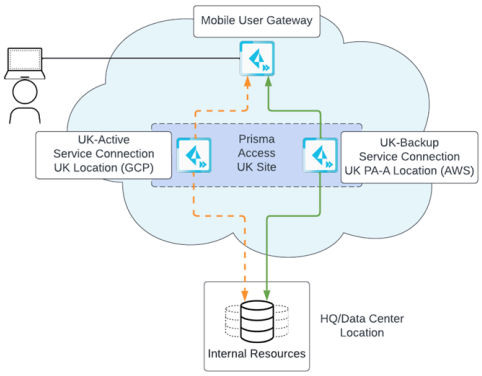
  Während des normalen Betriebs greifen mobile Benutzer über die Dienstverbindung „UK-Active“ auf interne Ressourcen in der Zentrale oder im Rechenzentrum zu.




  Wenn ein GCP-Ausfall die Dienstverbindung „UK-Active“ beeinträchtigt, führt Prisma Access ein Failover auf die Dienstverbindung „UK-Backup“ durch, die auf AWS gehostet wird. Auf diese Weise ermöglicht Prisma Access mobilen Benutzern den Zugriff auf die Ressourcen

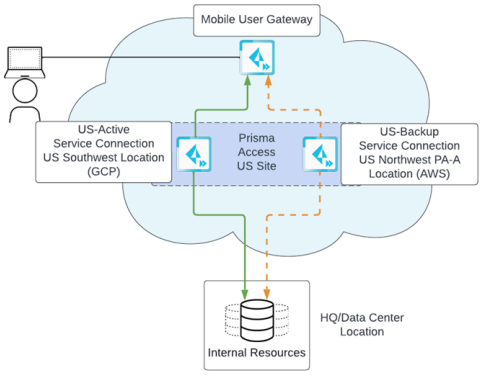
 ©2025 Palo Alto Networks, Inc.

im Rechenzentrum oder am Hauptsitz – auch dann, wenn ein Cloud-Provider ausfällt. Im folgenden Diagramm ist der Datenverkehrsfluss dargestellt.




- **Verschiedene geografische Regionen** – Wenn Sie bei einem regionalen Ausfall Redundanz gewährleisten möchten, können Sie zwei oder mehr Dienstverbindungen an verschiedenen Compute-Standorten sowie verschiedene Cloud-Anbieter angeben, die Ihnen bei einem Ausfall in einer geografischen Region einen Backup-Zugriff ermöglichen. Im folgenden Diagramm hat der Administrator Dienstverbindungen von Standorten in den Vereinigten Staaten („US-Active“ am Standort „US Southwest“ und „US-Backup“ am Standort „US Northwest PA-A“) integriert und einen Standort erstellt, an dem „US-Active“ die aktive Dienstverbindung am Standort und „US-Backup“ die Back-up-Dienstverbindung am Standort ist.

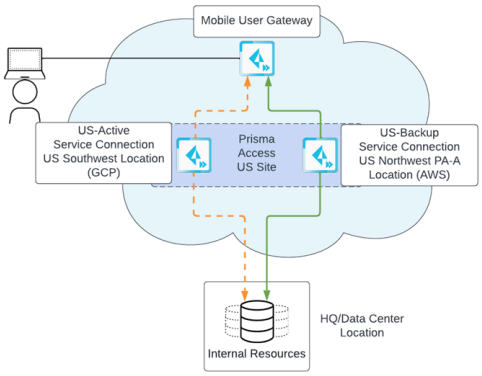
  Da Sie Dienstverbindungen an verschiedenen Compute-Standorten sowie verschiedene Cloud-Anbieter eingebunden haben, wurde ein Standort konfiguriert, der Ihnen sowohl geografische als auch Cloud-Anbieter-Redundanz bietet.




  Wenn der Standort „US-Active“ ausfällt (entweder wegen eines Ausfalls bei einem Cloud-Anbieter oder aufgrund eines regionalen Ausfalls), wird ein Failover der Dienstverbindung zum Standort „US-Backup“ durchgeführt, der einen anderen Cloud-Anbieter und einen

 ©2025 Palo Alto Networks, Inc.

anderen Compute-Standort verwendet als die Dienstverbindung „US-Active“, wie im folgenden Diagramm dargestellt.

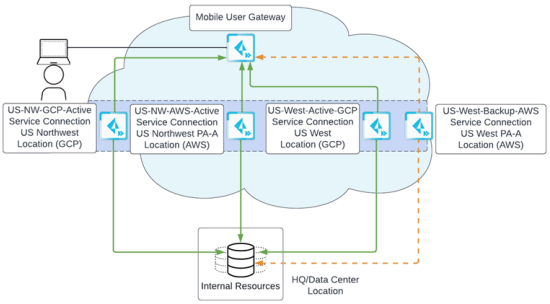



- **Verbindung mit hoher Bandbreite, die mehrere Dienstverbindungen verwendet** – Wenn Sie eine Verbindung mit höherer Bandbreite zu Ihren internen Ressourcen benötigen, können Sie einen Standort mit mehreren aktiven Verbindungen erstellen. Im folgenden Diagramm sind die vier einzubindenden Standorte dargestellt, wobei eine Kombination aus GCP- und AWS-Cloud-Anbietern verwendet wird:
  - „US-NW-GCP-Active“ unter Verwendung des Standorts „US Northwest (GCP)“
  - „US-NW-AWS-Active“ unter Verwendung des Standorts „US Northwest PA-A (AWS)“
  - „US-West-Active-GCP“ unter Verwendung des Standorts „US-West (GCP)“
  - „US-West-Backup-AWS“ unter Verwendung des Standorts „US-West PA-A (AWS)“

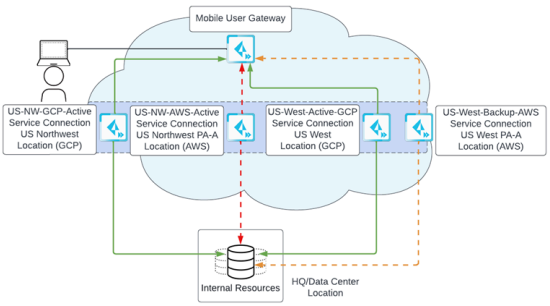
  Im Standort werden drei der Dienstverbindungen als aktive Dienstverbindungen angegeben, wobei eine vierte Dienstverbindung als Back-up angegeben wird. Wenn Sie drei

 ©2025 Palo Alto Networks, Inc.

Dienstverbindungen als aktiv angeben, erhalten Sie effektiv die dreifache Bandbreite für Ihre internen Ressourcen im Vergleich zu einer einzelnen Dienstverbindung.

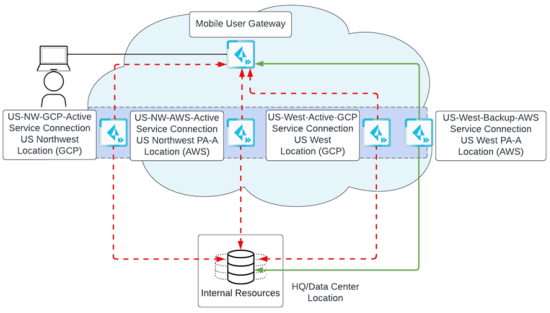



Fällt eine der aktiven Dienstverbindungen aus, wird die Back-up-Verbindung nicht in Betrieb genommen. Stattdessen leitet Prisma Access den Datenverkehr auf die verbleibenden aktiven und funktionierenden Dienstverbindungen um, wie im folgenden Diagramm dargestellt.




Wenn alle aktiven Dienstverbindungen ausfallen, wird die Back-up-Dienstverbindung in Betrieb genommen und als aktive Verbindung festgelegt.

*Wenn Sie mehrere Dienstverbindungen als Back-up-Dienstverbindungen konfigurieren, nimmt Prisma Access alle Back-up-Dienstverbindungen in Betrieb und verteilt die Last des Dienstverbindungsverkehrs auf diese.*




Halten Sie sich bei der Konfiguration redundanter Cloud-Anbieter-Dienstverbindungen an die folgenden Richtlinien:

 ©2025 Palo Alto Networks, Inc.

- Sie können Dienstverbindungen an bevorzugten oder alternativen Standorten hinzufügen.

  Palo Alto Networks empfiehlt Ihnen dringend, den bevorzugten Cloud-Anbieter als aktive Dienstverbindung an einem Standort zu verwenden.
- Alle Dienstverbindungen an einem Standort müssen auf dieselbe Ressource in derselben Zentrale oder im selben Rechenzentrumsstandort verweisen. An einem Standort können keine Dienstverbindungen vorhanden sein, die auf verschiedene Ressourcen an verschiedenen Standorten verweisen.
- Sie müssen an einem Standort mindestens eine aktive Dienstverbindung auswählen. Es können jedoch auch mehrere aktive Dienstverbindungen an einem Standort vorhanden sein. Die folgende Standortkonfiguration ist gültig:
  - USA (Mitte), aktiv
  - USA (Mitte) PA-A, Backup
  - USA (Ost), aktiv
  - USA (Ost) PA-A, Backup
- Wenn an einem Standort mehrere aktive Dienstverbindungen vorliegen und eine aktive Dienstverbindung ausfällt, wird der Datenverkehr auf die andere aktive Dienstverbindung umgeleitet (d. h. die Back-up-Dienstverbindung wird nicht genutzt, solange eine der aktiven Dienstverbindungen vorhanden ist).
- Verwenden Sie die folgenden Richtlinien für das statische und dynamische Routing für Dienstverbindungen:
  - Wenn Sie statisches Routing für Dienstverbindungen verwenden, stellen Sie sicher, dass die Subnetze, die Sie für die Dienstverbindungen angeben, auf dieselben Subnetze verweisen.

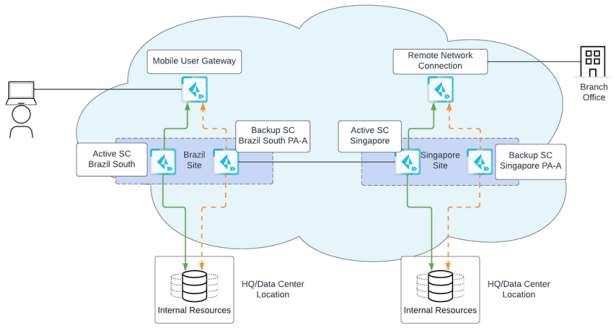
    Wenn z. B. an einem Standort 192.168.41.0/24, 192.168.44.0/24 und 192.168.47.0/24 als Subnetze für die aktiven Dienstverbindungen verwendet werden, stellen Sie sicher, dass Sie dieselben Subnetze für die Back-up-Dienstverbindungen angeben.
  - Wenn Sie dynamisches Routing (BGP) für Dienstverbindungen verwenden, stellen Sie sicher, dass alle Dienstverbindungen dieselben Präfixe für dasselbe Rechenzentrum oder dieselbe Zentrale ankündigen.
- Prisma Access verwendet BGP-Multi Exit Discriminator-(MED-)Werte, um zwischen aktiven und Back-up-Dienstverbindungen an einem Standort zu unterscheiden, wie in der folgenden Tabelle dargestellt. Beachten Sie, dass sich die MED-Werte für aktive Dienstverbindungen ändern, je nachdem, ob Sie einen sekundären IPSec-Tunnel für die aktive Dienstverbindung aktiviert haben oder nicht. Prisma Access kündigt diese MED-Werte beim CPE (BGP-Peer) an.

| Verbindungstyp | MED-Wert |
|---|---|
| **Aktive IPSec-Dienstverbindungen an einem Standort** | |
| Aktive Dienstverbindung, kein sekundärer IPSec-Tunnel konfiguriert | 0 |
| Aktive Dienstverbindung, sekundärer IPSec-Tunnel konfiguriert, primärer Tunnel | 100 |

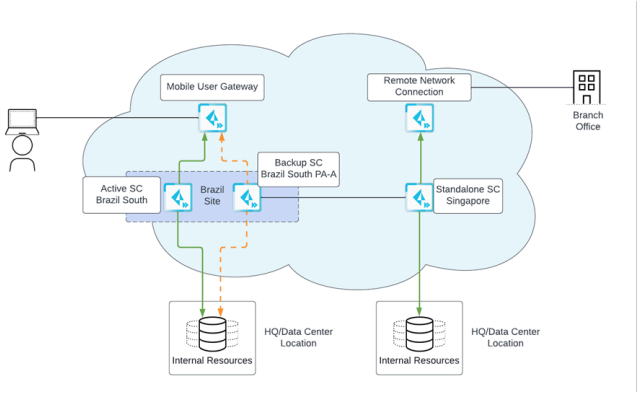
 ©2025 Palo Alto Networks, Inc.

| Verbindungstyp | MED-Wert |
|---|---|
| Aktive Dienstverbindung, sekundärer IPSec-Tunnel konfiguriert, sekundärer Tunnel | 200 |
| **Back-up-IPSec-Dienstverbindungen an einem Standort** | |
| Back-up-Dienstverbindung, primärer Tunnel (unabhängig davon, ob ein sekundärer IPSec-Tunnel konfiguriert ist oder nicht) | 500 |
| Back-up-Dienstverbindung, sekundärer IPSec-Tunnel konfiguriert, sekundärer Tunnel | 600 |

- Sie können mehrere Standorte in einer einzigen Prisma Access-Bereitstellung hinzufügen, wie im folgenden Diagramm veranschaulicht.




- Sie können weiterhin eine einzelne, eigenständige Dienstverbindung verwenden, um auf interne Ressourcen zuzugreifen. Sie können auch eigenständige Dienstverbindungen mit aktiven und Back-up-Dienstverbindungen kombinieren, wie im folgenden Diagramm gezeigt.




- Multicloud-Redundanz für Dienstverbindungen wird nicht unterstützt, wenn Hot-Potato-Routing für Dienstverbindungen verwendet wird.
- Verwenden Sie die CLI nicht, um Dienstverbindungen einzubinden und zu konfigurieren. Wenn Sie die CLI für das Onboarding von Dienstverbindungen benötigen, wenden Sie sich an Ihr Team von Palo Alto Networks.

 ©2025 Palo Alto Networks, Inc.

## Konfigurieren und Aktivieren der Cloud-Provider-Redundanz für Dienstverbindungen

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Führen Sie die folgenden Schritte aus, um mehrere Dienstverbindungen für Cloud-Anbieter zu konfigurieren.

**STEP 1 |** (Nur vorhandene Prisma Access-Bereitstellungen) Wenn Sie Ihr Plug-in auf eine Version aktualisiert haben, die die Redundanz von Cloud-Anbietern unterstützt, führen Sie nach dem Upgrade auf das unterstützte Plug-in die Aktion **Commit und Push** aus.

Die Multicloud-Redundanz für Dienstverbindungen wird ab Prisma Access Version 3.1 Preferred und Innovation unterstützt. Nachdem Sie das Cloud-Services-Plug-in aktualisiert haben, müssen Sie die Aktion **Commit und Push** ausführen, damit die Änderungen an der Cloud-Redundanz in der Benutzeroberfläche angezeigt werden.

Wenn Sie eine neue Bereitstellung (kein Upgrade) verwenden, überspringen Sie diesen Schritt.

 ©2025 Palo Alto Networks, Inc.

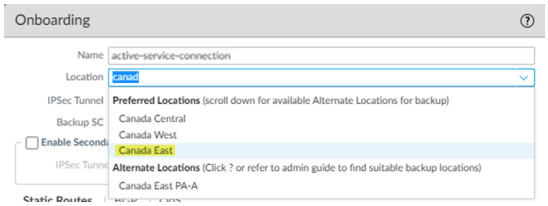
**STEP 2 |** Erstellen Sie die Dienstverbindungen, die als aktive und Backup-Dienstverbindungen an einem Standort verwendet werden sollen.

*Nachdem Sie bevorzugte und alternative Standorte erstellt und Ihre Änderungen mit „Commit und Push“ festgeschrieben und übertragen haben, können Sie diese Standorte nicht mehr ändern. Beispielsweise können Sie den bevorzugten Standort nicht mehr von Kanada Ost in Kanada Ost PA-A ändern und den alternativen Standort nicht mehr von Kanada Ost PA-A in Kanada Ost.*

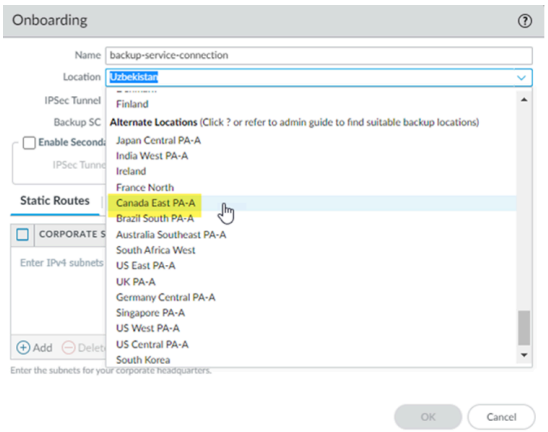
1. Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Dienstverbindung**aus.
2. **Fügen** Sie eine Dienstverbindung hinzu, die Sie als aktive Dienstverbindung an einem Standort festlegen.

   Treffen Sie in der Liste der bevorzugten oder alternativen Standorte Ihre Auswahl.

   *Um nach einem Standort zu suchen, geben Sie zunächst den Namen für den **Standort** ein.*




3. **Fügen** Sie eine Dienstverbindung hinzu, die Sie als Backup-Dienstverbindung eines Standorts festlegen wollen.



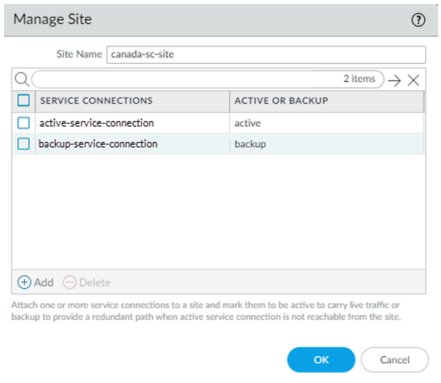

4. (Optional) Setzen Sie das Onboarding der Dienstverbindungen fort, die abhängig vom Bedarf als aktive und Backup-Standorte verwendet werden sollen.

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Erstellen Sie einen Standort; ordnen Sie ihm die Dienstverbindungen zu, die Sie als aktive oder Backup-Dienstverbindungen für den Standort hinzugefügt haben.

1. **Fügen** Sie unter **Standorte verwalten** einen neuen Standort hinzu.
2. **Fügen** Sie die Dienstverbindungen hinzu, die Sie eingebunden haben.
3. Bestimmen Sie die Dienststandorte, die Sie als **aktiv** und **Backup** zum Standort hinzugefügt haben.

   Sie können mehrere aktive und Backup-Standorte erstellen. Geben Sie mindestens einen Standort als aktiven Standort an.
4. Klicken Sie auf **OK**.
5. (Optional) Fügen Sie nach Bedarf weitere Standorte für Ihre aktiven und Backup-Dienstverbindungen hinzu.




**STEP 4 |** Führen Sie für Ihre Änderungen die Aktion **Commit und Push** aus.

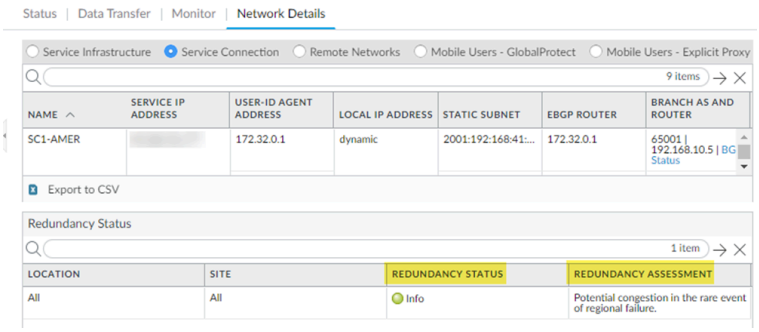
**STEP 5 |** Überprüfen Sie den Status Ihrer Standorte.

1. Wählen Sie **Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Dienstverbindung** > **Redundanzstatus** aus.
2. Überprüfen Sie die Informationen in den Feldern **Redundanzstatus** und **Redundanzbewertung**. Mit dem Redundanzstatus erhalten Sie den Status der von Ihnen bereitgestellten Standorte und mit der Redundanzbewertung erhalten Sie weiterführende Informationen zu den bereitgestellten Dienstverbindungen am Standort.

| Redundanzstatus | Redundanzbewertung |
|---|---|
| Info | Bei regionalen Ausfällen kann es zu Überlastungen Ihrer Dienstverbindungen kommen. |
| Warnung | Alle Dienstverbindungen werden in einer einzigen Region bereitgestellt. Bitte prüfen Sie die Möglichkeit zur Bereitstellung an nahe gelegenen Standorten.<br><br>Diese Meldung informiert Sie darüber, dass alle Ihre Dienstverbindungen in einer einzigen Region bereitgestellt werden. |

 ©2025 Palo Alto Networks, Inc.

| Redundanzstatus | Redundanzbewertung |
|---|---|
| Achtung: | Alle Dienstverbindungen, die eine Verbindung zu dem Standort herstellen, werden in einer einzigen Region bereitgestellt. Bitte prüfen Sie die Möglichkeit zur Bereitstellung an nahe gelegenen Standorten.<br><br>Diese Meldung informiert Sie darüber, dass alle Dienstverbindungen, die eine Verbindung zu einem Standort herstellen, in einer einzigen Region bereitgestellt werden. |




## Unterstützte Standorte im Land für aktive und Backup-Standorte mit Cloud-Anbieter-Redundanz

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Panorama | • Prisma Access-Lizenz |

Wenn Sie eine Bereitstellung konfigurieren möchten, bei der sich der aktive und der Backup-Standort im selben Land befinden, wählen Sie aus dieser Liste der bevorzugten und alternativen Standorte im Land die gewünschten Standorte aus.

| Bevorzugte Standorte | Alternative Standorte |
|---|---|
| Australien (Südost) | Australien (Südost), PA-A |
| Bahrain, PA-A | Bahrain |
| Brasilien (Süd) | Brasilien (Süd), PA-A |
| Kanada (Ost) | Kanada (Ost), PA-A |
| Frankreich (Nord), PA-A | Frankreich (Nord) |
| Deutschland (Mitte) | Deutschland (Mitte), PA-A |

 ©2025 Palo Alto Networks, Inc.

| Bevorzugte Standorte | Alternative Standorte |
|---|---|
| Indien (West) | Indien (West), PA-A |
| Irland, PA-A | Irland |
| Japan (Mitte) | Japan (Mitte), PA-A |
| Singapur | Singapur, PA-A |
| Südafrika (West), PA-A | Südafrika (West) |
| Südkorea, PA-A | Südkorea |
| GB | GB, PA-A |
| Vereinigte Arabische Emirate, PA-A | Vereinigte Arabische Emirate |
| USA (Mitte) | USA (Mitte), PA-A |
| USA (Ost) | USA (Ost), PA-A |
| USA (Nordwest) | USA (Nordwest), PA-A |
| USA (West) | USA (West), PA-A |

## Internetgebundenen Datenverkehr mittels Datenverkehrslenkung an Dienstverbindungen weiterleiten

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz<br>❑ Wenn Zertifikatsperrungslisten (Certificate Revocation List, CRL) und Online-Zertifikatstatusprotokolle (Online Certificate Status Protocol, OCSP) direkt ins Internet gesendet werden sollen, ist Prisma Access Version 5.1.1 oder höher erforderlich. |

Mit Prisma Access können Sie Regeln für die Datenverkehrslenkung erstellen, um Ziele für internetgebundenen Datenverkehr von mobilen Benutzern und Remote-Netzwerk-Verbindungen festzulegen. Sie können den Datenverkehr angeben, der vor dem Senden ins Internet an eine Dienstverbindung umgeleitet werden soll, oder den Datenverkehr, der direkt ins Internet gehen soll. Diese Funktionalität wird als *Datenverkehrslenkung* (Traffic Steering) bezeichnet.

 ©2025 Palo Alto Networks, Inc.

Alternativ können Sie Prisma Access so konfigurieren, dass eine Standardroute von Ihrem CPE zu Prisma Access zugelassen wird, sodass Prisma Access internetgebundenen mobilen Benutzerverkehr an die beste Dienstverbindung in Ihrer Bereitstellung weiterleitet.

## Standardrouten mit Prisma Access-Datenverkehrslenkung

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Verwenden Sie die Standardroutenfunktion in Prisma Access, um Standardrouten zu akzeptieren, die von Ihrem CPE bei Dienstverbindungen angekündigt werden. Sie können BGP oder statische Routen verwenden, um die Standardroute anzukündigen. Prisma Access verwendet BGP, um diese Routen über mehrere Dienstverbindungen anzukündigen, wodurch Prisma Access den Datenverkehr mobiler Benutzer über die beste Dienstverbindung für einen bestimmten mobilen Benutzerstandort leiten kann. Um Dienstverbindungen für die Annahme von Standardrouten zu aktivieren, geben Sie **Standardroute über Dienstverbindung akzeptieren** ein, wenn Sie Datenverkehrslenkung in Prisma Access konfigurieren.

Nachdem Sie Standardrouten aktiviert haben, wird Ihr internetgebundener Datenverkehr an Dienstverbindungen geleitet und verlässt das Netzwerk nicht an den Standorten der mobilen Benutzer. Diese Funktion kann nützlich sein, wenn Sie internetgebundenen Datenverkehr an das Rechenzentrum umleiten möchten, beispielsweise wenn der Sicherheitsstack eines Drittanbieters in Ihrem Rechenzentrum vorhanden ist und Sie möchten, dass der Stack den Datenverkehr zusätzlich durchsucht oder überprüft.

Beachten Sie beim Implementieren von Standardrouten die folgenden Richtlinien:

- Standardrouten gelten nur für Bereitstellungen mobiler Benutzer. Remote-Netzwerkverbindungen funktionieren normal und ohne Änderung, wenn Sie Standardrouten aktivieren.
- Sie müssen keine Ziel-Dienstverbindungen oder Datenverkehrslenkungsregeln angeben, wenn Sie Standardrouten zulassen, obwohl diese für die Verwendung mit Standardrouten unterstützt werden.
- Wenn Sie die Einstellung **Standardroute über Dienstverbindung akzeptieren** angeben, akzeptieren alle Prisma Access-Dienstverbindungen, mit Ausnahme von dedizierten Dienstverbindungen, Standardrouten und verwenden die Routen bei Entscheidungen zur Datenverkehrslenkung.
- Bevor Sie diese Einstellung aktivieren, stellen Sie sicher, dass Ihre Rechenzentren Standardrouten senden. Anderenfalls schlägt das Routing über Dienstverbindungen fehl.
- Palo Alto Networks empfiehlt, dass alle Rechenzentren eine Standardroute ankündigen. wenn Prisma Access die Routen empfängt. Anschließend kann die beste Dienstverbindung zur Verwendung für den Remote-Netzwerkstandort ausgewählt werden.
- Verwenden Sie daher beim Konfigurieren von Dienstverbindungen entweder nur statische Routen oder nur BGP für die Verbindungen. Palo Alto Networks empfiehlt,

 ©2025 Palo Alto Networks, Inc.

Dienstverbindungen, die BGP und statische Routen verwenden, bei der Verwendung von Standardrouten nicht zu kombinieren.

- (Nur für Prisma Access (Managed by Panorama)-Bereitstellungen) Die Verwendung von Standardrouten wird mit Bereitstellungen mit mehreren Mandanten unterstützt.
- Prisma Access leitet SAML-Authentifizierungsdatenverkehr für clientloses VPN, ein Portal oder ein Gateway nicht über die Standardroute an einen öffentlichen Identitätsanbieter (Public Identity Provider, IdP) weiter.

Weitere Informationen und Beispiele für die Implementierung von Standardrouten mit Datenverkehrslenkung finden Sie unter Beispiel für Standardrouten mit Verkehrslenkung, Beispiel für Standardrouten mit Datenverkehrslenkung direkt ins Internetund Beispiel für Standardrouten mit Datenverkehrslenkung und dedizierter Dienstverbindung.

## Datenverkehrslenkung in Prisma Access

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

In Standardbereitstellungen von Prisma Access bietet eine Dienstverbindung Zugriff auf interne Netzwerkressourcen, z. B. Authentifizierungsdienste und private Apps in Ihrer Zentrale oder in Ihrem Rechenzentrum. Dienstverbindungen verarbeiten internen Datenverkehr, für den kein Internetzugang erforderlich ist. In einigen Fällen möchten Sie möglicherweise internetgebundenen Datenverkehr zum Rechenzentrum umleiten. Mit der Datenverkehrslenkung können Sie Datenverkehr mobiler Benutzer oder Remote-Netzwerkverkehr zu einer Dienstverbindung umleiten, bevor dieser ins Internet gesendet wird.

Sie können die Datenverkehrslenkung mit mobilen Benutzerbereitstellungen, Remote-Netzwerkbereitstellungen oder einer Kombination aus beidem verwenden. Verwenden Sie die Datenverkehrslenkung, um internetgebundenen Netzwerkverkehr basierend auf vielen Kriterien wie IP-Adressen, Benutzern, URLs, benutzerdefinierten URL-Kategorien, Diensttyp (HTTP oder HTTPS), Benutzer-ID, dynamischen Adressgruppen (DAGs), dynamischen Benutzergruppen (DUGs) und IP-basierten externen dynamischen Listen (EDLs) zu lenken.

Von der Datenverkehrslenkung werden zwei Aktionstypen unterstützt:

- **An das Ziel weiterleiten** – Verwenden Sie die Kriterien in den Regeln zur Datenverkehrslenkung, um internetgebundenen Datenverkehr über ein von Ihnen erstelltes Ziel weiterzuleiten, das eine oder mehrere Dienstverbindungen verwendet.
- **An das Internet weiterleiten** – Verwenden Sie die Kriterien in den Regeln zur Datenverkehrslenkung, um den Datenverkehr direkt von seiner Quelle (Standort mobiler Benutzer oder Remote-Netzwerkverbindung) ins Internet weiterzuleiten, ohne zu einer Dienstverbindung weitergeleitet zu werden.

Wenn die Weiterleitung an ein Ziel erfolgt, können Sie zwei Zielgruppentypen erstellen: dediziert und nicht dediziert.

- Eine Dienstverbindung, die nur für den auf Datenverkehrslenkung bezogenen Datenverkehr genutzt wird, ist eine *dedizierte Dienstverbindung*. Wenn Sie eine Dienstverbindung für

 ©2025 Palo Alto Networks, Inc.

die Verwendung als dedizierte Dienstverbindung festlegen möchten, wählen Sie **Nur für Datenverkehrslenkung vorgesehen** aus, wenn Sie in Panorama Datenverkehrslenkung in Prisma Access konfigurieren. Wählen Sie **Nur für PBF vorgesehen** aus, wenn Sie eine Regel zur Datenverkehrslenkung in Strata Cloud Manager einrichten.

Möglicherweise möchten Sie eine dedizierte Dienstverbindung konfigurieren, wenn Sie den Sicherheitsstack eines Drittanbieters verwenden, der sich außerhalb des internen Netzwerks Ihrer Organisation befindet, um Datenverkehr zu verarbeiten, bevor er an eine öffentliche SaaS-Anwendung oder das Internet gesendet wird. Da der Sicherheitsstack nicht Teil des Netzwerks Ihrer Organisation ist, möchten Sie nicht, dass diese Dienstverbindung internen Netzwerkverkehr verarbeitet.

- Eine Dienstverbindung, die zur Datenverkehrslenkung und für auf die Standarddienstverbindung bezogenen Datenverkehr verwendet wird (wie z. B. Datenverkehr, der an einen Authentifizierungsserver im Rechenzentrum geleitet wird), ist eine *nicht dedizierte Dienstverbindung*.

Wenn Sie eine Dienstverbindung als dedizierte Dienstverbindung festlegen, führt dies zu folgenden Änderungen an Ihrer Bereitstellung:

- (Nur für Prisma Access (Managed by Strata Cloud Manager)-Bereitstellungen) Die Dienstverbindungen wenden Quell-NAT auf den weitergeleiteten Datenverkehr an. Die Quell-IP-Adresse ist die **EBGP-Router**-Adresse der Dienstverbindung, die aus dem Infrastruktur-Subnetz übernommen wird.
- Die Zone für alle Dienstverbindungen, die diesem Ziel zugeordnet sind, wird von „Vertrauenswürdig“ in „Nicht vertrauenswürdig“ geändert. Überprüfen Sie Ihre Zonenzuordnung und gehen Sie wie unter Konfigurieren von Zonenzuordnungs- und Sicherheitsrichtlinien für dedizierte Datenverkehrslenkungsverbindungen beschrieben vor, um sicherzustellen, dass Ihr Netzwerk diese Änderung widerspiegelt.
- Dienstverbindungen, die als dedizierte Dienstverbindungen konfiguriert sind, nehmen weder intern noch extern am BGP-Routing teil.
- (Nur für Prisma Access (Managed by Panorama)-Bereitstellungen) Sofern Ihre dedizierte Dienstverbindung BGP verwendet, wird als BGP-Status **Nicht aktiviert** angezeigt, wenn Sie die Statusseite öffnen (**Panorama** > **Cloud Service** > **Status** > **Überwachen** > **Dienstverbindung**), eine Region auswählen und dann die Registerkarte „Status“ auswählen. Den BGP-Status einer Dienstverbindung können Sie auf der Konfigurationsseite der Dienstverbindungen überprüfen (**Panorama** > **Cloud Services** > **Konfiguration** > **Dienstverbindung**).
- (Nur für Prisma Access (Managed by Panorama)-Bereitstellungen) Standardmäßig wenden die Dienstverbindungen Quell-NAT auf den weitergeleiteten Datenverkehr an. Die Quell-IP-Adresse ist die **Benutzer-ID-Agent-Adresse** der Dienstverbindung (**Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Dienstverbindung** > **Benutzer-ID-Agent-Adresse**), die aus dem Infrastruktursubnetz (**Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Dienstinfrastruktur**) übernommen wird.

  (Nur für Prisma Access (Managed by Panorama)-Bereitstellungen) Sie können Quell-NAT deaktivieren und die Quell-IP-Adressen Ihrer Organisation für die dedizierte Dienstverbindung verwenden. Wählen Sie dazu **Quell-NAT für bestimmte Dienstverbindungen deaktivieren** aus, wenn Sie ein Ziel im Bereich **Ziel-Dienstverbindungen für Datenverkehrslenkung hinzufügen**.

 ©2025 Palo Alto Networks, Inc.

## Anforderungen an die Datenverkehrslenkung

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Bevor Sie die Datenverkehrslenkung in Ihrer Prisma Access-Bereitstellung implementieren, stellen Sie sicher, dass Ihre Netzwerkumgebung die folgenden Infrastrukturanforderungen erfüllt:

- Prisma Access muss in der Lage sein, eine Verbindung mit dem IPSec-fähigen CPE (z. B. einem Router oder SD-WAN-Gerät) herzustellen, das Ihre Organisation zum Beenden der Dienstverbindung verwendet, und die IP-Adresse für das Gerät muss von Prisma Access aus erreichbar sein.

  Sie erstellen eine Dienstverbindung mit den IPSec- und IKE-Standard-Verschlüsselungsprofilen zwischen dem Speicherort des Stacks und Prisma Access. Sie können statische Routen, BGP oder eine Kombination aus beidem verwenden, wenn Sie eine Dienstverbindung konfigurieren und die Datenverkehrslenkung verwenden. Wenn Sie Standardrouten mit Datenverkehrslenkung verwenden, empfiehlt Palo Alto Networks, entweder nur BGP oder nur statische Routen zu verwenden. Wenn Sie statisches Routing verwenden, geben Sie die öffentliche IP-Adresse an, die vom CPE der Organisation als **Peer-Adresse** verwendet wird, wenn Sie ein IKE-Gateway erstellen.
- Prisma Access gleicht möglicherweise die ersten Pakete einer URL aus einer URL-Kategorie in einer Regel zur Datenverkehrslenkung nicht ab, was bedeutet, dass die ersten Pakete einer Netzwerksitzung (z. B. ein TCP-Handshake) möglicherweise nicht mit der Regel übereinstimmen. Palo Alto Networks empfiehlt, dass Sie für URLs, die Sie in Regeln zur Datenverkehrslenkung verwenden, eine Sicherheitsrichtlinienregel erstellen, sodass sie die nicht vertrauenswürdige Zone durchlaufen können, damit der Handshake abgeschlossen werden kann, wenn eine neue Sitzung beginnt.
- Wenn Sie diese Konfiguration mit einem Sicherheitsstack verwenden, muss der Stack-Speicherort von der Dienstverbindung aus über eine standardmäßige IPSec-Tunnelkonfiguration erreichbar sein.

Beachten Sie beim Konfigurieren der Datenverkehrslenkung die folgenden Richtlinien:

- Sie können bis zu 1.000 URLs (aggregiert) in einer Konfiguration für die Datenverkehrslenkung angeben, einschließlich regulärer URLs und Platzhalter-URLs (*.example.com) in benutzerdefinierten URL-Kategorien.

  Diese Zahl umfasst sowohl manuell eingegebene URLs, Platzhalter-URLs als auch URLs, die in einer benutzerdefinierten URL-Kategorie eingegeben werden.
- Prisma Access stellt URLs in benutzerdefinierten URL-Kategorien ein Sternchen voran, wenn Sie diese Kategorie in einer Regel zur Datenverkehrslenkung verwenden. Wenn Sie dieselben

 ©2025 Palo Alto Networks, Inc.

URL-Kategorierichtlinien sowohl für Regeln zur Datenverkehrslenkung als auch für andere Sicherheitsrichtlinienregeln verwenden, gelten diese Änderungen für beide Regeltypen.

Wenn Sie mit benutzerdefinierten URL-Kategorien arbeiten, die nicht in Regeln zur Datenverkehrslenkung verwendet werden, ändert Prisma Access die URLs in diesen Kategorien nicht.

- Verwenden Sie URLs in Kleinbuchstaben, wenn Sie URLs in eine Regel für die Weiterleitung von Datenverkehr eingeben und wenn Sie einer benutzerdefinierten URL-Kategorie URLs hinzufügen.
- Sie können maximal 100 Regeln für die Weiterleitung von Datenverkehr konfigurieren.
- Wenn Sie den primären und den Backup-Tunnel konfiguriert haben, funktioniert die Datenverkehrslenkung mithilfe von Regeln zur Datenverkehrslenkung nach einem Failover vom primären (aktiven) zum Backup-Tunnel nicht. Standardrouten mit Prisma Access-Datenverkehrslenkung funktioniert in einem Failover-Szenario mit primären und Backup-Tunneln.

## Beispiel für Standardrouten mit Verkehrslenkung

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Das folgende Beispiel zeigt eine Prisma Access-Beispielbereitstellung mit den folgenden Komponenten:

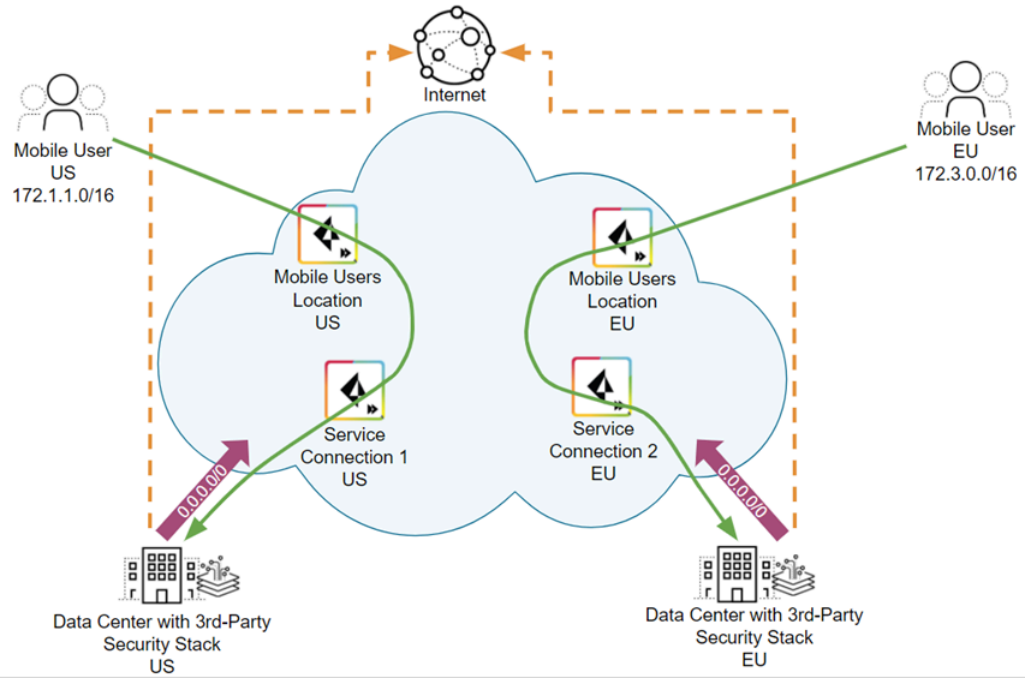
- Zwei Prisma Access-Standorte mit mobilen Benutzern: einer in den Vereinigten Staaten (US) und einer in Europa (EU).
- Zwei Prisma Access-Dienstverbindungen: eine in den Vereinigten Staaten (US) und eine in der EU. Beide Rechenzentren senden Standardrouten an die Dienstverbindungen (**Standardroute über Dienstverbindung akzeptieren** ist aktiviert).
- Zwei Rechenzentren: eines in den Vereinigten Staaten (US) und eines in der EU.

  Jedes Rechenzentrum verfügt über einen Sicherheitsstack von Drittanbietern. Aus diesem Grund möchten Sie, dass der gesamte internetgebundene Datenverkehr über das Rechenzentrum geleitet wird, bevor er ins Internet gelangt.

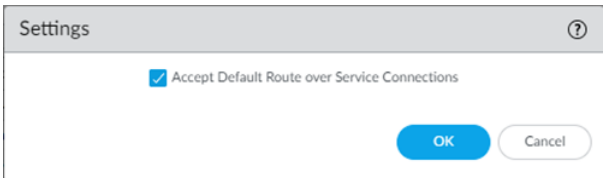
Wenn ein mobiler Benutzer Rechenzentrumsdatenverkehr sendet, überprüft Prisma Access die entsprechenden Routingtabellen, ermittelt die nächstgelegene Dienstverbindung und leitet den Datenverkehr an diese Dienstverbindung weiter. Im folgenden Beispiel sendet Prisma Access Rechenzentrumsdatenverkehr von den mobilen Benutzern in den USA an die Dienstverbindung „Service Connection“ und Datenverkehr von den mobilen Benutzern in der EU an die Dienstverbindung „Service Connection 2“.

*Verwenden Sie mit Standardrouten keine Dienstverbindungen, die **nur für Datenverkehrslenkung vorgesehen** sind. Dedizierte Dienstverbindungen nehmen nicht am BGP-Routing teil, sodass sie keine BGP-Werbung von der Zentrale oder vom Rechenzentrum empfangen können.*

 ©2025 Palo Alto Networks, Inc.




Um Standardrouten zu aktivieren, wählen Sie **Standardroute über Dienstverbindungen akzeptieren** aus, wenn Sie Einstellungen für die Datenverkehrslenkung konfigurieren. Nachdem Sie diese Einstellung konfiguriert und einen Commit für Ihre Änderungen ausgeführt sowie Ihre Änderungen per Push übertragen haben, sendet Prisma Access internetgebundenen Datenverkehr über die Dienstverbindungen.

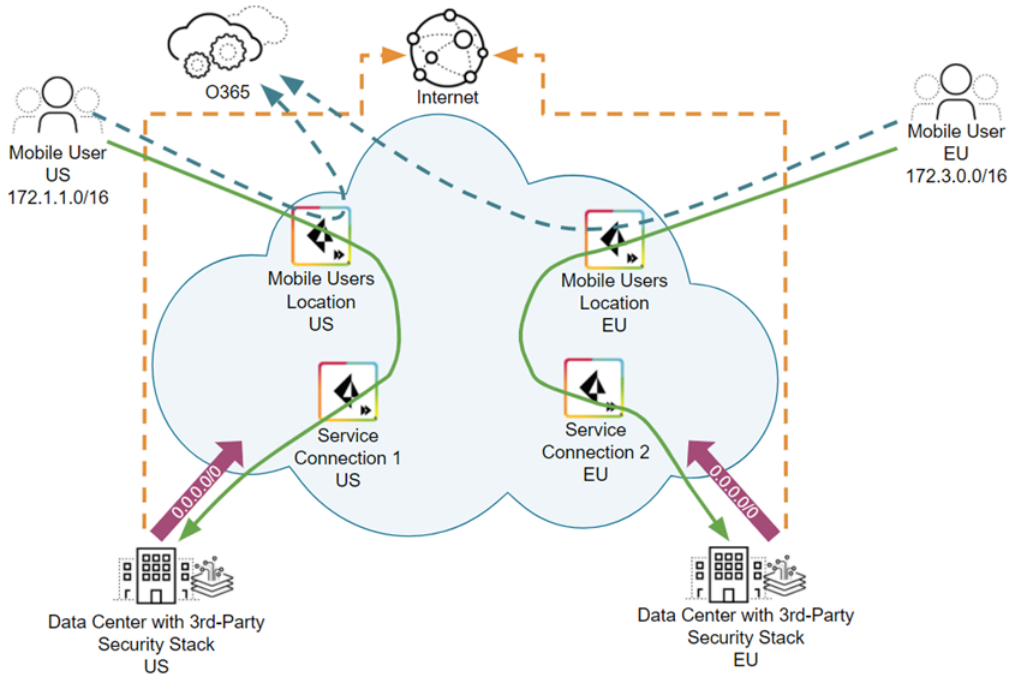



## Beispiel für Standardrouten mit Datenverkehrslenkung direkt ins Internet

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Das folgende Beispiel zeigt, wie Sie den an externe SaaS-Anwendungen gebundenen Datenverkehr gezielter lenken können. In diesem Fall möchten Sie den Office 365-Datenverkehr direkt vom Standort des mobilen Benutzers ins Internet leiten, anstatt ihn zur weiteren Verarbeitung an das Rechenzentrum zu senden. Verwenden Sie für diese Konfiguration die Datenverkehrslenkung zusammen mit Standardrouten.

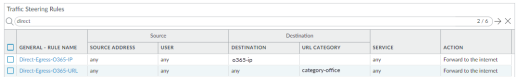
 ©2025 Palo Alto Networks, Inc.




Damit Prisma Access Office 365-Datenverkehr direkt ins Internet routen kann, gehen Sie wie folgt vor:

- Erstellen Sie eine EDL (**Objekt** > **Externe dynamische Listen**) mit IP-Adressen, die mit den Office 365-Adressen übereinstimmen.
- Erstellen Sie eine benutzerdefinierte URL-Kategorie (**Objekte,** > **Benutzerdefinierte Objekte** > **URL-Kategorie**) mit URLs, die mit der Office 365-URL übereinstimmen.
- Befolgen Sie die Schritte auf der Seite Datenverkehrslenkung in Prisma Access konfigurieren und geben Sie die von Ihnen erstellte EDL und URL-Kategorie als Ziel-Übereinstimmungskriterien mit der **Aktion An das Internet weiterleiten** an.

Bei dieser Konfiguration wird der Office 365-Datenverkehr direkt ins Internet gesendet, während der übrige internetgebundene Datenverkehr zur weiteren Verarbeitung an das Rechenzentrum gesendet wird, bevor er ins Internet gelangt.



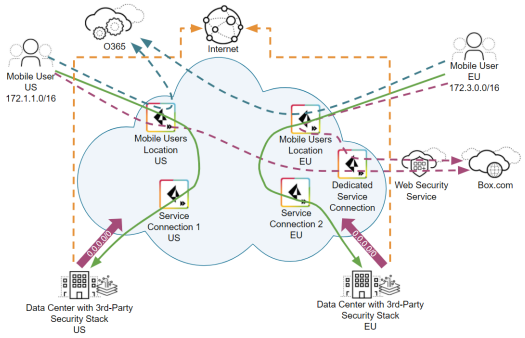
## Beispiel für Standardrouten mit Datenverkehrslenkung und dedizierter Dienstverbindung

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

In diesem Beispiel verfügen Sie zusätzlich zur vorherigen Konfiguration über einen Internetsicherheitsdienst eines Drittanbieters und möchten Datenverkehr von box.com senden, damit dieser vom Sicherheitsdienst verarbeitet wird, bevor er Ihr System verlässt und ins Internet gelangt. Sie möchten keinen anderen internetgebundenen Datenverkehr an den

 ©2025 Palo Alto Networks, Inc.

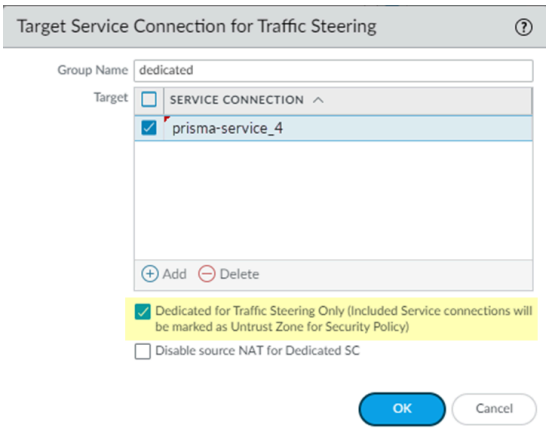
Sicherheitsdienst senden. Aus diesem Grund erstellen Sie eine dedizierte Dienstverbindung für den Datenverkehr von box.com. Nachdem Ihre Konfiguration abgeschlossen ist, sendet Prisma Access Zieldatenverkehr für *.box.com an den Stapel.




Um diese Bereitstellung zu aktivieren, führen Sie die folgenden Aktionen auf der Registerkarte „Datenverkehrslenkung“ aus:

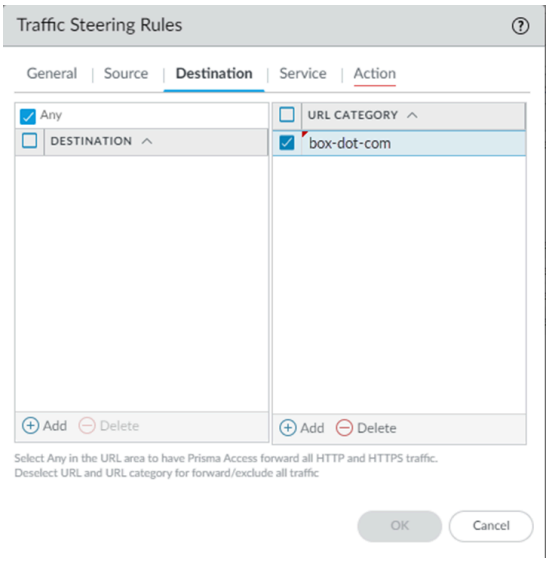
- Erstellen Sie eine Ziel-Dienstverbindungsgruppe, die dem Ziel eine oder mehrere Dienstverbindungen zuweist, und wählen Sie **Nur für Datenverkehrslenkung vorgesehen** aus, wodurch die Ziel-Dienstverbindungen als dediziert festgelegt werden.

  *Wenn Sie ein Ziel mit mehr als einer Dienstverbindung erstellen, wählt Prisma Access die beste Dienstverbindung aus, um den internetgebundenen Datenverkehr weiterzuleiten.*

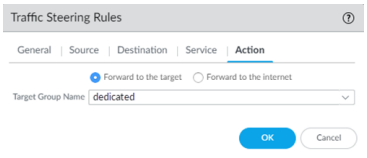



 ©2025 Palo Alto Networks, Inc.

- Erstellen Sie eine Datenverkehrslenkungsregel, die Datenverkehr an die URL weiterleitet. Der folgende Screenshot zeigt, dass dem Datenverkehrsziel eine benutzerdefinierte URL-Kategorie zugewiesen wird, die die URL *.box.com enthält.




- Erstellen Sie in der Datenverkehrslenkungsregel die **Aktion An das Ziel weiterleiten** und geben Sie den von Ihnen erstellten Zielgruppennamen an (in diesem Fall **dedicated**).




## Richtlinien für Regeln zur Datenverkehrslenkung in Prisma Access

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Panorama | • Prisma Access-Lizenz |

Die Datenverkehrslenkung kann eine Vielzahl möglicher Konfigurationen verarbeiten. Es ist jedoch wichtig zu verstehen, wie Prisma Access Regeln verarbeitet, damit Sie Regeln erstellen können, die einfach zu pflegen und zu verwalten sind. Um Sie beim Erstellen der Regeln zu unterstützen, die für Ihre Bereitstellung am besten funktionieren, befolgen Sie diese Richtlinien:

- Prisma Access wertet Regeln in der Reihenfolge aus, in der Sie sie erstellen (von oben nach unten). Geben Sie oben spezifischere Regeln und unten allgemeinere Regeln an.
- Erstellen Sie mehrere Regeln mit weniger übereinstimmenden Kriterien, anstatt weniger Regeln mit mehreren Kriterientypen. Das Erstellen einfacherer Regeln beschleunigt das Erstellen von Regeln und vereinfacht das Ändern einer Regel.
- Da Sie eine Regel nach dem Erstellen in einer Liste nicht mehr nach oben oder unten verschieben können, planen Sie Ihre Regelreihenfolge sorgfältig, bevor Sie die Regeln erstellen.
- Regeln, die **beliebige** Quelladressen und Benutzer, **beliebige** Quellziele und URL-Kategorien sowie **beliebige** Dienste angeben, werden nicht unterstützt. Verwenden Sie spezifischere

 ©2025 Palo Alto Networks, Inc.

Regeln. Geben Sie beispielsweise eine Regel für **beliebigen** Quell- oder Zieldatenverkehr sowie jeweils einen Dienst der Typen **service-http** und **service-https** an.

- Wenn Sie Regeln für Benutzer im Feld **Quellbenutzer** angeben möchten, stellen Sie sicher, dass Prisma Access zwischen Benutzern unterscheiden kann, wenn derselbe Benutzername zum einen von Benutzern verwendet wird, die sich lokal authentifizieren, und zum anderen von Benutzern verwendet wird, die LDAP verwenden. Geben Sie dazu LDAP-Benutzer im Format `Domäne/Benutzername` und lokale Benutzer im Format `Benutzername` (ohne den Domänennamen) an.
- Wenn Sie eine lokale Firewall der nächsten Generation als Mastergerät konfiguriert haben, können Sie Benutzer- und Gruppeninformationen für Gerätegruppen mobiler Benutzer in Regeln zur Datenverkehrslenkung und in Sicherheitsrichtlinienregeln automatisch einfügen lassen, indem Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Mobile Benutzer** auswählen, auf das Zahnradsymbol klicken, um die Einstellungen zu bearbeiten, und im Bereich Gerätegruppen das **Mastergerät** auswählen. Während dadurch das Mastergerät in jede Gerätegruppe eingefügt wird, werden nur die Benutzer- und Gruppeninformationen für mobile Benutzer in Sicherheitsrichtlinienregeln eingefügt.
- Wenn in einer Regel zur Datenverkehrslenkung eine EDL (des Typs „IP-Liste“) verwendet wird und die EDL-Quell-URL der EDL auf eine URL aktualisiert wird, auf die nicht zugegriffen werden kann, verwendet Prisma Access möglicherweise weiterhin die zwischengespeicherte IP-Liste der vorherigen URL.
- Prisma Access umgeht die Datenverkehrslenkung für Regeln mit dem Diensttyp HTTP oder HTTPS, wenn Sie eine Anwendungsüberschreibungsrichtlinie für die TCP-Ports 80 und 443 verwenden.

  Darüber hinaus funktioniert die Datenverkehrslenkung nicht für URLs aus URL-Kategorien, auf die in der Regel zur Datenverkehrslenkung verwiesen wird, wenn Sie eine Anwendungsüberschreibungsrichtlinie für die TCP-Ports 80 oder 443 konfiguriert haben.
- Sie können Ziel-IP-Adressen und URL-Kategorien in derselben Regel angeben. Wenn Sie dies tun, verwendet Prisma Access ein logisches ODER, um die Zielkriterien in der Regel zu verarbeiten. Allerdings werden die URLs und der Datenverkehr der URL-Kategorie basierend auf den TCP-Ports 80 und 8080 für HTTP und TCP-Port 443 für HTTPS verarbeitet.

  Bei einer Regel mit IP-Adressen und URL-Kategorien stimmt der Datenverkehr mit der Regel überein, wenn entweder die IP-Adresse oder die URL-Kategorie übereinstimmt. Der Datenverkehr der URL-Kategorie wird jedoch nur auf der Grundlage der Ports 80, 443 und 8080 verarbeitet. Palo Alto Networks empfiehlt, anstelle solcher Regeln einfachere Regeln zu erstellen.

Wenn Sie beispielsweise die folgenden Regeln für Ihren Netzwerkverkehr durchsetzen möchten, gehen Sie wie folgt vor:

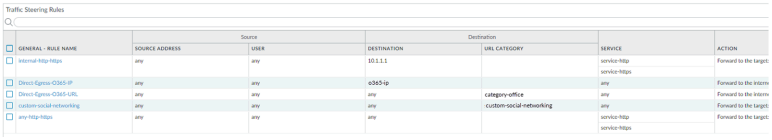
- In Ihrem Rechenzentrum befindet sich ein interner HTTP-Server mit der IP-Adresse 10.1.1.1 und Sie möchten internen HTTP- und HTTPS-Datenverkehr zu diesem Server leiten. Die IP-Adresse des Servers ist 10.1.1.1.

  Datenverkehr zu diesem Server sollte nicht ins Internet gelangen und intern verarbeitet werden. Wählen Sie daher ein nicht dediziertes Ziel für diesen Datenverkehr aus, da dieser Zieltyp sowohl internen als auch internetgebundenen Datenverkehr verarbeitet.
- Sie möchten, dass Datenverkehr von office365.com direkt ins Internet geleitet wird.

 ©2025 Palo Alto Networks, Inc.

- Sie möchten, dass Datenverkehr von *.example.com oder beliebiger Datenverkehr, der in der benutzerdefinierten URL-Kategorie **custom-social-networking** definiert ist, zu einer dedizierten Verbindung weitergeleitet wird.
- Sie möchten, dass jeder andere HTTP- und HTTPS-Datenverkehr das gleiche nicht dedizierte Dienstverbindungsziel verwendet, das auch für den internen HTTP-Server verwendet wird.

Erstellen Sie für dieses Beispiel die Regeln, beginnend mit der spezifischsten Regel bis zur am wenigsten spezifischen Regel, wie im folgenden Screenshot veranschaulicht. Fügen Sie nicht zuerst die Regel hinzu, die den gesamten HTTP- und HTTPS-Datenverkehr erlaubt, da Prisma Access sonst den gesamten HTTP- und HTTPS-Datenverkehr auf die nicht dedizierte Verbindung leiten würde, ohne eine der anderen Regeln zu bewerten.




## Konfigurieren von Zonenzuordnungs- und Sicherheitsrichtlinien für dedizierte Datenverkehrslenkungsverbindungen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Wenn Sie ein Ziel erstellen, das eine dedizierte Dienstverbindung verwendet, ändert sich die Zone für die dedizierte Dienstverbindung von **vertrauenswürdig** in **nicht vertrauenswürdig** (nicht dedizierte Dienstverbindungsziele ändern ihre Zonen nicht). Da Sie keine Zonen erstellen oder die Zonenzuordnung für Dienstverbindungen konfigurieren können, nehmen Sie stattdessen Änderungen an der Zonenzuordnung und an der Sicherheitsrichtlinie für dedizierte Dienstverbindungen für die mobilen Benutzer und Gerätegruppen vor. Führen Sie die folgenden Schritte aus, um die Zonenzuordnung für dedizierte Verbindungen zu konfigurieren.

*In diesen Schritten ist eine Beispielkonfiguration abgebildet. Sie können dieses Beispiel an Ihre Bereitstellung anpassen.*

**STEP 1 |** Wählen Sie **Netzwerk** > **Zonen** aus.

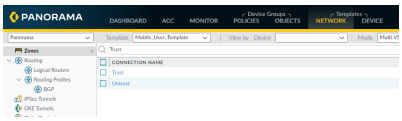
**STEP 2 |** Wählen Sie die richtige **Vorlage** aus der Dropdown-Liste aus (entweder **Mobile_User_Template** für mobile Benutzer oder **Remote_Network_Template** für Remote-Netzwerke).

Wenn Sie über einen mobilen Benutzer und eine Remote-Netzwerkbereitstellung verfügen, müssen Sie diese Schritte zweimal ausführen: einmal in der Vorlage **Mobile_User_Template** und einmal in der Vorlage **Remote_Network_Template**.

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Sie müssen zwei Zonen für Ihre vertrauenswürdigen und nicht vertrauenswürdigen Zonen **hinzufügen**.

In diesem Beispiel werden zwei Zonen mit dem Namen **Trust** (Vertrauenswürdig) und **Untrust** (Nicht vertrauenswürdig) erstellt.

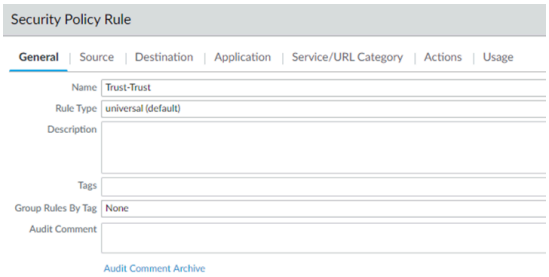



**STEP 4 |** Erstellen Sie Standardrichtlinien für die von Ihnen erstellten Zonen.

1. Wählen Sie **Richtlinien** > **Sicherheit** > **Nach-Regeln** aus.
2. Wählen Sie die richtige **Gerätegruppe** aus der Dropdown-Liste aus (entweder **Mobile_User_Device_Group** für Remote-Netzwerke oder **Remote_Network_Device_Group** für mobile Benutzer).

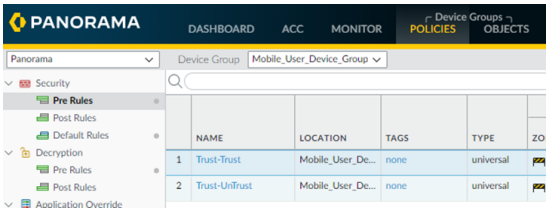
   Wenn eine Bereitstellung für mobile Benutzer und Remote-Netzwerke vorliegt, müssen Sie diese Schritte zweimal ausführen: einmal in der Vorlage **Mobile_User_Device_Group** und einmal in der Vorlage**Remote_Network_Device_Group**.
3. Sie müssen eine Standardrichtlinie **hinzufügen**, die für Datenverkehr zwischen vertrauenswürdigen Zonen verwendet wird.

   Mit dieser Richtlinie kann **beliebiger** Datenverkehr für den gesamten Datenverkehr aller **Quell-**, **Benutzer-**, **Ziel-**, **Anwendungs-** und **Dienst-/URL-Kategorie** passieren.




4. Sie müssen eine Standardrichtlinie zur Verwendung mit Datenverkehr zwischen vertrauenswürdigen und nicht vertrauenswürdigen Zonen **hinzufügen**. Verwenden Sie dabei dieselben Parameter wie für die Richtlinie zwischen vertrauenswürdigen Zonen.

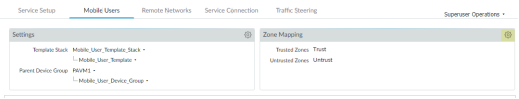
   Wenn Sie fertig sind, stehen Ihnen zwei Sicherheitsrichtlinien zur Verfügung: eine für Datenverkehr zwischen vertrauenswürdigen Zonen und eine für Datenverkehr zwischen vertrauenswürdigen und nicht vertrauenswürdigen Zonen.



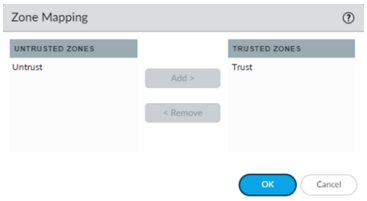

 ©2025 Palo Alto Networks, Inc.

**STEP 5 |** Definieren Sie die Zonenzuordnung für die Remote-Netzwerke und/oder mobilen Benutzer, wie für Ihre Bereitstellung erforderlich.

1. Legen Sie die Zonenzuordnung für die Remote-Netzwerke und/oder mobilen Benutzer fest.
   - Wählen Sie für mobile Benutzer **Panorama** > **Cloud Services** > **Konfiguration** > **Mobile Benutzer** aus.
   - Wählen Sie für Remote-Netzwerke **Panorama** > **Cloud Services** > **Konfiguration** > **Remote-Netzwerke** aus.
2. Klicken Sie auf das Zahnradsymbol neben **Zonenzuordnung**, um die Einstellungen zu bearbeiten.




3. Legen Sie die **Zonenzuordnung** für Ihre Bereitstellung fest, verschieben Sie die Zone für vertrauenswürdigen Datenverkehr in die **vertrauenswürdigen Zonen** und die Zone für nicht vertrauenswürdigen Datenverkehr in die **nicht vertrauenswürdigen Zonen**. Klicken Sie dann auf **OK**.




## Datenverkehrslenkung in Prisma Access konfigurieren

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz<br>❑ Wenn Zertifikatsperrungslisten (Certificate Revocation List, CRL) und Online-Zertifikatstatusprotokolle (Online Certificate Status Protocol, OCSP) direkt ins Internet gesendet werden sollen, ist Prisma Access 5.1.1 oder höher erforderlich. |

Mit der Datenverkehrslenkung können Sie Prisma Access so konfigurieren, dass Datenverkehrslenkungsregeln erstellt werden, um Ziele für internetgebundenen Datenverkehr von mobilen Benutzern und Remote-Netzwerkverbindungen festzulegen. Sie können den Datenverkehr angeben, der vor dem Senden ins Internet an eine Dienstverbindung umgeleitet werden soll, oder den Datenverkehr, der direkt ins Internet gehen soll. Konfigurieren Sie die Datenverkehrslenkung für Ihre Prisma Access-Bereitstellung, indem Sie die folgenden Schritte ausführen.

- Strata Cloud Manager

 ©2025 Palo Alto Networks, Inc.

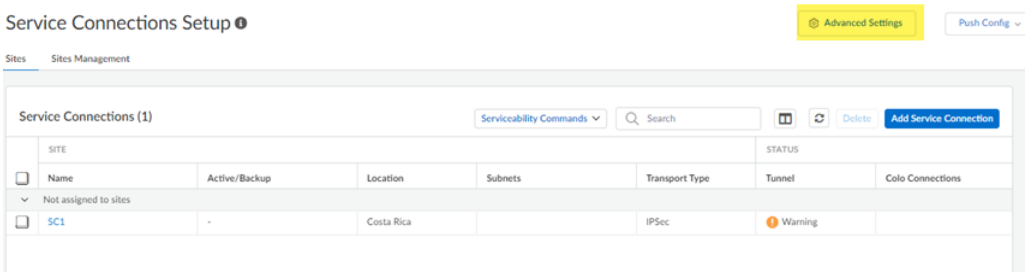
- Panorama

### Datenverkehrslenkung in Prisma Access (Strata Cloud Manager) konfigurieren

In Prisma Access-Bereitstellungen bietet eine Dienstverbindung Zugriff auf interne Netzwerkressourcen, z. B. Authentifizierungsdienste und private Apps in Ihrer Zentrale oder in Ihrem Rechenzentrum. Dienstverbindungen verarbeiten internen Datenverkehr, für den kein Internetzugang erforderlich ist. In einigen Fällen möchten Sie möglicherweise internetgebundenen Datenverkehr zum Rechenzentrum umleiten. Mit der Datenverkehrslenkung können Sie Datenverkehr mobiler Benutzer oder Remote-Netzwerkverkehr zu einer Dienstverbindung umleiten, bevor dieser ins Internet gesendet wird. Konfigurieren Sie die Datenverkehrslenkung für Ihre Prisma Access-Bereitstellung, indem Sie die folgenden Schritte ausführen.

**STEP 1 |** Binden Sie Ihre Dienstverbindungen, mobilen Benutzer und Remote-Netzwerke ein (abhängig von Ihrer Bereitstellung).

**STEP 2 |** Gehen Sie zu **Workflows** > **Einrichtung Prisma Access** > **Dienstverbindungen** > **Erweiterte Einstellungen**.




**STEP 3 |** Konfigurieren Sie die **Datenverkehrslenkung**.

1. (Optional, nur Bereitstellungen für mobile Benutzer) Lassen Sie zu, dass Prisma Access die über eine oder mehrere Dienstverbindungen von der CPE angekündigte Standardroute akzeptiert und installiert. Klicken Sie dazu auf das Zahnradsymbol, um die Einstellungen zu öffnen, und wählen Sie **Standardroute über Dienstverbindung akzeptieren** aus.

   Für Standardrouten gelten Richtlinien, die Sie befolgen müssen, wenn Sie sie verwenden. Beispielsweise werden Standardrouten nur für Bereitstellungen für mobile Benutzer unterstützt und haben keine Auswirkungen auf Remote-Netzwerkbereitstellungen. Prüfen Sie diese Richtlinien, bevor Sie Standardrouten mit Datenverkehrslenkung implementieren.

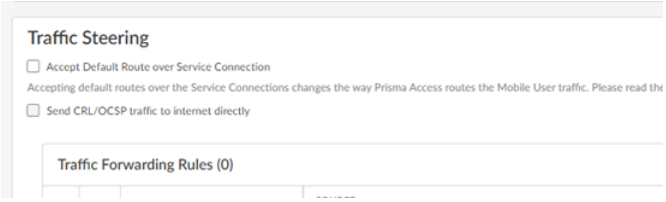
**STEP 4 |** (Optional) Lassen Sie zu, dass Prisma Access Certificate Revocation List-(CRL-) und Online Certificate Status Protocol-(OCSP-)Datenverkehr direkt ins Internet sendet, indem Sie **CRL/ OCSP-Datenverkehr direkt ins Internet senden** auswählen.

Wählen Sie diese Option aus, wenn Sie über einen OCSP- oder CRP-Server im öffentlichen Internet verfügen und diesen Datenverkehr über die nicht vertrauenswürdige Zone direkt

 ©2025 Palo Alto Networks, Inc.

ins Internet senden möchten. Wenn Sie diese Option nicht auswählen, sendet Prisma Access diesen Datenverkehr an die Dienstverbindung.

*Vergewissern Sie sich, dass Sie für Ihre Prisma Access-Bereitstellung ein Upgrade auf mindestens Version 5.1.1 durchgeführt haben, bevor Sie **CRL/OCSP-Datenverkehr direkt ins Internet senden** auswählen.*




**STEP 5 |** Erstellen Sie Regeln für das von Ihnen erstellte Ziel und wenden Sie diese auf das Ziel an.

1. **Regel hinzufügen**.
2. Geben Sie einen eindeutigen **Namen** für die Regel ein.
3. Im Bereich **Quelle**:
   - Geben Sie die Liste der abzugleichenden Benutzer an.

     Sie können **Entspricht beliebigem Benutzer**, **Voranmeldung abgleichen**, **Bekannten Benutzer abgleichen**, **Unbekannt abgleichen** oder **Benutzer hinzufügen** aktivieren und den/die abzugleichenden Benutzer auswählen.
   - Wählen Sie **Quell-Adressentitäten** aus. Sie können eines oder mehrere der folgenden Objekte auswählen:
     - Eine IP-Adresse
     - Eine Adressgruppe
     - Eine externe dynamische Liste EDL) mit IP-Adressen oder URLs
4. Geben Sie im Bereich **Ziel** eine der folgenden **Ziel-Adressenentitäten** an, oder wählen Sie im Feld „URL-Kategorie“ die Option **Beliebig** aus, um Datenverkehr gemäß den Regeln verarbeiten zu lassen:
   - Eine IP-Adresse
   - Eine Adressgruppe
   - Eine externe dynamische Liste (EDL) mit IP-Adressen oder URLs
5. Geben Sie eine **URL-Kategorie** an.

   Wenn Sie eine benutzerdefinierte URL-Kategorie erstellen, geben Sie URLs in Kleinbuchstaben ein. Die Datenverkehrslenkung unterstützt benutzerdefinierte und

 ©2025 Palo Alto Networks, Inc.

vordefinierte URL-Kategorien. Sie können Platzhalter mit den URLs in URL-Kategorien verwenden. Die folgenden Platzhalterformate werden unterstützt:

- *.example.com
- *.fqdn.example.com

Die folgenden Formate werden nicht unterstützt:

- *
- *.*
- *example.com
- example.com/ (nachgestellte Schrägstriche in URLs werden in URL-Kategorien, die mit Datenverkehrslenkung verwendet werden, nicht unterstützt)
- example.com/path (nur Domänennamen werden unterstützt)
- *fqdn.example.com
- fqdn.example.*

Verwenden Sie die folgenden Richtlinien beim Konfigurieren von Zieloptionen:

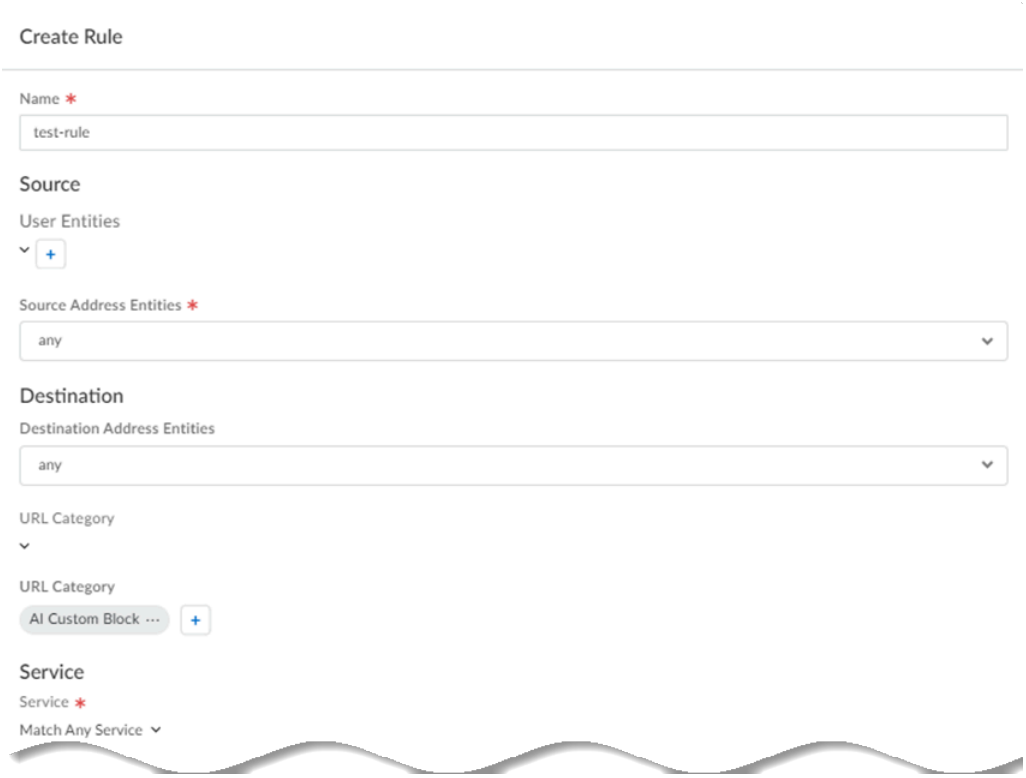
- Wenn Sie eine URL-Kategorie angeben, gleicht Prisma Access nur HTTP- und HTTPS-Datenverkehr ab, auch wenn der Dienst auf **Beliebige** festgelegt ist.
- Erstellen Sie keine benutzerdefinierte URL-Kategorie mit dem Typ **Kategorie-Übereinstimmung**.

Erstellen Sie keine benutzerdefinierte URL-Kategorie mit dem Namen **Custom_URL_Category_TFR**.

6. Geben Sie einen **Diensttyp** an und **fügen Sie einen Dienst hinzu**.

   Geben Sie **service-http** an, um HTTP-Datenverkehr weiterzuleiten, und geben Sie **service-https** an, um HTTPS-Datenverkehr festzulegen. Wählen Sie **Entspricht beliebigem Dienst** aus, um Datenverkehr eines beliebigen Diensttyps weiterzuleiten.

 ©2025 Palo Alto Networks, Inc.




7. Erstellen Sie eine Dienstverbindungsgruppe und geben Sie eine **Aktion** an.
   1. Wählen Sie **Neu erstellen** oder **Verwalten** für eine Gruppe aus und geben Sie einen eindeutigen **Namen** für sie ein.
   2. Geben Sie die **Dienstverbindung** oder Dienstverbindungen zur Verwendung mit dem Ziel an.

      Die Verwendung mehrerer Dienstverbindungen in einer Ziel-Dienstverbindungsgruppe, die in einer Datenverkehrslenkungsregel referenziert wird, wird von Palo Alto Networks nicht empfohlen (unabhängig davon, ob es sich um dedizierte oder nicht dedizierte Verbindungen handelt). Darüber hinaus kann eine bestimmte Dienstverbindung nur in einem Ziel vorhanden sein, und Sie können keine einzelne Dienstverbindung zu zwei verschiedenen Zielen hinzufügen.
   3. (Optional) Sie können eine dedizierte Dienstverbindung verwenden, um den Datenverkehr zum Sicherheitsstack oder zur Cloud eines Drittanbieters zu lenken, der bzw. die sich nicht an Ihrem Standort befindet und nicht am Routing teilnehmen muss. Um eine Dienstverbindung für die Verwendung als dedizierte Dienstverbindung festzulegen, aktivieren Sie **Nur für Datenverkehrslenkung vorgesehen**.

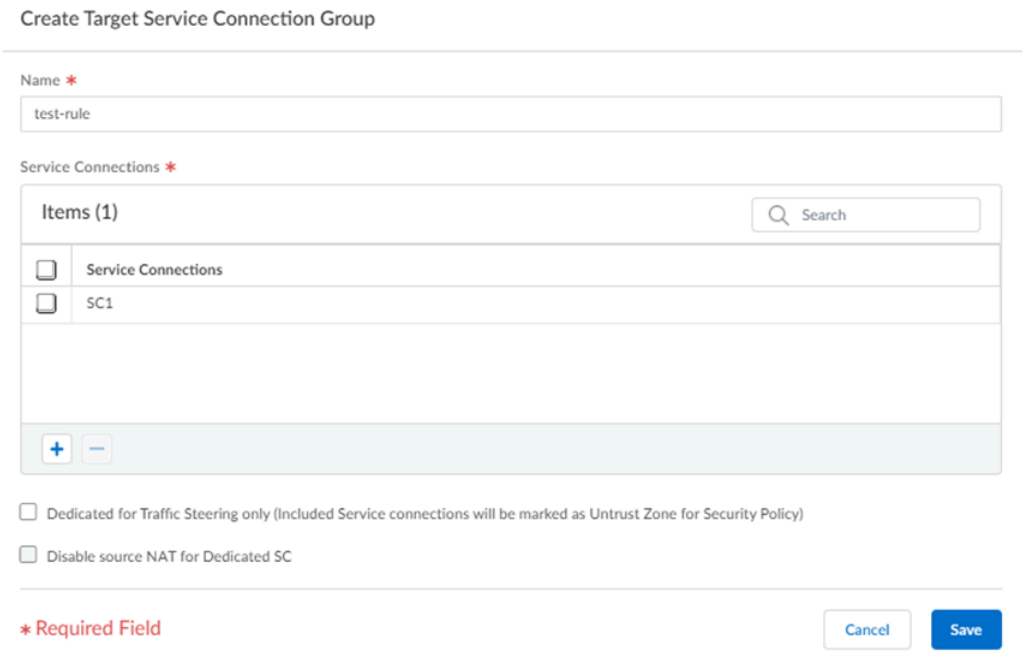
      *Dedizierte Dienstverbindungen ändern ihre Zonen und sind für Sicherheitsrichtlinienregeln als nicht vertrauenswürdige Zonen gekennzeichnet.*

      Deaktivieren Sie **Nur für Datenverkehrslenkung vorgesehen**, wenn Sie sowohl normalen, auf die Dienstverbindung bezogenen Datenverkehr als auch Datenverkehr zur Datenverkehrslenkung über die Dienstverbindung senden möchten. Mit dieser Auswahl bleibt die Zone für die Dienstverbindung als vertrauenswürdig erhalten.

 ©2025 Palo Alto Networks, Inc.

4. Deaktivieren Sie Quell-NAT für dedizierte Dienstverbindungen, indem Sie **Quell-NAT für bestimmte Dienstverbindungen deaktivieren** aktivieren. Quell-NAT ist standardmäßig aktiviert (das Kontrollkästchen ist deaktiviert).

   Wenn Sie Quell-NAT deaktivieren, verwendet Prisma Access die Quell-IP-Adressen Ihrer Organisation für die dedizierte Dienstverbindung. Wenn Sie Quell-NAT aktivieren, verwendet Prisma Access die **EBGP-Router**-Adresse der Dienstverbindung (**Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Dienstverbindung** > **EBGP-Router**) als Quell-IP-Adresse. Dies gilt auch dann, wenn der Datenverkehr die dedizierte Dienstverbindung verlassen hat.
5. **Save (Speichern)** Sie Ihre Änderungen.




8. Leiten Sie Datenverkehr an das angegebene Dienstverbindungsziel weiter, oder senden Sie den Datenverkehr direkt ins Internet, ohne die Dienstverbindung zu durchlaufen.
   - Damit Prisma Access Datenverkehr an ein Dienstverbindungsziel weiterleitet, wählen Sie **An das Ziel weiterleiten** aus und klicken Sie anschließend auf die Schaltfläche **Ziel-Dienstverbindungsgruppe**.

     Geben Sie diese Option an, wenn Datenverkehr vorliegt, den Sie aufgrund von Listenbeschränkungen für SaaS-Anwendungen an Ihre bestehende oder ältere

 ©2025 Palo Alto Networks, Inc.

Umgebung senden müssen, oder wenn Sie einen Datenverkehrsfluss erstellen möchten, um bestimmten Internet-Verkehr zurück in Ihr lokales Netzwerk zu leiten.

- Damit Prisma Access Datenverkehr direkt ins Internet weiterleitet, ohne diesen zuerst an eine Dienstverbindung zu senden, wählen Sie **An das Internet weiterleiten** aus.

  Geben Sie diese Option an, wenn Sie eine Standardroute an Prisma Access senden und einen Teil des Datenverkehrs direkt ins Internet leiten möchten.




**STEP 6 |** Wählen Sie **Konfiguration übertragen** aus, um Ihre Änderungen zu speichern.

### Datenverkehrslenkung in Prisma Access (Panorama) konfigurieren

**STEP 1 |** Binden Sie Ihre Dienstverbindungen, mobilen Benutzer und Remote-Netzwerke ein (abhängig von Ihrer Bereitstellung).

**STEP 2 |** Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Datenverkehrslenkung** aus.

**STEP 3 |** (Optional, nur Bereitstellungen für mobile Benutzer) Lassen Sie zu, dass Prisma Access die über eine oder mehrere Dienstverbindungen von der CPE angekündigte Standardroute akzeptiert und installiert. Klicken Sie dazu auf das Zahnradsymbol, um die Einstellungen zu öffnen, und wählen Sie **Standardroute über Dienstverbindung akzeptieren** aus.

Für Standardrouten gelten Richtlinien, die Sie befolgen müssen, wenn Sie sie verwenden. Beispielsweise werden Standardrouten nur für Bereitstellungen für mobile Benutzer unterstützt und haben keine Auswirkungen auf Remote-Netzwerkbereitstellungen. Prüfen Sie diese Richtlinien, bevor Sie Standardrouten mit Datenverkehrslenkung implementieren.

**STEP 4 |** (Optional) Lassen Sie zu, dass Prisma Access Certificate Revocation List-(CRL-) und Online Certificate Status Protocol-(OCSP-)Datenverkehr direkt ins Internet sendet, indem Sie **CRL/ OCSP-Datenverkehr direkt ins Internet senden** auswählen.

Wählen Sie diese Option aus, wenn Sie über einen OCSP- oder CRP-Server im öffentlichen Internet verfügen und diesen Datenverkehr über die nicht vertrauenswürdige Zone direkt

 ©2025 Palo Alto Networks, Inc.

ins Internet senden möchten. Wenn Sie diese Option nicht auswählen, sendet Prisma Access diesen Datenverkehr an die Dienstverbindung.

*Vergewissern Sie sich, dass Sie für Ihre Prisma Access-Bereitstellung ein Upgrade auf mindestens Version 5.1.1 durchgeführt haben, bevor Sie **CRL/OCSP-Datenverkehr direkt ins Internet senden** auswählen.*




**STEP 5 |** (Optional) Erstellen Sie eine Zielgruppe und weisen Sie dieser eine Dienstverbindung zu.

1. Wählen Sie im Bereich **Ziel-Dienstverbindungen für Datenverkehrslenkung** die Option **Hinzufügen** aus, um eine Gruppe hinzuzufügen, und geben Sie dieser Gruppe einen **Gruppennamen**.
2. Wählen Sie **Hinzufügen** aus, um dem Datenverkehr ein **Ziel** hinzuzufügen. Geben Sie dabei die **Dienstverbindung** an, die mit dem Ziel verwendet werden soll, und klicken Sie dann auf **OK**.

   Die Verwendung mehrerer Dienstverbindungen in einer Ziel-Dienstverbindungsgruppe, die in einer Datenverkehrslenkungsregel referenziert wird, wird von Palo Alto Networks nicht empfohlen (unabhängig davon, ob es sich um dedizierte oder nicht dedizierte Verbindungen handelt). Darüber hinaus kann eine bestimmte Dienstverbindung nur in einem Ziel vorhanden sein, und Sie können keine einzelne Dienstverbindung zu zwei verschiedenen Zielen hinzufügen.
3. Wählen Sie aus, ob die mit diesem Ziel verknüpften Dienstverbindungen als dedizierte Dienstverbindung festgelegt werden sollen.

   - Sie können eine dedizierte Dienstverbindung verwenden, um den Datenverkehr zum Sicherheitsstack oder zur Cloud eines Drittanbieters zu lenken, der bzw. die sich nicht an Ihrem Standort befindet und nicht am Routing teilnehmen muss. Um eine Dienstverbindung für die Verwendung als dedizierte Dienstverbindung festzulegen, aktivieren Sie **Nur für Datenverkehrslenkung vorgesehen**.

     *Dedizierte Dienstverbindungen ändern ihre Zonen.*

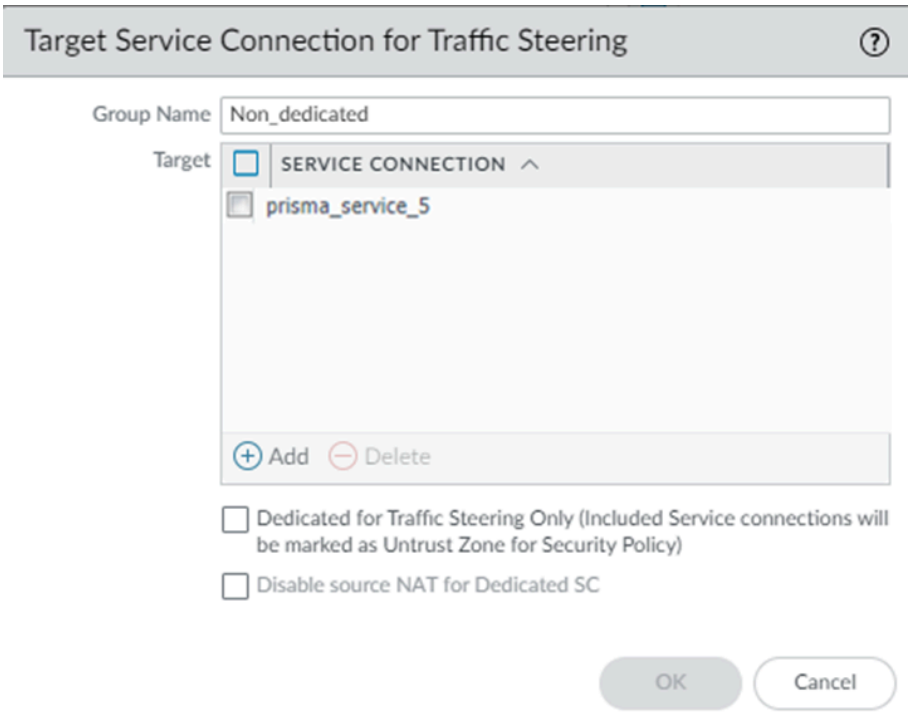
   - Deaktivieren Sie **Nur für Datenverkehrslenkung vorgesehen**, wenn Sie sowohl normalen, auf die Dienstverbindung bezogenen Datenverkehr als auch Datenverkehr zur Datenverkehrslenkung über die Dienstverbindung senden möchten. Mit dieser Auswahl bleibt die Zone für die Dienstverbindung als vertrauenswürdig erhalten.

 ©2025 Palo Alto Networks, Inc.

4. Wählen Sie aus, ob Quell-NAT aktiviert oder deaktiviert werden soll.

   Um Quell-NAT für dedizierte Dienstverbindungen zu deaktivieren, aktivieren Sie die Option **Quell-NAT für bestimmte Dienstverbindungen deaktivieren**. Quell-NAT ist standardmäßig aktiviert (das Kontrollkästchen ist deaktiviert).

   Wenn Sie Quell-NAT deaktivieren, verwendet Prisma Access die Quell-IP-Adressen Ihrer Organisation für die dedizierte Dienstverbindung. Wenn Sie Quell-NAT aktivieren, verwendet Prisma Access die **EBGP-Router**-Adresse der Dienstverbindung (**Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Dienstverbindung** > **EBGP-Router**) als Quell-IP-Adresse. Dies gilt auch dann, wenn der Datenverkehr die dedizierte Dienstverbindung verlassen hat.




 ©2025 Palo Alto Networks, Inc.

**STEP 6 |** Erstellen Sie Regeln für das von Ihnen erstellte Ziel und wenden Sie diese auf das Ziel an.

1. Wählen Sie im Bereich **Datenverkehrslenkungsregeln** die Option **Hinzufügen** aus, um eine Datenverkehrslenkungsregel hinzuzufügen.
2. Geben Sie auf der Registerkarte **Allgemein** einen **Namen** für die Datenverkehrslenkungsregel ein.
3. Legen Sie auf der Registerkarte **Quelle** Regeln für den Quelldatenverkehr fest.
   - Geben Sie im Feld **Quelladresse** eines oder mehrere der folgenden Objekte an, oder wählen Sie **Beliebige** aus, um Datenverkehr von beliebigen Quellen an dieses Ziel weiterzuleiten:
     - Eine IP-Adresse
     - Ein Adressobjekt, das Sie in Panorama erstellt haben (**Objekte** > **Adressen**)
     - Eine dynamische Adressgruppe (DAG)
     - Eine externe dynamische Liste (EDL) , die IP-Adressen oder URLs verwendet
   - Geben Sie im Feld **Quellbenutzer** Regeln für den Quelldatenverkehr an. Sie können die folgenden Benutzerinformationen angeben:
     - Users (Benutzer)

       Geben Sie Benutzer entweder im Format *Domäne/Benutzer* oder *Benutzer@Domäne* ein.
     - Benutzergruppen

       Verwenden Sie bei der Eingabe von Benutzergruppen vollständig ausgewählte Namen (Distinguished Names, DNs).
     - Benutzer, die auf Panorama konfiguriert sind (**Gerät** > **Lokale Benutzerdatenbank** > **Benutzer**)
     - Benutzergruppen, die auf Panorama konfiguriert sind (**Gerät** > **Lokale Benutzerdatenbank** > **Benutzergruppen**)

   Wenn Sie Adressobjekte, DAGs, EDLs, Benutzer oder Benutzergruppen verwenden, geben Sie diese als **Freigegeben** ein, um sie für alle Gerätegruppen in Prisma Access

 ©2025 Palo Alto Networks, Inc.

freizugeben. Geben Sie außerdem 0.0.0.0/0 nicht in Adressobjekte, DAGs oder EDLs ein. Geben Sie stattdessen 0.0.0.0/0 direkt in die Regel ein.

*Prisma Access verwendet zum automatischen Ausfüllen ausschließlich Benutzer aus der Gerätegruppe der mobilen Benutzer.*

4. Geben Sie auf der Registerkarte **Ziel** die folgenden Werte an:

   - Geben Sie im Bereich **Ziel** eines der folgenden Kriterien an, oder wählen Sie **Beliebige** aus, damit Datenverkehr nach den Regeln im Feld **URL-Kategorie** verarbeitet wird:
     - Eine IP-Adresse oder ein Präfix
     - Ein Adressobjekt, das Sie in Panorama erstellt haben (**Objekte** > **Adressen**)
     - Eine dynamische Adressgruppe (DAG)
     - Eine IP-Adresse, die auf Externe dynamische Liste (EDL) basiert

     *Geben Sie 0.0.0.0/0 nicht in Adressobjekte, DAGs oder EDLs ein. Geben Sie stattdessen 0.0.0.0/0 direkt in die Regel ein.*

     Lassen Sie **Beliebige** ausgewählt, um den gesamten Datenverkehr weiterzuleiten, damit er nach den Regeln im Bereich **URL-Kategorie** verarbeitet wird. Wenn Sie Regeln in den Bereichen **Ziel**und **URL-Kategorie** angeben, verarbeitet Prisma Access zuerst die Regeln in der Kategorie **Ziel**.
   - Geben Sie in das Feld **URL-Kategorie** eine benutzerdefinierte URL-Kategorie ein (**Objekte** > **Benutzerdefinierte Objekte** > **URL-Kategorie**). Wenn Sie eine benutzerdefinierte URL-Kategorie erstellen, geben Sie URLs in Kleinbuchstaben ein. Datenverkehrslenkung unterstützt benutzerdefinierte URLs und vordefinierte URL-Kategorien.

     Sie können Platzhalter mit den URLs in URL-Kategorien verwenden. Die folgenden Platzhalterformate werden unterstützt:

     - *.example.com

 ©2025 Palo Alto Networks, Inc.

- *.fqdn.example.com

Die folgenden Formate werden nicht unterstützt:

- *
- *.*
- *example.com
- example.com/ (nachgestellte Schrägstriche in URLs werden in URL-Kategorien, die mit Datenverkehrslenkung verwendet werden, nicht unterstützt)
- example.com/*Pfad* (es werden nur Domänennamen unterstützt)
- *fqdn.example.com
- fqdn.example.*

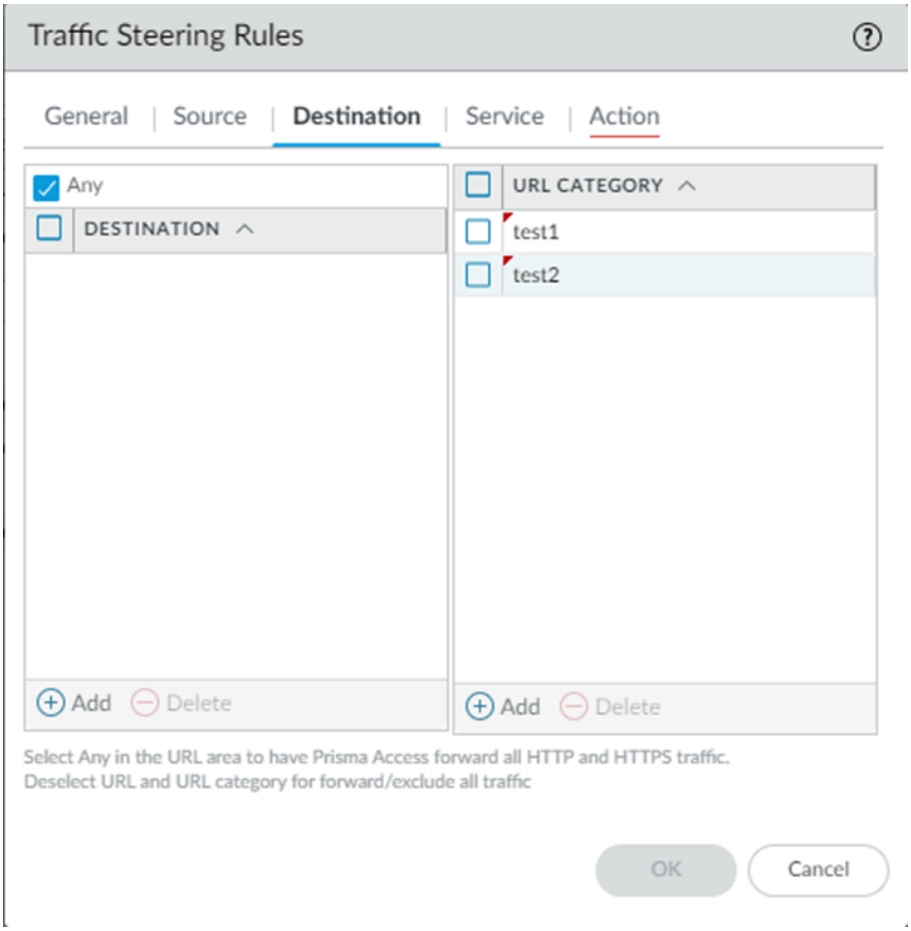
URLs in benutzerdefinierten URL-Kategorien verwenden den gleichen URL-Musterabgleich wie Firewalls der nächsten Generation.

Beachten Sie beim Konfigurieren von Zieloptionen die folgenden Richtlinien:

- Wenn Sie eine URL-Kategorie angeben, stimmt Prisma Access nur HTTP- und HTTPS-Datenverkehr ab, auch wenn der Dienst auf „Beliebige“ festgelegt ist.
- Erstellen Sie keine benutzerdefinierte URL-Kategorie des Typs **Kategorie-Übereinstimmung**.
- Erstellen Sie keine benutzerdefinierte URL-Kategorie mit dem Namen **Custom_URL_Category_TFR**, denn für von Prisma Access 1.7 nach 2.0 migrierte Bereitstellungen werden URLs, die ab Version 1.7 im URL-Bereich eingegeben wurden, in eine benutzerdefinierte URL-Kategorie mit dem Namen

 ©2025 Palo Alto Networks, Inc.

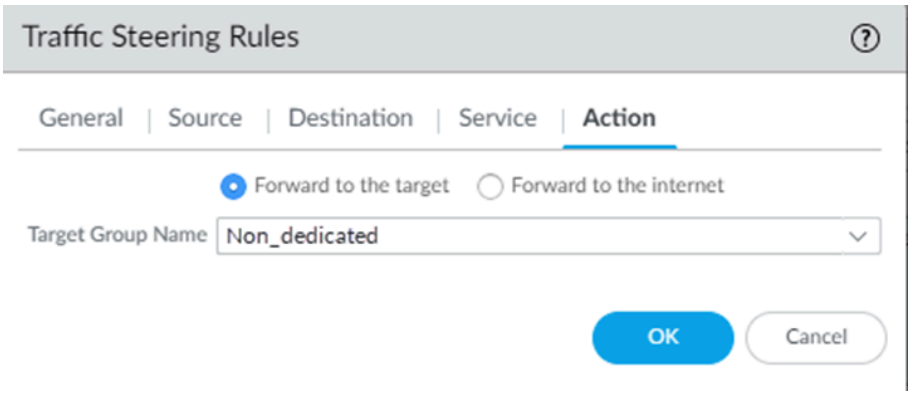
**Custom_URL_Category_TFR***Zahl* verschoben, wobei *Zahl* für eine Zahl steht, die an die benutzerdefinierte URL-Kategorie angehängt wird.




5. Geben Sie auf der Registerkarte **Dienst** einen Diensttyp an.

   Geben Sie **service-http** an, um HTTP-Datenverkehr weiterzuleiten, und geben Sie **service-https** an, um HTTPS-Datenverkehr festzulegen. Wählen Sie **Beliebige** aus, um Datenverkehr eines beliebigen Diensttyps weiterzuleiten.
6. Wählen Sie auf der Registerkarte **Aktion** den **Zielgruppennamen** aus, den Sie auf die Regeln für die Datenverkehrslenkung anwenden möchten.
7. Leiten Sie Datenverkehr an das angegebene Dienstverbindungsziel weiter, oder senden Sie den Datenverkehr direkt ins Internet, ohne die Dienstverbindung zu durchlaufen.
   - Damit Prisma Access Datenverkehr an ein Dienstverbindungsziel weiterleitet, wählen Sie **An das Ziel weiterleiten** aus und klicken Sie anschließend auf die Schaltfläche **Name der Zielgruppe**.
   - Damit Prisma Access Datenverkehr direkt ins Internet weiterleitet, ohne diesen zuerst an eine Dienstverbindung zu senden, wählen Sie **An das Internet weiterleiten** aus.

 ©2025 Palo Alto Networks, Inc.



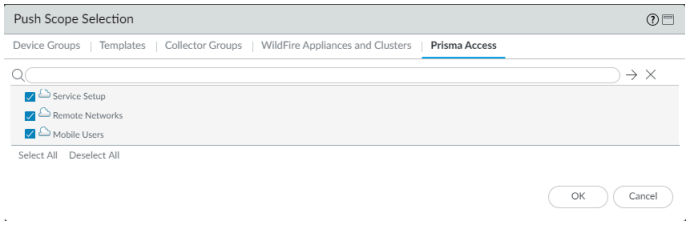

8. Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

**STEP 7 |** Optional Geben Sie zusätzliche Regeln für die Datenverkehrslenkung an.

Prisma Access verarbeitet mehrere Regeln in der Reihenfolge, in der Sie sie erstellen (von oben nach unten).

**STEP 8 |** Führen Sie einen Commit aus und übertragen Sie Ihre Änderungen per Push, um sie in Prisma Access zu aktivieren.

1. Wählen Sie im Übertragungsumfang **Commit** > **Commit und Push** sowie **Auswahl bearbeiten** aus.
2. Wählen Sie **Prisma Access** und anschließend **Diensteinrichtung**, **Remote-Netzwerke** und **Mobile Benutzer** aus.




3. Klicken Sie auf **OK**, um Ihre Änderungen im Übertragungsumfang zu speichern.
4. Führen Sie einen **Commit** aus und übertragen Sie die Änderung per **Push**.

## Routing für Dienstverbindungsverkehr

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Prisma Access verwendet BGP für dynamisches Routing und die BGP-Pfadauswahl, um Routen in der Routentabelle zu installieren. Wenn Prisma Access Datenverkehr über Dienstverbindungen an Ihre Zentrale oder Ihr Rechenzentrum leitet, verwendet es Routingmethoden, die diesen Datenverkehr effektiv leiten. Prisma Access verwendet ein Standardroutingmodell, das für die meisten Netzwerkbereitstellungen entwickelt wurde. Allerdings sind nicht alle Netzwerke der Organisation gleich. Sie können mit Prisma Access einen anderen Modus für

 ©2025 Palo Alto Networks, Inc.

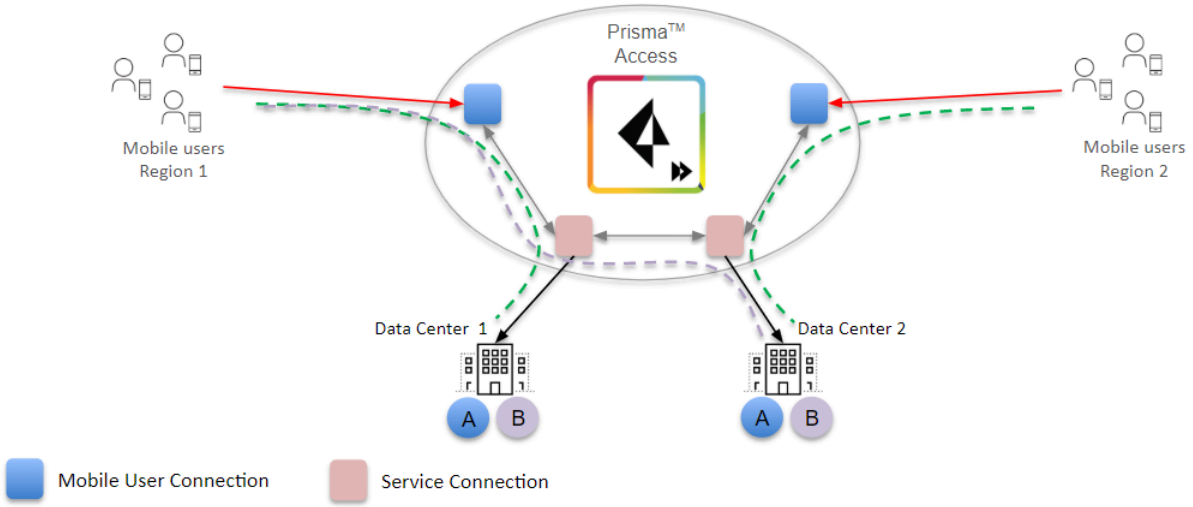
das Dienstverbindungsrouting auswählen, um eine breitere Palette von Bereitstellungen zu ermöglichen.

*Das Ändern der Prisma Access-Dienstverbindung erfordert ein gründliches Verständnis der Topologie und der Routinggeräte Ihrer Organisation sowie ein Verständnis der Funktionsweise von Prisma Access, wie in diesem Abschnitt beschrieben. Lesen Sie diesen Abschnitt sorgfältig durch, bevor Sie die standardmäßige Routingmethode ändern.*

Prisma Access unterstützt statisches und dynamisches Routing mit BGP für Dienstverbindungen und Remote-Netzwerkverbindungen. Wenn Sie BGP-Routing für Ihre Verbindungen verwenden, erhält das Netzwerk Ihrer Organisation BGP-Informationen von Prisma Access.

Bevor Sie entscheiden, welches Dienstverbindungsrouting verwendet werden soll, sollten Sie verstehen, wie Prisma Access den Datenverkehr zwischen mobilen Benutzern, Remote-Netzwerken und Dienstverbindungen leitet, da das Routing, das vom mobilen Benutzerverkehr und vom Remote-Netzwerkverkehr zwischen Dienstverbindungen verwendet wird, unterschiedlich ist.

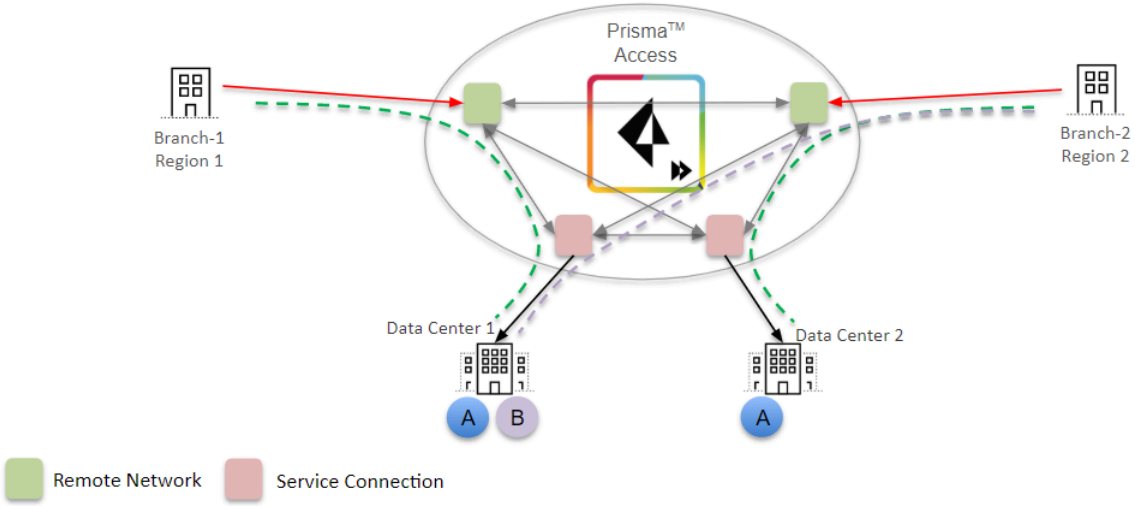
**Dienstverbindungsrouting für mobile Benutzer** – Für die Verbindung mobiler Benutzer wird ein IPSec-Tunnel mit der nächstgelegenen Dienstverbindung gebildet. Prisma Access verwendet iBGP für das interne Routing und eBGP zum Peeren mit dem Customer Premises Equipment im Rechenzentrum. Im folgenden Diagramm ist dargestellt, wie mobile Benutzer in den Regionen 1 und 2 zu den jeweiligen Dienstverbindungen in dieser Region geleitet werden. Mobile Benutzer in Region 1 greifen auf die Anwendungen **A** und **B** im Rechenzentrum 1 zu. Wenn das Netzwerk Ihrer Organisation BGP-Routing für seine Dienstverbindungen verwendet und bei einer Dienstverbindung ein ISP-Fehler in Rechenzentrum 1 auftritt, erkennt Prisma Access den Ausfall und leitet den Datenverkehr für die Anwendungen **A** und **B** nach der BGP-Konvergenz an Rechenzentrum 2 weiter, wodurch Redundanz für die Rechenzentren Ihres Netzwerks bereitgestellt wird.




 ©2025 Palo Alto Networks, Inc.

*Prisma Access verwendet das folgende Timing mit BGP, wenn ein Fehler erkannt wird: Wenn Sie das BGP-Routing konfigurieren und die Tunnelüberwachung aktiviert haben, besteht die kürzeste Standardhaltezeit zur Feststellung eines Fehlers bei einem Sicherheitsparameterindex (SPI) über die Tunnelüberwachung. Hierbei werden alle Routen zu einem Peer entfernt, wenn ein Tunnelfehler festgestellt wird, der länger als 15 aufeinanderfolgende Sekunden anhält. Auf diese Weise wird bei der Tunnelüberwachung das Verhalten der BGP-Routen ermittelt. Wenn Sie die Tunnelüberwachung nicht konfigurieren, bestimmt der Hold-Timer, wie lange der Tunnel inaktiv sein darf, bevor die Route entfernt wird. Prisma Access verwendet den Standardwert für die BGP-Haltezeit (90 Sekunden), der in RFC 4271 definiert ist. Hierbei handelt es sich um die maximal zulässige Wartezeit, nach deren Ablauf Prisma Access eine Route für einen inaktiven SPI entfernt. Wenn für das Peer-BGP-Gerät eine kürzere konfigurierte Haltezeit festgelegt wurde, verwendet der BGP-Hold-Timer den niedrigeren Wert. Nach der erfolgreichen Installation des sekundären Tunnels hat die sekundäre Route so lange Vorrang, bis der primäre Tunnel wieder einsatzbereit ist. Wenn sowohl die primäre als auch die sekundäre Route aktiv sind, hat die primäre Route Vorrang.*

**Remote-Netzwerk-/Dienstverbindungsrouting** – Prisma Access Erstellt ein vollständiges Mesh-Netzwerk mit anderen Remote-Netzwerken und Dienstverbindungen. Wie bei mobilen Benutzern verwendet Prisma Access iBGP für das interne Routing und eBGP für die Peer-to-Peer-Verbindung mit dem Customer Premises Equipment, um Routen auszutauschen. Wenn ein Benutzer in Zweigstelle 1 auf Anwendung **A** vom Rechenzentrum 1 im Rechenzentrum Ihrer Organisation zugreift und die Verbindung zwischen Zweigstelle 1 und Rechenzentrum 1 unterbrochen wird, leitet Prisma Access den Datenverkehr für Anwendung **A** nach BGP-Konvergenz an Rechenzentrum 2 weiter.




Nachdem Sie verstanden haben, wie das Prisma Access-Dienstverbindungsrouting funktioniert und wie es mit Ihrem Netzwerk zusammenhängt, können Sie einen der folgenden Routingmodi für Dienstverbindungen auswählen:

- Standard-Routing – Dies ist das Standardroutingmodell, das Prisma Access verwendet.

  Verwenden Sie diesen Routingmodus, wenn Prisma Access die besten BGP-Pfadauswahlmechanismen verwenden soll, ohne die BGP-Attribute anpassen zu müssen. In

 ©2025 Palo Alto Networks, Inc.

diesem Modus berücksichtigt Prisma Access jedes Attribut, das von dem Customer Premises Equipment (CPE) angekündigt wird.

- Hot-Potato-Routing – Prisma Access leitet den Datenverkehr so schnell wie möglich an das Netzwerk Ihrer Organisation weiter.

  Verwenden Sie diese Routingmethode, wenn das Netzwerk Ihrer Organisation die meisten Routingentscheidungen treffen soll.

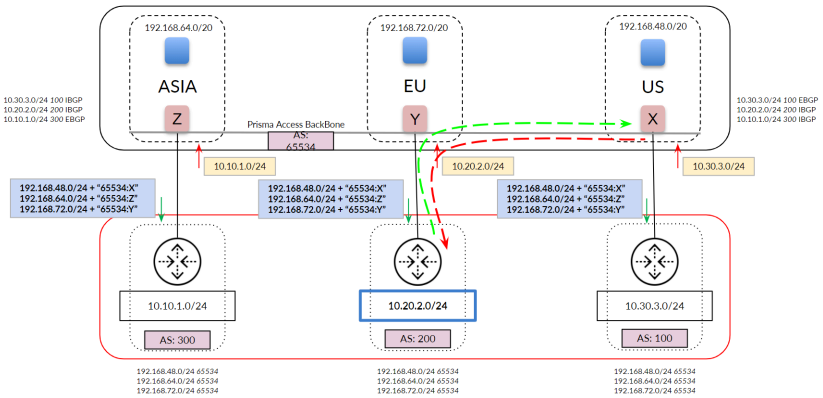
## Prisma Access-Standardrouting

In der folgenden Abbildung ist ein Beispiel für den Datenverkehr der Prisma Access-Routingdienstverbindung im Standardroutingmodus dargestellt. Das Netzwerk der Organisation verfügt über drei separate Netzwerke in drei Rechenzentren und verfügt nicht über ein Backbone, das die Netzwerke verbindet. Im Standardroutingmodus werden in den drei Netzwerken mobile Benutzerpools gleichermaßen angekündigt, wie in der folgenden Abbildung dargestellt.

Beachten Sie, dass Prisma Access beim Ankündigen mobiler Benutzerrouten die Subnetze in /24-Adressblöcke der Klasse C aufteilt, bevor sie angekündigt werden. Auf diese Weise kündigt es die /20-Subnetze der mobilen Benutzer in /24-Chunks an, da Präfixe von den Gateways verbraucht werden.

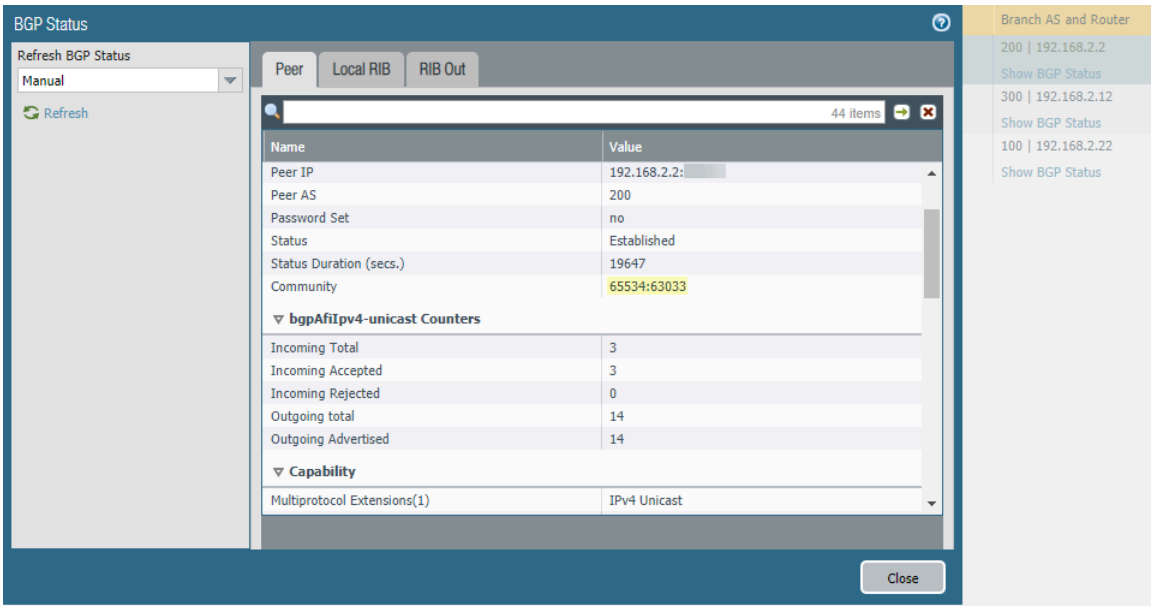
Beachten Sie, wie Prisma Access BGP-Routenankündigungen verwendet:

- Prisma Access passt die BGP-Standardattribute für angekündigte Routen mobiler Benutzer nicht an (Prisma Access ergänzt die Routenankündigungen um seine AS-Anzahl).
- Prisma Access kündigt Routen mobiler Benutzer in Blöcken von /24-Subnetzen an und ergänzt die über die Dienstverbindung angekündigten Routen durch BGP-Community-Werte. In der folgenden Abbildung ist eine Bereitstellung für mobile Benutzer mit drei Dienstverbindungen und drei verschiedenen IP-Adressblöcken dargestellt, die für den IP-Adresspool mobiler Benutzer angegeben wurden: `192.168.64.0/20` für die Region **Asien, Australien und Japan**, `192.168.72.0/20` für die Region **Afrika, Europa und Naher Osten** und `192.168.48.0/20` für die Region **Nordamerika und Südamerika**. Prisma Access teilt diese Routen in Blöcke von /24 ein und kündigt sie mit der AS-Nummer **65534** an, fügt aber auch BGP-Community-Werte an die Anzeigen an (**Z** für Asien, **Y** für die EU und **X** für die USA). Diese Routen sind in der Mitte der Abbildung dargestellt. Auf diese Weise können Sie Dienstverbindungen in Ihrem Netzwerk auch dann unterscheiden, wenn Prisma Access ihnen dieselbe AS-Nummer zuweist.



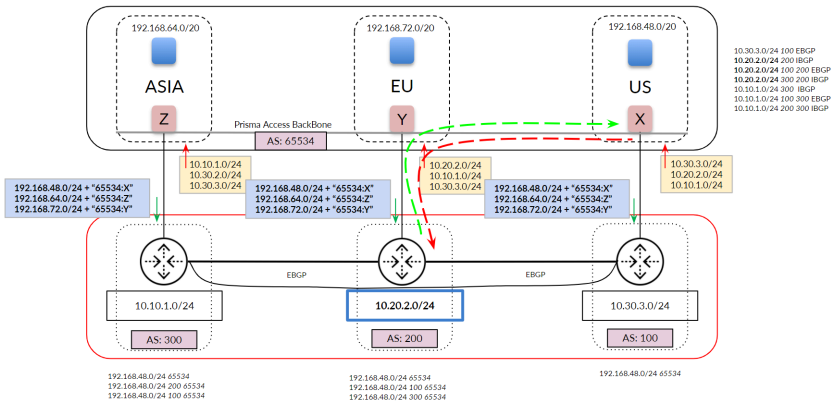

Sie können die Community-Zeichenfolge anzeigen, indem Sie **Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Dienstverbindung** > **BGP-Status anzeigen** auswählen und auf der Registerkarte **Peer** nach dem Feld **Community** suchen.

 ©2025 Palo Alto Networks, Inc.



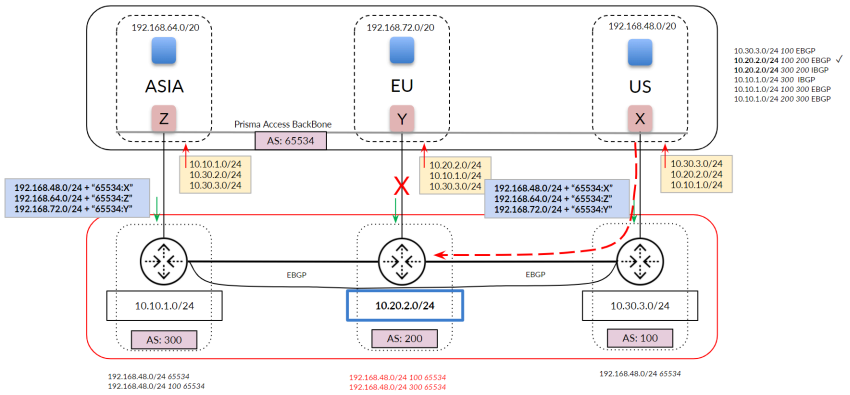

In der folgenden Abbildung ist ein gängigeres Netzwerk mit einem vollständig vermaschten eBGP-Backbone dargestellt. Oben rechts sind die Routen abgebildet, von denen Prisma Access über das Netzwerk Ihrer Organisation erfahren hat. Beachten Sie die zusätzlichen Routen, von denen Prisma Access über das Prisma Access-Backbone (iBGP) und das Backbone (eBGP) Ihrer Organisation erfahren hat.

Für den Datenverkehr zwischen mobilen Benutzern in der Region **Nordamerika und Südamerika** (im Diagramm „US“) und dem Rechenzentrum in der Region **Afrika, Europa und Naher Osten** Ihrer Organisation (im Diagramm „EU“) wählt Prisma Access den Pfad über die EU-Dienstverbindung, da Routen mit kürzerem AS-PFAD bevorzugt werden.



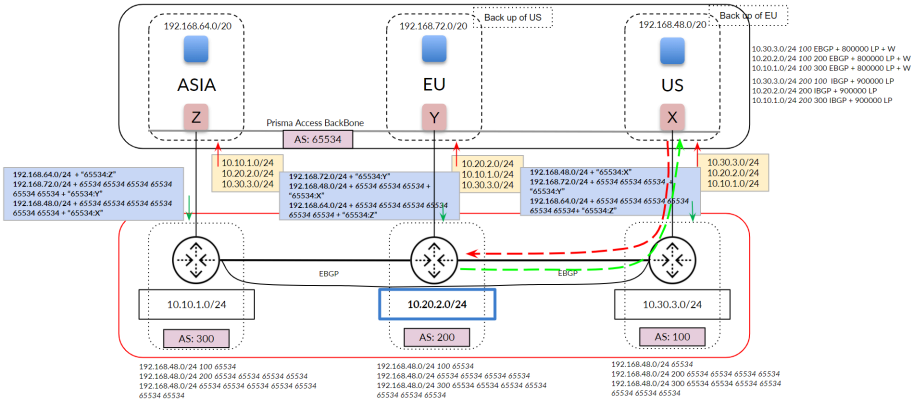

Bei Bereitstellungen mit einem vollständig vermaschten eBGP-Backbone kann es zu Asymmetrien kommen, wenn Prisma Access ein bestimmtes Rechenzentrum aufgrund eines ISP/CPE-Fehlers im Rechenzentrum des Kunden nicht erreichen kann. Die folgende Abbildung zeigt, was geschehen könnte, wenn die Verbindung zur EU-Dienstverbindung ausfällt. Ihr Netzwerk erkennt den Ausfall der Verbindung und erstellt eine neue Routentabelle für AS 200. Datenverkehr von der US-Dienstverbindung zu AS 200 nutzt den Pfad über AS 100, da die eBGP-Route für Ihr Backbone zwischen AS 200 und AS 100 gegenüber der iBGP-Route zwischen der EU- und der US-Dienstverbindung vorgezogen wird. Es ist jedoch nicht garantiert, dass der zurückfließende Datenverkehr über denselben Pfad geroutet wird, weil das lokale CPE beide Pfade (rot dargestellt) auswählen kann, um den Datenverkehr zurückzugeben.

 ©2025 Palo Alto Networks, Inc.




In den obigen Beispielen ist ein Netzwerk dargestellt, dessen Routen nicht aggregiert wurden (d. h., Sie haben vor dem Senden der BGP-Routenankündigung an Prisma Access keine Routenzusammenfassung durchgeführt). Im folgenden Beispiel ist ein Netzwerk dargestellt, das seine Routen zu 10.0.0.0/8 vor dem Senden an Prisma Access zusammenfasst. Wenn Sie Standardrouting auswählen, kann diese Konfiguration zu Problemen durch asymmetrisches Routing führen, da Prisma Access aus den zusammengefassten Routen nicht den richtigen Rückgabepfad ermitteln kann.

*Wenn Ihre Prisma Access-Bereitstellung über Remote-Netzwerke verfügt, empfiehlt Palo Alto Networks, keine Routenzusammenfassung für Dienstverbindungen zu verwenden. Die Routenzusammenfassung für Dienstverbindungen ist nur für Bereitstellungen für mobile Benutzer bestimmt.*




Wenn Sie die Routenaggregation für mobile Benutzer verwenden, wird dringend empfohlen, Hot-Potato-Routing anstelle von Standardrouting zu aktivieren. Dabei übergibt Prisma Access den Datenverkehr so schnell wie möglich an das Netzwerk Ihrer Organisation. Darüber hinaus wird empfohlen, für jede Dienstverbindung eine **Backup-Dienstverbindung** auszuwählen, wie im folgenden Abschnitt beschrieben, um ein deterministisches Routingverhalten zu erhalten.

## Prisma Access-Hot-Potato-Routing

Wenn Sie **Hot-Potato-Routing** auswählen, leitet Prisma Access den an Dienstverbindungen/Rechenzentren gebundenen Datenverkehr so schnell wie möglich aus seinem internen Netzwerk.

Beim Hot-Potato-Routing stellt Prisma Access den AS-Pfad (AS-PATH) den von Gateways gesendeten BGP-Präfixankündigungen voran. Diese Voreinstellung wird ausgeführt, wenn die Präfixe aus der Dienstverbindung heraus den lokalen CPEs Ihrer Organisation angekündigt

 ©2025 Palo Alto Networks, Inc.

werden. Prisma Access stellt die AS-Pfade so voran, dass Ihr CPE den primären und sekundären Tunneln die richtige Präferenz gibt, sodass bei Ausfall des primären Tunnels Ihr CPE den sekundären Tunnel als Backup wählt.

Wenn Sie eine andere IP-Adresse für den sekundären BGP-Peer (das Backup) angegeben haben, fügt Prisma Access weitere Voranstellungen basierend auf dem Tunneltyp hinzu, wie in der folgenden Tabelle aufgeführt.

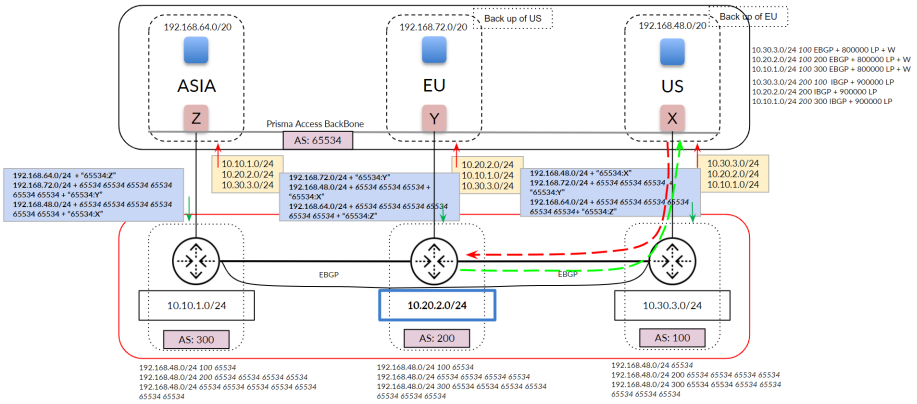
| Präfixtyp | Typ des Dienstverbindungstunnel | Anzahl der AS-Pfad-Voranstellungen | Gesamtzahl der AS-PFADE, die auf dem CPE angezeigt werden |
|---|---|---|---|
| Gatewaypräfixe von der primären Dienstverbindung | Primärer oder sekundärer Tunnel mit gleicher BGP-Peer-IP-Adresse | 0 | 1 |
| Gatewaypräfixe von der Backup-Dienstverbindung | Primärer oder sekundärer Tunnel mit gleicher BGP-Peer-IP-Adresse | 3 | 4 |
| Gatewaypräfixe von allen anderen Dienstverbindungen | Primärer oder sekundärer Tunnel mit gleicher BGP-Peer-IP-Adresse | 6 | 7 |
| Gatewaypräfixe von der primären Dienstverbindung | Sekundärer Tunnel mit einer anderen BGP-Peer-IP-Adresse | 1 | 2 |
| Gatewaypräfixe von der Backup-Dienstverbindung | Sekundärer Tunnel mit einer anderen BGP-Peer-IP-Adresse | 4 | 5 |
| Gatewaypräfixe von allen anderen Dienstverbindungen | Sekundärer Tunnel mit einer anderen BGP-Peer-IP-Adresse | 7 | 8 |

Im Hot-Potato-Routing-Modus können Sie mit Prisma Access eine Backup-Dienstverbindung während des Onboardings angeben. Durch die Angabe einer **Backup-Dienstverbindung** wird Prisma Access darüber informiert, dass diese Dienstverbindung als Backup verwendet werden soll, wenn eine Dienstverbindung ausfällt.

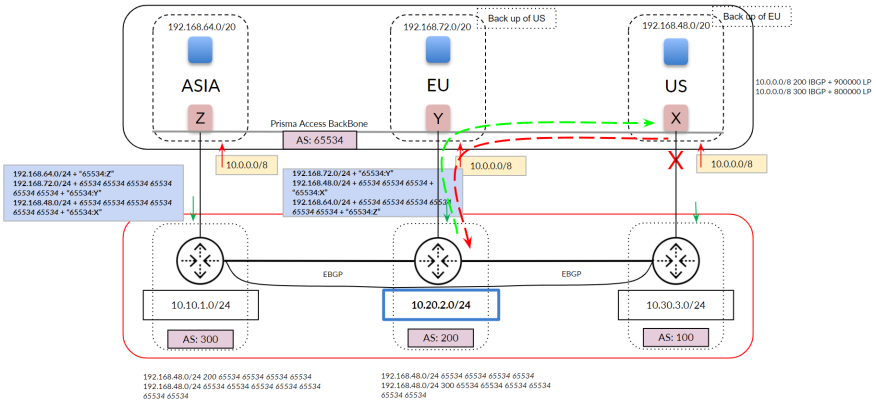
In der folgenden Abbildung ist eine Hot-Potato-Routing-Konfiguration für den Datenverkehr zwischen der US-Dienstverbindung und AS 200 dargestellt, wobei die EU-Dienstverbindung als **Backup-Dienstverbindung** der US-Dienstverbindung konfiguriert ist. Mithilfe von Hot-Potato-Routing sendet Prisma Access den Datenverkehr von seinem nächstgelegenen Ausgangspfad über die US-Dienstverbindung. Der zurückfließende Datenverkehr nimmt den gleichen Pfad über

 ©2025 Palo Alto Networks, Inc.

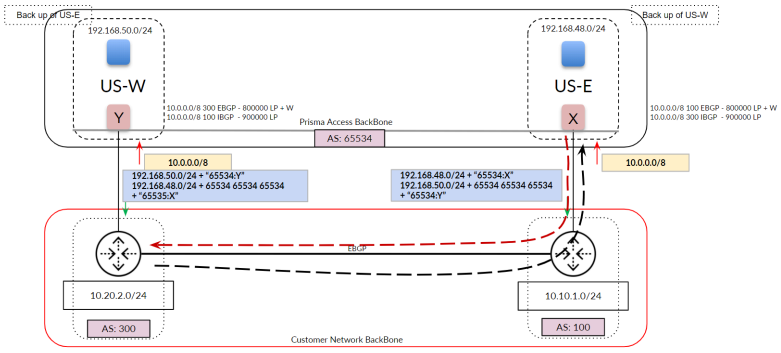
AS 100, da dieser Pfad einen kürzeren AS-Pfad zum Pool der mobilen Benutzer am US-Standort hat. Prisma Access stellt den AS-Pfad seinen Präfixankündigungen voran, abhängig davon, ob es sich bei dem Tunnel um einen primären Tunnel oder einen Backup-Tunnel handelt oder ob er weder als primärer Tunnel noch als Backup-Tunnel verwendet wird.




Da Sie eine Backup-Dienstverbindung eingerichtet haben, sendet das Hot-Potato-Routing den Datenverkehr auf kürzestem Weg über die EU-Dienstverbindung hinaus, wenn die US-Dienstverbindung ausfällt. Dieses Routingszenario gilt auch für Netzwerke, die eine Routenaggregation verwenden.




Sie können auch Backup-Dienstverbindungen für mehrere Dienstverbindungen in einer Region verwenden. Die folgende Abbildung zeigt eine Prisma Access-Bereitstellung mit zwei Dienstverbindungen in der Region Nordamerika. In diesem Fall geben Sie die **Backup-Dienstverbindung** US-E für die Dienstverbindung US-W an und umgekehrt, um symmetrisches Routing zu gewährleisten.




 ©2025 Palo Alto Networks, Inc.

## Konfigurieren von Routingeinstellungen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

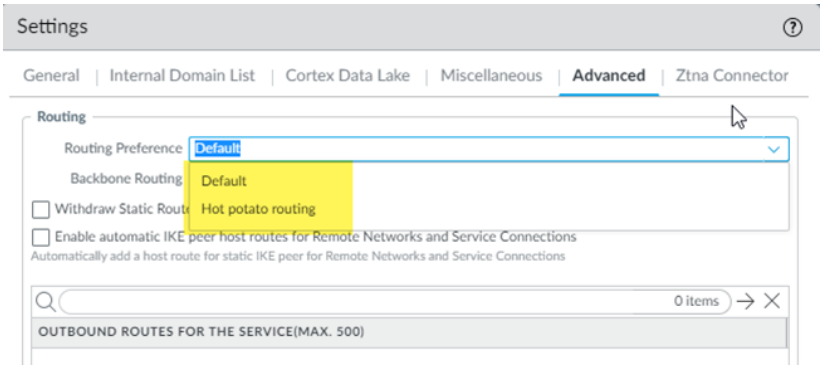
Führen Sie die folgenden Schritte aus, um die Routingeinstellungen zu aktivieren.

*Um diese Routingeinstellungen zu konfigurieren, müssen Sie das BGP-Routing und nicht das statische Routing für Ihre Dienstverbindungen verwenden.*

**STEP 1 |** Konfigurieren Sie Ihre Dienstverbindung.

**STEP 2 |** (Optional) Wählen Sie das Routing für Ihre Dienstverbindungen aus.

1. Rufen Sie in der Panorama-Anwendung, die zur Verwaltung von Prisma Access verwendet wird, **Panorama** > **Cloud Services** > **Konfiguration** > **Diensteinrichtung** auf und klicken Sie dann auf das Zahnradsymbol, um die **Einstellungen** zu bearbeiten.
2. Wählen Sie in den **Erweiterten** Einstellungen Ihre **Routing-Präferenz** (entweder **Standard** oder **Hot-Potato**) aus.



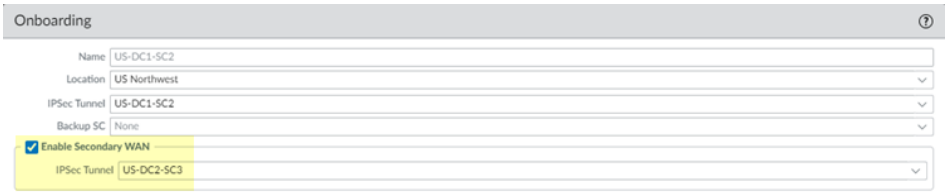

**STEP 3 |** (Optional, nur Hot-Potato-Routing-Bereitstellungen) Wenn Sie eine bevorzugte Dienstverbindung angeben möchten, die verwendet werden soll, wenn ein Link ausfällt, konfigurieren Sie beim Konfigurieren einer Dienstverbindung eine **Backup-SC**.

Sie können jede bereits hinzugefügte Dienstverbindung auswählen. Prisma Access verwendet bei einem Linkausfall die von Ihnen ausgewählte **Backup-SC** als bevorzugte Dienstverbindung. Durch Auswahl einer Backup-Dienstverbindung (Backup-SC) können Probleme aufgrund asymmetrischen Routings verhindert werden, wenn Sie mehr als zwei Dienstverbindungen eingebunden haben. Diese Auswahl steht nur im Hot-Potato-Routing-Modus zur Verfügung.

1. Wählen Sie **Panorama** > **Cloud Service** > **Konfiguration** > **Dienstverbindung** aus
2. Wählen Sie die zu konfigurierende Dienstverbindung aus oder verwenden Sie **Hinzufügen**, um eine neue Dienstverbindung hinzuzufügen.

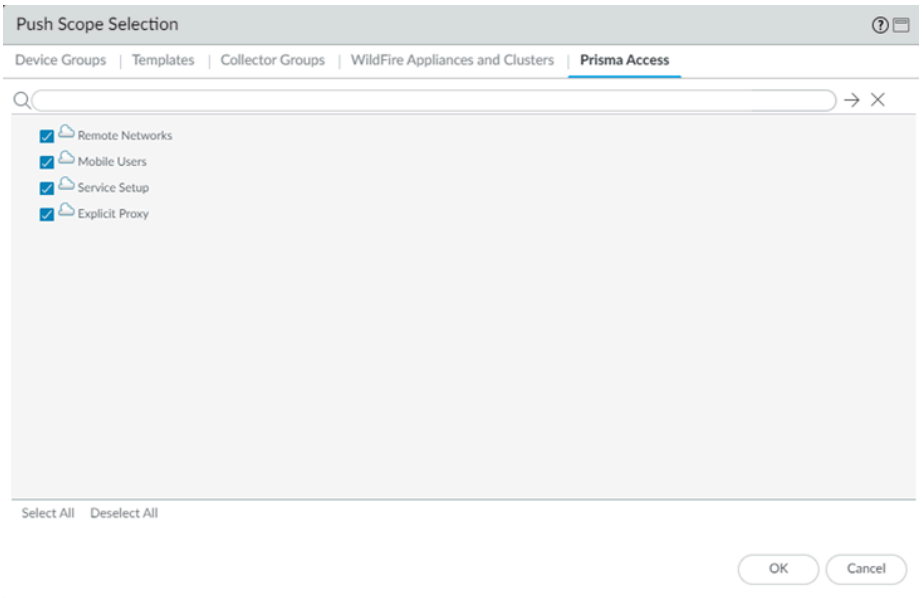
 ©2025 Palo Alto Networks, Inc.

3. Wählen Sie eine Dienstverbindung aus, die als bevorzugte Backup-Dienstverbindung (**Backup-SC**) verwendet werden soll.




**STEP 4 |** Schreiben Sie Ihre Änderungen in Panorama fest und übertragen Sie die Konfigurationsänderungen an Prisma Access.

1. Klicken Sie auf **Commit** > **Commit und Push**.
2. Wählen Sie **Auswahlen bearbeiten** aus und stellen Sie auf der Registerkarte Prisma Access sicher, dass **Diensteinrichtung** im **Übertragungsumfang** ausgewählt wurde. Klicken Sie anschließend auf **OK**.

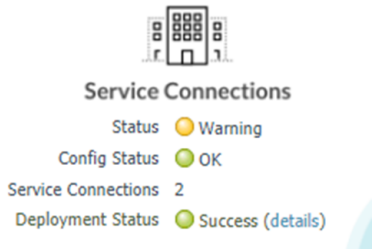



3. Klicken Sie auf **Commit und Push**.

 ©2025 Palo Alto Networks, Inc.

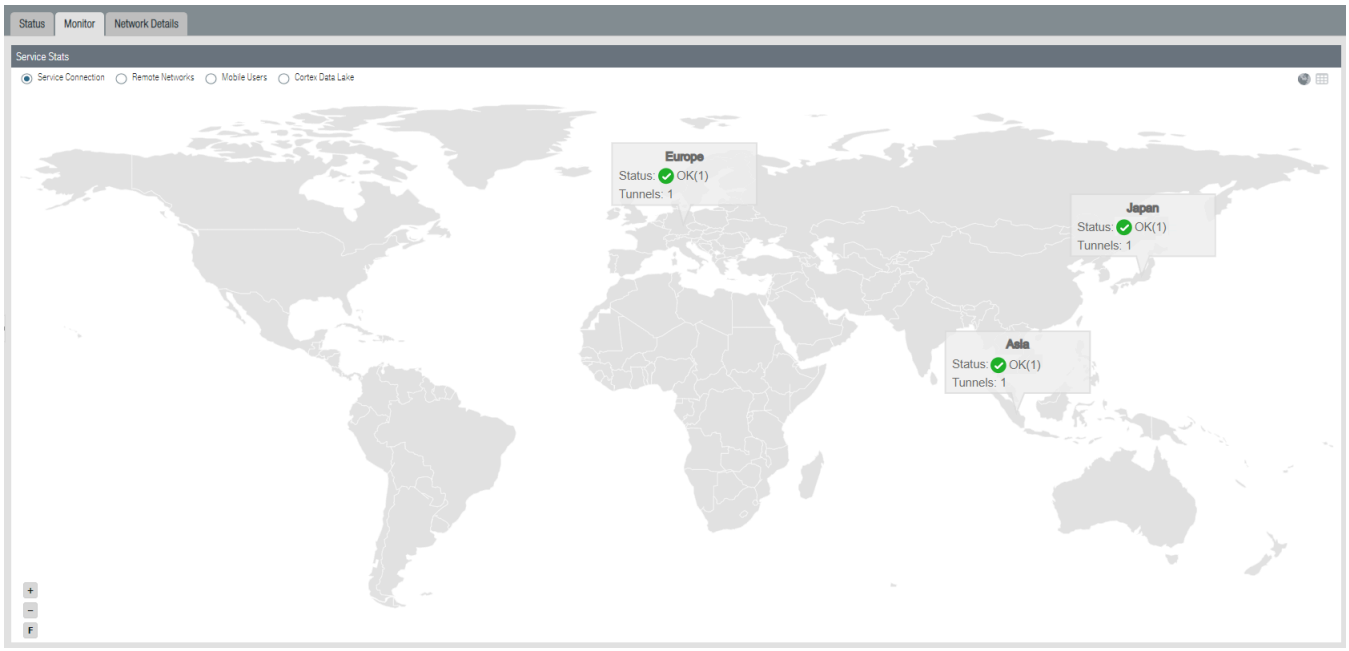
**STEP 5 |** Vergewissern Sie sich, dass Ihre Dienstverbindung aktiv ist, indem Sie **Panorama > Cloud Services > Status > Status** auswählen und überprüfen, ob der Status **OK** angezeigt wird.

Im Bereich **Bereitstellungsstatus** können Sie den Fortschritt der Onboarding- und Bereitstellungsjobs verfolgen, bevor sie abgeschlossen sind. Außerdem erhalten Sie hier weitere Informationen zum Status abgeschlossener Jobs.



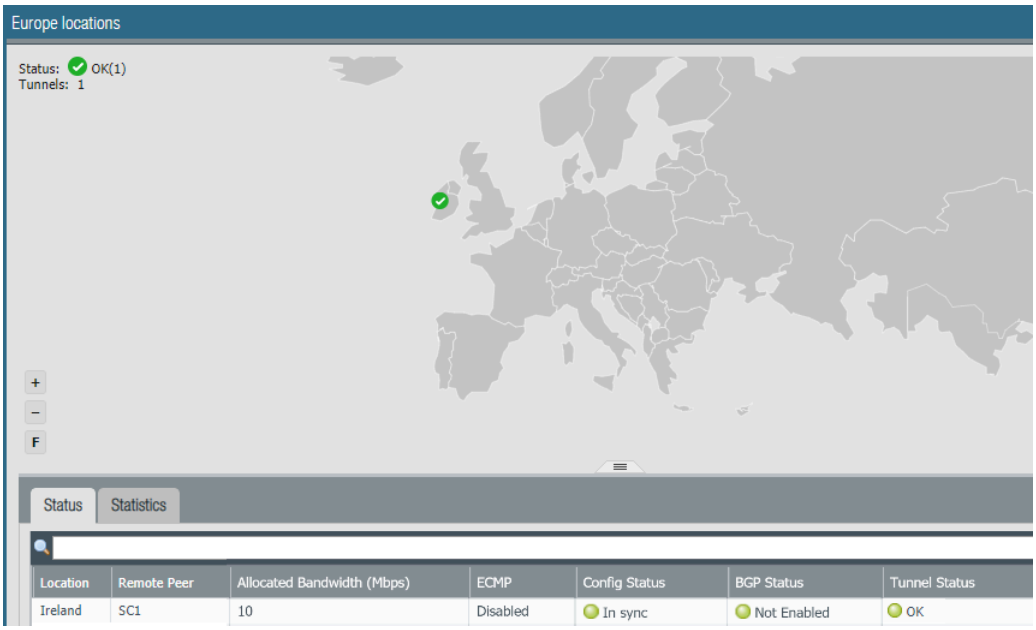

Wenn der Status nicht **OK** lautet, bewegen Sie den Mauszeiger über das Statussymbol, um Fehler anzuzeigen.

Um eine grafische Darstellung der Dienstverbindung zusammen mit Statusdetails anzuzeigen, wählen Sie auf der Registerkarte **Überwachen** die Option **Dienstverbindung** aus.




Wählen Sie eine Region aus, um weiterführende Details zu dieser Region abzufragen.

 ©2025 Palo Alto Networks, Inc.




Klicken Sie auf die Registerkarten unter der Karte, um weitere Informationen zu den Dienstverbindungen anzuzeigen.

Registerkarte **Status**:

- **Standort** – Der Standort, an dem Ihre Dienstverbindung bereitgestellt wird.
- **Remote-Peer** – Der Unternehmensstandort, zu dem diese Dienstinfrastruktur einen IPSec-Tunnel einrichtet.
- **Zugewiesene Bandbreite** – Die Anzahl der zugewiesenen Dienstverbindungen multipliziert mit 300 Mbit/s.

  Diese Anzahl spiegelt nicht die verfügbare Dienstverbindungsbandbreite wider.

  *Während jede Dienstverbindung circa 1 Gbit/s Durchsatz bereitstellt, hängt der tatsächliche Durchsatz von mehreren Faktoren ab, darunter:*

  - *Datenverkehrsmix (z. B. Rahmengröße)*
  - *Latenz und Paketverlust zwischen der Dienstverbindung und dem Standort der Zentrale oder des Rechenzentrums*
  - *Leistungsgrenzen der Dienstanbieter*
  - *Leistungsgrenzen für Kundenterminierungsgeräte*
  - *Sonstiger Datenverkehr des Kunden im Rechenzentrum*
- **ECMP** – Wenn Sie für diese Dienstverbindung ECMP (Equal Cost Multipath) konfiguriert haben. Da ECMP nicht für Dienstverbindungen verwendet wird, lautet dieser Status **Deaktiviert**.

 ©2025 Palo Alto Networks, Inc.

- **Konfigurationsstatus** – Der Status Ihrer letzten Konfigurationsübertragung an den Dienst. Wenn die lokale Konfiguration und die Konfiguration in der Cloud übereinstimmen, lautet der Konfigurationsstatus **Synchron**. Wenn Sie lokal eine Änderung vorgenommen und die Konfiguration noch nicht in die Cloud übertragen haben, wird möglicherweise der Status **Nicht synchron** angezeigt. Bewegen Sie den Mauszeiger über die Statusanzeige, um detailliertere Informationen zu erhalten. Nach dem Festschreiben und Übertragen der Konfiguration in Prisma Access ändert sich der Konfigurationsstatus in **Synchron**.
- **BGP-Status** – Zeigt Informationen zum BGP-Status zwischen der Firewall oder dem Router am Standort Ihres Unternehmens bzw. der Zentrale und Prisma Access an, wo die Dienstverbindung eingerichtet wird. Obwohl der Status beim Durchlaufen der verschiedenen BGP-Status nur kurz angezeigt wird (**Inaktiv**, **Aktiv**, **Offen Senden**, **Offen Anstehend**, **Offen Bestätigen**), wird der BGP-Status meist angezeigt:
  - **Verbinden** – Der Router im Rechenzentrum bzw. in der Zentrale versucht, die BGP-Peer-Beziehung zu Prisma Access herzustellen.
  - **Eingerichtet** – Die BGP-Peer-Beziehung wurde eingerichtet.

  In diesem Feld wird auch angezeigt, ob sich die BGP-Verbindung in einem Fehlerzustand befindet:
  - **Warnung** – Seit mehr als acht Minuten wurde der BGP-Status nicht aktualisiert. Dies kann auf einen Ausfall der Firewall hindeuten.
  - **Fehler** – Der BGP-Status ist unbekannt.
- **Tunnelstatus** – Der Betriebsstatus der Verbindung zwischen Prisma Access und Ihrer Dienstverbindung.

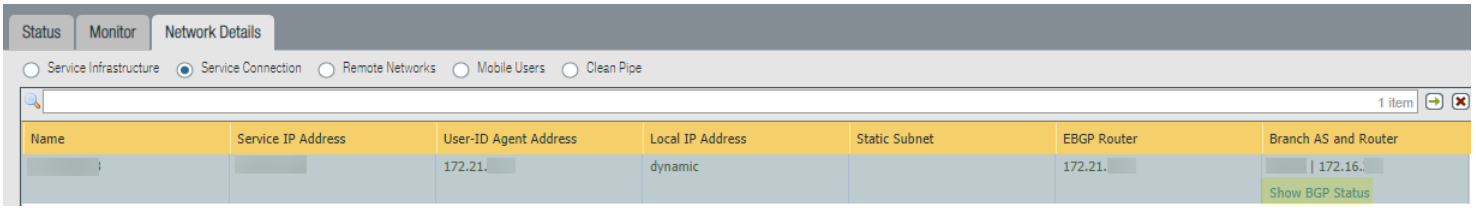
Registerkarte **Statistiken**:

- **Standort** – Der Standort, an dem Ihre Dienstverbindung bereitgestellt wird.
- **Remote-Peer** – Der Unternehmensstandort, zu dem die Dienstverbindung einen IPSec-Tunnel einrichtet.
- **Eingangsbandbreite (Mbit/s)** – Die Bandbreite vom Standort der Zentrale/des Rechenzentrums bis zu Prisma Access.
- **Höchste Eingangsbandbreite (Mbit/s)** – Die Spitzenlast vom Standort der Zentrale/des Rechenzentrums in den Cloud-Dienst.
- **Ausgangsbandbreite (Mbit/s)** – Die Bandbreite von Prisma Access bis zum Standort der Zentrale/des Rechenzentrums.
- **Höchste Ausgangsbandbreite (Mbit/s)** – Die Spitzenlast von Prisma Access bis zum Standort der Zentrale/des Rechenzentrums.
- **QoS** – Wählen Sie diese Schaltfläche aus, um ein Grafikdiagramm anzuzeigen, das eine Echtzeitstatistik und eine QoS-Langzeitstatistik einschließlich der Anzahl der gelöschten

 ©2025 Palo Alto Networks, Inc.

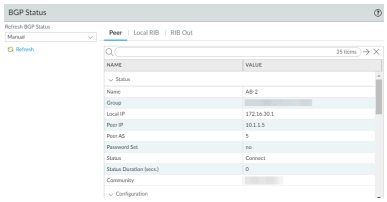
Pakete pro Klasse anzeigt. Dieses Diagramm wird nur für Dienstverbindungen oder Remote-Netzwerkverbindungen angezeigt, bei denen QoS aktiviert ist.

Wenn Sie BGP konfiguriert haben, können Sie dessen Status überprüfen, indem Sie **Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Dienstverbindung** > **BGP-Status anzeigen**auswählen.



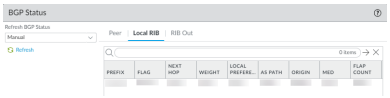

Daraufhin wird der Dialog für den BGP-Status angezeigt. Diese Tabelle enthält folgende Informationen:

- **Peer** – Routinginformationen für den BGP-Peer, einschließlich Status, Gesamtzahl der Routen, Konfigurations- und Laufzeitstatistiken sowie Zähler. Die Gesamtzahl der Routen wird im Bereich **bgpAfiIpv4-unicast Counters** in den Feldern **Gesamtwert eingehend** und **Gesamtwert ausgehend** angezeigt.




- **Lokale RIB** – BGP-Routen, die Prisma Access lokal nutzt. Prisma Access wählt diese Informationen aus der BGP-RIB-Eingabetabelle aus, in der die von benachbarten Netzwerkgeräten gesendeten Informationen gespeichert werden, wendet lokale BGP-Importrichtlinien und -Routingentscheidungen an und speichert die lokalen RIB-Informationen in der Routinginformationsbasis (RIB).

  Beachten Sie, dass nur die ersten 256 Einträge angezeigt werden. Um zusätzliche Einträge anzuzeigen, geben Sie im Feld „Filter“ ein Subnetz oder eine IP-Adresse ein und klicken Sie dann auf „Filter anwenden“, um eine Teilmenge der Routingeinträge bis zur maximalen Anzahl von 256 anzuzeigen.




- **RIB Out** – Routinginformationen, die Prisma Access über BGP-Aktualisierungsnachrichten an seine Peers mitteilt.

## Netzwerk mit hoher Bandbreite mithilfe mehrerer Dienstverbindungen erstellen

Wenn für einen Standort Ihrer Zentrale oder Ihres Rechenzentrums zusätzliche Bandbreite für Dienstverbindungen erforderlich ist, können Sie für diesen Standort mehrere Dienstverbindungen konfigurieren.

 ©2025 Palo Alto Networks, Inc.

Keine der Prisma Access-Dienstverbindungen weist eine Bandbreitenbegrenzung auf, aber Palo Alto Networks geht davon aus, dass jede Dienstverbindung einen Durchsatz von etwa 1 Gbit/s bieten kann. Während diese Bandbreite in der Regel ausreicht, um auf interne Ressourcen am Standort einer Zentrale oder eines Rechenzentrums zuzugreifen, erfordern andere Bereitstellungen möglicherweise zusätzliche Bandbreite. Zum Beispiel, wenn Sie eine interne oder private SaaS-Anwendung in einem Rechenzentrum hosten.

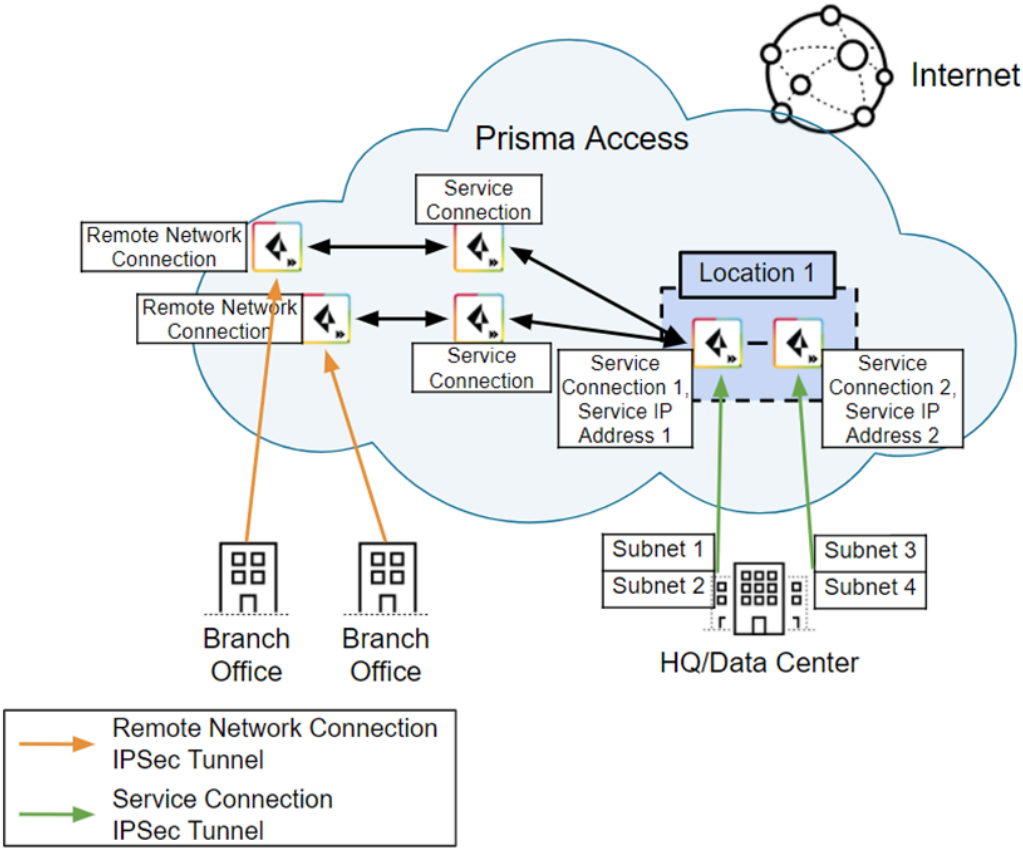
Um eine Dienstverbindung mit hoher Bandbreite zum Standort einer Zentrale oder eines Rechenzentrums zu erstellen, binden Sie den Standort mithilfe mehrerer Dienstverbindungen am selben Prisma Access-Standort ein.

*Während Prisma Access die maximale Anzahl von Dienstverbindungen, die Sie an einem einzelnen Remote-Netzwerkstandort einer Zentrale oder eines Rechenzentrums einbinden können, nicht einschränkt, empfiehlt Palo Alto Networks, nicht mehr als vier Dienstverbindungen in einer Bereitstellung mit hoher Bandbreite zu verwenden. Wenn Sie mehr Bandbreite für den Zugriff auf interne Apps benötigen, verwenden Sie anstelle mehrerer Dienstverbindungen die Option* ZTNA-Connector *oder* Colo-Connect.

Im folgenden Diagramm ist eine Prisma Access-Remote-Netzwerkbereitstellung mit dem Standort einer Zentrale oder eines Rechenzentrums dargestellt, die zwei Dienstverbindungen vom selben Prisma Access-Standort aufweist, wodurch effektiv eine Bandbreite von 2 Gbit/s zwischen dem Standort und dem Prisma Access-Standort bereitgestellt wird.

Zusätzlich zu den Dienstverbindungen, die für den Zugriff mit hoher Bandbreite bereitgestellt werden, ist im Diagramm ein weiterer Satz von Dienstverbindungen dargestellt. Diese Dienstverbindungen stellen normale Routingfunktionen für Prisma Access bereit (in diesem Diagramm bieten sie internen Routingzugriff zwischen den Remote-Netzwerkverbindungen und den Dienstverbindungen mit hoher Bandbreite). Palo Alto Networks empfiehlt, dass Sie bei der Bereitstellung einer Verbindung mit hoher Bandbreite Dienstverbindungen reservieren, um nur Zugriff auf die Ressource in der Zentrale oder im Rechenzentrum zu ermöglichen, und zusätzliche Dienstverbindungen bereitstellen, die für das interne Routing zwischen Remote-Netzwerken, mobilen Benutzern und den Ressourcen im Rechenzentrum verwendet werden.

 ©2025 Palo Alto Networks, Inc.




Jede Dienstverbindung ist aktiv und verfügt über eine eigene **Dienst-IP-Adresse** . Sie verwenden diese Adresse zum Beenden des IPSec-Tunnels für jede Dienstverbindung.

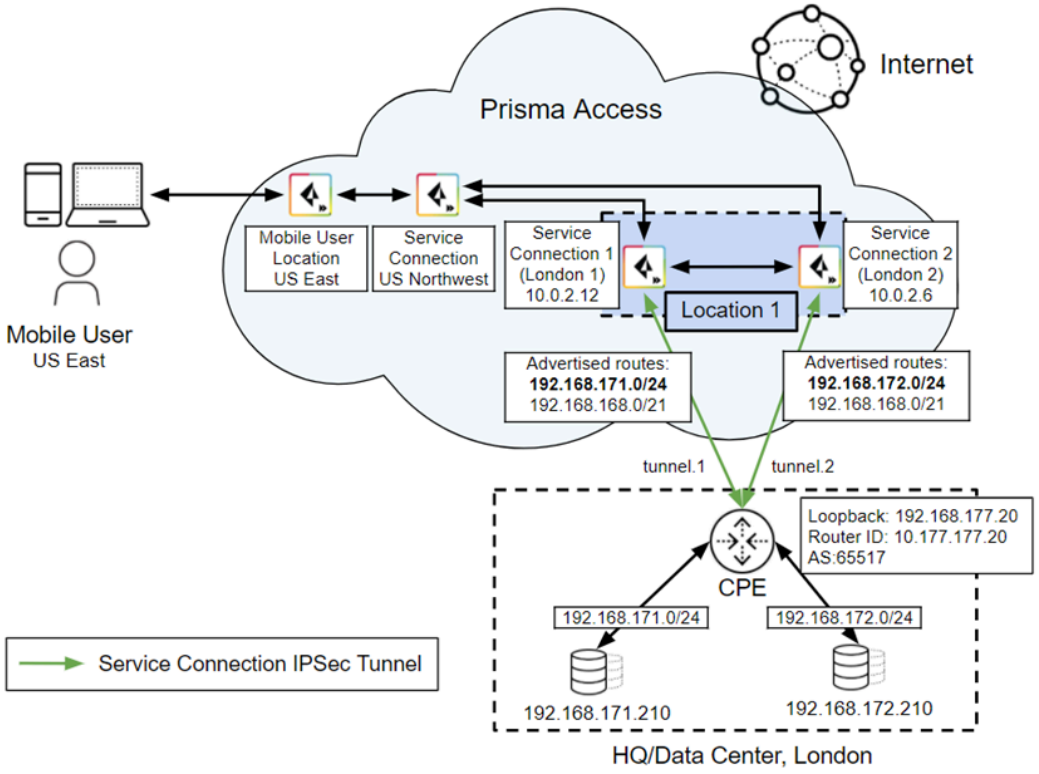
## Erstellen einer Verbindung mit hoher Bandbreite zu einer Zentrale oder einem Rechenzentrumsstandort

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Gehen Sie wie folgt vor, um mehrere Dienstverbindungen zu einem einzelnen Standort einer Zentrale oder eines Rechenzentrums zu konfigurieren.

Die Schritte in diesem Abschnitt verwenden ein Bereitstellungsbeispiel, wie im folgenden Diagramm dargestellt. In diesem Beispiel stellt der Standort der Londoner Zentrale eine Verbindung zu zwei verschiedenen Dienstverbindungen (London 1 und London 2) her. Dabei werden zwei verschiedene IPSec-Tunnel verwendet, die an zwei verschiedenen Customer Premises Equipment(CPE)-Schnittstellen („tunnel.1“ und „tunnel.2“) beendet werden.

 ©2025 Palo Alto Networks, Inc.




In diesem Beispiel und den Schritten in diesem Abschnitt wird eine Firewall der nächsten Generation verwendet, um die Dienstverbindungen auf dem CPE zu beenden. Als CPE können Sie jedoch jedes CPE verwenden, das symmetrisches Routing und PBF oder richtlinienbasiertes Routing unterstützt.

*Diese Schritte dienen lediglich zur Orientierung. Jeder Anwendungsfall kann zusätzliche Entwurfs- und Planungsschritte erfordern, die über den Rahmen dieses Dokuments hinausgehen.*

**STEP 1 |** Bevor Sie mehrere Dienstverbindungen von einem einzelnen Prisma Access-Standort an einem einzelnen Standort bereitstellen, vergewissern Sie sich, dass Ihr Netzwerk die folgenden Voraussetzungen erfüllt:

- Sie müssen die Subnetze am Standort der Zentrale oder des Rechenzentrums aufteilen und für jede Dienstverbindung ein eindeutiges Subnetz ankündigen.
- Ihre Kundenendgeräte (Customer Premises Equipment, CPE) müssen die folgenden Netzwerkfunktionen unterstützen und Sie müssen in der Lage sein, diese zu konfigurieren:
  - Richtlinienbasierte Weiterleitung (PBF) oder richtlinienbasiertes Routing – Ihr CPE muss in der Lage sein, selektiv einen bestimmten Pfad für eine bestimmte lokale Quell-IP-Adresse und ein bestimmtes Subnetz auszuwählen.
  - Symmetrische Rückkehr – Sie müssen in der Lage sein, Ihr CPE so zu konfigurieren, dass symmetrischer Datenverkehr zu und von einer bestimmten IP-Adresse und einem bestimmten Subnetz möglich ist, und Sie müssen eine symmetrische Rückgabe für Failover-Tunnel konfigurieren, falls einer der Tunnel ausfällt.

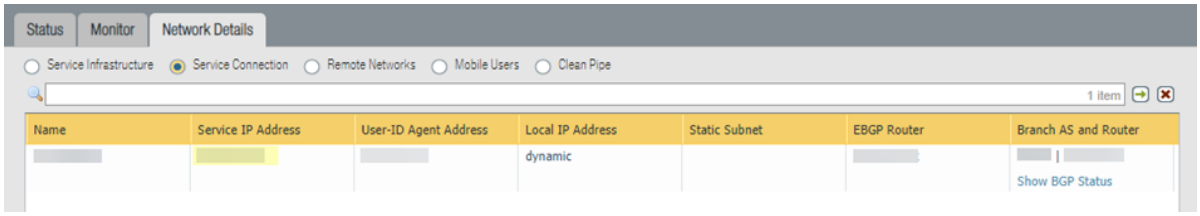
 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Erstellen Sie die Dienstverbindungen und richten Sie Konnektivität für die IPSec-Tunnel ein, die für die Dienstverbindungen verwendet werden.

1. Konfigurieren Sie auf der Panorama-Instanz, die Prisma Access verwaltet, eine Dienstverbindung und erstellen Sie eine neue IPSec-Tunnel-Konfiguration sowie Einstellungen für IKE-Gateway, IPSec-Verschlüsselungsprofil und Tunnelüberwachung.

   *Prisma Access bietet vordefinierte IPSec-Vorlagen, mit denen Sie die Erstellung des IPSec-Tunnels vereinfachen können.*

2. Suchen Sie die IP-Adresse, die als Remote-Seite des IPSec-Tunnels von Ihrem CPE zu Prisma Access verwendet werden soll. Wählen Sie dazu **Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** aus, klicken Sie auf das Optionsfeld **Dienstverbindung** und notieren Sie sich die **Dienst-IP-Adresse** für den Standort.




3. Erstellen Sie auf Ihrem CPE einen IPSec-Tunnel zu den Dienstverbindungen.

   1. Überprüfen Sie, ob die IKE- und IPSec-Tunnel dieselben Verschlüsselungsprofile zur Authentifizierung und Verschlüsselung zwischen den Peers verwenden.
   2. Verwenden Sie die **Dienst-IP-Adresse** als Peer-IP-Adresse für den Tunnel.

   Wenn Sie eine Firewall der nächsten Generation als CPE verwenden, wählen Sie **Netzwerk** > **IPSec-Tunnel** aus und erstellen Sie zwei Tunnel für die Dienstverbindungen (**tunnel.1** und **tunnel.2** im folgenden Screenshot).




**STEP 3 |** Erstellen Sie für das CPE Einstellungen für den virtuellen Router.

Sie erstellen BGP-Routinginstanzen, die ein Subnetz an einem Tunnel und das andere Subnetz an einem anderen Tunnel ankündigen, wodurch der Lastausgleich der beiden aktiven Tunnel sichergestellt wird.

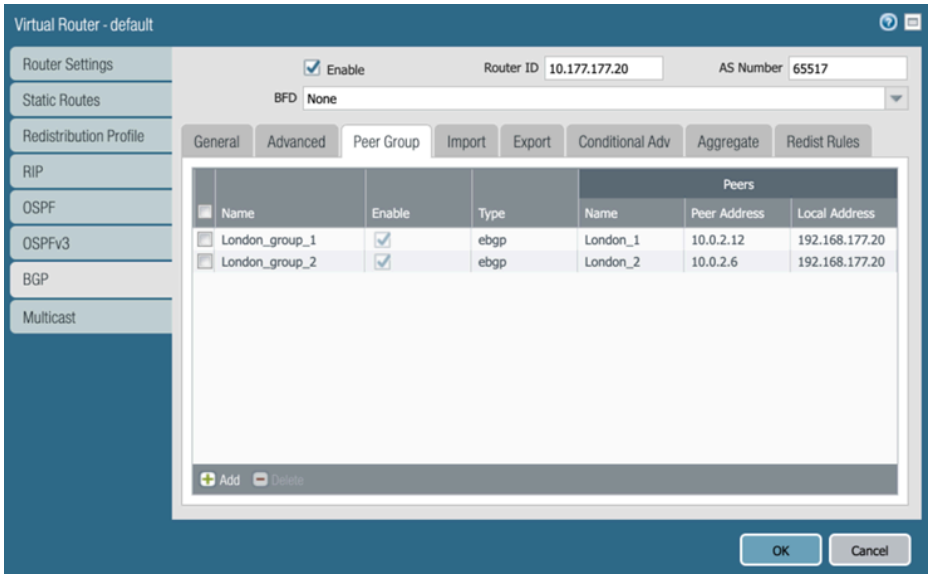
Wenn Sie als CPE eine Firewall der nächsten Generation verwenden, wählen Sie **Netzwerk** > **Virtuelle Router** aus, um Einstellungen für virtuelle Router **hinzuzufügen**. Anschließend müssen Sie eine **BGP-Peer-Gruppe** für jeden Tunnel **hinzufügen**, indem Sie die folgenden Einstellungen angeben:

- Geben Sie eine **Router-ID** und die **AS-Nummer** des CPE-Routers an (in diesem Beispiel 10.177.177.20 bzw. 65517).
- Geben Sie die Adresse des **EBGP-Routers** der Dienstverbindungen (**Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Dienstverbindung** > **EBGP-Router**) als **Peer-Adresse**

 ©2025 Palo Alto Networks, Inc.

für die Dienstverbindungen an (in diesem Beispiel 10.0.2.12 für Dienstverbindung 1 und 10.0.2.6 für Dienstverbindung 2).

- Für die **lokale Adresse** können Sie die Loopback-Adresse des CPE angeben (in diesem Beispiel 192.168.177.20).




**STEP 4 |** Erstellen Sie ein zusammengefasstes Subnetz für die IP-Adressen, das für beide Tunnel verwendet wird.

Durch die Bereitstellung eines zusammengefassten Subnetzes ist Redundanz gewährleistet. Wenn beide Tunnel aktiv sind, nutzt der Datenverkehr die spezifischsten Routen, um sein Ziel zu erreichen. Beispielsweise nutzt 192.168.171.0/24 „tunnel.1“, um sein Ziel zu erreichen. Durch das Hinzufügen eines zusammengefassten Subnetzes, das alle angekündigten Subnetze abdeckt (in diesem Beispiel 192.168.168.0/21), wird sichergestellt, dass der Datenverkehr von 192.168.171.0/24 von „tunnel.2“ aus erreichbar ist, wenn „tunnel.1“ ausfällt, und dass der Datenverkehr von 192.168.172.0/24 von „tunnel.1“ aus erreichbar ist, wenn „tunnel.2“ ausfällt.

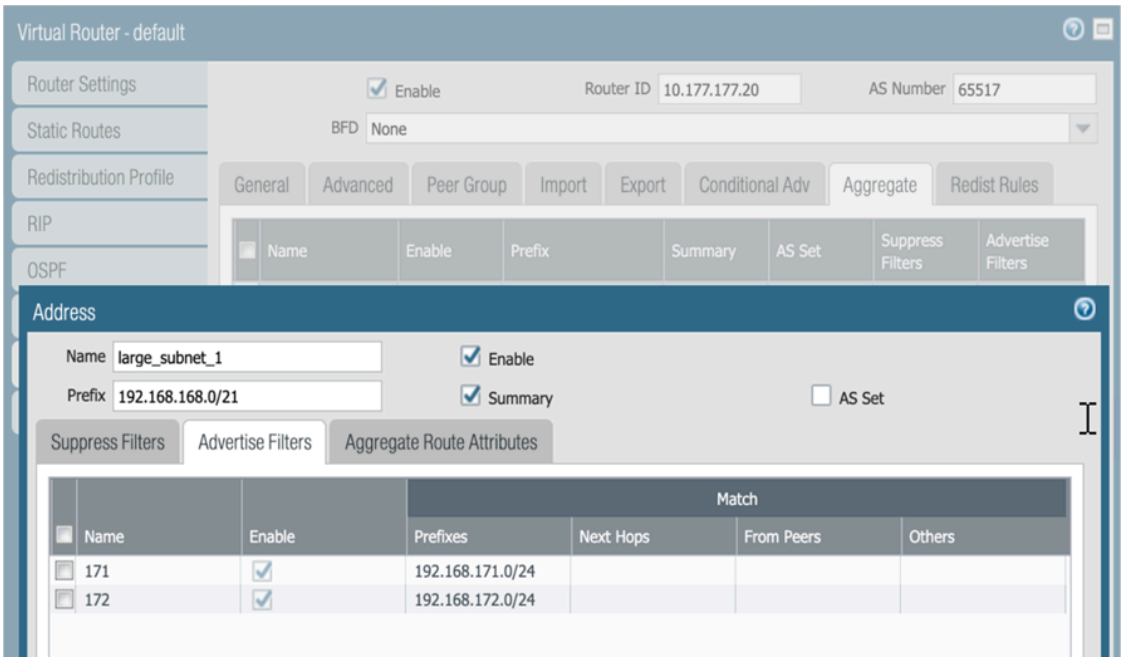
Wenn Sie eine Firewall der nächsten Generation als CPE verwenden, gehen Sie wie folgt vor.

1. Fahren Sie mit der Änderung des virtuellen Routerprofils fort, um Routenaggregationsparameter **hinzuzufügen** (**Netzwerk** > **Virtuelle Router** > **BGP** > **Aggregieren**).

 ©2025 Palo Alto Networks, Inc.

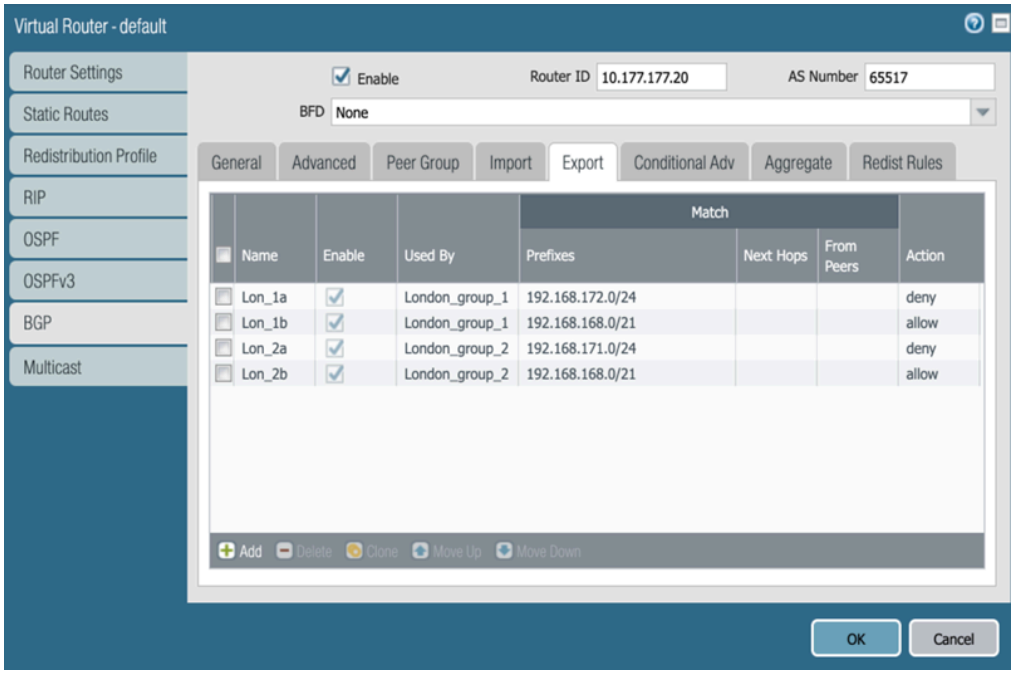
2. Geben Sie eine Zusammenfassung der Subnetze für die Subnetze ein, die Sie für die Dienstverbindungen ankündigen.

   Geben Sie in diesem Beispiel das **Präfix 192.168.168.0/21** ein, das die beiden Rechenzentrumssubnetze zusammenfasst.




3. Geben Sie Einstellungen für den **Export** ein, um sicherzustellen, dass die Tunnel die richtigen Subnetze ankündigen.

   In diesem Beispiel geben Sie für die Subnetze die **Aktion Ablehnen** und **Zulassen** an, sodass das erste Subnetz (192.168.171.0/24) von „tunnel.1“ aus erreichbar ist und das zweite Subnetz (192.168.172.0/24) von „tunnel.2“ aus erreichbar ist.




 ©2025 Palo Alto Networks, Inc.

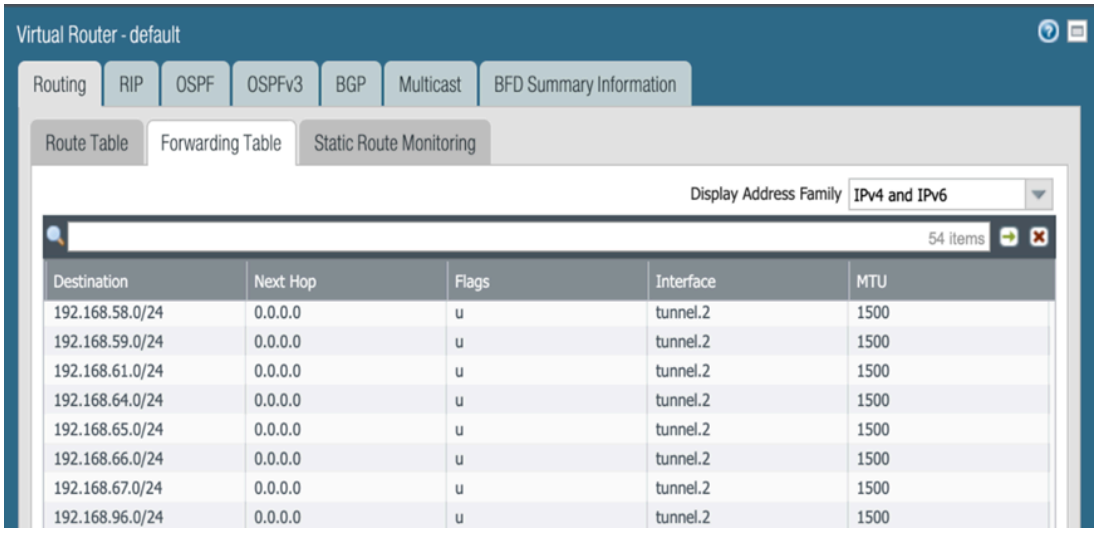
**STEP 5 |** (Nur Bereitstellungen mit mehr als zwei Dienstverbindungen) Wenn Sie mehr als zwei Dienstverbindungen benötigen, um die Benutzer mit einer Bandbreite von über 2 Gbit/s mit privaten Ressourcen zu verbinden, stellen Sie den exportierten Routen AS-PATH voran, damit die Dienstverbindungen im Falle eines Failovers symmetrisches Routing zum und vom Rechenzentrum verwenden. Weitere Einzelheiten finden Sie unter Konfigurieren von mehr als zwei Dienstverbindungen zum Standort einer Zentrale oder eines Rechenzentrums.

**STEP 6 |** Um eine symmetrische Rückkehr sicherzustellen (sodass der Datenverkehr von 192.168.171.0/24 immer „tunnel.1“ und der Datenverkehr von 192.168.172.0 immer „tunnel.2“ verwendet), geben Sie PBF oder richtlinienbasierte Routingregeln ein.

Standardmäßig installiert BGP, unabhängig vom bevorzugten Tunnel, Routen in der Routingtabelle für die unterschiedlichsten Ziele. Der folgende Screenshot veranschaulicht,

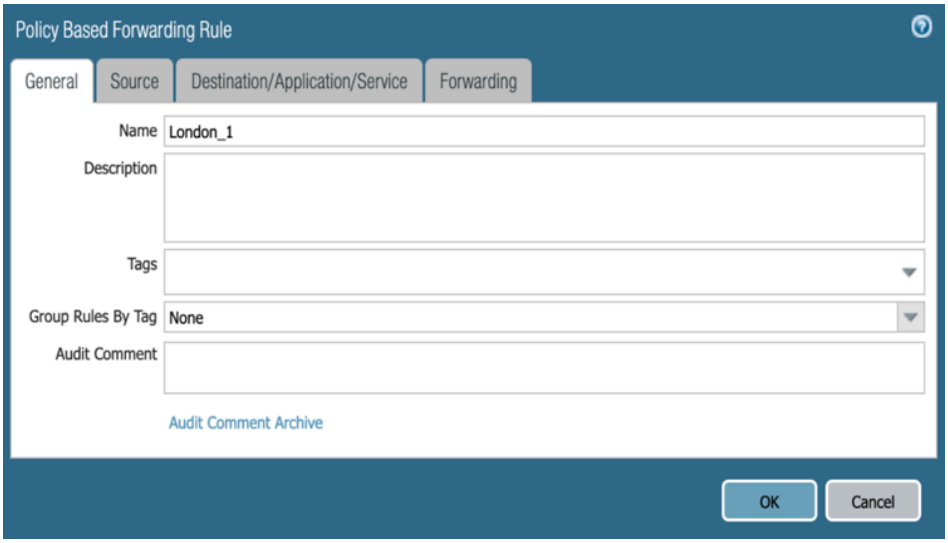
 ©2025 Palo Alto Networks, Inc.

dass BGP alle Ziele aus dem Subnetz 192.168.168.0/21 für „tunnel.2“ ankündigt, was zu asymmetrischem Routing für Datenverkehr von 192.168.171.0/24 führen kann.




Um symmetrisches Routing sicherzustellen, konfigurieren Sie einen Satz mit PBF- oder routenbasierten Weiterleitungsregeln. Wenn Sie eine Firewall der nächsten Generation als CPE verwenden, gehen Sie wie folgt vor.

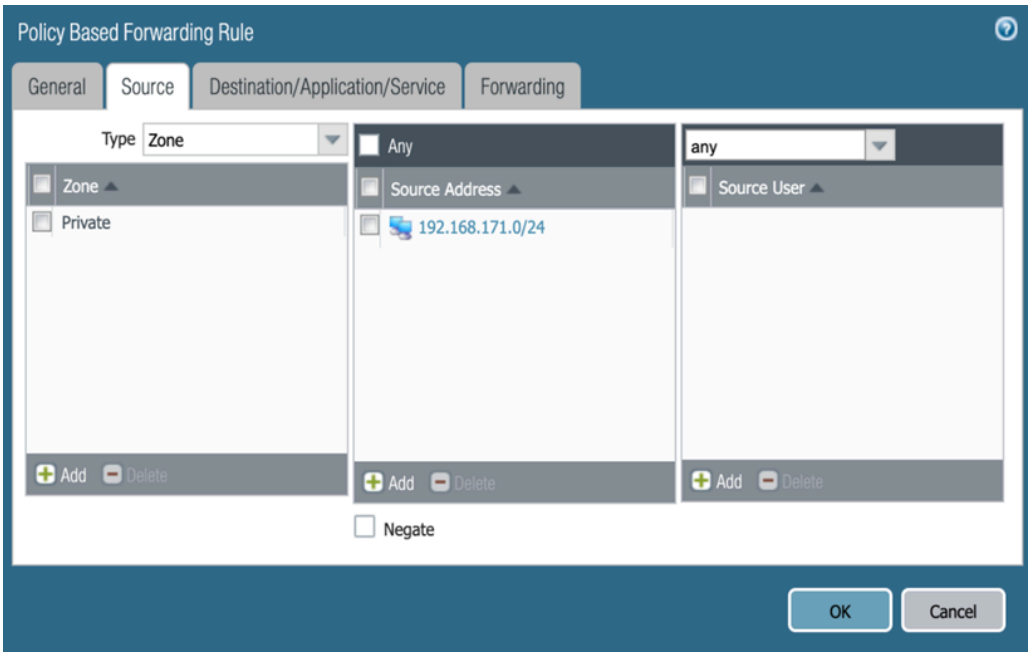
1. Wählen Sie **Richtlinien** > **Richtlinienbasierte Weiterleitung** aus, um eine PBF-Richtlinienregel **hinzuzufügen**.



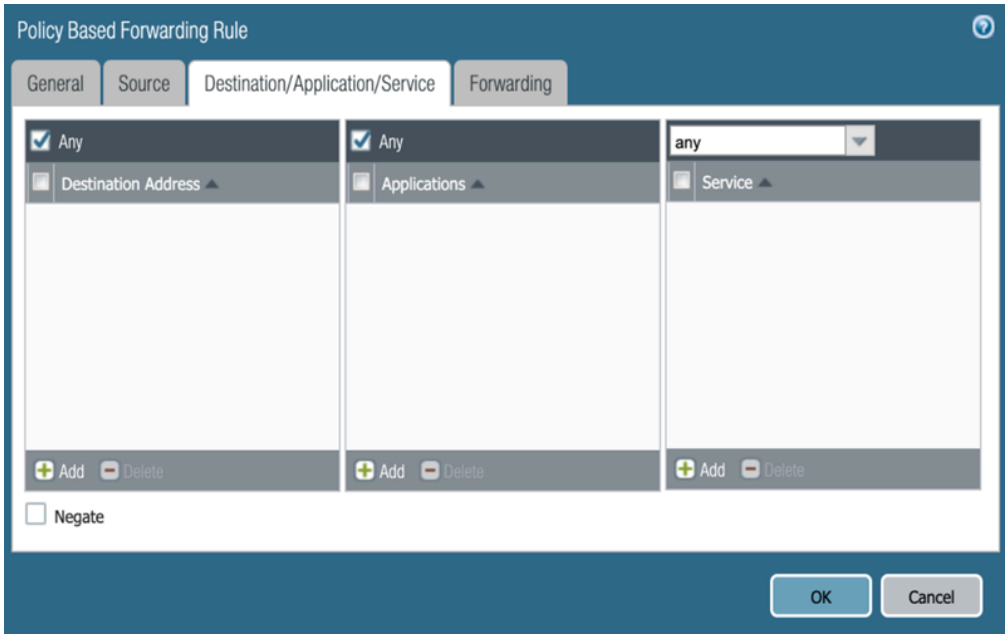

2. Wählen Sie **Quelle** aus, um eine **Quelladresse** zur Verwendung für die richtlinienbasierte Weiterleitung **hinzuzufügen**.

   In diesem Fall möchten Sie eine richtlinienbasierte Weiterleitung für „tunnel.1“ erstellen und geben daher das Subnetz 192.168.171.0/24 ein.

 ©2025 Palo Alto Networks, Inc.




3. Wählen Sie **Ziel/Anwendung/Dienst** sowie eine **beliebige** Zieladresse und eine **beliebige** Anwendung aus.

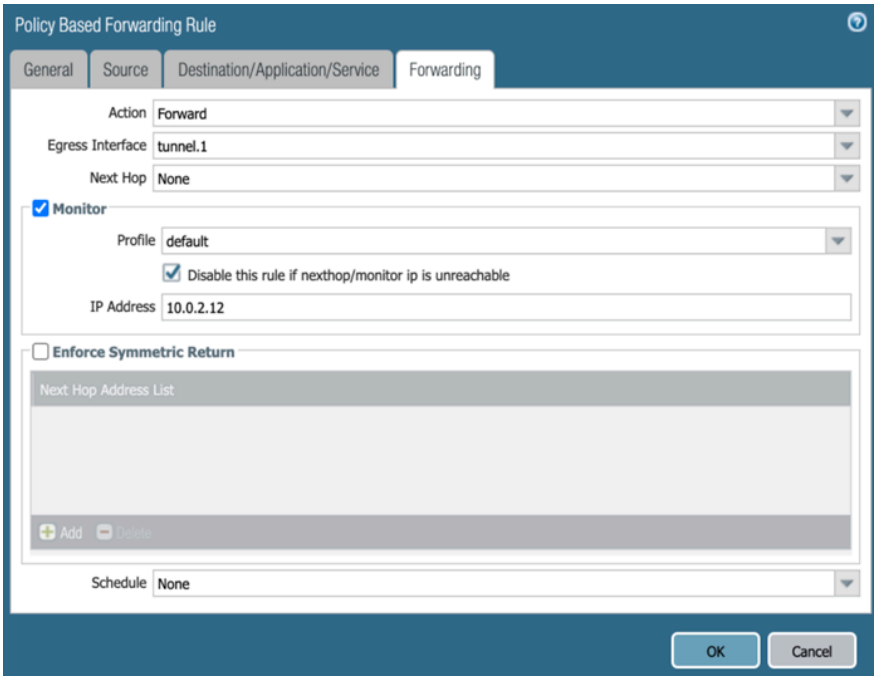



4. Wählen Sie **Weiterleitung** aus und geben Sie die folgenden Parameter an. Klicken Sie anschließend auf **OK**:
   - Wählen Sie für **Aktion** die Option **Weiterleiten** aus.
   - Wählen Sie eine **Ausgangsschnittstelle** des Tunnels aus, an die Sie das IP-Subnetz weiterleiten möchten (in diesem Fall**tunnel.1**).
   - Wählen Sie **Überwachen** und die folgenden Überwachungsprofile aus:
     - Wählen Sie das **Profil Standard** aus.

 ©2025 Palo Alto Networks, Inc.

- Aktivieren Sie **Diese Regel deaktivieren, wenn Nexthop/Überwachungs-IP nicht erreichbar ist**.
- Geben Sie als **IP-Adresse** die **EBGP-Router-Adresse** der Dienstverbindung an (**Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Dienstverbindung** > **EBGP-Router**).

Durch Aktivieren der Überwachung und Auswählen der EBGP-Router-Adresse der Dienstverbindung wird sichergestellt, dass die Firewall bei einem Ausfall von „tunnel.1“ die PBF-Richtlinie deaktiviert und den Datenverkehr über den Tunnel umleitet, der noch aktiv ist („tunnel.2“).




5. Wiederholen Sie Schritt 6, wobei die **EBGP-Router**-Adresse von Dienstverbindung 1 durch die **EBGP-Router**-Adresse von Dienstverbindung 2 und das Subnetz von „tunnel.1“ durch das Subnetz von „tunnel.2“ ersetzt wird.

   Am Ende sind zwei PBF-Richtlinien vorhanden: eine für „tunnel.1“ und eine für „tunnel.2“.

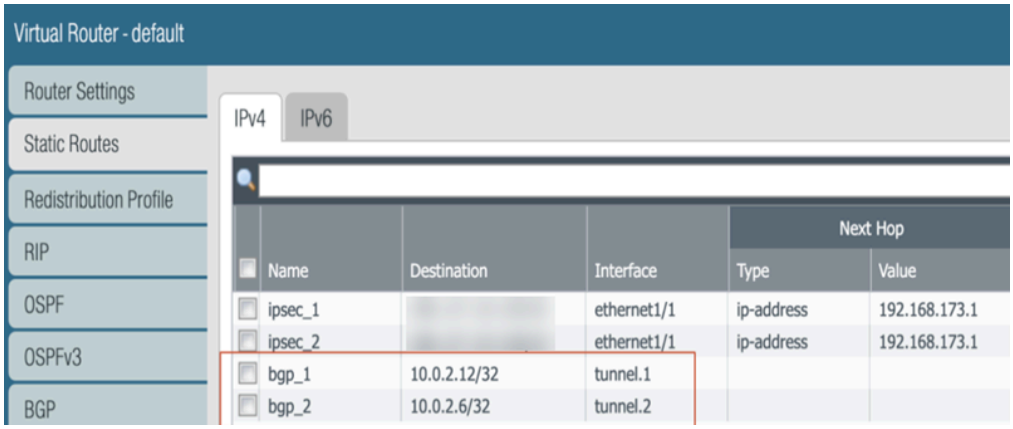



**STEP 7 |** Wählen Sie **Netzwerk** > **Virtuelle Router** > **Statische Routen** aus und weisen Sie die **EBGP-Router**-Adresse von Dienstverbindung 1 der **Schnittstelle** von **tunnel.1** zu. Weisen Sie anschließend die **EBGP-Router**-Adresse von Dienstverbindung 2 der **Schnittstelle** von **tunnel.2** zu.

Durch die Eingabe spezifischer statischer Routen für jede der BGP-Adressen des Routers wird sichergestellt, dass die Tunnelüberwachung ordnungsgemäß funktioniert, da die IP-Adresse

 ©2025 Palo Alto Networks, Inc.

des EBGP-Routers von Dienstverbindung 1 nur über „tunnel.1“ und die IP-Adresse des EBGP-Routers von Dienstverbindung 2 nur über „tunnel.2“ erreichbar ist.




## Konfigurieren von mehr als zwei Dienstverbindungen zum Standort einer Zentrale oder eines Rechenzentrums

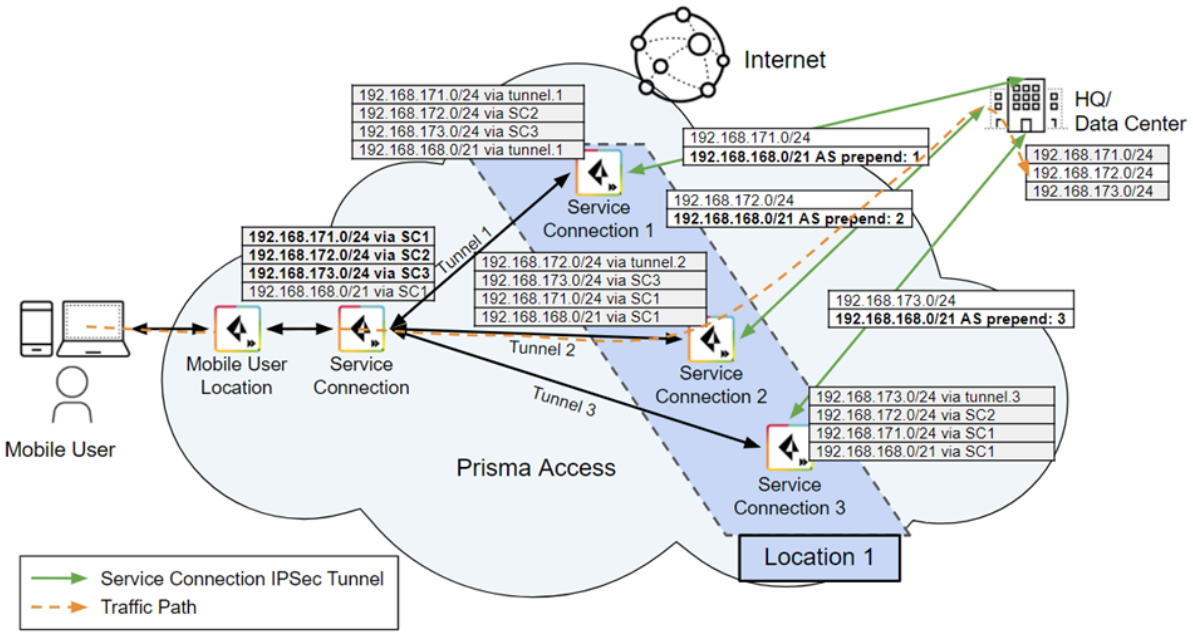
| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Wenn Sie zwei Tunnel für eine Dienstverbindung mit hoher Bandbreite verwenden, steht im Falle eines Tunnelausfalls nur noch ein Datenverkehrspfad zur Verfügung, was die Konfiguration eines Failover-Pfads vereinfacht. Wenn Sie mehr als zwei Verbindungen für eine Verbindung mit hoher Bandbreite verwenden, müssen Sie zusätzliche Konfigurationsmaßnahmen durchführen, um beim Tunnel-Failover ein einheitliches Verhalten sicherzustellen.

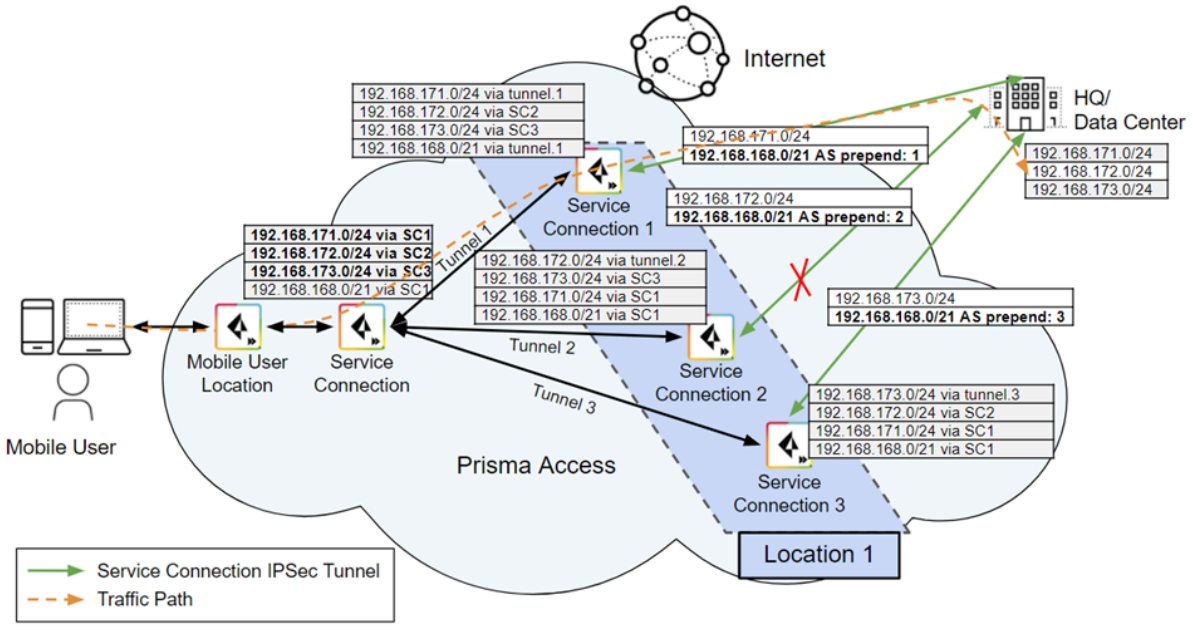
Da Sie ein zusammengefasstes Subnetz für den Tunnel-Failover verwenden, müssen Sie explizit angeben, welcher Dienstverbindungstunnel verwendet werden soll, wenn ein Failover auftritt. Da beim BGP-Routing die geringste Anzahl von AS-PATHs für eine Route ausgewählt wird, können Sie den Routen die AS-PATH-Angaben voranstellen, damit BGP im Falle eines Failovers einen Tunnel bevorzugt.

Das folgende Beispiel zeigt Routingtabellen für eine Dienstverbindung mit hoher Bandbreite, die drei Dienstverbindungen benutzt. Sind alle drei Tunnel aktiv, nutzt Prisma Access die spezifischeren Routen, um die Subnetze am Standort der Zentrale oder des Rechenzentrums zu erreichen. Da der Benutzer auf eine Ressource im Subnetz 192.168.172.0/24 zugreift, überprüft die dem mobilen Benutzer nächstgelegene Dienstverbindung die zugehörige Routingtabelle und wählt Tunnel 2 als Pfad zur Rechenzentrumsressource aus.

 ©2025 Palo Alto Networks, Inc.




Wenn Tunnel 2 ausfällt, ist die spezifischere Route zur Ressource im Subnetz 192.168.172.0/24 nicht verfügbar, sodass die Dienstverbindung, die dem Benutzer am nächsten liegt, das zusammengefasste Subnetz 192.168.168.0/21 verwendet. Sie haben für die Dienstverbindung 1 nur eine AS-PATH-Voranstellung konfiguriert; Prisma Access wählt daher Tunnel 1 als Failover-Pfad aus, da er weniger AS-PATH-Voranstellungen aufweist.

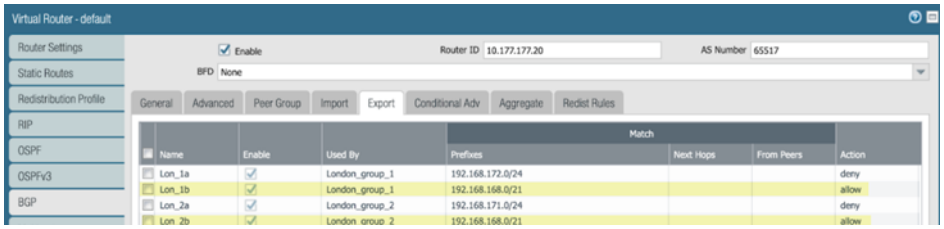



Führen Sie die folgenden Schritte aus, um Routen eine Voranstellung hinzuzufügen, wenn Sie eine Firewall der nächsten Generation als CPE verwenden.

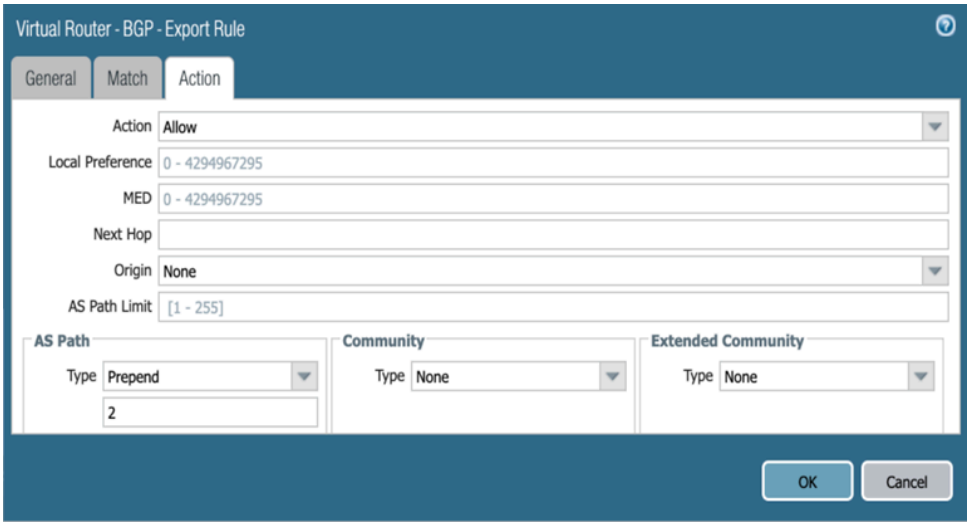
**STEP 1 |** Wählen Sie die BGP-Exportprofile des virtuellen Routers (**Netzwerk** > **Virtuelle Router** > **BGP** > **Exportieren**) aus.

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Ändern Sie die Exportregel, die Sie beim Konfigurieren der Dienstverbindungen mit der **Aktion Zulassen** erstellt haben.




**STEP 3 |** Fügen Sie im Bereich für den AS-Pfad eine **Voranstellung** hinzu und geben Sie dann die Anzahl der hinzuzufügenden AS-PATH-Voranstellungen ein (in diesem Beispiel **2**).




**STEP 4 |** Wiederholen Sie die Schritte 2 und 3 für jede Exportregel, für die als **Aktion Zulassen** angegeben wurde, und fügen Sie AS-PATH-Voranstellungen hinzu, die den von Ihnen für Ihre Bereitstellung geplanten Failover-Szenarien entsprechen.

In den in diesem Abschnitt verwendeten Beispielen fügen Sie für den Tunnel zum Standort des Rechenzentrums für die Dienstverbindung 1 (Tunnel.1) die AS-PATH-Voranstellung 1 hinzu. Für den Tunnel, der für die Dienstverbindung 2 (Tunnel.2) verwendet wird, wird die AS-PATH-Voranstellung 2 hinzugefügt. Für den Tunnel, der für die Dienstverbindung 3 (Tunnel.3) verwendet wird, wird die AS-PATH-Voranstellung 3 hinzugefügt.

Nach Abschluss dieser Arbeitsschritte werden in diesem Beispiel im Falle eines Failovers die folgenden Tunnel verwendet:

- Fällt tunnel.2 oder tunnel.3 aus, wird der Datenverkehr für das entsprechende Subnetz von tunnel.1 übernommen, der über den kürzesten mitgeteilten AS-PATH verfügt.
- Fällt tunnel.1 aus, wird der Datenverkehr für sein Subnetz (192.168.171.0/24) von tunnel.2 übernommen, der über den kürzesten mitgeteilten AS-PATH verfügt.

**STEP 5 |** Fügen Sie Backup-PBF- oder richtlinienbasierte Routingrichtlinien hinzu, um bei Auftreten eines Tunnelausfalls den symmetrischen Rückkehrdatenverkehr zu gewährleisten.

Während die AS-PATH-Voranstellungen sicherstellen, dass der Datenverkehr von Prisma Access zum Rechenzentrum im Falle eines Failovers einen bestimmten Tunnel nutzt, müssen Sie auch eine symmetrische Rückkehr für den Datenverkehr vom Rechenzentrum zu Prisma

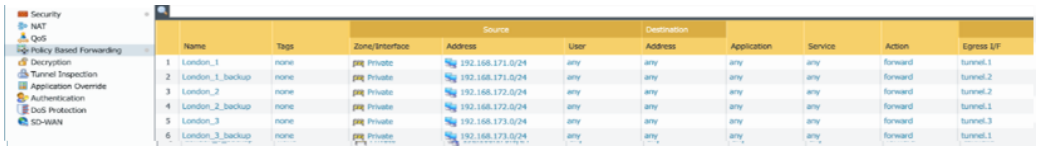
 ©2025 Palo Alto Networks, Inc.

Access sicherstellen. Verwenden Sie PBF- oder richtlinienbasierte Routingrichtlinien, die die Failover-Szenarien widerspiegeln, die Sie für den Datenverkehr von Prisma Access zum Rechenzentrum erstellt haben, um einen symmetrischen Rückkehrdatenverkehr sicherzustellen.

In diesem Beispiel erstellen Sie für den tunnel.1-Datenverkehr mit der Quell-IP 192.168.171.0/24 eine Backup-PBF-Richtlinie, die im Falle eines Failovers den Rückkehrdatenverkehr zwingend über tunnel.2 ausführt. Die erste PBF-Regel wird deaktiviert, wenn die IP-Adresse für die Tunnelüberwachung nicht erreichbar ist. Im Falle eines Failovers wertet das CPE (in diesem Beispiel eine Firewall der nächsten Generation) die nächste Regel in der Liste aus.




Sie fügen dann weitere PBF-Regeln hinzu, die den Failover-Szenarien entsprechen, die Sie für den Datenverkehr von Prisma Access zum Rechenzentrum erstellt haben.




# Benutzer-ID- und Geräte-ID-Zuordnung für Dienstverbindungen mit Quell-NAT beibehalten

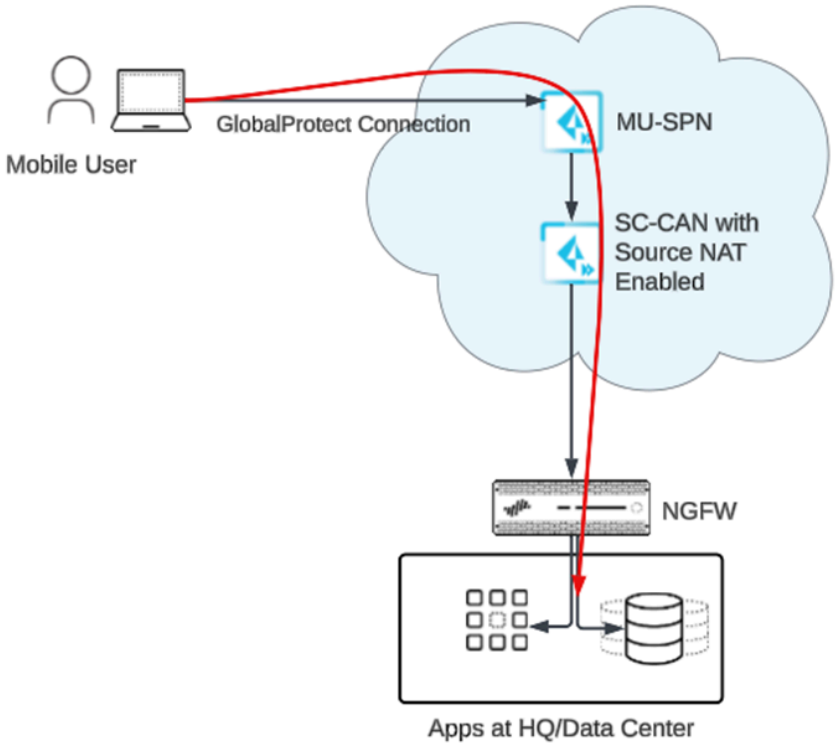
| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz<br>❑ Firewall der nächsten Generation (NGFW) mit einer Mindestversion von PAN-OS 11.2<br>❑ Diese Funktionalität verwendet Geneve-Kapselung. Stellen Sie sicher, dass alle nachgelagerten Firewalls zusätzlich zu den NGFWs mit PAN-OS 11.2 oder höher in der Lage sind, die Geneve-Kapselung zu entkapseln.<br>Diese Funktionalität wird beim Zugriff mit dynamischen Rechten nicht unterstützt. |

In Prisma Access verwenden Sie Dienstverbindungen, auch als Service Connection – Corporate Access Nodes (SC-CANs) bezeichnet, um private Apps zu sichern. Um den Zugriff auf die Apps basierend auf Benutzer-ID oder Geräte-ID einzuschränken, können Sie eine Firewall der nächsten Generation (Next-Generation Firewall, NGFW) im Rechenzentrum oder in der Zentrale bereitstellen, in dem bzw. der sich die privaten Apps befinden. Anschließend konfigurieren Sie Richtlinienregeln auf der NGFW basierend auf Benutzer-ID-Zuordnung, Geräte-ID-Zuordnung oder beidem.

 ©2025 Palo Alto Networks, Inc.

Um diese Regeln verwenden zu können, muss die NGFW die Zuordnung der Benutzer-ID oder Geräte-ID vom SC-CAN erhalten. Wenn Benutzer jedoch mithilfe von GlobalProtect eine Verbindung mit Prisma Access herstellen und der SC-CAN die **Quell-NAT des Datenverkehrs** aktiviert hat, kann die NGFW diese Zuordnung nicht erhalten. Wenn die **Quell-NAT des Datenverkehrs** auf dem SC-CAN aktiviert ist, führt sie NAT auf dem IP-Adresspool für mobile Benutzer durch und kündigt diese IP-Adressen nicht im Rechenzentrum oder am Standort der Zentrale an.

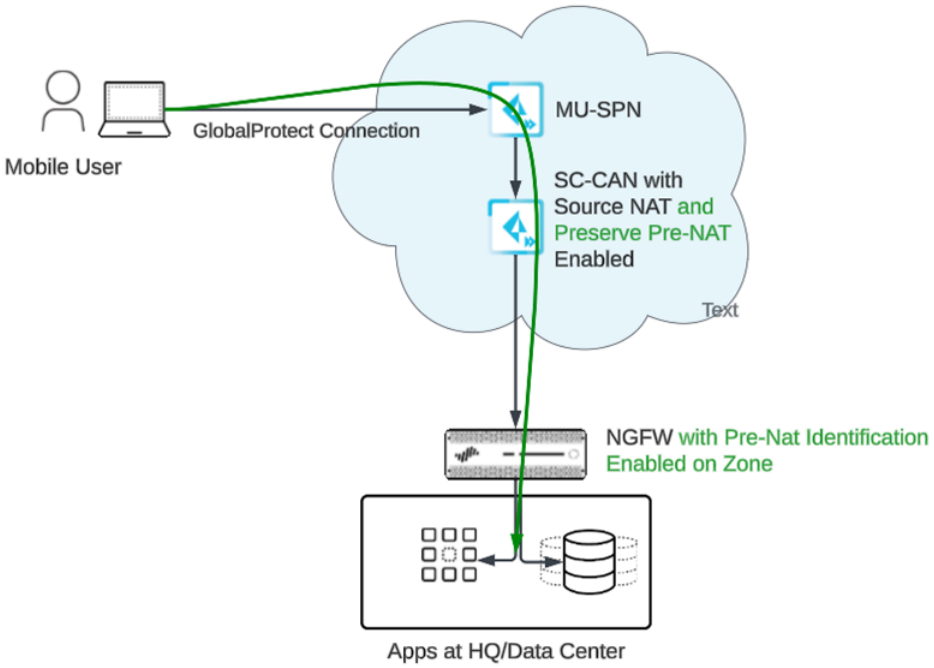
In diesem Fall kann die NGFW die Benutzer- oder Geräte-ID der GlobalProtect-Benutzer nicht abrufen, was bedeutet, dass Sie Richtlinien basierend auf Benutzer- oder Geräte-ID nicht durchsetzen können.




Um sicherzustellen, dass Ihr Netzwerk die Benutzer-ID- oder Geräte-ID-Zuordnung an die Zentrale oder das Rechenzentrum verteilt, führen Sie das in einem der folgenden Abschnitte aufgeführte Verfahren aus, mit dem die NGFW Sicherheitsrichtlinienregeln auf der Grundlage der Benutzer-ID-Zuordnung durchsetzen kann, die sie von GlobalProtect übernimmt.

*Voraussetzung ist eine NGFW mit einer PAN-OS-Mindestversion von 11.2. Die Dienstverbindung muss nicht auf der NGFW enden, sondern kann auf einem anderen IPSec-fähigen Gerät enden, solange sich die NGFW hinter dem Punkt befindet, an dem die Dienstverbindung endet.*

 ©2025 Palo Alto Networks, Inc.




- Strata Cloud Manager
- Panorama

## Benutzer-ID- und Geräte-ID-Zuordnung für Dienstverbindungen mit Quell-NAT (Strata Cloud Manager) beibehalten

Gehen Sie wie folgt vor, damit Prisma Access in Prisma Access (Managed by Strata Cloud Manager) Benutzer-ID-Zuordnungen von GlobalProtect-Benutzern an eine NGFW in der Zentrale oder im Rechenzentrum verteilen kann.

Bei dieser Vorgehensweise wird vorausgesetzt, dass Sie die folgende Netzwerkkonfiguration eingerichtet haben:

- Sie haben die **Quell-NAT des Datenverkehrs** auf der Dienstverbindung aktiviert.
- Sie haben eine NGFW in der Zentrale oder im Rechenzentrum bereitgestellt, in dem sich die privaten Apps befinden.
- Sie haben Sicherheitsrichtlinienregeln für Prisma Access auf der NGFW basierend auf Zonen angewendet, die Sie in der NGFW erstellt haben.

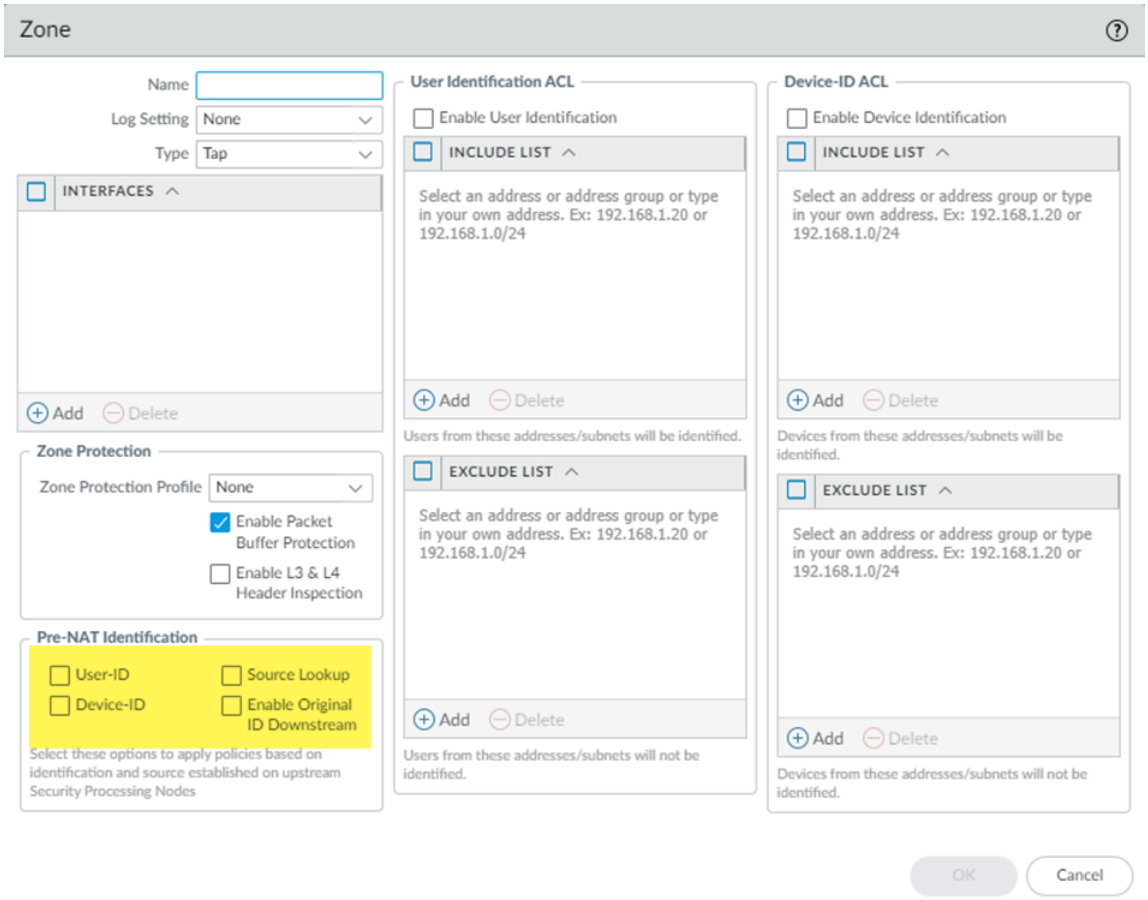
 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** Geben Sie Parameter für die Identifikation vor der Netzwerkadressübersetzung (Pre-NAT-Identifikation) auf der NGFW ein.

1. Melden Sie sich bei der NGFW, beim SCM oder bei der Panorama-Instanz an, von der die NGFW verwaltet wird, und wählen Sie anschließend **Netzwerk** > **Zonen** aus.
2. Sie müssen eine Zone **hinzufügen** oder eine bestehende Zone auswählen.
3. Wählen Sie einen oder mehrere Parameter für die **Pre-NAT-Identifikation** aus:
   - **Benutzer-ID** – Behält die Benutzer-ID-Zuordnung für mobile Benutzer bei, die vor der NAT-Verarbeitung der IP-Adressen verwendet wurde. Aktivieren Sie diese Einstellung, wenn Sie Benutzer-IDs in Sicherheitsrichtlinienregeln verwenden.
   - **Geräte-ID** – Behält die Geräte-ID-Zuordnung für mobile Benutzer bei, die vor der NAT-Verarbeitung der IP-Adressen verwendet wurde. Aktivieren Sie diese Einstellung, wenn Sie die Geräte-ID in Sicherheitsrichtlinienregeln verwenden.
   - **Quell-Abfrage** – Ermöglicht den Abgleich der ursprünglichen Quell-IP-Adresse, die von GlobalProtect empfangen wurde. Wenn Sie die Quell-Abfrage in QoS- oder richtlinienbasierten Weiterleitungsrichtlinien verwenden, basiert der Quell-IP-Vergleich auf der Quell-IP-Adresse vor der NAT-Verarbeitung. Wenn beispielsweise eine Sicherheitsrichtlinie vorlag, die eine Quell-IP-Adresse von 1.1.1.1 und eine beliebige Ziel-IP-Adresse (Any) zuließ, wird 1.1.1.1 mit der Pre-NAT-Quell-IP-Adresse im Paket-Header verglichen.
   - **Original-ID für nachgelagerte NGFW aktivieren** – Wenn zwei NGFWs hintereinander vorliegen, geben Sie diese Option an, damit die erste NGFW die Informationen vor der NAT an die zweite NGFW sendet, nachdem die erste NGFW den Datenverkehr

 ©2025 Palo Alto Networks, Inc.

überprüft und Richtlinien darauf angewendet hat. Dies ist die Standardkonfiguration auf SC-CANs.




4. Klicken Sie auf **OK** und **Commit**, um Ihre Änderungen festzuschreiben.

**STEP 2 |** Erstellen Sie eine CLI-Sitzung (Command Line Interface) mit der NGFW und geben Sie im Konfigurationsmodus den folgenden Befehl ein:

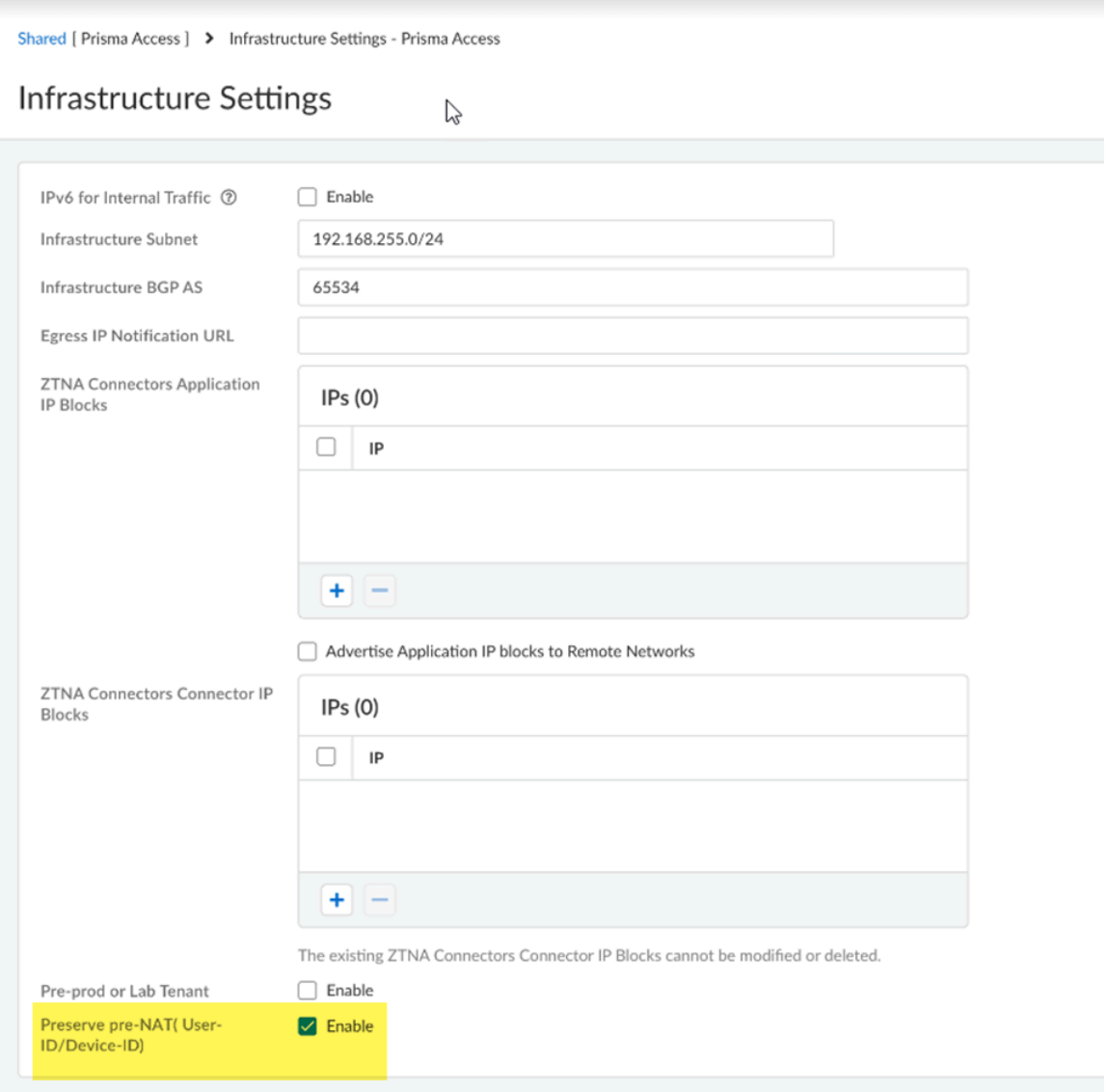
```
set deviceconfig setting preserve-prenat-feature yes
```

Wenn Sie diese Funktion in Zukunft deaktivieren müssen, geben Sie den Befehl `set deviceconfig setting preserve-prenat-feature no` ein.

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Aktivieren Sie Pre-NAT-Einstellungen in Strata Cloud Manager.

1. Wählen Sie **Workflows** > **Einrichtung Prisma Access** > **Prisma Access** > **Infrastruktureinstellungen** aus.
2. **Aktivieren** Sie **Pre-NAT (Benutzer-ID/Geräte-ID) beibehalten**.




3. Wählen Sie **Konfiguration übertragen** aus, um Ihre Änderungen zu speichern.

## Benutzer-ID- und Geräte-ID-Zuordnung für Dienstverbindungen mit Quell-NAT (Panorama) beibehalten

Gehen Sie wie folgt vor, damit Prisma Access in Prisma Access (Managed by Panorama) Benutzer-ID-Zuordnungen von GlobalProtect-Benutzern an eine NGFW in der Zentrale oder im Rechenzentrum verteilen kann.

Bei dieser Vorgehensweise wird vorausgesetzt, dass Sie die folgende Netzwerkkonfiguration eingerichtet haben:

- Sie haben die **Quell-NAT des Datenverkehrs** auf der Dienstverbindung aktiviert.

 ©2025 Palo Alto Networks, Inc.

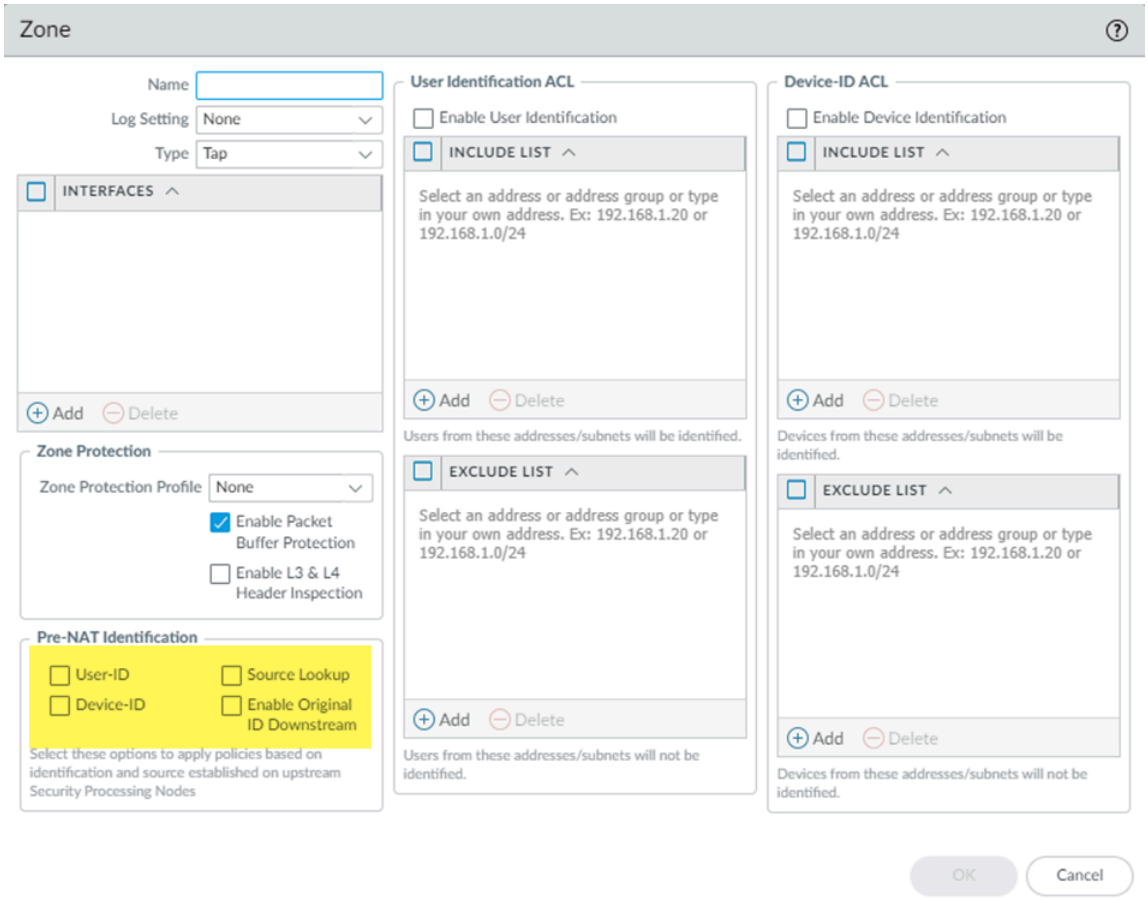
- Sie haben eine NGFW in der Zentrale oder im Rechenzentrum bereitgestellt, in dem sich die privaten Apps befinden.
- Sie haben Sicherheitsrichtlinienregeln für Prisma Access auf der NGFW basierend auf Zonen angewendet, die Sie in der NGFW erstellt haben.

**STEP 1 |** Geben Sie Parameter für die Identifikation vor der Netzwerkadressübersetzung (Pre-NAT-Identifikation) auf der NGFW ein.

1. Melden Sie sich bei der NGFW, beim SCM oder bei der Panorama-Instanz an, von der die NGFW verwaltet wird, und wählen Sie anschließend **Netzwerk** > **Zonen** aus.
2. Sie müssen eine Zone **hinzufügen** oder eine bestehende Zone auswählen.
3. Wählen Sie einen oder mehrere Parameter für die **Pre-NAT-Identifikation** aus:
   - **Benutzer-ID** – Behält die Benutzer-ID-Zuordnung für mobile Benutzer bei, die vor der NAT-Verarbeitung der IP-Adressen verwendet wurde. Aktivieren Sie diese Einstellung, wenn Sie Benutzer-IDs in Sicherheitsrichtlinienregeln verwenden.
   - **Geräte-ID** – Behält die Geräte-ID-Zuordnung für mobile Benutzer bei, die vor der NAT-Verarbeitung der IP-Adressen verwendet wurde. Aktivieren Sie diese Einstellung, wenn Sie die Geräte-ID in Sicherheitsrichtlinienregeln verwenden.
   - **Quell-Abfrage** – Ermöglicht den Abgleich der ursprünglichen Quell-IP-Adresse, die von GlobalProtect empfangen wurde. Wenn Sie die Quell-Abfrage in QoS- oder richtlinienbasierten Weiterleitungsrichtlinien verwenden, basiert der Quell-IP-Vergleich auf der Quell-IP-Adresse vor der NAT-Verarbeitung. Wenn beispielsweise eine Sicherheitsrichtlinie vorlag, die eine Quell-IP-Adresse von 1.1.1.1 und eine beliebige Ziel-IP-Adresse (Any) zuließ, wird 1.1.1.1 mit der Pre-NAT-Quell-IP-Adresse im Paket-Header verglichen.
   - **Original-ID für nachgelagerte NGFW aktivieren** – Wenn zwei NGFWs hintereinander vorliegen, geben Sie diese Option an, damit die erste NGFW die Informationen vor der NAT an die zweite NGFW sendet, nachdem die erste NGFW den Datenverkehr

 ©2025 Palo Alto Networks, Inc.

überprüft und Richtlinien darauf angewendet hat. Dies ist die Standardkonfiguration auf SC-CANs.




4. Klicken Sie auf **OK** und **Commit**, um Ihre Änderungen festzuschreiben.

**STEP 2 |** Erstellen Sie eine CLI-Sitzung (Command Line Interface) mit der NGFW und geben Sie im Konfigurationsmodus den folgenden Befehl ein:

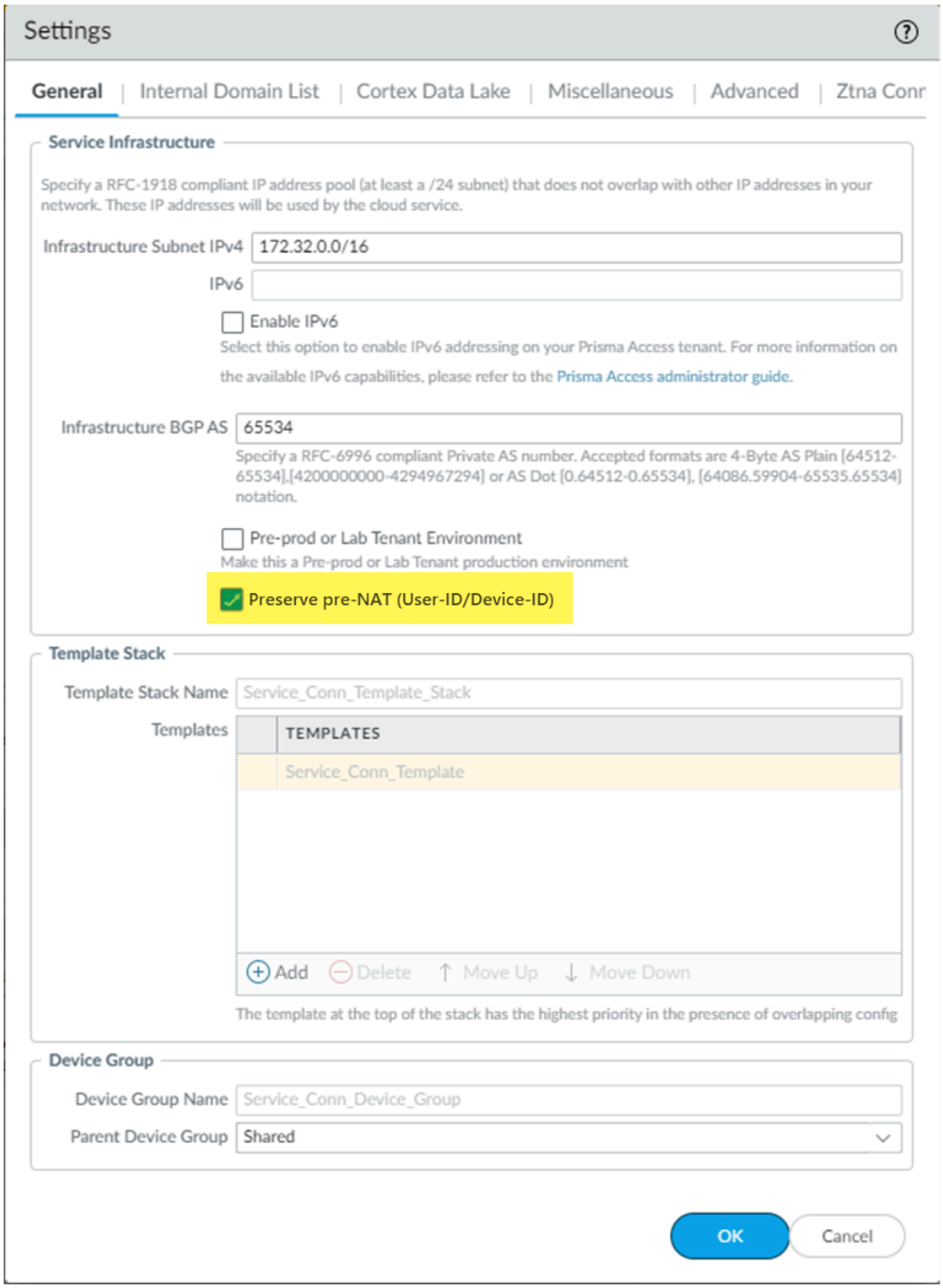
```
set deviceconfig setting preserve-prenat-feature yes
```

Wenn Sie diese Funktion in Zukunft deaktivieren müssen, geben Sie den Befehl `set deviceconfig setting preserve-prenat-feature no` ein.

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Aktivieren Sie Pre-NAT-Einstellungen in der Panorama-Instanz, von der Prisma Access verwaltet wird.

1. Gehen Sie zu **Panorama** > **Cloud Services** > **Konfiguration** > **Diensteinrichtung** und klicken Sie auf das Zahnrad, um die **Einstellungen** zu bearbeiten.
2. Wählen Sie **Pre-NAT (Benutzer-ID/Geräte-ID) beibehalten** aus.




3. Führen Sie für Ihre Änderungen die Aktion **Commit und Push** aus.

 ©2025 Palo Alto Networks, Inc.

# Erweiterte Bereitstellungen von Prisma Access Mobile Benutzer – GlobalProtect

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

In den folgenden Abschnitten sind die erweiterten Bereitstellungen aufgeführt, die in einer Bereitstellung des Typs „Mobile Benutzer – GlobalProtect“ verfügbar sind:

- Unterstützung der Registrierung von dynamischem DNS für „Mobile Benutzer – GlobalProtect“
- Kompromittierte Geräte in einer GlobalProtect-Bereitstellung von Prisma Access identifizieren und unter Quarantäne stellen
- IPv6-Datenverkehr in Bereitstellungen von „Mobile Benutzer – GlobalProtect“ gezielt umleiten oder blockieren
- HIP-Informationen mit Prisma Access weitergeben
- Anzeigen von HIP-Berichten
- Unterstützung für Gzip-Codierung in clientlosem VPN
- Replikation des Datenverkehrs in Prisma Access

## Mehrere Portale in Prisma Access konfigurieren

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz<br>❑ Mindestens erforderliche GlobalProtect-Clientversion: 6.1 (Nur Windows und macOS) |

Sie können zwei Portale basierend auf Portnummern im selben Prisma Access-Mandanten konfigurieren, wobei jedes Portal eine andere Authentifizierungsmethode unterstützt. Aktivieren Sie diese Funktion, um mobile Benutzer von einer Authentifizierungsmethode auf eine andere umzustellen, ohne dass hierzu ein neuer Prisma Access-Mandant erstellt werden muss. Diese Konfiguration ermöglicht eine größere Flexibilität bei der Authentifizierung, da Sie Benutzer schrittweise auf die cloudbasierte Authentifizierung umstellen können, ohne dass dazu eine separate Prisma Access-Instanz erforderlich ist.

Prisma Access mit mehreren GlobalProtect-Portalen verwendet für jedes Portal innerhalb desselben Mandanten eine andere Portnummer. Konfigurieren Sie das erste GlobalProtect-Portal über den Standardport 443. Wenn Sie die Funktion für mehrere Portale aktivieren, konfiguriert Prisma Access ein zweites GlobalProtect-Portal mit dem alternativen Port 8443 und ermöglicht mit demselben FQDN, der auch beim ersten Portal verwendet wurde, Verbindungen zu dem zweiten Portal. Die Funktion zur Nutzung mehrerer Portale unterstützt nur zwei Portale pro FQDN.

 ©2025 Palo Alto Networks, Inc.

Wenn ein Benutzer über den Port 443 eine Verbindung zum Portal herstellt, wird der Datenverkehr ohne Änderung der IP-Adresse an das erste Authentifizierungsportal gesendet. Dieser Ablauf wird von Konfigurationen ohne die GlobalProtect-Funktion für mehrere Portale unverändert übernommen. Wenn ein Benutzer eine Verbindung über den Port 8443 herstellt, trifft der Datenverkehr stattdessen auf eine NAT-Regel des Ziels. Dies führt den Benutzer zum zweiten Authentifizierungsportal unter einer anderen IP-Adresse. Nach der Authentifizierung bei jedem der Portale wird der Benutzer an das Gateway mit dem Cookie für die Authentifizierungsüberschreibung weitergeleitet. Diese Funktion hängt von den Cookie-Einstellungen für die Authentifizierungsüberschreibung ab und ist sowohl für Portale als auch für Gateways aktiviert.

Die folgende Tabelle beschreibt die GlobalProtect-Unterstützung mehrerer Portale mit Kombinationen von Authentifizierungsmethoden und Zertifikaten, die die Legacy-Authentifizierung (wie RADIUS oder LDAP) auf dem primären Portal und die Cloud-Authentifizierung (wie SAML oder SAML mit CAS) auf dem sekundären Portal verwenden.

| Benutzerauthentifizierung auf dem primären Portal | Benutzerauthentifizierung auf dem sekundären Portal | Optionen für die Verbindungsmethode |
|---|---|---|
| Legacy, Kein Zertifikat | Cloud, Kein Zertifikat | Benutzeranmeldung (immer aktiviert, On-Demand) |
| Legacy, <auth profile selection> UND Clientzertifikat<br>Hinweis: Das Zertifikatsprofil muss dasselbe sein. | Cloud, <auth profile selection> UND Clientzertifikat<br>Hinweis: Das Zertifikatsprofil muss dasselbe sein. | Benutzeranmeldung (immer aktiviert, On-Demand)<br>Voranmeldung (immer aktiviert, On-Demand) |
| Legacy, Kein Zertifikat | Cloud, <auth profile selection> ODER Clientzertifikat | Benutzeranmeldung (immer aktiviert, On-Demand) |
| Legacy, <auth profile selection> ODER Clientzertifikat<br>Mehrere Portalkonfigurationen unterstützen keine Clients, die nur das Clientzertifikat zur Authentifizierung verwenden | Cloud, Kein Zertifikat | Benutzeranmeldung (immer aktiviert, On-Demand)<br>Voranmeldung (immer aktiviert, On-Demand), wenn Zertifikat |
| Legacy, <auth profile selection> ODER Clientzertifikat<br>Mehrere Portalkonfigurationen unterstützen keine Clients, | Cloud, <auth profile selection> ODER Clientzertifikat<br>Mehrere Portalkonfigurationen unterstützen keine Clients, | Benutzeranmeldung (immer aktiviert, On-Demand)<br>Voranmeldung (immer aktiviert, On-Demand), wenn Zertifikat |

 ©2025 Palo Alto Networks, Inc.

| Benutzerauthentifizierung auf dem primären Portal | Benutzerauthentifizierung auf dem sekundären Portal | Optionen für die Verbindungsmethode |
|---|---|---|
| die nur das Clientzertifikat zur Authentifizierung verwenden | die nur das Clientzertifikat zur Authentifizierung verwenden | |

Stellen Sie Folgendes sicher, bevor Sie mehrere Portale konfigurieren:

- Beide Portale verfügen über die gleichen oder aber über keine Zertifikatprofile
- Die den Authentifizierungsprofilen zugeordnete Zulassungsliste sollte identisch sein
- Wenn Sie ein Cookie zur Authentifizierungsüberschreibung auf dem Portal akzeptieren, stellen Sie sicher, dass die Cookie-Lebensdauer sowohl auf dem Portal als auch auf dem Gateway gleich ist
- Mehrere Portalkonfigurationen bieten keine Unterstützung für die ausschließliche Benutzung der Clientauthentifizierung auf Zertifikatsbasis

> Clientloses VPN *wird in einer Bereitstellung mit mehreren Portalen nicht zur Verwendung auf dem sekundären Portal unterstützt. Clientloses VPN funktioniert jedoch auf dem primären Portal mit Ihrer vorhandenen Authentifizierungsmethode.*

- Strata Cloud Manager
- Panorama

## Konfigurieren mehrerer Portale in Prisma Access (Strata Cloud Manager)

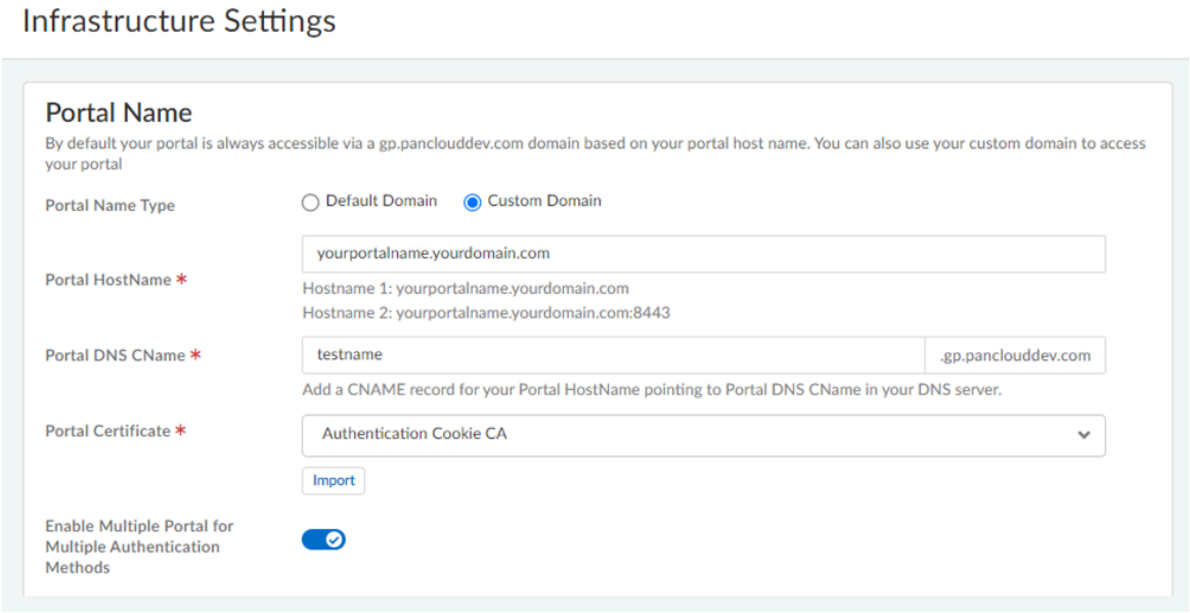
**STEP 1 |** Wenden Sie sich an den Support von Palo Alto Networks, um diese Funktionalität aktivieren zu lassen.

**STEP 2 |** Konfigurieren Sie einen mobilen Benutzer und die zugehörige Authentifizierungsmethode.

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Aktivieren Sie mehrere Portale für dasselbe Gateway.

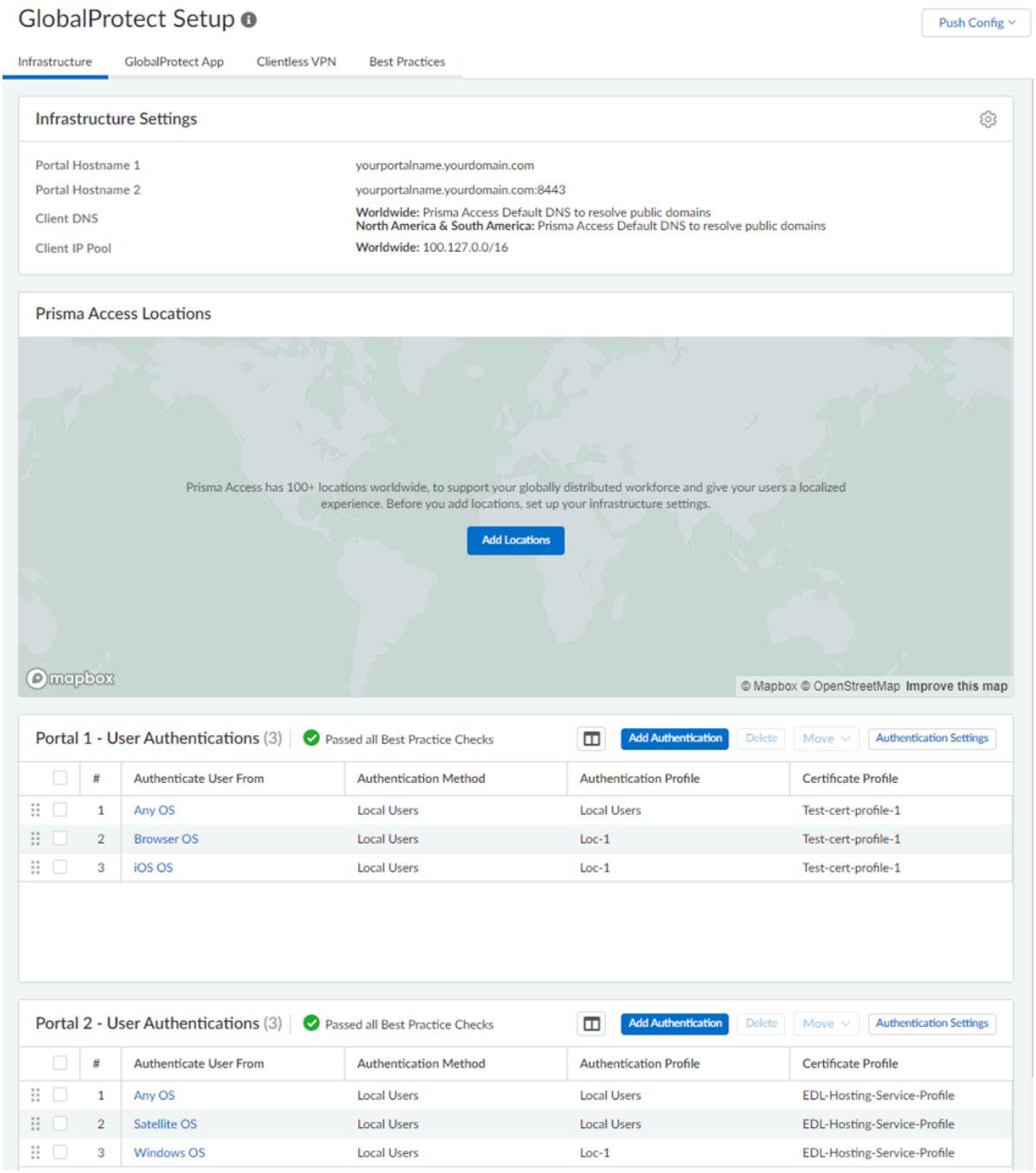
1. Wählen Sie **Workflows** > **Prisma Access Einrichtung** > **GlobalProtect** > **GlobalProtect-Einrichtung** > **Infrastruktur** aus.
2. Bearbeiten Sie die **Infrastruktureinstellungen**.
3. **Aktivieren Sie mehrere Portale für mehrere Authentifizierungsmethoden**.




Das neue Portal wird für den Port 8443 für denselben Mandanten angezeigt. Dieses Portal übernimmt die Konfigurationseinstellungen vom ursprünglichen Port, nämlich Port 443.

 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** Bearbeiten Sie die Portalkonfigurationen, um die Authentifizierungseinstellungen zu aktualisieren.

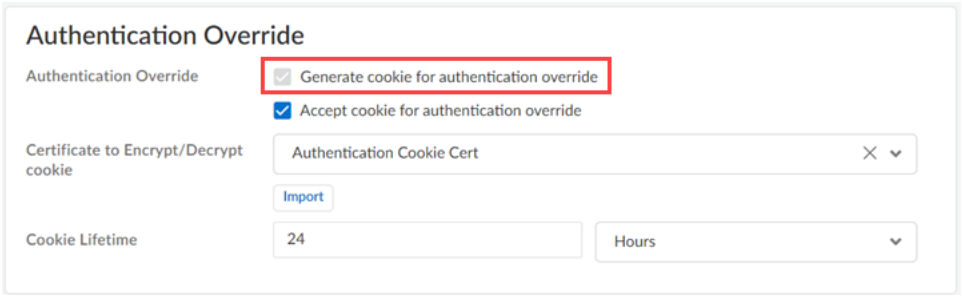



Sie können nur die **Authentifizierungseinstellungen** des Portals und die Authentifizierungseinstellungen für das **Zertifikatprofil** bearbeiten.

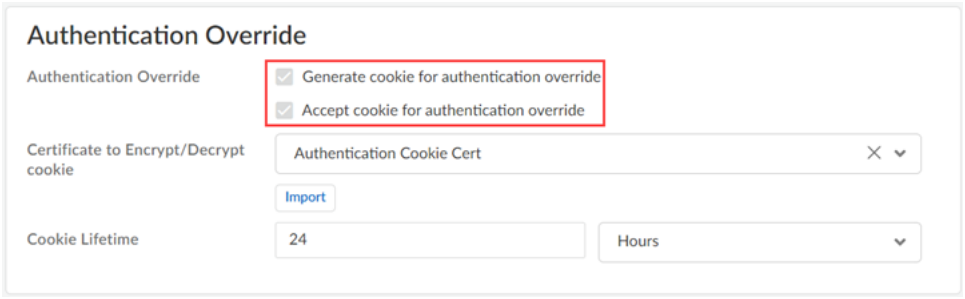
Wenn Sie in beiden Portalen die zertifikatsbasierte Authentifizierung verwenden, stellen Sie sicher, dass beide Portale dasselbe Client-Zertifikatprofil zur Authentifizierung verwenden.

Mit dieser Funktion können die Einstellungen zur Authentifizierungsüberschreibung Cookies für beide Portale in den GlobalProtect-App-Einstellungen generieren.

 ©2025 Palo Alto Networks, Inc.




Mit dieser Funktion können die Einstellungen zur Authentifizierungsüberschreibung Cookies für beide Portale in den Tunneleinstellungen generieren und akzeptieren.




**STEP 5 |** Speichern Sie alle Änderungen und verwenden Sie **Push**, um die Konfigurationsänderungen an Prisma Access zu übertragen.

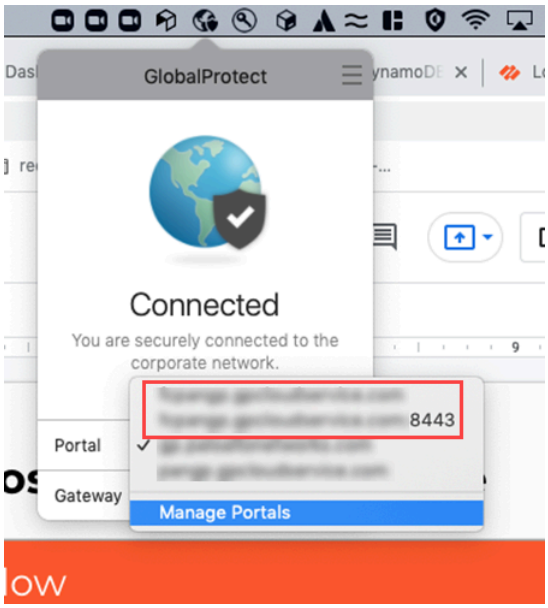
**STEP 6 |** Fügen Sie die Portale manuell oder mithilfe der Endpunktverwaltungssoftware in der GlobalProtect-App hinzu.

 ©2025 Palo Alto Networks, Inc.

**STEP 7 |** Überprüfen Sie, ob Sie mit unterschiedlichen Authentifizierungsprofilen für das Gateway eine Verbindung zu beiden Portalen herstellen können.

1. Melden Sie sich bei Ihrem Windows-Computer an.
2. Stellen Sie eine Verbindung zu den Portalen in Ihrer GlobalProtect-App her.

   Wenn Sie die Verbindung zwischen Portalen mit unterschiedlichen Authentifizierungsmethoden ändern, authentifizieren Sie die Benutzeranmeldung.




*Falls das Authentifizierungscookie abläuft, wenn Sie eine Verbindung zum Portal 8443 herstellen und zum manuellen Gateway wechseln, stellt GlobalProtect eine Verbindung zum* ***besten verfügbaren Gateway*** *her.*

*Wenn Ihre GlobalProtect-App zwischengespeicherte Portalkonfigurationen verwendet, funktioniert der Fallback auf das Portal nicht.*

*Wenn Sie für das sekundäre Portal eine SAML-basierte Authentifizierung verwenden, geben Sie beim Integrieren die Werte wie folgt ein:*

- ***URL für Single Sign-On****: Geben Sie* ***`https://Portal-FQDN:443/SAML20/SP/ACS`***

  *ein. Portal-FQDN ist der FQDN für das Prisma Access-Portal*

  *. Verwenden Sie das Portal* ***443*** *auch dann, wenn Sie das sekundäre Portal (8443) konfiguriert haben.*
- ***Zielgruppen-URI (SP-Entitäts-ID)****: Geben Sie* ***`https://Portal-FQDN:443/SAML20/SP ein`***

## Konfigurieren mehrerer Portale in Prisma Access (Panorama)

**STEP 1 |** Wenden Sie sich an Ihren Palo Alto Networks-Ansprechpartner, um diese Funktionalität zu aktivieren.

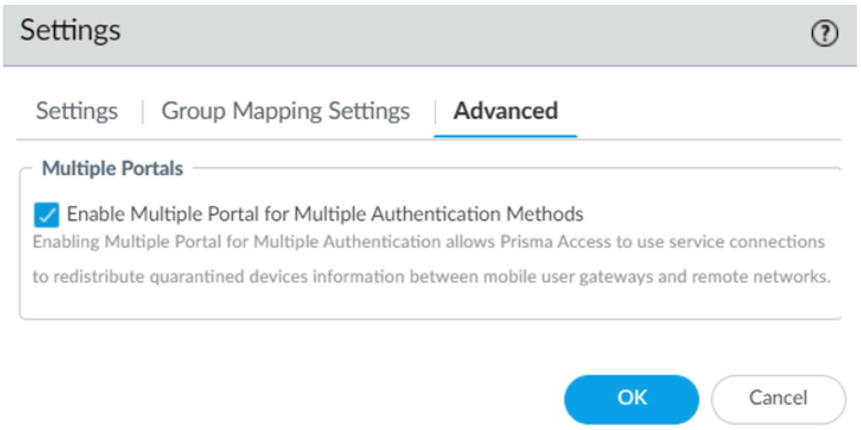
 ©2025 Palo Alto Networks, Inc.

*Wenn Sie mehrere GlobalProtect-Portale mit Datenverkehrslenkung konfigurieren, dann sollten Sie nicht die **Standardrouten über Dienstverbindungen akzeptieren** (**Panorama** > **Cloud Services** > **Konfiguration** > **Datenverkehrslenkung** > **Einstellungen** > **Standardroute über Dienstverbindung akzeptieren**). Andernfalls können mobile Benutzer keine Verbindung zum sekundären Portal herstellen.*

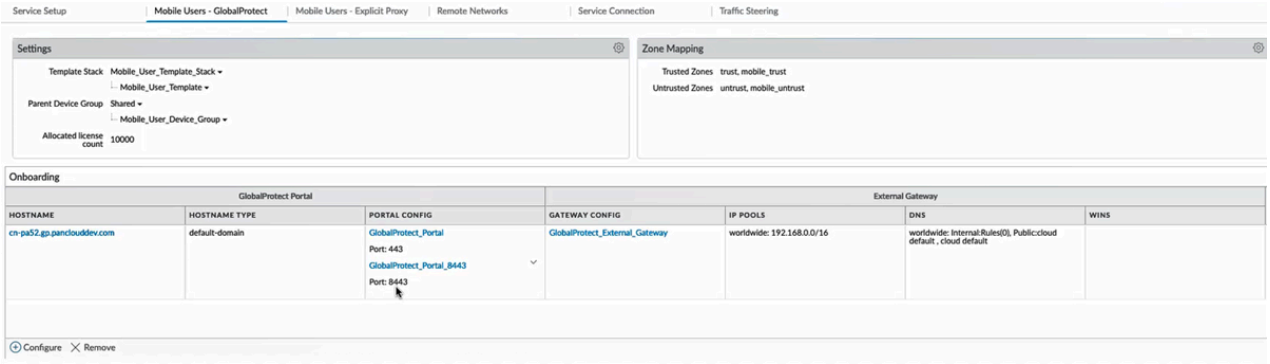
**STEP 2 |** Konfigurieren Sie einen mobilen Benutzer und die zugehörige Authentifizierungsmethode.

**STEP 3 |** Wählen Sie **Cloud Services** > **Konfiguration** > **Mobile Benutzer – GlobalProtect** > **Einstellungen** > **Erweitert** aus.

**STEP 4 |** **Aktivieren Sie mehrere Portale für mehrere Authentifizierungsmethoden.**




Das neue Portal wird für den Port 8443 für denselben Mandanten angezeigt. Dieses Portal übernimmt die Konfigurationseinstellungen vom ursprünglichen Port, nämlich Port 443.




 ©2025 Palo Alto Networks, Inc.

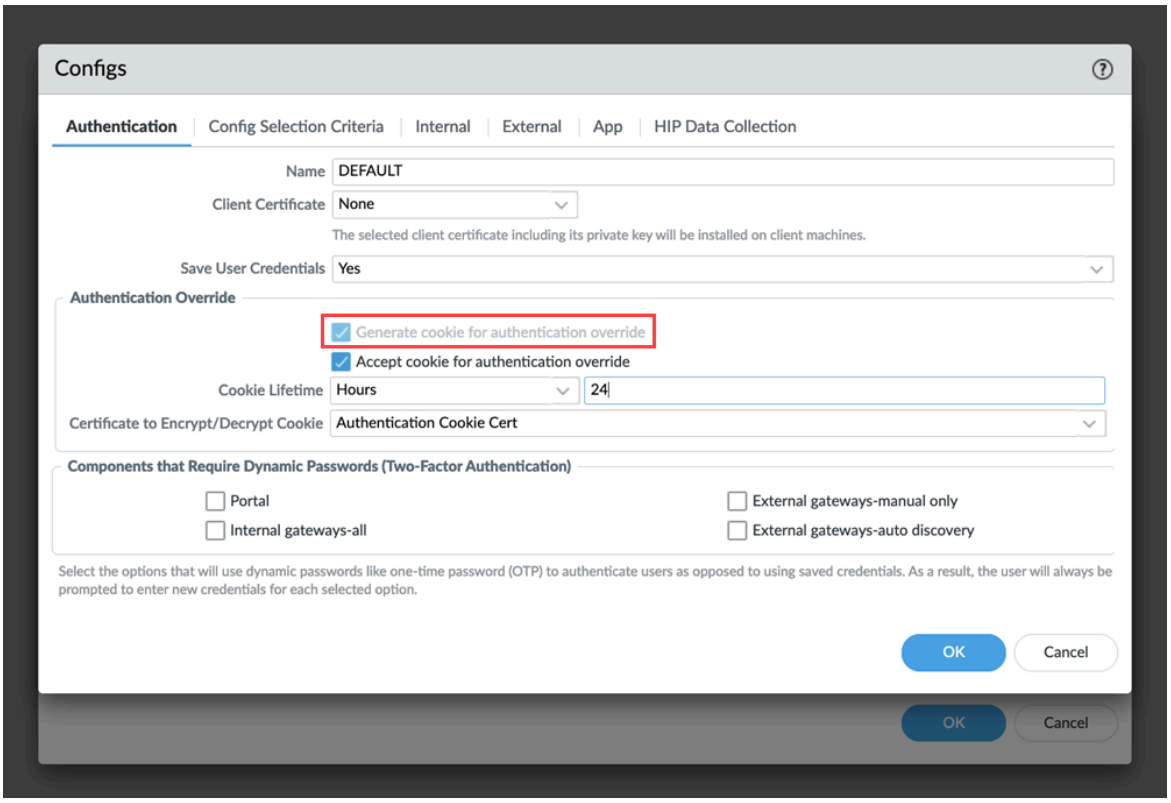
**STEP 5 |** Bearbeiten Sie die Portalkonfigurationen, um die Authentifizierungseinstellungen zu aktualisieren.

1. Klicken Sie auf den Portal-Hyperlink oder wählen Sie **Panorama** > **Vorlagen** > **Netzwerk** > **GlobalProtect** > **Portale** aus und klicken Sie auf den Portal-Hyperlink.
2. Fügen Sie im Abschnitt **Authentifizierung** durch Auswahl von **Hinzufügen** eine **Clientauthentifizierung** mit einem anderen **Authentifizierungsprofil** hinzu.

Sie können nur die Authentifizierungseinstellungen für die **Clientauthentifizierung** und die Authentifizierungseinstellungen für das **Zertifikatprofil** bearbeiten.

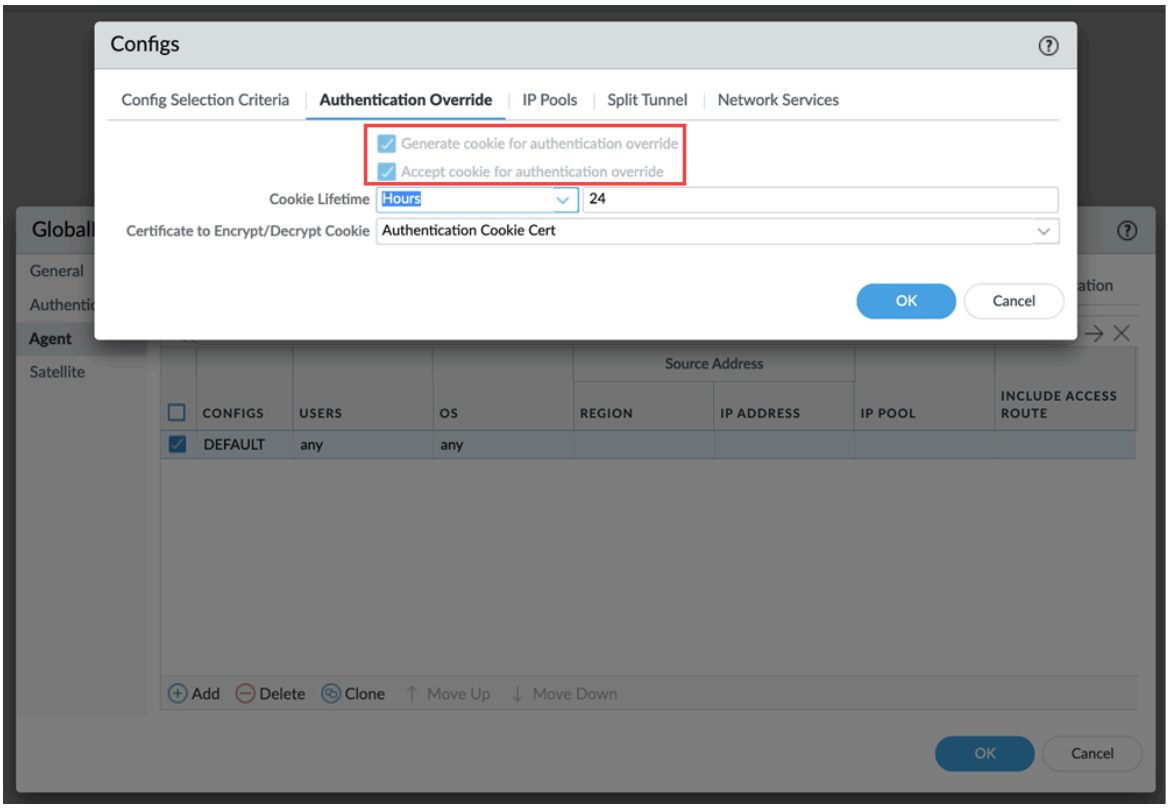
Wenn Sie in beiden Portalen eine zertifikatsbasierte Authentifizierung verwenden, stellen Sie sicher, dass das Gateway keine zertifikatsbasierte Authentifizierung verwendet.

Mit dieser Funktion können die Einstellungen zur Authentifizierungsüberschreibung Cookies für beide Portale in den GlobalProtect-App-Einstellungen generieren.



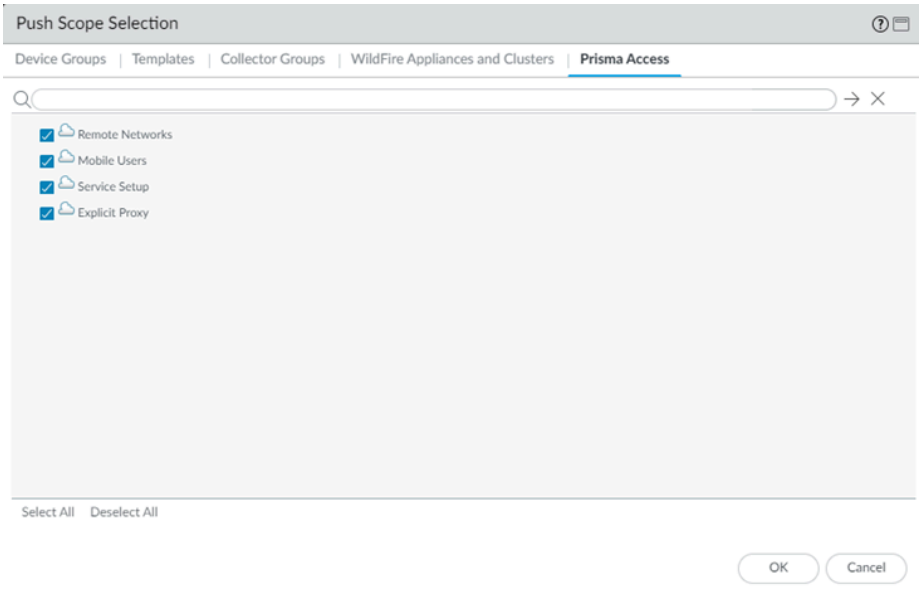

Mit dieser Funktion können die Einstellungen zur Authentifizierungsüberschreibung Cookies für beide Portale in den Tunneleinstellungen generieren und akzeptieren.

 ©2025 Palo Alto Networks, Inc.




**STEP 6 |** Schreiben Sie alle Änderungen in Panorama fest und übertragen Sie die Konfigurationsänderungen per Push an Prisma Access.

1. Klicken Sie auf **Commit** > **Commit und Push**.
2. Wählen Sie **Auswahlen bearbeiten** aus und vergewissern Sie sich dann auf der Registerkarte **Prisma Access**, dass **Mobile Benutzer** im **Übertragungsumfang** ausgewählt wurde. Klicken Sie dann auf **OK**.




3. Klicken Sie auf **Commit und Push**.

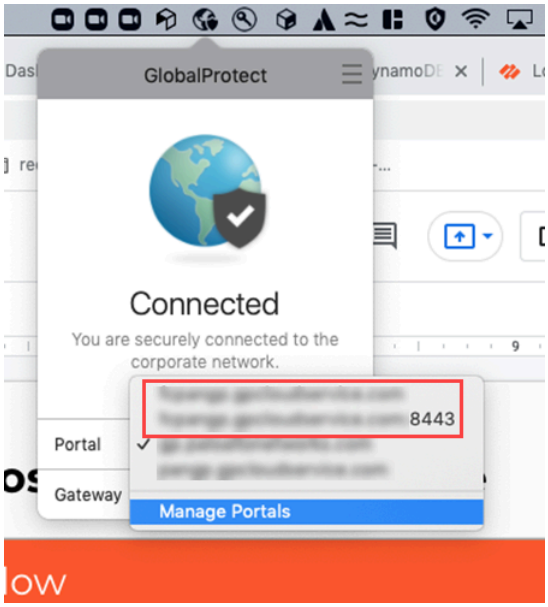
 ©2025 Palo Alto Networks, Inc.

**STEP 7 |** Fügen Sie die Portale manuell oder mithilfe der Endpunktverwaltungssoftware in der GlobalProtect-App hinzu.

**STEP 8 |** Überprüfen Sie, ob Sie mit unterschiedlichen Authentifizierungsprofilen für das Gateway eine Verbindung zu beiden Portalen herstellen können.

1. Melden Sie sich bei Ihrem Windows-Computer an.
2. Stellen Sie eine Verbindung zu den Portalen in Ihrer GlobalProtect-App her.

   Wenn Sie die Verbindung zwischen Portalen mit unterschiedlichen Authentifizierungsmethoden ändern, authentifizieren Sie die Benutzeranmeldung.




   *Falls das Authentifizierungscookie abläuft, wenn Sie eine Verbindung zum Portal 8443 herstellen und zum manuellen Gateway wechseln, stellt GlobalProtect eine Verbindung zum **besten verfügbaren Gateway** her.*

   *Wenn Ihre GlobalProtect-App zwischengespeicherte Portalkonfigurationen verwendet, funktioniert der Fallback auf das Portal nicht.*

3. Zeigen Sie die Protokolle beider Portale an, indem Sie **Überwachen** > **Protokolle** > **GlobalProtect** auswählen, um das Portal und Authentifizierungsinformationen anzuzeigen.

*Wenn Sie für das sekundäre Portal eine SAML-basierte Authentifizierung verwenden, geben Sie beim Integrieren die Werte wie folgt ein:*

- ***URL für Single Sign-On**: Geben Sie **`https://Portal-FQDN:443/SAML20/SP/ACS`***

  *ein. Portal-FQDN ist der FQDN für das Prisma Access-Portal*

  *. Verwenden Sie das Portal **`443`** auch dann, wenn Sie das sekundäre Portal (8443) konfiguriert haben.*
- ***Zielgruppen-URI (SP-Entitäts-ID)**: Geben Sie **`https://Portal-FQDN:443/SAML20/SP ein`***

 ©2025 Palo Alto Networks, Inc.

# Dynamische DNS-Registrierungsunterstützung für Remote-Fehlerbehebung und Updates

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama)<br>• Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access-Lizenz, einschließlich mobile Benutzer – GlobalProtect<br>❑ Minimal erforderliche Prisma Access-Version: 5.1 Innovation (mindestens PAN-OS-Dataplane-Version 11.2 erforderlich) |

Wenn sich ein mobiler Benutzer mit GlobalProtect-Agent remote mit Prisma Access verbindet, weist das GlobalProtect-Gateway dem Benutzer eine IP-Adresse und einen Endpunkt-FQDN zu. Prisma Access aktualisiert jedoch nicht die DNS-Server in Ihrem Unternehmen mit diesen Informationen. Da DNS-Server die vom mobilen Benutzer zugewiesene IP-Adresse und FQDN-Informationen nicht kennen, können Ihr IT-Administrator und die Apps in Ihrem Netzwerk Remote-Endpunkte nicht mithilfe des FQDN identifizieren und aktualisieren.

Mithilfe der dynamischen DNS-Registrierung können Sie Prisma Access mit IP-Adressverwaltungs(IPAM)-Anbietern integrieren, um mithilfe von „nsupdate“ dynamisch A- und PTR-Einträge in den DNS-Servern zu erstellen.

- Direkte Integration mit führenden IPAM-Anbietern wie InfoBlox, BlueCat und Windows.
- DDNS-Updates werden entweder mit Transaktionssignatur (TSIG) oder Kerberos als Authentifizierungsprotokoll durchgeführt, um sichere Updates der DNS-Datenbank zu gewährleisten.
- Echtzeit-DDNS-Updates werden von Prisma Access zum DNS-Server mithilfe von nsupdate-Batch-Aufrufen durchgeführt, die auf Verbindungs- und Trennereignissen von GlobalProtect basieren. Diese Updates verwenden einen DDNS-Dienst auf dem Sicherheitsverarbeitungsknoten der mobilen Benutzer (MU-SPN).

Nachdem Sie diese Lösung eingerichtet haben, können Sie die folgenden Aktionen ausführen:

- Sie können Softwaretools wie Microsoft Endpoint Configuration Manager (MECM) verwenden, um Software-Updates auf GlobalProtect-Endpunkte per Push zu übertragen.
- IT- und Helpdesk-Mitarbeiter können den GlobalProtect-Endpunkt über den FQDN des Geräts verbinden und verwalten.
- Sie können Kundenanwendungen (z. B. Bankanwendungen) implementieren, die auf Reverse-DNS-Lookups basieren, um den Zugriff von genehmigten GlobalProtect-Endpunkten aus zu ermöglichen.

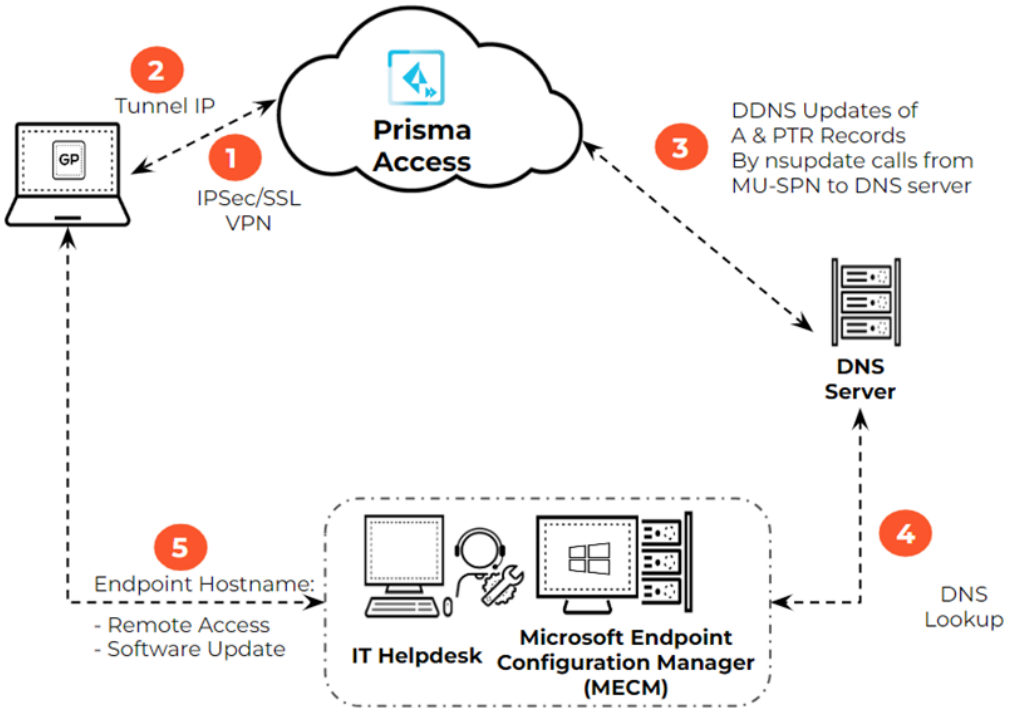
*Diese DDNS-Lösung ist nicht kompatibel mit der Lösung Dynamische DNS-Registrierungsunterstützung für mobile Benutzer – GlobalProtect, die Strata Logging Service verwendet, um die DDNS-Updates auf den Server per Push zu übertragen. Wenn Sie die vorhandene Lösung mit Strata Logging Service implementiert haben und diese Lösung dann bereitstellen, verwendet Prisma Access diese Lösung und deaktiviert die vorhandene Lösung mit Strata Logging Service.*

 ©2025 Palo Alto Networks, Inc.

## Anwendungsfall für die dynamische DNS-Registrierungsunterstützung

Das folgende Diagramm veranschaulicht einen typischen Anwendungsfall für die DDNS-Lösung von Prisma Access. In diesem Beispiel möchten Sie GlobalProtect-Endpunkte mithilfe von MECM aktualisieren oder möchten, dass sich der IT-Helpdesk zur Fehlerbehebung remote am GlobalProtect-Endpunkt anmelden kann.

1. GlobalProtect richtet einen SSL-Tunnel zwischen dem GlobalProtect-Endpunkt und dem Prisma Access-Gateway ein.
2. GlobalProtect sendet Hostname, Domänenname und Tunnel-IP-Adresse des mobilen Benutzergeräts durch den Tunnel an das lokale oder Prisma Access Gateway.
3. Prisma Access stellt DDNS-Updates von A- und PTR-Einträgen mit „nsupdate“ zum DNS-Server bereit und Prisma Access stellt diese sicheren Updates in Echtzeit bereit, wenn es An- und Abmeldeereignisse verarbeitet.
4. Der IT-Administrator oder eine Unternehmenssoftware verwendet diese Datensätze über eine DNS- oder RDNS-Lookup-Funktion und löst den Endpunktnamen oder die IP-Adresse auf.
5. Der IT-Administrator oder die Endpunktverwaltungssoftware verwendet diese Informationen, um den Endpunkt zu verwalten oder Software-Updates per Push zu übertragen.




## Anforderungen an die Netzwerkkonnektivität

Bevor Sie diese Lösung implementieren, stellen Sie sicher, dass Ihr Netzwerk die folgenden Anforderungen erfüllt:


©2025 Palo Alto Networks, Inc.

- Sie haben Routen hinzugefügt, um die Verbindung zum DNS-Server vom MU-SPN und von Prisma Access-Dienstverbindungen sicherzustellen.

  Fügen Sie dazu Routen aus dem Prisma Access-Infrastruktursubnetz hinzu, die Sie in **Workflows** > > **Einrichtung Prisma Access** > **Prisma Access** > **Infrastruktursubnetz** und im IP-Adresspool von mobile Benutzer – GlobalProtect finden, der sich in **Workflows** > **Einrichtung Prisma Access** > **GlobalProtect** > **Client-IP-Pool** befindet.
- Sie haben Konnektivität hergestellt, indem Sie eine Dienstverbindung zwischen Prisma Access und dem IPSec-Terminierungsgerät (z. B. einer Firewall oder einem Router der nächsten Generation) erstellt haben, das Konnektivität zum DNS-Server hat.
- Sie haben sichergestellt, dass Ihr DNS-Server über den IPSec-Tunnel der Dienstverbindung erreichbar ist.
- Sie haben verifiziert, dass nsupdate-Befehle, die von Prisma Access-Sicherheitsverarbeitungsknoten (SPNs) für mobile Benutzer – GlobalProtect gesendet werden, zulässig sind und den DNS-Server erreichen können.

  Die Schritte, die Sie ausführen, um diese Konnektivität zu erreichen, unterscheiden sich je nach Standort und Typ des verwendeten DNS-Servers. Beispiel:

  - Wenn sich der DNS-Server im Rechenzentrum befindet, können Sie Konnektivität mithilfe von IPSec-Tunneln vom SPN für mobile Benutzer – GlobalProtect zu Dienstverbindungen und dann von der Dienstverbindung zum Gateway-Router (z. B. einer Firewall der nächsten Generation, die als VM konfiguriert ist) einrichten, hinter dem sich der DNS-Server befindet.
  - Wenn sich der DNS-Server in der Cloud befindet, können Sie Konnektivität zum DNS-Server über den SPN für mobile Benutzer – GlobalProtect mithilfe entsprechender Sicherheitsrichtlinienregeln herstellen.
- Sie haben Forward- und Reverse-Lookup-Zonen auf den DNS-Servern konfiguriert.
- Sie haben einen Infoblox-, Bluecat- oder Windows-DNS-Server implementiert, der „nsupdate“ unterstützt.
- Wenn Sie die Berechtigungen für Zonen einzeln beibehalten, stellen Sie sicher, dass Sie Sicherheitsrichtlinienregeln erstellt haben, um „nsupdate“ von Geräten zuzulassen, die über den richtigen TSIG- oder Kerberos-Schlüssel verfügen.

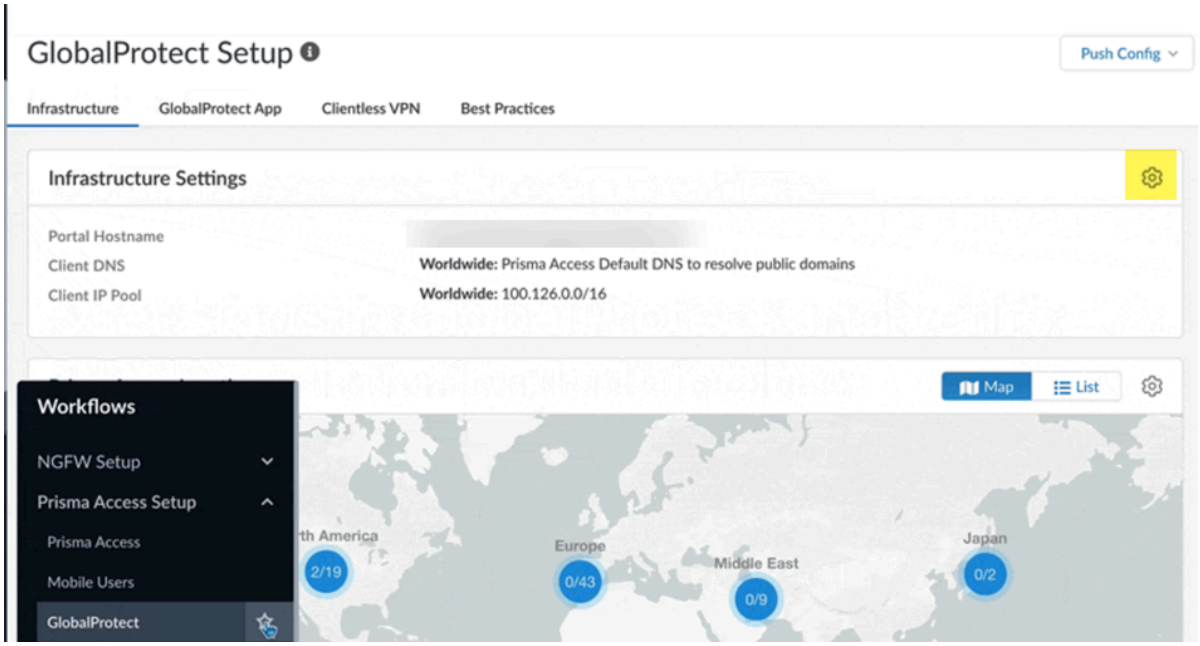
Verwenden Sie zum Konfigurieren dieser Lösung eines der folgenden Verfahren, je nach Bereitstellungstyp.

- Cloud Management
- Panorama

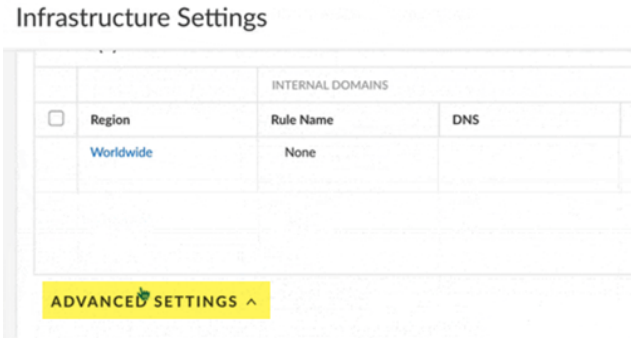
## Dynamische DNS-Updates für Prisma Access (Managed by Strata Cloud Manager) konfigurieren

 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** Rufen Sie über Strata Cloud Manager die Optionen **Workflows** > **GlobalProtect** aus und klicken Sie dann auf das Zahnradsymbol, um die **Infrastruktureinstellungen** zu bearbeiten.




**STEP 2 |** Wählen Sie **Erweiterte Einstellungen** aus.




**STEP 3 |** Konfigurieren Sie die Einstellungen für **Dynamische DNS-Unterstützung**.

1. Wählen Sie **Dynamische DNS-Unterstützung für GlobalProtect** aus.
2. Wählen Sie den **Domänentyp** aus.

   - **Fallback-Domäne** – Die für die nsupdate-Ereignisse verwendete Domäne fällt auf die Domäne zurück, die Sie im Bereich **Fallback-Domäne** angeben. Verwenden Sie diese Option, wenn die GlobalProtect-Clients mit keiner Domäne oder aber mit derselben Domäne verknüpft werden, die der DDNS-Dienst zum Aktualisieren der Datensätze auf dem DNS-Server verwendet.

     Wenn Sie **Fallback-Domäne** auswählen und sich Benutzer, die nicht mit einer Domäne verbunden sind, bei GlobalProtect anmelden, werden deren Informationen unter der Zone der Fallback-Domäne hinzugefügt, die auf dem DNS-Server erstellt wird.

     Wenn GlobalProtect-Clients, die sich bei GlobalProtect anmelden, zu einer unerwarteten Domäne gehören, die auf dem DNS-Server nicht konfiguriert ist,

 ©2025 Palo Alto Networks, Inc.

schlägt die Ausführung von nsupdate möglicherweise fehl. Wählen Sie in diesem Fall **Domäne überschreiben** aus, um die unbekannte Domäne mit der Domäne zu überschreiben, die dem DNS-Server bekannt ist.

- **Domäne überschreiben** – Prisma Access verwendet nur die Domäne, die Sie zum Aktualisieren des DNS-Servers angeben, und überschreibt alle anderen Domänen. Wenn sich GlobalProtect-Clients bei einer anderen Domäne anmelden, verwendet der DDNS-Dienst die Domäne, die Sie hier angeben, um die DNS A- und PTR-Einträge zu aktualisieren.

3. Wählen Sie im Feld **Fallback-Domäne** die Domäne aus, die zum Aktualisieren der PTR-Einträge für Fallback- oder Override-Domänen verwendet wird.
4. Wählen Sie die **DNS-Server-IP**-Adresse aus.
5. Wählen Sie den **Servertyp** (entweder **TSIG** oder **Kerberos**) aus.
6. (Nur TSIG-Bereitstellungen) Wählen Sie den für TSIG zu verwendenden **TSIG-Schlüssel** aus.

   Vergewissern Sie sich, dass die TSIG-Datei das richtige Format hat und den Dateityp .key aufweist.

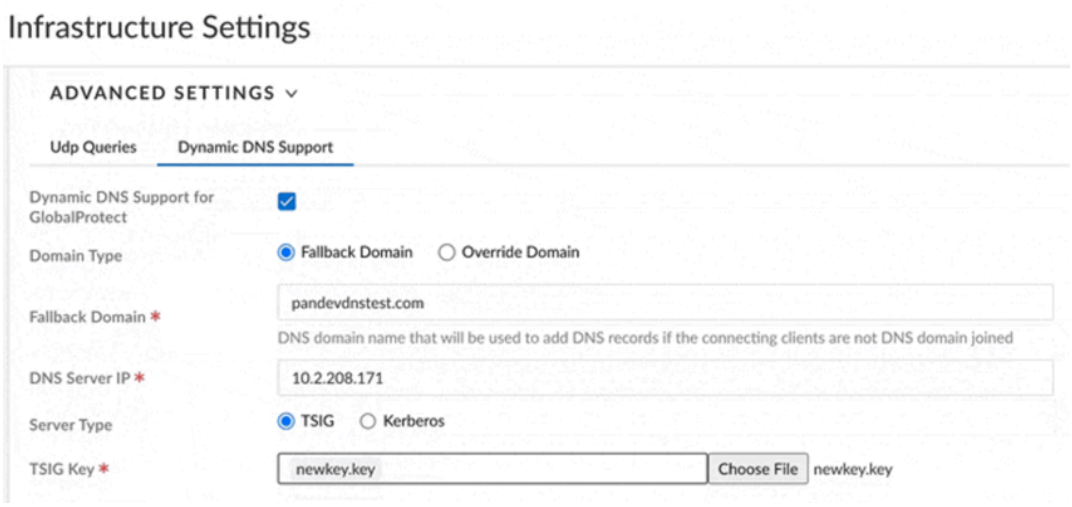
   Wenn Sie einen Kerberos-Authentifizierungstyp auswählen, laden Sie einen Authentifizierungsschlüssel über eine .key-Datei hoch. Auf diese Weise wird die uncodierte Kerberos-Schlüsseltabellendatei vom DNS-Server abgerufen.

   Die TSIG-Datei muss im folgenden Format vorliegen:

   ```
   key "ddns-gp" { algorithm hmac-sha256; secret
    "aBCDEFGhiJklMNO89PQR+8stUVWX+YZAbcdeFgHI5J="; };
   ```

7. (Nur Kerberos-Bereitstellungen) Geben Sie die zu verwendenden Kerberos-Optionen an.
   - Geben Sie die IP-Adresse für den **Kerberos-Domänencontroller** ein.
   - Geben Sie die IP-Adresse für den **Kerberos-Admin-Server** ein.
   - Geben Sie den **Kerberos-Benutzernamen** ein.
   - Geben Sie die zu verwendende **Kerberos-Schlüsseltabelle** (Keytab) ein.

     Vergewissern Sie sich, dass der Kerberos-Schlüssel das richtige Format hat.



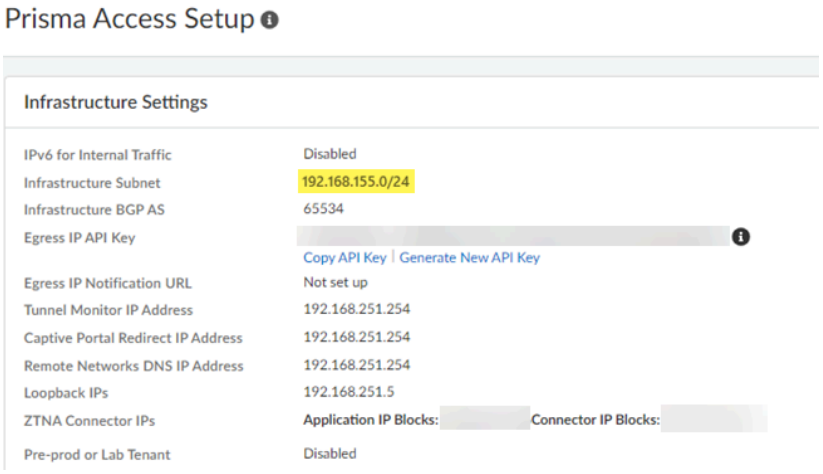

 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** **Save (Speichern)** Sie Ihre Änderungen.

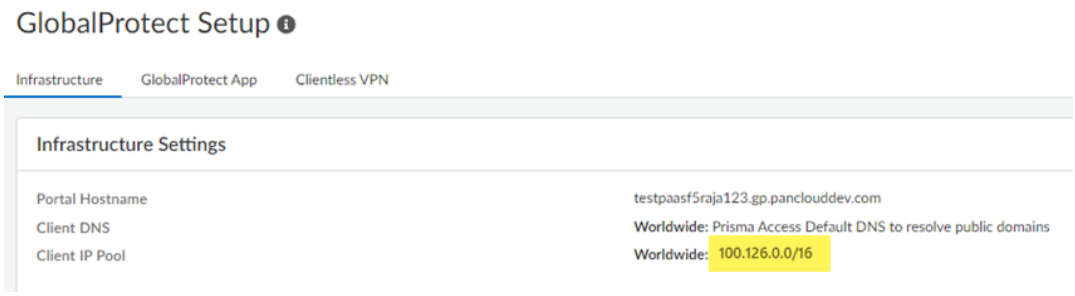
**STEP 5 |** Richten Sie auf Ihrem DNS-Server Vorwärts- und Rückwärts-Lookup-Zonen ein.

Beachten Sie die Dokumentation Ihres IPAM-Anbieters, um diese Zonen einzurichten. Dieser Schritt erfordert, dass Sie das **Infrastruktursubnetz** und den **Client-IP-Pool** über Prisma Access eingeben.

- Um das Infrastruktursubnetz zu finden, wählen Sie **Workflows** > **Einrichtung Prisma Access** > **Prisma Access** aus und notieren Sie das **Infrastruktursubnetz**.



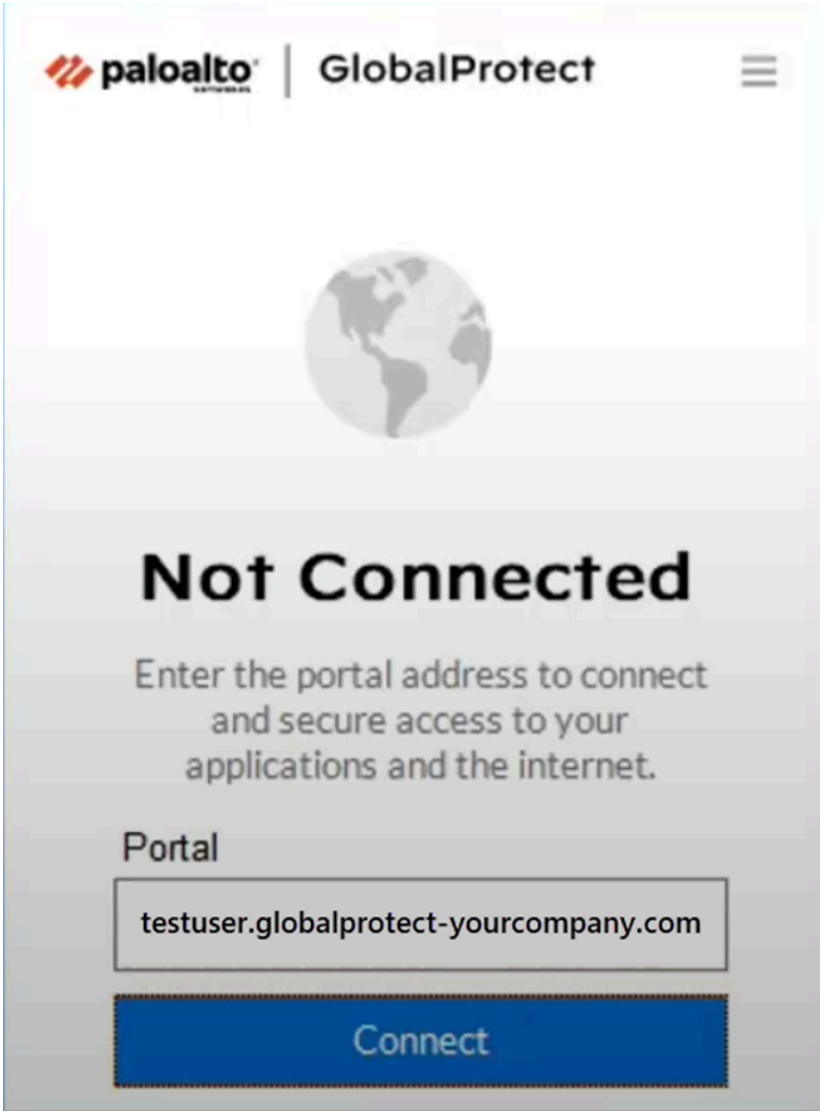

- Um den IP-Adresspool für mobile GlobalProtect-Benutzer zu finden, wählen Sie **Workflows** > **Einrichtung Prisma Access** > **GlobalProtect** aus und notieren dann den **Client-IP-Pool**.




 ©2025 Palo Alto Networks, Inc.

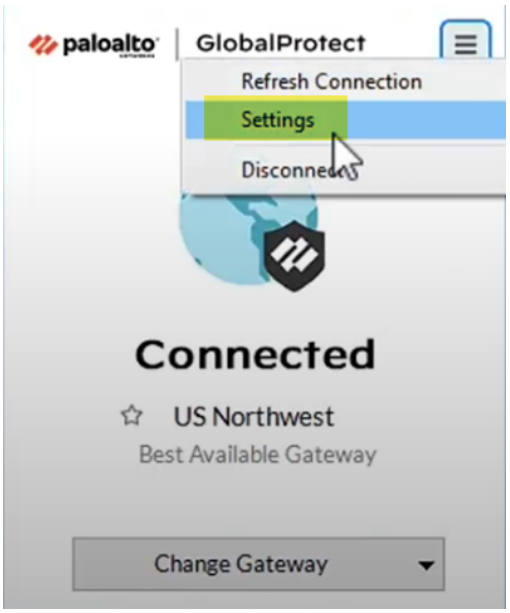
**STEP 6 |** Vergewissern Sie sich, dass die DNS-Einträge auf dem IPAM-DNS-Server aktualisiert werden.

1. Öffnen Sie einen Client-Computer und stellen Sie eine Verbindung zu einem Prisma Access GlobalProtect-Gateway her.

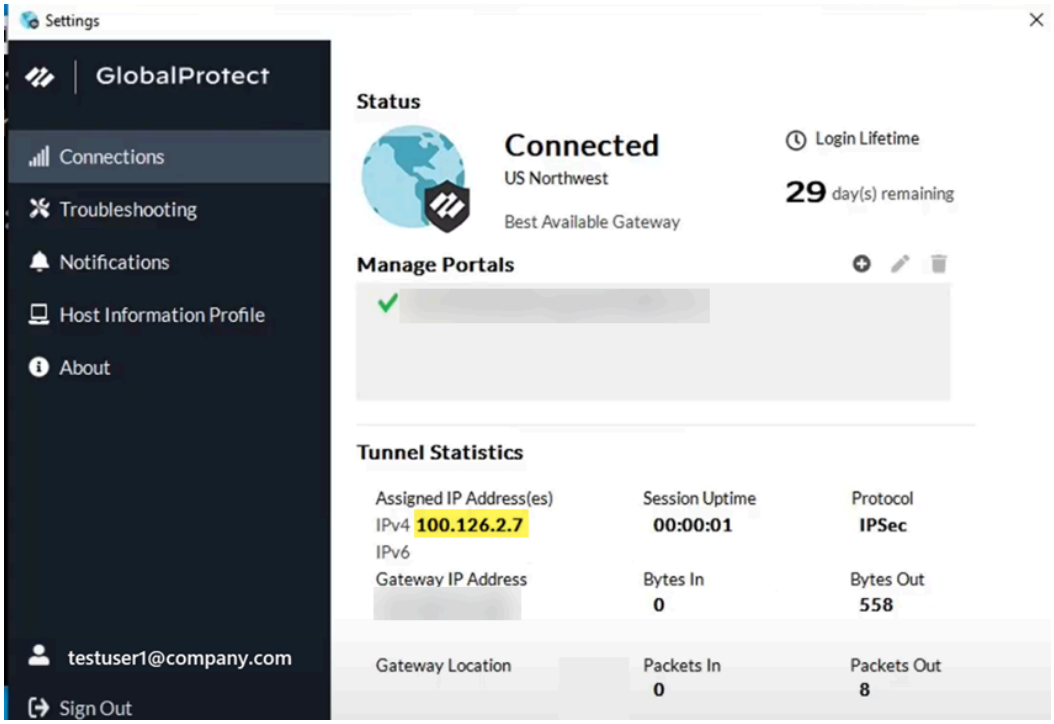



2. Wählen Sie GlobalProtect-**Einstellungen** aus und überprüfen Sie die GlobalProtect-IP-Adresse, die dem Benutzer von Prisma Access zugewiesen wurde.

 ©2025 Palo Alto Networks, Inc.

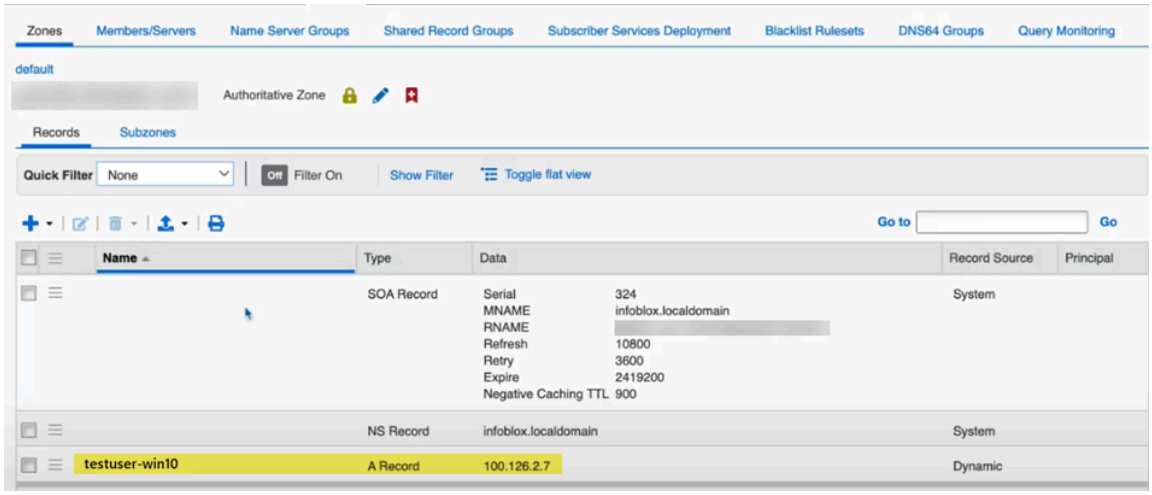



Unter **Zugewiesene IP-Adresse(n)** (100.126.2.7) ist ersichtlich, dass die IP-Adresse aus dem GlobalProtect-IP-Adresspool (100.126.0.0/16) stammt.

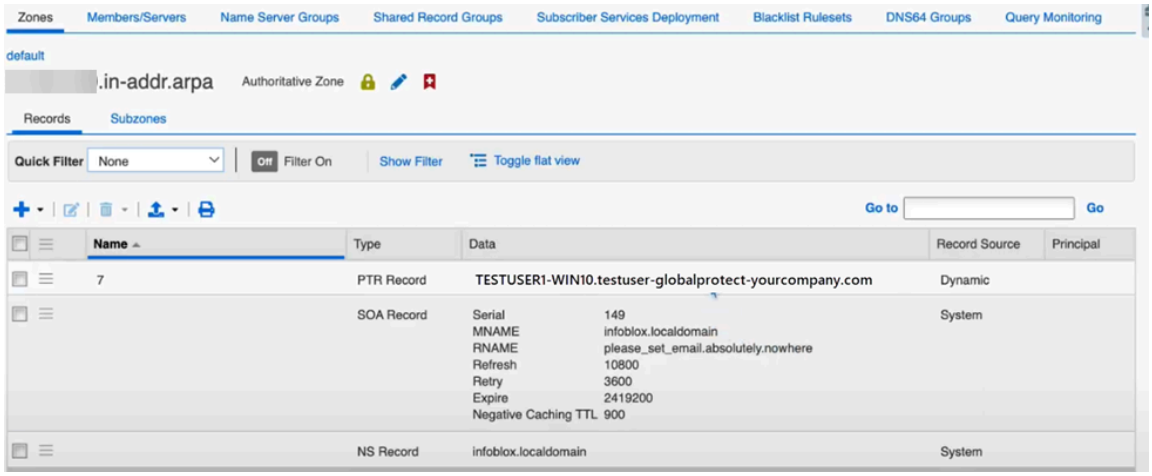



3. Zeigen Sie auf dem IPAM-DNS-Server den Benutzerdatensatz an.
   In diesem Beispiel heißt der Benutzer `testuser1-win10`.

 ©2025 Palo Alto Networks, Inc.




Das DNS-Rückwärts-Lookup zeigt auch den Benutzernamen im PTR-Datensatz an.




4. Melden Sie den Benutzer von GlobalProtect ab und überprüfen Sie die Datensätze, um sicherzustellen, dass der DNS-Server die Datensätze für den Benutzer gelöscht hat.

## Dynamische DNS-Updates für Prisma Access (Managed by Panorama) konfigurieren

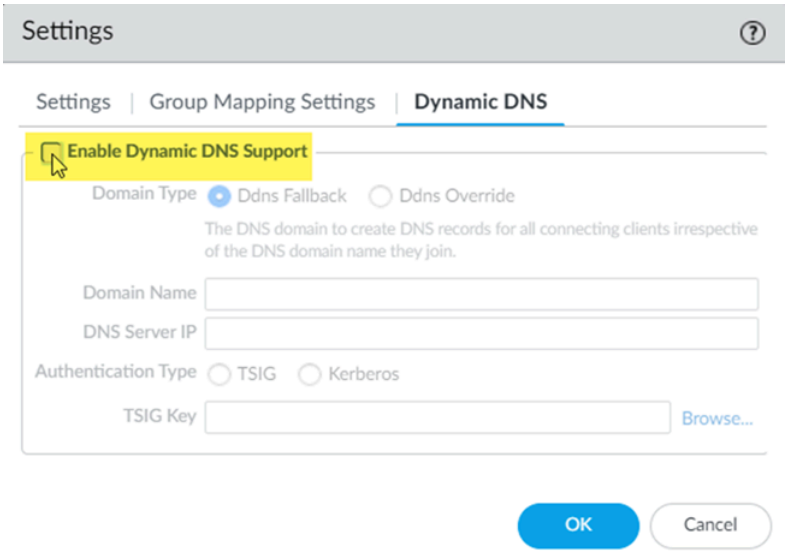
Gehen Sie wie folgt vor, um für Prisma Access (Managed by Panorama) dynamische DNS-Updates zu konfigurieren.

**STEP 1 |** Rufen Sie in Panorama **Cloud Services** > **Konfiguration** > **Mobile Benutzer – GlobalProtect** auf und klicken Sie dann auf das Zahnradsymbol, um die **Einstellungen** zu bearbeiten.

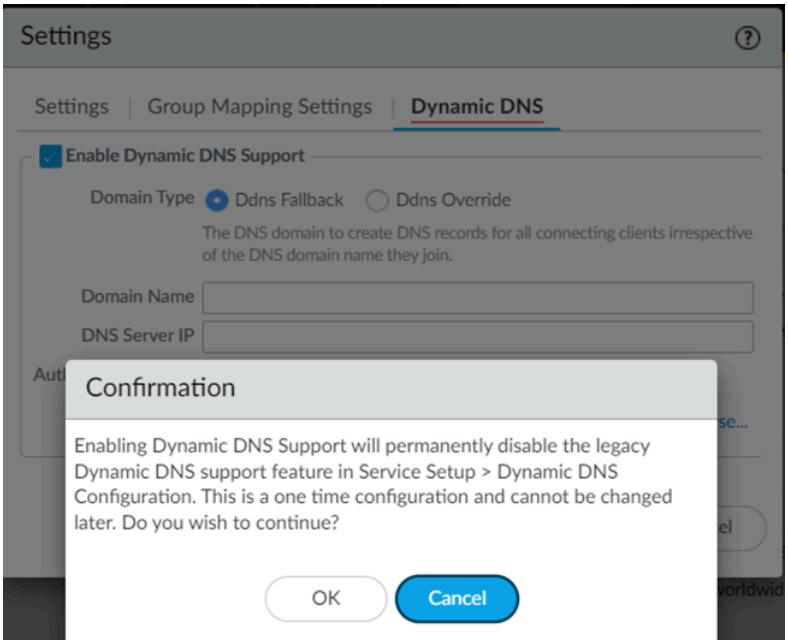
**STEP 2 |** Wählen Sie **Dynamisches DNS** aus.

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** **Dynamische DNS-Unterstützung aktivieren.**




**STEP 4 |** Wenn Sie mit einer älteren Version der dynamischen DNS-Unterstützung arbeiten, werden Sie darauf hingewiesen, dass durch die Aktivierung der aktualisierten Unterstützung die ältere Version der Unterstützung dauerhaft deaktiviert wird. Klicken Sie auf **OK**, um fortzufahren.




**STEP 5 |** Konfigurieren Sie die Einstellungen für **Dynamischen DNS**.

1. Wählen Sie **Dynamische DNS-Unterstützung aktivieren** aus.
2. Wählen Sie den **Domänentyp** aus.
   - **DDNS-Fallback** – Die für die nsupdate-Ereignisse verwendete Domäne fällt auf die Domäne zurück, die Sie im Bereich **Domänenname** angegeben haben. Verwenden Sie diese Option, wenn die GlobalProtect-Clients mit keiner Domäne oder aber mit

 ©2025 Palo Alto Networks, Inc.

derselben Domäne verknüpft werden, die der DDNS-Dienst zum Aktualisieren der Datensätze auf dem DNS-Server verwendet.

Wenn Sie **DDNS-Fallback** auswählen und sich Benutzer, die nicht mit einer Domäne verbunden sind, bei GlobalProtect anmelden, werden ihre Informationen unter der DDNS-Fallback-Zone hinzugefügt, die auf dem DNS-Server erstellt wurde.

Wenn GlobalProtect-Clients, die sich bei GlobalProtect anmelden, zu einer unerwarteten Domäne gehören, die auf dem DNS-Server nicht konfiguriert ist, schlägt die Ausführung von nsupdate möglicherweise fehl. Wählen Sie in diesem Fall **DDNS-Überschreibung** aus, um die unbekannte Domäne mit der Domäne überschreiben, die dem DNS-Server bekannt ist.

- **DDNS-Überschreibung** – Prisma Access verwendet nur die Domäne, die Sie zum Aktualisieren des DNS-Servers angeben, und überschreibt alle anderen Domänen. Wenn sich GlobalProtect-Clients bei einer anderen Domäne anmelden, verwendet der DDNS-Dienst die Domäne, die Sie hier angeben, um die DNS A- und PTR-Einträge zu aktualisieren.

3. Wählen Sie im Feld **Domänenname** die Domäne aus, die zur Aktualisierung der PTR-Datensätze für Fallback- oder Domänennamen verwendet wird.
4. Wählen Sie die **DNS-Server-IP**-Adresse aus.
5. Wählen Sie den **Authentifizierungstyp** (entweder **TSIG** oder **Kerberos**) aus.
6. (Nur TSIG-Bereitstellungen) Wählen Sie den für TSIG zu verwendenden **TSIG-Schlüssel** aus.

   Stellen Sie sicher, dass die TSIG-Datei das richtige Format hat und den Dateityp .key aufweist.

   - Wenn Sie eine von Panorama verwaltete Bereitstellung mit der Plug-in-Version 5.2.0 oder höher ausführen und einen Kerberos-Authentifizierungstyp auswählen, dann laden Sie einen Authentifizierungsschlüssel über eine .key-Datei hoch, die die base64-codierte Zeichenfolge des vom DNS-Server abgerufenen Kerberos-Schlüssels enthält. Beispiel:
     `"ABCDEFGHIJKLMNOPQRSTUV5WXYZOUy5DT00ADUFabcDluaXN0cmF0b3IAAAABAAAAAAEAE`
   - Wenn Sie eine von Panorama verwaltete Bereitstellung mit einer Plug-in-Version unter 5.1.0 ausführen und einen Kerberos-Authentifizierungstyp auswählen, dann laden Sie einen Authentifizierungsschlüssel über eine .key-Datei hoch, deren unverschlüsselte Kerberos-Schlüsseltabellendatei vom DNS-Server abgerufen wird.

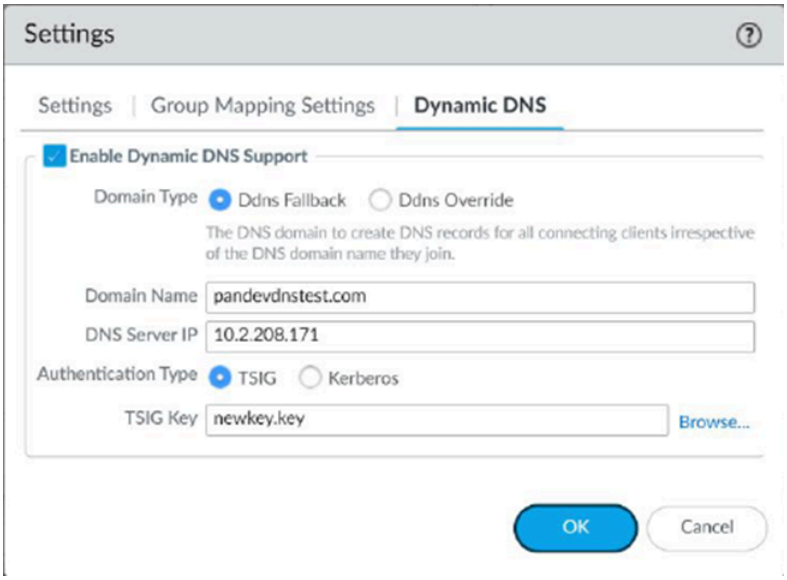
   Die TSIG-Datei sollte im folgenden Format vorliegen:

```
key „ddns-gp“ {algorithm hmac-sha256; secret
 „abcdefghijklmno89pqr+8stuvwx+yzabcdefghi5J=“;};
```

 ©2025 Palo Alto Networks, Inc.

7. (Nur Kerberos-Bereitstellungen) Geben Sie die zu verwendenden Kerberos-Optionen an.
   - Geben Sie die IP-Adresse für den **Kerberos-Domänencontroller** ein.
   - Geben Sie die IP-Adresse für den **Kerberos-Admin-Server** ein.
   - Geben Sie den **Kerberos-Benutzernamen** ein.
   - Geben Sie die zu verwendende **Kerberos-Schlüsseltabelle** (Keytab) ein.

     Verwenden Sie die Base64-Codierung für den Kerberos-Schlüssel, bevor Sie ihn hochladen.



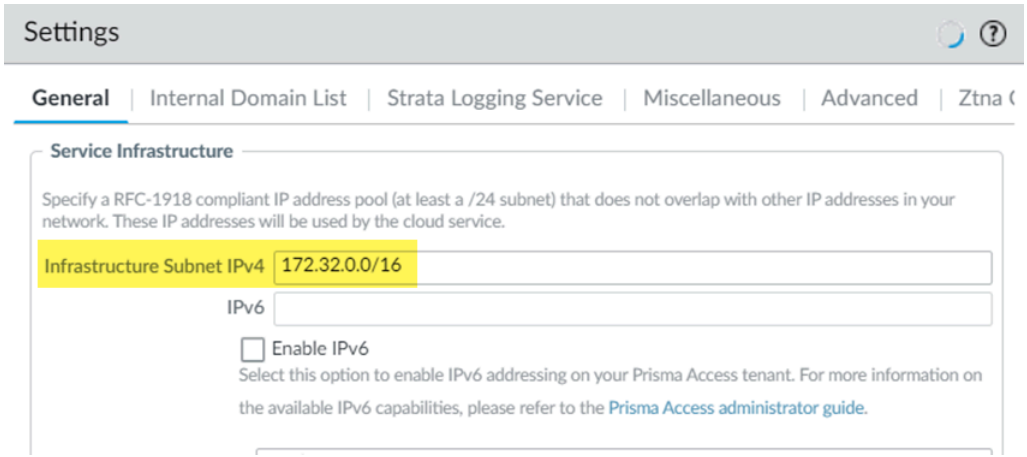

**STEP 6 |** **Save (Speichern)** Sie Ihre Änderungen.

 ©2025 Palo Alto Networks, Inc.

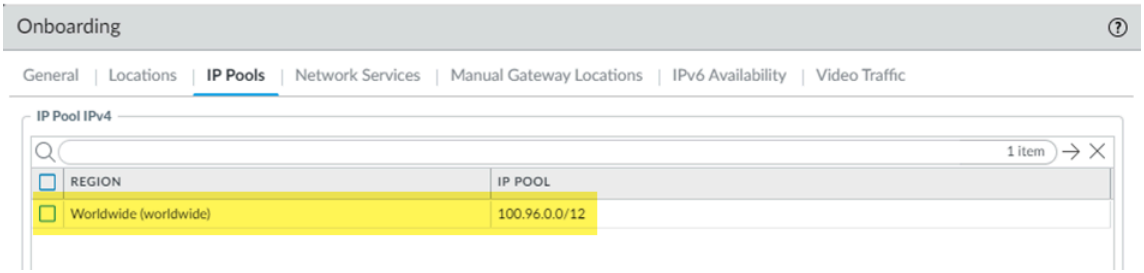
**STEP 7 |** Richten Sie auf Ihrem DNS-Server Vorwärts- und Rückwärts-Lookup-Zonen ein.

Beachten Sie die Dokumentation Ihres IPAM-Anbieters, um diese Zonen einzurichten. Dieser Schritt erfordert, dass Sie das **Infrastruktursubnetz** und den **Client-IP-Pool** über Prisma Access eingeben.

- Um das Infrastruktursubnetz zu finden, rufen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Diensteinrichtung** auf und klicken dann auf das Zahnradsymbol, um die **Einstellungen** zu bearbeiten. Notieren Sie den Wert für **Infrastruktursubnetz-IPv4**.



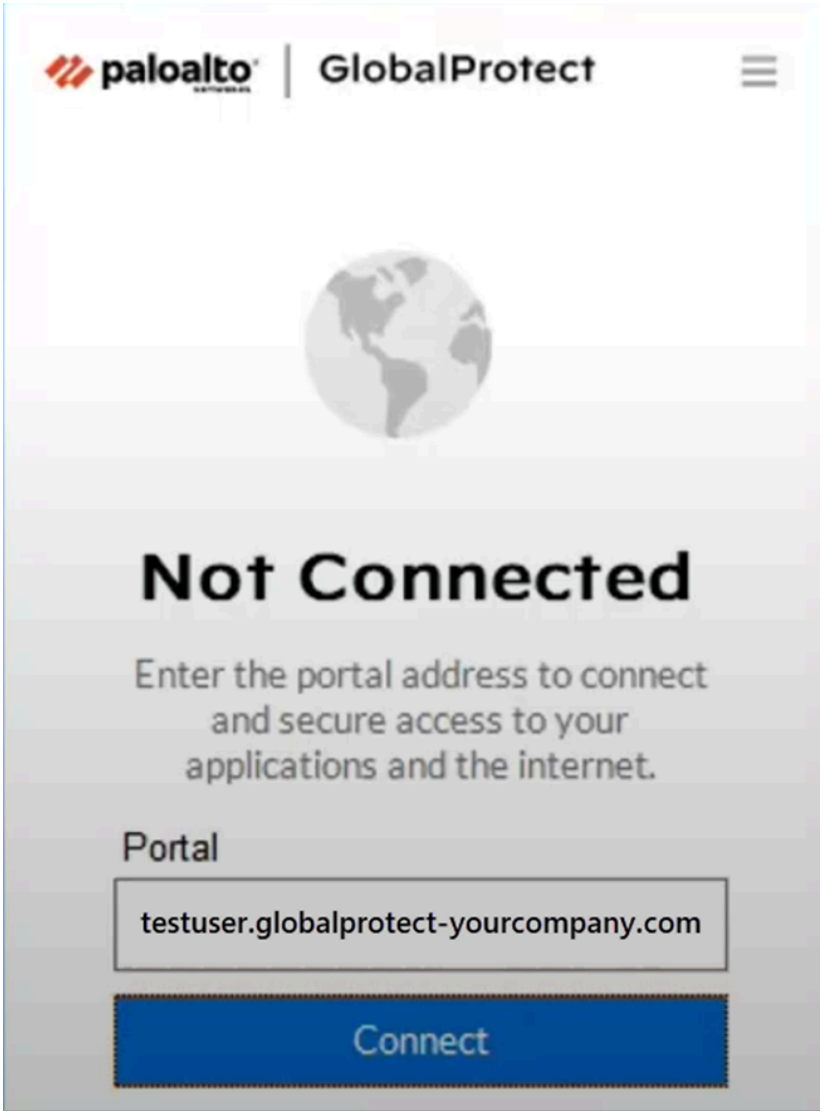

- Um den GlobalProtect-IP-Adresspool für mobile Benutzer zu finden, rufen Sie **Panorama** > **Cloud Services** > **Mobile Users – GlobalProtect** auf und wählen Sie dann den **Hostnamen** aus. Wählen Sie **IP-Pools** aus und notieren Sie den Wert für **IP-Pool IPv4**.




 ©2025 Palo Alto Networks, Inc.

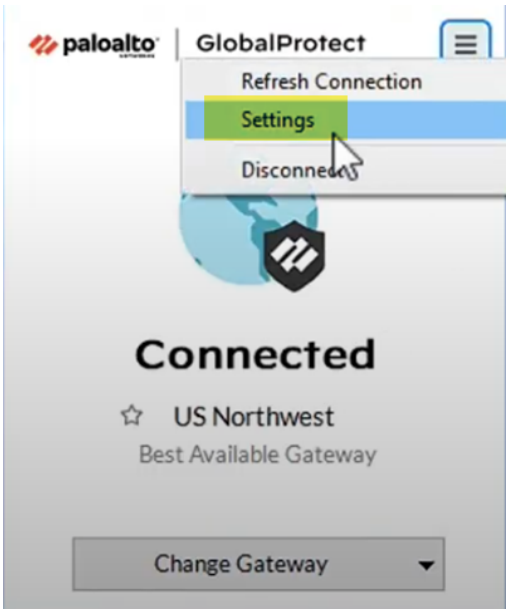
**STEP 8 |** Vergewissern Sie sich, dass die DNS-Einträge auf dem IPAM-DNS-Server aktualisiert werden.

1. Öffnen Sie einen Client-Computer und stellen Sie eine Verbindung zu einem Prisma Access GlobalProtect-Gateway her.

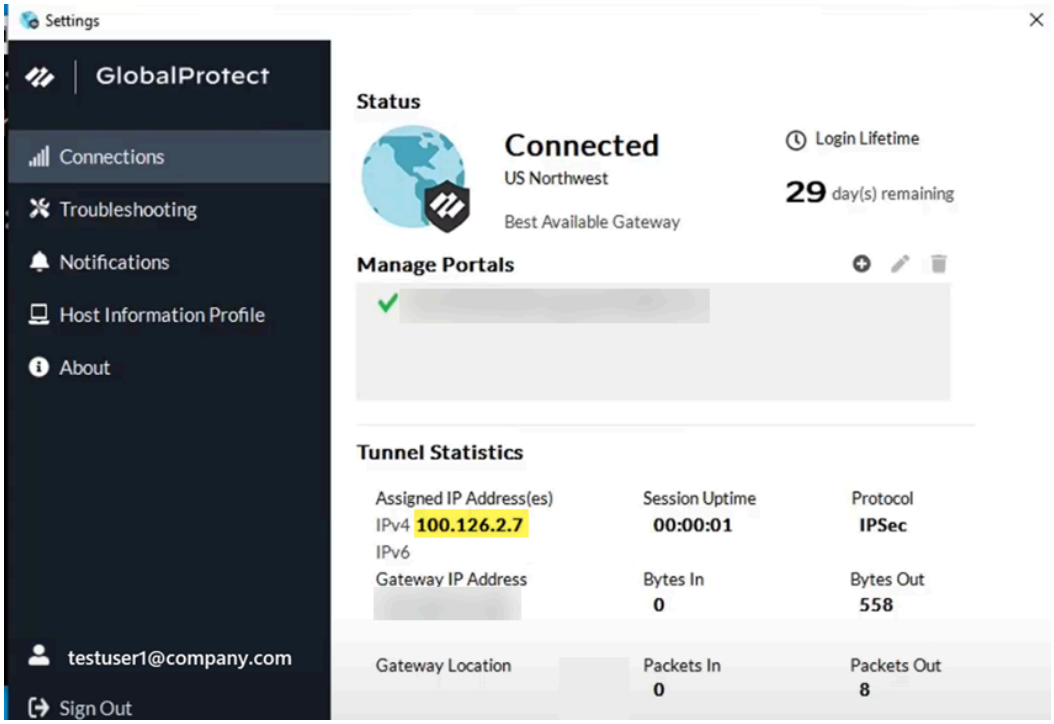



2. Wählen Sie GlobalProtect-**Einstellungen** aus und überprüfen Sie die GlobalProtect-IP-Adresse, die dem Benutzer von Prisma Access zugewiesen wurde.

 ©2025 Palo Alto Networks, Inc.

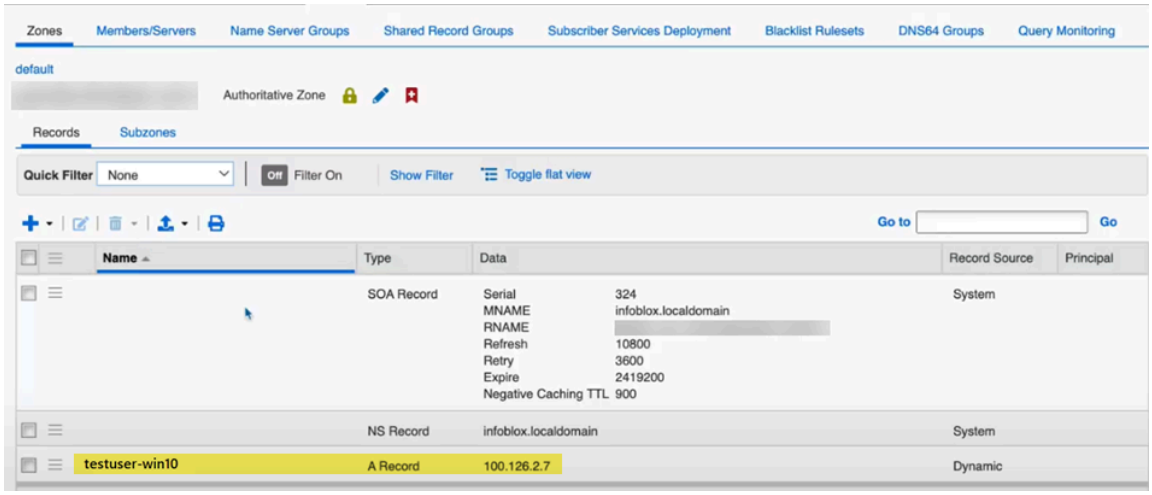



Unter **Zugewiesene IP-Adresse(n)** (100.126.2.7) ist ersichtlich, dass die IP-Adresse aus dem GlobalProtect-IP-Adresspool (100.126.0.0/16) stammt.

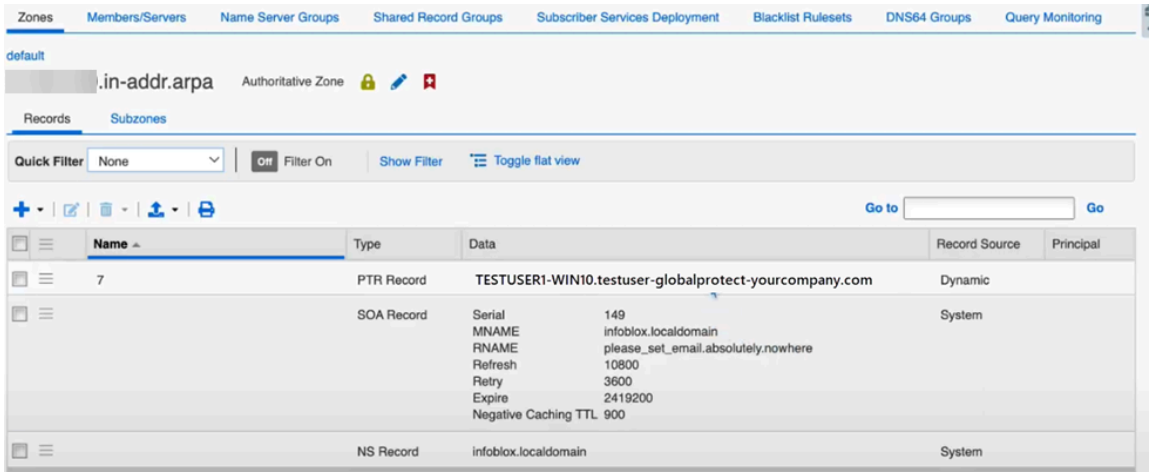



3. Zeigen Sie auf dem IPAM-DNS-Server den Benutzerdatensatz an.
   In diesem Beispiel heißt der Benutzer `testuser1-win10`.

 ©2025 Palo Alto Networks, Inc.




Das DNS-Rückwärts-Lookup zeigt auch den Benutzernamen im PTR-Datensatz an.




4. Melden Sie den Benutzer von GlobalProtect ab und überprüfen Sie die Datensätze, um sicherzustellen, dass der DNS-Server die Datensätze für den Benutzer gelöscht hat.

# Unterstützung der Registrierung von dynamischem DNS für „Mobile Benutzer – GlobalProtect“

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama)<br>• Firewalls der nächsten Generation, die von Panorama mit einer gültigen Strata Logging Service-Lizenz und einem Cloud Services-Plug-in verwaltet werden | ❑ Prisma Access-Lizenz<br>❑ Minimum Required Prisma Access Version: 3.1.1 Preferred oder Innovation<br>❑ Unterstützt auf Panorama-Instanzen, auf denen Version 10.2 und höher ausgeführt wird (nicht unterstützt auf Panorama-Instanzen, auf denen Version 10.1 ausgeführt wird) |

 ©2025 Palo Alto Networks, Inc.

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| | ❑ Ihre Client-Endpunkte müssen einer Domäne beigetreten sein. |

*Diese Funktionalität ist für Prisma Access-Bereitstellungen ab Prisma Access (Managed by Panorama) 3.1.1 verfügbar.*

*Diese Funktionalität ist für Prisma Access (Managed by Strata Cloud Manager)-Bereitstellungen nicht verfügbar.*

Wenn ein mobiler Benutzer mithilfe von GlobalProtect eine Remote-Verbindung zu Prisma Access mit GlobalProtect herstellt, werden die DNS-Server in Ihrem Unternehmen nicht mit der dem GlobalProtect-Gateway zugeordneten IP-Adresse aktualisiert. Vor dem Aktivieren von dynamischem DNS (DDNS) erfolgt keine Zuordnung von Tunnel-IP-Adressen zum Endpunktnamen, die als Adress- und Zeigerdatensätze (A und PTR) protokolliert werden. Daher kann Ihr IT-Administrator oder Ihre Benutzerverwaltungssoftware den Remote-Endpunktnamen nicht der IP-Adresse zuordnen.

Nachdem Sie die DDNS-Funktion in Prisma Access aktiviert haben, überprüft das Prisma Access Cloud Services-Plug-in alle 15 Minuten GlobalProtect-Ereignisse in Strata Logging Service, um Endpunkthostnamen, Domänennamen und Tunnel-IP-Adressen zu erfassen. Dabei werden mithilfe von NSUPDATE dynamisch A- und PTR-Datensätze im DNS-Server erstellt.

#### Dynamischer DNS-Workflow für „Mobile Benutzer – GlobalProtect“

Wenn sich nach dem Aktivieren von DDNS ein mobiler Benutzer mit der GlobalProtect-App anmeldet:

Lesen Sie die folgenden Abschnitte, um einen Überblick darüber zu erhalten, wie DDNS funktioniert, welche Richtlinien und Anforderungen es gibt und wie Sie es aktivieren können.

1. GlobalProtect richtet einen SSL-Tunnel zwischen dem GlobalProtect-Endpunkt und einem lokalen Gateway oder Prisma Access-Gateway ein.
2. GlobalProtect sendet Hostname, Domänenname und Tunnel-IP-Adresse des mobilen Benutzergeräts durch den Tunnel an das lokale Gateway oder Prisma Access-Gateway.
3. Diese Informationen werden vom lokalen Gateway oder von Prisma Access als GlobalProtect-Ereignisse an Strata Logging Service weitergeleitet.
4. Das Prisma Access Cloud Services-Plug-in prüft Strata Logging Service alle 15 Minuten, um den DNS-Server zu aktualisieren.

   Empfängt das Plug-in die GlobalProtect-Ereignisse nicht von Strata Logging Service, wird die Anfrage maximal fünf Mal wiederholt. Wenn die Wiederholungsanfragen nicht erfolgreich waren, wiederholt das Plug-in den Vorgang alle 15 Minuten (maximal vier Mal). Daher kann das Plug-in Aktualisierungen für ein Zeitintervall von einer Stunde erhalten.

   Wenn Sie häufigere Aktualisierungen wünschen, können Sie den Befehl `debug plugins cloud_services set-gp-ddns-interval` eingeben, um das Aktualisierungsintervall auf fünf Minuten zu ändern. A ist zum Aktualisieren des Zeitintervalls nicht erforderlich. Wenn Sie das Intervall auf fünf Minuten ändern, kann das Cloud Services-Plug-in maximal 15.000 Datensätze mit einer Netzwerklatenz von 50 ms aktualisieren und Aktualisierungen für ein Zeitintervall von 20 Minuten erhalten.

 ©2025 Palo Alto Networks, Inc.

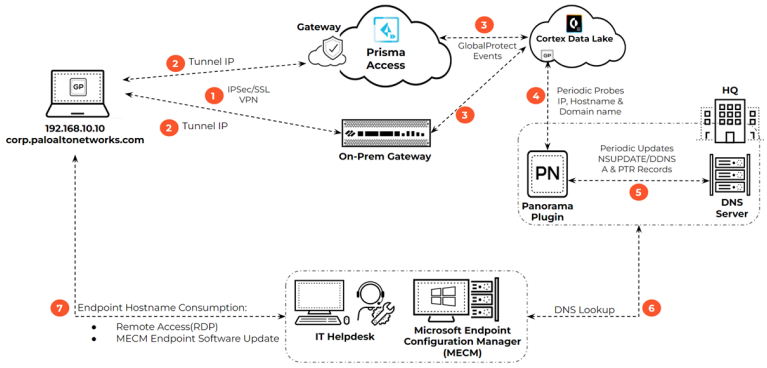
- *Nachdem Sie das Zeitintervall mit dem Befehl geändert haben, ist kein **Commit** erforderlich.*
- *Diese Zahlen stammen aus einer kontrollierten Umgebung und können unter realen Betriebsbedingungen anders lauten.*

5. Nach Erhalt der Aktualisierungen von Strata Logging Service speichert das Cloud Services-Plug-in die A- und PTR-Datensätze als NSUPDATE und aktualisiert den primären DNS-Server alle 15 Minuten.

   Wenn Sie das Zeitintervall mit dem Befehl `debug plugins cloud_services set-gp-ddns-interval` auf fünf Minuten geändert haben, aktualisiert das Plug-in den DNS-Server alle fünf Minuten.

   Wenn das Plug-in nicht in der Lage ist, den DNS-Server über NSUPDATE zu aktualisieren, wiederholt das Plug-in den Aktualisierungsvorgang maximal fünf Mal. Wenn die Aktualisierungen nicht erfolgreich waren, wiederholt das Plug-in den Aktualisierungsvorgang alle 15 Minuten bzw. alle fünf Minuten, sofern Sie das Intervall auf fünf Minuten geändert haben – jeweils maximal vier Mal. Daher versucht das Plug-in, die Ereignisse, die für maximal eine Stunde (wenn Sie ein 15-minütiges Intervall verwenden) oder 20 Minuten (wenn Sie ein 5-minütiges Intervall verwenden) protokolliert werden, zu aktualisieren, und beginnt danach von vorne.
6. Sobald die A- und PTR-Datensätze von mobilen GlobalProtect-Benutzern auf dem DNS-Server verfügbar sind, verwendet ein IT-Administrator oder eine Unternehmenssoftware diese Datensätze über eine DNS- oder RDNS-Suche und löst den Endpunktnamen oder die IP-Adresse auf.
7. Der IT-Administrator oder die Endpunktverwaltungssoftware verwendet diese Informationen, um den Endpunkt zu verwalten oder Softwareaktualisierungen per Push zu übertragen.

Dieser Workflow ist in der folgenden Abbildung veranschaulicht.




*Zum Anzeigen der Verbindungsfehlerprotokolle wählen Sie **Dashboard** > **Systemprotokolle** oder **Überwachen** > **Protokolle** > **System** für **Mobile_User_Device_Group** aus.*

### Dynamisches DNS – Richtlinien und Anforderungen

Stellen Sie vor dem Aktivieren von DDNS sicher, dass Ihr Bereitstellungs- und DNS-Server die folgenden Richtlinien und Anforderungen erfüllt:

- Ihre Client-Endpunkte müssen einer Domäne beigetreten sein.

 ©2025 Palo Alto Networks, Inc.

- Aktualisieren Sie Ihren GlobalProtect-Client auf die folgenden Versionen der GlobalProtect-App, basierend auf Ihrem Betriebssystem:
  - Windows: 5.2.11 oder höher
  - Mac: 5.2.11 oder höher
  - Linux: 5.3.3 oder höher
- Aktivieren Sie Strata Logging Service, wenn Sie nicht Prisma Access als lokales Gateway verwenden.
- Es ist ein Infoblox-DNS-Server mit einer Mindestversion von 8.6.1 oder höher erforderlich, der DDNS-Aktualisierungen über NSUPDATE unterstützt.
- DDNS wird von Prisma Access-Bereitstellungen mit mehreren Mandanten nicht unterstützt.
- Speichern Sie den Authentifizierungsschlüssel von Ihrem DNS-Server im base64-Format mit der Dateiendung .key. Sie können den Schlüssel nur in diesem Format in Prisma Access hochladen.
- Aktivieren Sie das NTP auf Ihrem DNS-Server und stellen Sie sicher, dass es dem von Prisma Access entspricht.
- Erstellen Sie Zonen in Infoblox für umgekehrte PTR- und Weiterleitungs-A-Adressen.

*Sie können dynamisches DNS in einer eigenständigen Bereitstellung mit Firewalls der nächsten Generation sowie mit Prisma Access bereitstellen. Für Firewalls gelten alle Voraussetzungen in diesem Abschnitt und Sie müssen zudem über eine gültige Strata Logging Service-Lizenz verfügen und das Cloud Services-Plug-in in Panorama für die Protokollierung verwenden.*

## DDNS für mobile Benutzer – GlobalProtect aktivieren

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Führen Sie die folgenden Schritte aus, um Ihren DNS-Server mit A- und PTR-Einträgen Ihrer mobilen GlobalProtect-Benutzer zu aktualisieren.

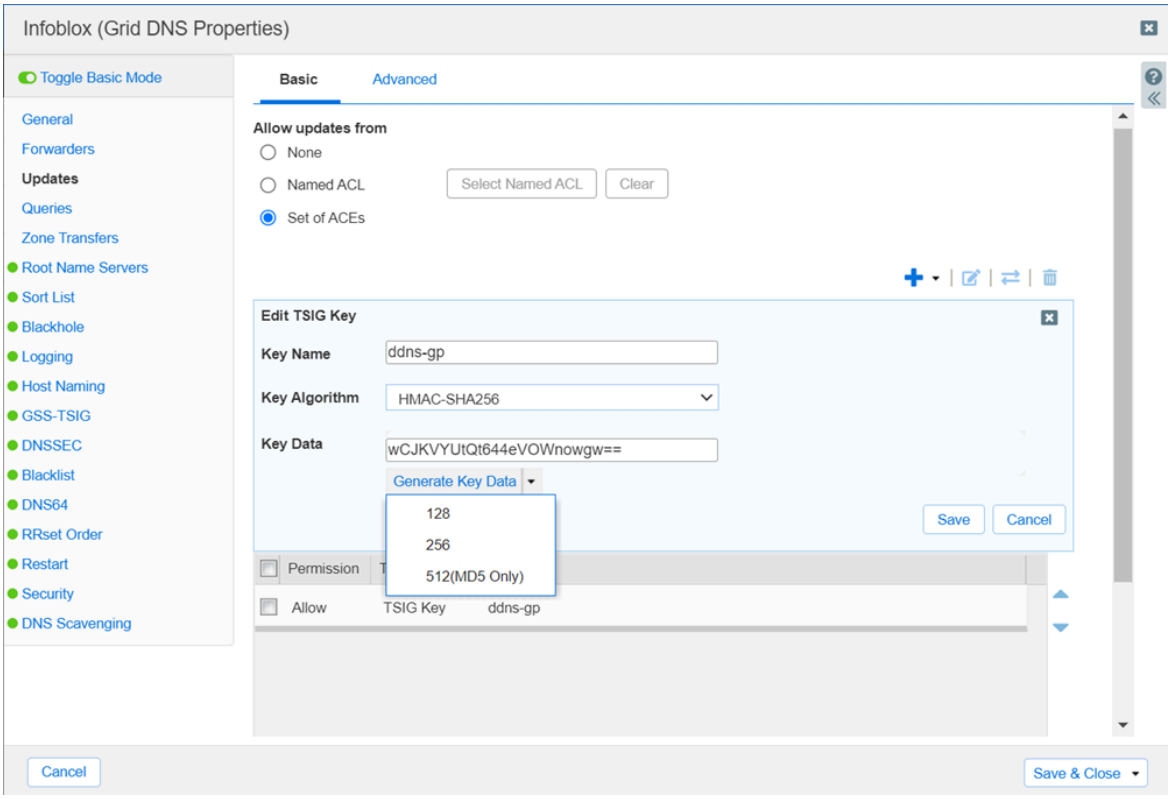
 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** Erstellen Sie einen Authentifizierungsschlüssel in Ihrem DNS-Server.

*Dieses Beispiel verwendet Infoblox als DNS-Server.*

1. Melden Sie sich bei Ihrem DNS-Server an.
2. Wählen Sie **Datenverwaltung** > **DNS** > **Grid-DNS-Eigenschaften** > **Updates** aus.
3. Lassen Sie Updates von **Reihe von ACEs** zu.
4. Fügen Sie einen **TSIG-Schlüssel** nach dem Ausfüllen der Details hinzu.

   - *Wählen Sie den Schlüsselalgorithmus **256** aus.*
   - ***Generieren Sie Schlüsseldaten**, um einen neuen Schlüssel zu erstellen. Wählen Sie die Schlüsseldaten **256** aus.*




5. Kopieren Sie die Schlüsseldaten in eine Datei im folgenden Format und speichern Sie die Datei mit der Dateiendung .key.

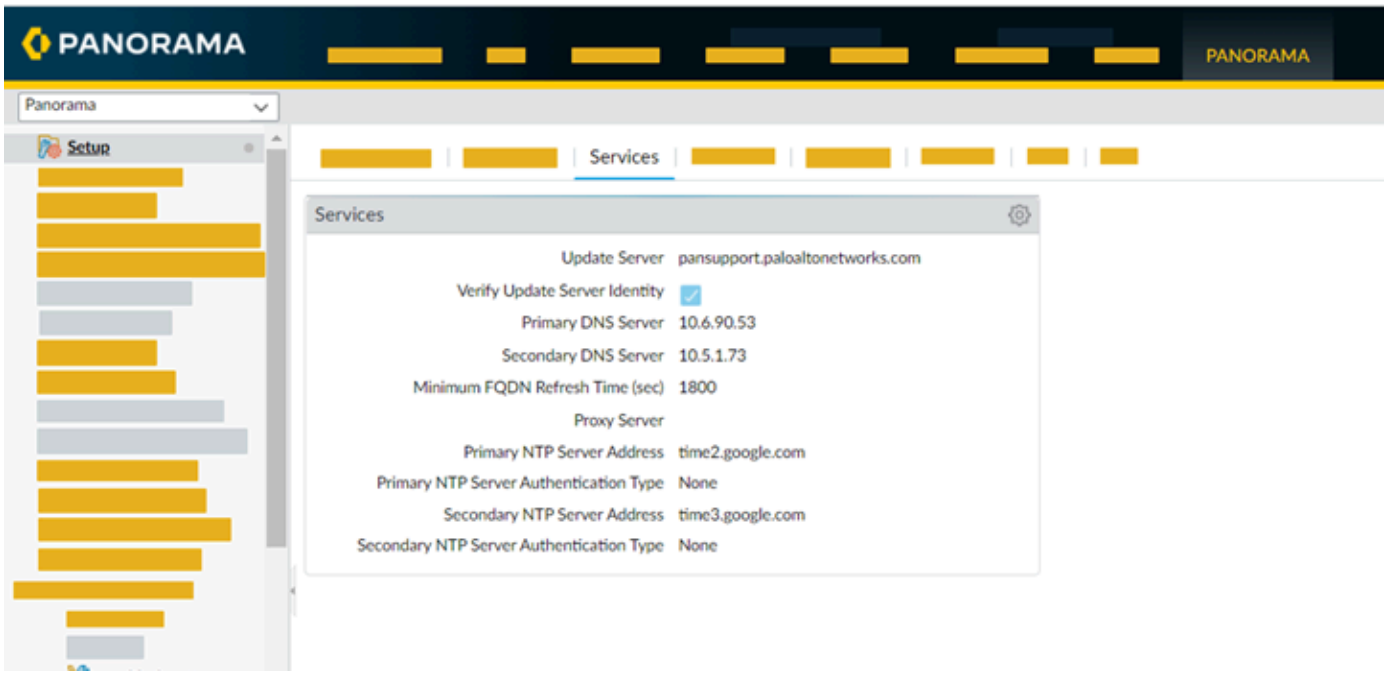
```
key "ddns-gp" { algorithm hmac-sha256; secret
 "wCJKVYUtQt644eVOWnowgw=="; };
```

Diesen Schlüssel laden Sie in einem späteren Schritt in das Cloud Services-Plugin von Prisma Access hoch.

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Geben Sie in Ihrer Prisma Access-Bereitstellung Ihren DNS-Server als primären DNS-Server an.

1. Wählen Sie **Panorama** > **Einrichtung** > **Dienste** aus.
2. **Bearbeiten** Sie die Einstellungen und aktualisieren Sie die Details des primären DNS-Servers.

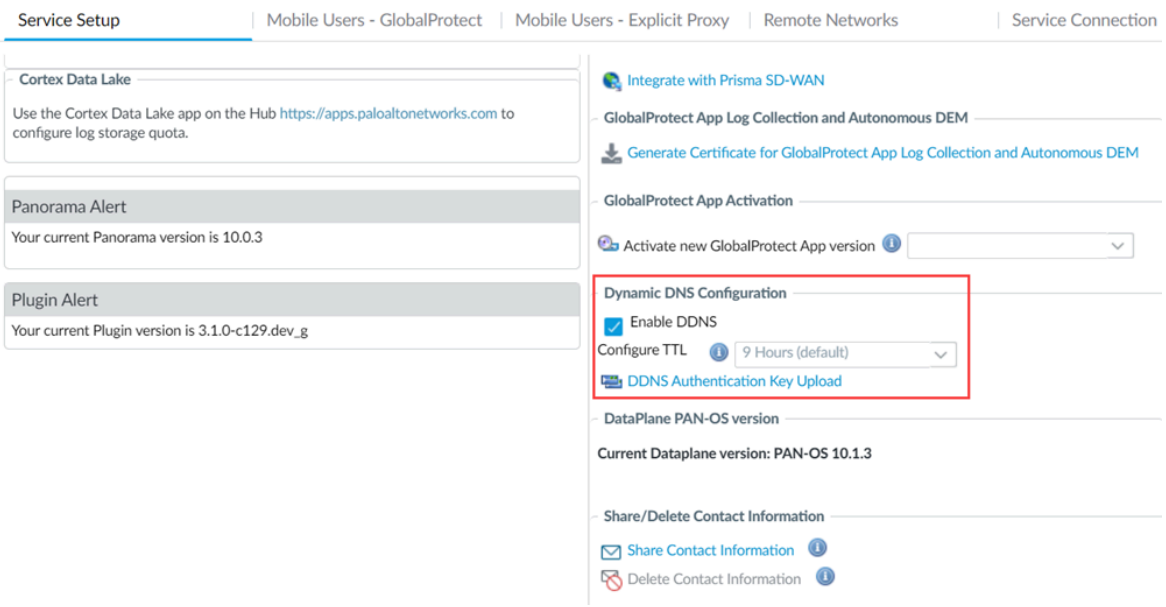



 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Konfigurieren Sie die DDNS-Einstellungen.

1. Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Diensteinrichtung** aus.
2. Wählen Sie **Dienstvorgänge** > **Konfiguration Dynamisches DNS** und **DDNS aktivieren** aus.
3. (Optional) **Konfigurieren Sie TTL**, den Time-to-Live(TTL)-Wert, auf die Frequenz, mit der Prisma Access den FDQN im Cache aktualisieren soll.

   Der Wert ist standardmäßig auf 9 Stunden eingestellt.




4. Laden Sie den DDNS-Authentifizierungsschlüssel, den Sie in Schritt 1 erstellt haben, von Ihrem DNS-Server hoch.

**STEP 4 |** **Führen Sie einen Commit in Panorama durch.**

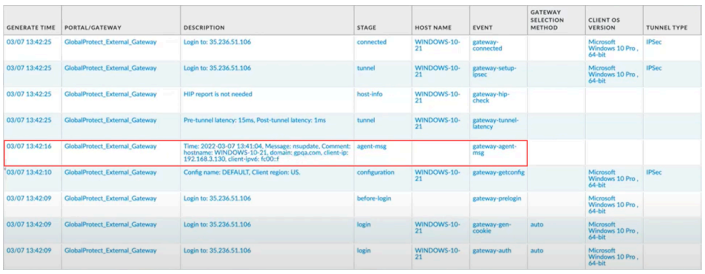
## Überprüfen der dynamischen DNS-Konfiguration (DDNS)

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Panorama | • Prisma Access-Lizenz |

Nachdem Sie DDNS aktiviert haben, überwachen Sie die Protokolle und beheben Sie Probleme, indem Sie die nachfolgenden Komponenten von Prisma Access überprüfen.

Wählen Sie die Optionen **Überwachen** > **Protokolle** > **GlobalProtect** aus. Die Gateway-Agent-Nachricht enthält den Hostnamen, den Domänennamen und die IP-Adresse des Tunnels. GlobalProtect sendet die Agent-Nachricht nur, wenn der Endpunkt Teil einer Domäne oder eines AD ist.


©2025 Palo Alto Networks, Inc.



| GENERATE TIME | PORTAL/GATEWAY | DESCRIPTION | STAGE | HOST NAME | EVENT | GATEWAY SELECTION METHOD | CLIENT OS VERSION | TUNNEL TYPE |
|---|---|---|---|---|---|---|---|---|
| 03/07 13:42:25 | GlobalProtect_External_Gateway | Login to: 35.236.51.106 | connected | WINDOWS-10-21 | gateway-connected | | Microsoft Windows 10 Pro , 64-bit | IPSec |
| 03/07 13:42:25 | GlobalProtect_External_Gateway | Login to: 35.236.51.106 | tunnel | WINDOWS-10-21 | gateway-setup-ipsec | | Microsoft Windows 10 Pro , 64-bit | IPSec |
| 03/07 13:42:25 | GlobalProtect_External_Gateway | HIP report is not needed | host-info | WINDOWS-10-21 | gateway-hip-check | | | |
| 03/07 13:42:25 | GlobalProtect_External_Gateway | Pre-tunnel latency: 15ms, Post-tunnel latency: 1ms | tunnel | WINDOWS-10-21 | gateway-tunnel-latency | | | |
| 03/07 13:42:16 | GlobalProtect_External_Gateway | Time: 2022-03-07 13:41:04, Message: msupdate, Comment: hostname: WINDOWS-10-21, domain: gpqa.com, client-ip: 192.168.3.130, client-ipv6: fc00:f | agent-msg | | gateway-agent-msg | | | |
| 03/07 13:42:10 | GlobalProtect_External_Gateway | Config name: DEFAULT, Client region: US. | configuration | WINDOWS-10-21 | gateway-getconfig | | Microsoft Windows 10 Pro , 64-bit | IPSec |
| 03/07 13:42:09 | GlobalProtect_External_Gateway | Login to: 35.236.51.106 | before-login | | gateway-prelogin | | Microsoft Windows 10 Pro , 64-bit | |
| 03/07 13:42:09 | GlobalProtect_External_Gateway | Login to: 35.236.51.106 | login | WINDOWS-10-21 | gateway-gen-cookie | auto | Microsoft Windows 10 Pro , 64-bit | |
| 03/07 13:42:09 | GlobalProtect_External_Gateway | Login to: 35.236.51.106 | login | WINDOWS-10-21 | gateway-auth | auto | Microsoft Windows 10 Pro , 64-bit | |

Aktivieren Sie den `gp_ddns_support.log`-Befehl in der Panorama CLI, um andere DDNS-Protokolle anzuzeigen.

# Kompromittierte Geräte in einer GlobalProtect-Bereitstellung von Prisma Access identifizieren und unter Quarantäne stellen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama)<br>• Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access-Lizenz |

Prisma Access ermöglicht es Ihnen, mit der GlobalProtect-App verbundene kompromittierte Geräte zu identifizieren und unter Quarantäne zu stellen. Hierfür müssen Sie Geräte entweder manuell oder automatisch zu einer Quarantäneliste hinzufügen. Nachdem Sie das Gerät unter Quarantäne gestellt haben, können Sie verhindern, dass das Gerät auf das Netzwerk zugreift, um eine konsistente Richtlinie zu gewährleisten.

Jeder Prisma Access-Standort mit mobilen Benutzern, kann seine Quarantäne-Informationen zwischen der Panorama-Instanz, die Prisma Access verwaltet, und der nächstgelegenen Dienstverbindung senden und empfangen. Wenn Sie über Firewalls oder Gateways der nächsten Generation verfügen, sollte die Dienstverbindung die Informationen zur Quarantäneliste an und von Panorama sowie an die und von den lokalen Firewalls oder Gateways neu verteilen. Sie sollten auch die Quarantänelisteninformationen von Panorama an die Dienstverbindung neu verteilen, um eine konsistente Richtliniendurchsetzung für alle Standorte mit mobilen Benutzern (Gateways) in Prisma Access sicherzustellen.

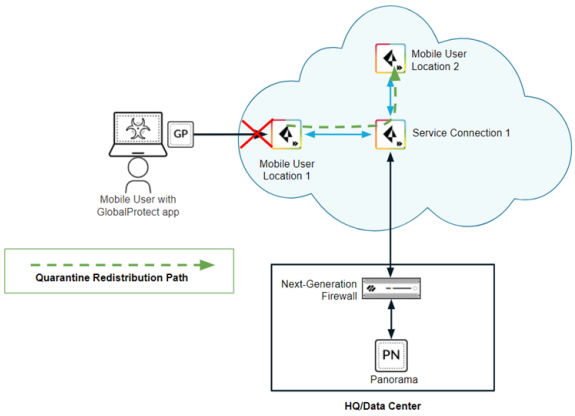
## Anwendungsfälle für die Umverteilung von Quarantänelisten

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama)<br>• Prisma Access (Managed by Strata Cloud Manager) | ❑ Prisma Access-Lizenz |

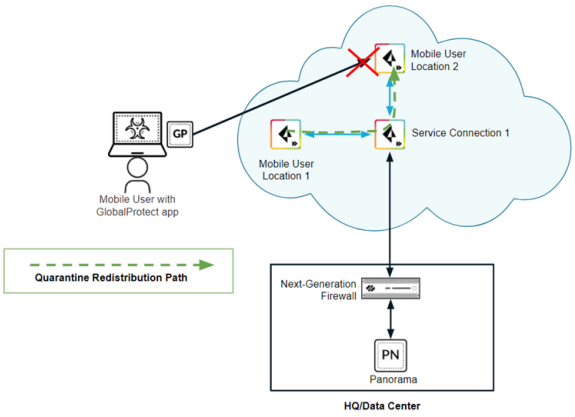
Im folgenden Abschnitt werden einige gängige Prisma Access-Bereitstellungen beschrieben, bei denen die Umverteilung von Quarantänelisten für die konsistente Durchsetzung von Richtlinien für kompromittierte Geräte nützlich ist.

 ©2025 Palo Alto Networks, Inc.

- **Umverteilung der Quarantäneliste zwischen Standorten für mobile Benutzer, die mit derselben Dienstverbindung verbunden sind**: Im folgenden Beispiel wird ein mobiler GlobalProtect-Benutzer, der mit Standort 1 für mobile Benutzer verbunden ist, kompromittiert und befindet sich automatisch in Quarantäne. Gemäß der Richtlinie blockiert oder beschränkt Prisma Access das unter Quarantäne stehende Gerät.



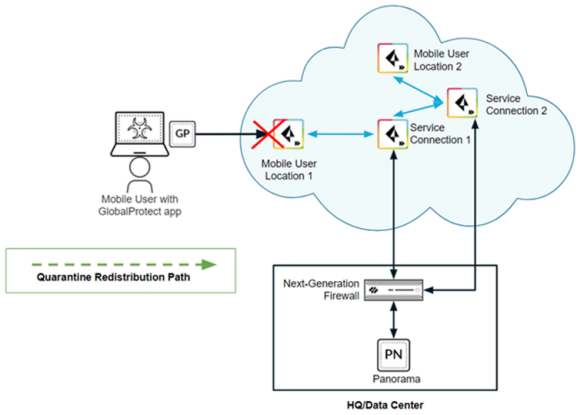

  Eine Dienstverbindung (in diesem Beispiel Dienstverbindung 1) verteilt die Quarantänelisteninformationen auf alle mobilen Benutzerstandorte, mit denen sie verbunden ist. Da der mobile Benutzerstandort 2 die umverteilten Quarantänelisteninformationen über die Dienstverbindung 1 empfängt, wird auch der Versuch des mobilen GlobalProtect-Benutzers blockiert, sich mit dem mobilen Benutzerstandort 2 zu verbinden.




- **Umverteilung der Quarantäneliste zwischen mobilen Benutzerstandorten, die mit verschiedenen Dienstverbindungen verbunden sind** – Im folgenden Beispiel gibt es zwei mobile Benutzerstandorte, die jedoch eine Verbindung zu zwei verschiedenen Dienstverbindungen herstellen. Ein GlobalProtect-Benutzer hat versucht, eine Verbindung

 ©2025 Palo Alto Networks, Inc.

zum mobilen Benutzerstandort 1 herzustellen. Der mobile Benutzerstandort 1 erkennt den GlobalProtect-Benutzerendpunkt als kompromittiert und stellt ihn unter Quarantäne.

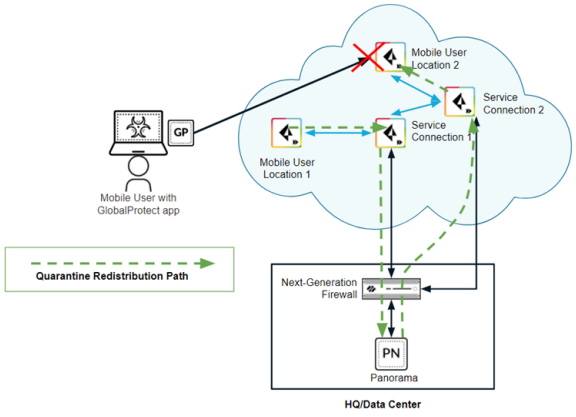



Gehen Sie wie folgt vor, um die Quarantänelisteninformationen vom mobilen Benutzerstandort 1 zum mobilen Benutzerstandort 2 umzuverteilen:

- Verteilen Sie die Quarantänelisteninformationen von Dienstverbindung 1 zu Panorama.
- Verteilen Sie die Quarantänelisteninformationen von Panorama auf die Dienstverbindung 2.

Wenn der GlobalProtect-Benutzer bei dieser Konfiguration eine Verbindung zum mobilen Benutzerstandort 1 herstellt und unter Quarantäne gestellt wird, werden die Quarantänelisteninformationen vom mobilen Benutzerstandort 1 auf den mobilen Benutzerstandort 2 umverteilt und alle Verbindungsversuche zum mobilen Benutzerstandort 2 werden blockiert.

*Diese Konfiguration ist auch gültig, wenn der GlobalProtect-Benutzer eine Verbindung zum mobilen Benutzerstandort 2 herstellt und in Quarantäne ist. Die Quarantänelisteninformationen werden vom mobilen Benutzerstandort 2 auf den mobilen Benutzerstandort 1 umverteilt.*



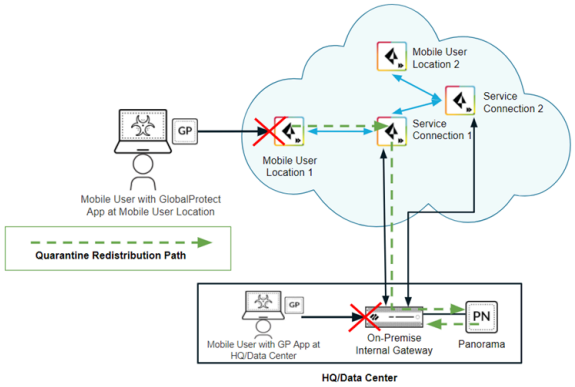

- **Umverteilung der Quarantäneliste zwischen Prisma Access und einer Firewall oder einem Gateway der nächsten Generation**: Im folgenden Beispiel versuchte ein GlobalProtect-Benutzer, eine Verbindung zum mobilen Benutzerstandort 1 herzustellen. Der mobile Benutzerstandort 1 erkennt den GlobalProtect-Benutzerendpunkt als kompromittiert und stellt ihn unter Quarantäne. Der mobile Benutzer begibt sich dann in die Unternehmenszentrale und

 ©2025 Palo Alto Networks, Inc.

versucht, sich erneut einzuloggen. Die Zentrale ist mit einer Firewall der nächsten Generation geschützt, die als GlobalProtect-Gateway mit interner Hosterkennung konfiguriert ist.

Der mobile Benutzerstandort 1 verteilt die Quarantänelisteninformationen über die Dienstverbindung 1 an Panorama und Panorama verteilt wiederum die Quarantänelisteninformationen an das interne Gateway vor Ort. Wenn der Benutzer versucht, sich vom Standort der Zentrale aus anzumelden, erkennt GlobalProtect, dass das lokale Gateway als internes Gateway konfiguriert ist, und verbindet sich ohne Tunnel mit dem Gateway.

Da die Quarantänelisteninformationen an das lokale Gateway umverteilt wurden, wird der Benutzer am Gateway basierend auf den konfigurierten Benutzerrichtlinien blockiert.



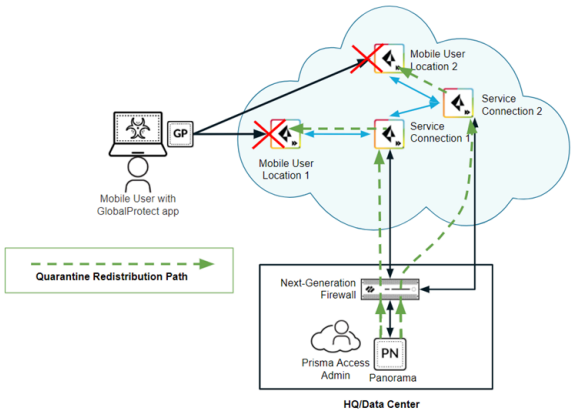

Wenn Sie eine Firewall oder ein Gateway der nächsten Generation mit Prisma Access verwenden, sollten Sie Panorama so konfigurieren, dass Quarantänelisteninformationen an die Firewall oder das Gateway, an alle Dienstverbindungen und an Panorama umverteilt werden.

- **Administrator stellt mobilen Benutzer in Panorama manuell unter Quarantäne**: In diesem Beispiel hat der Prisma Access-Administrator einen mobilen Benutzer manuell zur Quarantäneliste der Panorama-App hinzugefügt, die Prisma Access verwaltet. Der Administrator hat eine Umverteilung zwischen Panorama, der Firewall der nächsten Generation und den Dienstverbindungen eingerichtet. Panorama verteilt die aktualisierten Quarantänelisteninformationen an die Firewall und die Dienstverbindungen. Die Dienstverbindungen verteilen dann wiederum die Quarantänelisteninformationen an die mobilen Benutzerstandorte um.

  Der mobile Benutzer war mit dem mobilen Benutzerstandort 1 verbunden. Nachdem der mobile Benutzerstandort 1 die aktualisierten Quarantänelisteninformationen erhalten hat, wird der Benutzer getrennt. Wenn der Benutzer versucht, eine Verbindung zum mobilen

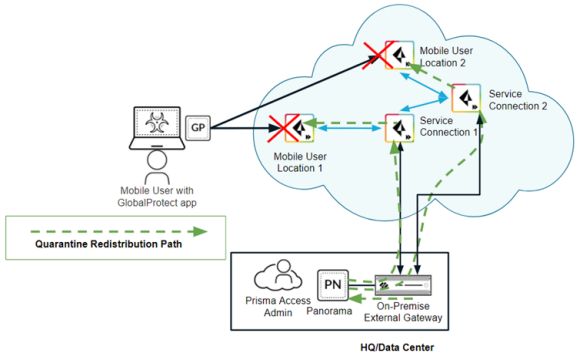
 ©2025 Palo Alto Networks, Inc.

Benutzerstandort 2 herzustellen, wird die Verbindung blockiert und der mobile Benutzer erhält eine Quarantänebenachrichtigung.




- **Der mobile Benutzer wird automatisch oder manuell am lokalen Gateway unter Quarantäne gestellt**: In diesem Beispiel wurde eine Firewall der nächsten Generation als externes Gateway am Standort der Unternehmenszentrale oder des Rechenzentrums konfiguriert. Der Administrator hat einen mobilen Benutzer am externen Gateway manuell unter Quarantäne gestellt. Das externe Gateway verteilt die Quarantänelisteninformationen vom externen Gateway an Panorama um.

  Nachdem Panorama die aktualisierten Quarantänelisteninformationen vom externen Gateway erhalten hat, verteilt es diese wiederum an die Serviceverbindungen 1 und 2 um, die sie dann an die mobilen Benutzerstandorte 1 und 2 umverteilen. Versucht ein mobiler Benutzer, eine Verbindung zum mobilen Benutzerstandort 1 oder 2 herzustellen, blockiert Prisma Access die Verbindung und der Benutzer erhält eine Quarantänebenachrichtigung.




## Konfigurieren der Quarantänelistenumverteilung in Prisma Access

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama)<br>• Prisma Access (Managed by Strata Cloud Manager) | ☐ Prisma Access-Lizenz |

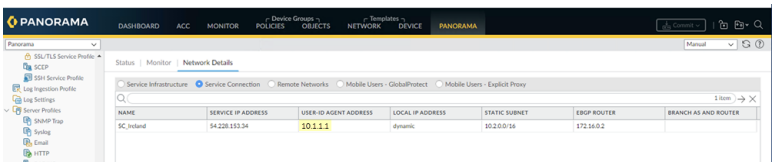

©2025 Palo Alto Networks, Inc.

Führen Sie die folgenden Schritte aus, um Quarantäneinformationen zwischen Dienstverbindungen, der zur Verwaltung von Prisma Access genutzten Panorama-Anwendung und Next-Generation Firewalls (NGFWs) umzuverteilen.

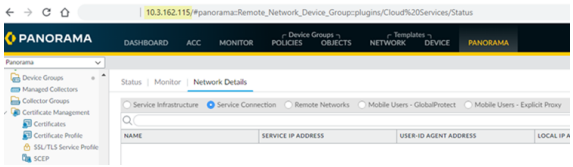
**STEP 1 |** Stellen Sie sicher, dass die Verwaltungs-IP-Adresse von Panorama mit der Benutzer-ID-Agent-Adresse für alle Dienstverbindungen kommunizieren kann, an die Sie Informationen zur Quarantäneliste umverteilen möchten.

Die Kommunikation zwischen der Benutzer-ID-Agent-Adresse der Dienstverbindung und der Verwaltungs-IP-Adresse von Panorama ist erforderlich, damit Prisma Access Quarantänelisteninformationen zwischen Panorama und den Dienstverbindungen senden und empfangen kann.

- Um die **Benutzer-ID-Agent-Adresse** aufzurufen, wählen Sie **Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Dienstverbindung** > **Benutzer-ID-Agent-Adresse** aus.




- Um die Verwaltungs-IP-Adresse der Panorama-Anwendung aufzurufen, die Prisma Access verwaltet, notieren Sie die IP-Adresse, die im Webbrowser angezeigt wird, wenn Sie auf Panorama zugreifen.




**STEP 2 |** Erlauben Sie Prisma Access, die Quarantänelisteninformationen umzuverteilen.

1. Wählen Sie in Panorama die Optionen **Panorama** > **Cloud Services** > **Konfiguration** > **Diensteinrichtung** aus.
2. Klicken Sie auf das Zahnradsymbol, um die Einstellungen zu bearbeiten.
3. Wählen Sie auf der Registerkarte **Erweitert Quarantänelistenumverteilung aktivieren** aus.

   Durch das Aktivieren der Quarantänelistenumverteilung kann Prisma Access die von einzelnen oder mehreren Standorten mit mobilen Benutzern (Gateways) empfangenen Quarantänelisteninformationen an Dienstverbindungen umverteilen.

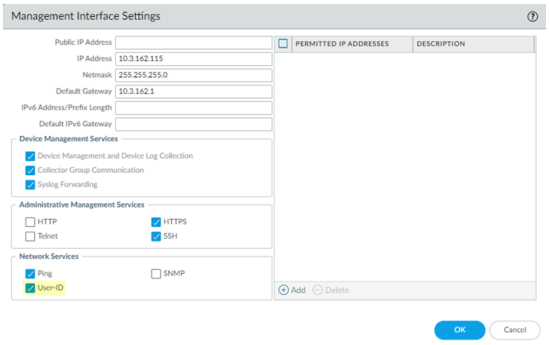



**STEP 3 |** Führen Sie die Aktion **Commit** und **Push** aus, um Ihre Änderungen festzuschreiben und zu übertragen.

 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** Konfigurieren Sie Panorama, um Quarantänelisteninformationen von Prisma Access zu erhalten, indem Sie die Einstellungen für die Verwaltungsschnittstelle konfigurieren.

1. Wählen Sie in der Panorama-Anwendung, die Prisma Access verwaltet, **Panorama** > **Einrichtung** > **Schnittstellen** aus.
2. Wählen Sie die **Verwaltungsschnittstelle** aus.
3. Wählen Sie **Benutzer-ID** aus.

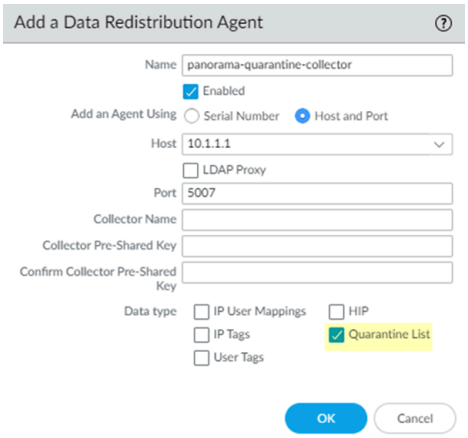



 ©2025 Palo Alto Networks, Inc.

**STEP 5 |** Konfigurieren Sie einen Datenweitergabe-Agent, der die Quarantänelisteninformationen von den Dienstverbindungen zu Panorama umverteilt.

1. Wählen Sie in der Panorama-Anwendung, die Prisma Access verwaltet, **Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Dienstverbindung** aus.
2. Notieren Sie die **Benutzer-ID-Agent-Adresse** (**Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Dienstverbindung** > **Benutzer-ID-Agent-Adresse**) für jede Dienstverbindung.
3. Wählen Sie **Panorama** > **Datenumverteilung** > **Agents** aus.
4. **Fügen** Sie einen Datenweitergabe-Agent hinzu, ordnen Sie ihm einen **Namen** zu und wählen Sie dann **Aktiviert** aus.
5. Geben Sie die **Benutzer-ID-Agent-Adresse** der Dienstverbindung als **Host** und 5007 als **Port** ein.

   *Stellen Sie sicher, dass Ihr Netzwerk den Zugriff auf diesen Port zwischen Panorama und Prisma Access nicht blockiert.*
6. (Optional) Wenn Sie diese Dienstverbindung als Kollektor konfiguriert haben (**Gerät** > **Datenumverteilung** > **Kollektoreinstellungen**), dann geben Sie einen Wert für **Kollektorname** und **Kollektor-PSK** ein.
7. Wählen Sie **Quarantäneliste** aus und klicken Sie dann auf **OK**.




8. Wiederholen Sie Schritt 5 für alle Dienstverbindungen in Ihrer Prisma Access-Bereitstellung.

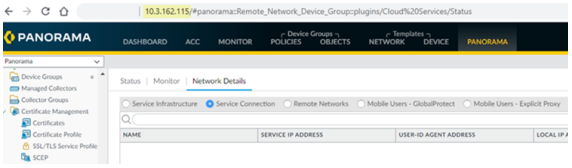
**STEP 6 |** Wählen Sie **Commit** > **Commit in Panorama** aus, um Ihre Änderungen lokal in der Panorama-Anwendung zu speichern, die Prisma Access verwaltet.

 ©2025 Palo Alto Networks, Inc.

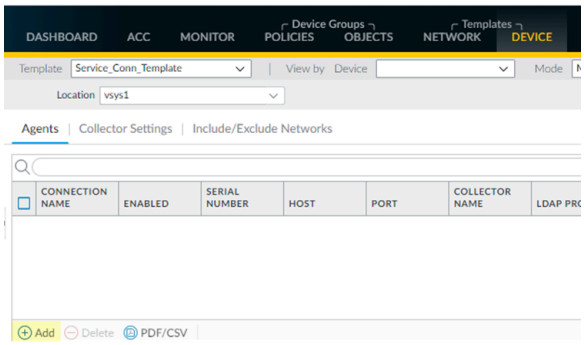
**STEP 7 |** Konfigurieren Sie einen Datenweitergabe-Agent, der Quarantänelisteninformationen von Panorama an die Dienstverbindungen umverteilt.

1. Suchen Sie die Verwaltungs-IP-Adresse der Panorama-Anwendung, die Prisma Access verwaltet.

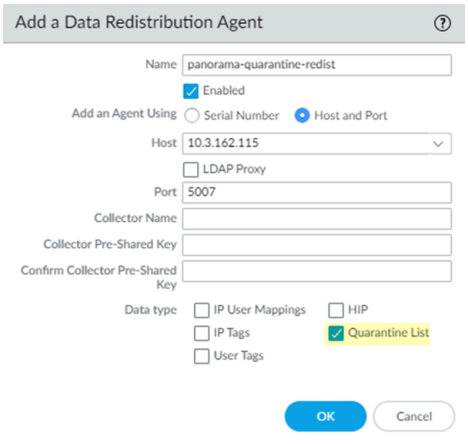
   Diese Adresse wird in der Adressleiste des Webbrowsers angezeigt, wenn Sie Panorama aufrufen.




2. Vergewissern Sie sich, dass Sie sich in der Vorlage **Service_Conn_Template** befinden, und wählen Sie dann **Gerät** > **Datenweitergabe** > **Agents** aus.




3. **Fügen** Sie einen Datenweitergabe-Agent hinzu, ordnen Sie ihm einen **Namen** zu und wählen Sie dann **Aktiviert** aus.
4. Geben Sie die Verwaltungs-IP-Adresse der Panorama-Anwendung als **Host** und 5007 als **Port** ein.



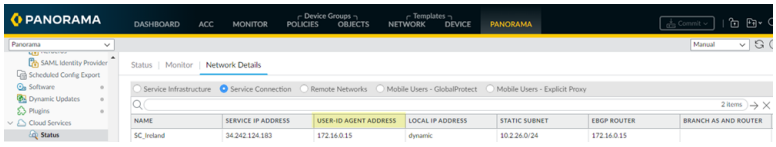

5. Wählen Sie **Quarantäneliste** aus und klicken Sie dann auf **OK**.

 ©2025 Palo Alto Networks, Inc.

**STEP 8 |** Konfigurieren Sie einen Datenweitergabe-Agent, der die Quarantänelisteninformationen von den Dienstverbindungen zu den Gateways der mobilen Benutzer umverteilt.

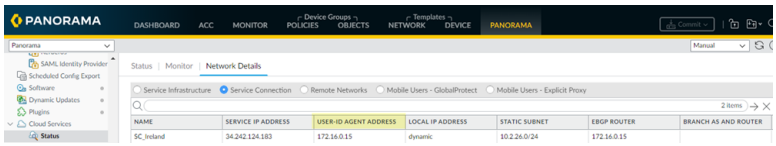
1. Wählen Sie in der Panorama-Anwendung, die Prisma Access verwaltet, **Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Dienstverbindung** aus.
2. Notieren Sie die **Benutzer-ID-Agent-Adresse** der Dienstverbindung, von der aus Sie Quarantänelisteninformationen umverteilen möchten.

   Da alle Dienstverbindungen über dieselben umverteilten Quarantänelisteninformationen verfügen, wählen Sie eine beliebige Dienstverbindung aus. Sie können auch mehrere Dienstverbindungen konfigurieren.




3. Vergewissern Sie sich, dass Sie sich in der Vorlage **Mobile_User_Template** befinden, und wählen Sie dann **Gerät** > **Datenweitergabe** > **Agents** aus.
4. **Fügen** Sie einen Datenweitergabe-Agent hinzu, ordnen Sie ihm einen **Namen** zu und wählen Sie dann die Option **Aktiviert** aus.
5. Geben Sie die **Benutzer-ID-Agent-Adresse** für die Dienstverbindung als Host und **5007** als Port ein.

   *Stellen Sie sicher, dass Ihr Netzwerk den Zugriff auf diesen Port zwischen Panorama und Prisma Access nicht blockiert.*
6. (Optional) Wenn Sie diese Dienstverbindung als Kollektor konfiguriert haben (**Gerät** > **Datenumverteilung** > **Kollektoreinstellungen**), dann geben Sie für **Kollektorname** und **Kollektor-PSK** einen Wert ein.
7. Wählen Sie **Quarantäneliste** aus und klicken Sie dann auf **OK**.




8. Führen Sie für Ihre Änderungen die Aktion **Commit und Push** aus.

**STEP 9 |** Zeigen Sie Ihre Quarantänelisteninformationen an, indem Sie **Panorama** > **Gerätequarantäne** auswählen.

Weitere Informationen finden Sie unter Quarantänegeräteinformationen anzeigen im GlobalProtect-Administratorhandbuch.

# IPv6-Datenverkehr in Bereitstellungen von „Mobile Benutzer – GlobalProtect“ gezielt umleiten oder blockieren

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager) | ☐ Prisma Access-Lizenz |

 ©2025 Palo Alto Networks, Inc.

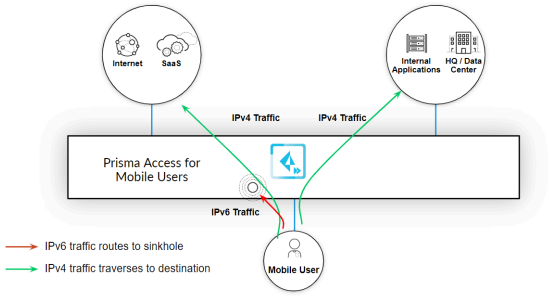
| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Panorama) | |

In einem Dual-Stack-Endpunkt, der sowohl IPv4- als auch IPv6-Datenverkehr verarbeiten kann, sendet die GlobalProtect-App den zu schützenden IPv4-Datenverkehr für mobile Benutzer durch den GlobalProtect-VPN-Tunnel an Prisma Access. IPv6-Datenverkehr für mobile Benutzer wird jedoch nicht standardmäßig an Prisma Access, sondern stattdessen an den lokalen Netzwerkadapter auf dem Endpunkt gesendet. Um die Angriffsfläche für IPv6-basierte Bedrohungen zu reduzieren, empfiehlt Palo Alto Networks, Prisma Access so zu konfigurieren, dass IPv6-Datenverkehr gezielt umgeleitet oder blockiert wird. Da Endpunkte automatisch ein Fallback auf eine IPv4-Adresse durchführen können, haben Sie die Möglichkeit, eine sichere und unterbrechungsfreie Benutzererfahrung für den Internet-Datenverkehr mobiler Benutzer zu ermöglichen.

*Die Standard-IPv6-Route hat Priorität vor anderen Routen. Wenn jedoch spezifischere IPv6-Routen über die physische Netzwerkschnittstelle vorhanden sind oder Sie die IPv6-Quelladresse der physischen Schnittstelle angeben, wird dieser Datenverkehr an den lokalen Netzwerkadapter gesendet.*

Darüber hinaus empfiehlt Palo Alto Networks, GlobalProtect so zu konfigurieren, dass der Netzwerkverkehr auf dem lokalen Netzwerkadapter vollständig deaktiviert wird. Wenn Sie über eine hybride Prisma Access-Bereitstellung mit lokalen Firewalls der nächsten Generation verfügen, die als GlobalProtect-Gateways konfiguriert sind, können Sie die IPv6-Sinkhole-Funktionalität auf dem lokalen GlobalProtect-Gateway konfigurieren.

Sie können Prisma Access so konfigurieren, dass der gesamte IPv6-Datenverkehr mobiler Benutzer umgeleitet oder blockiert wird. Wenn Sie diese Funktion aktivieren, weist Prisma Access dem Verbindungsendpunkt zusätzlich zu einer IPv4-Adresse eine IPv6-Adresse zu. Anschließend wird der IPv6-Datenverkehr an Prisma Access weitergeleitet und basierend auf einer integrierten Sicherheitsrichtlinie verworfen wie in der folgenden Abbildung dargestellt.



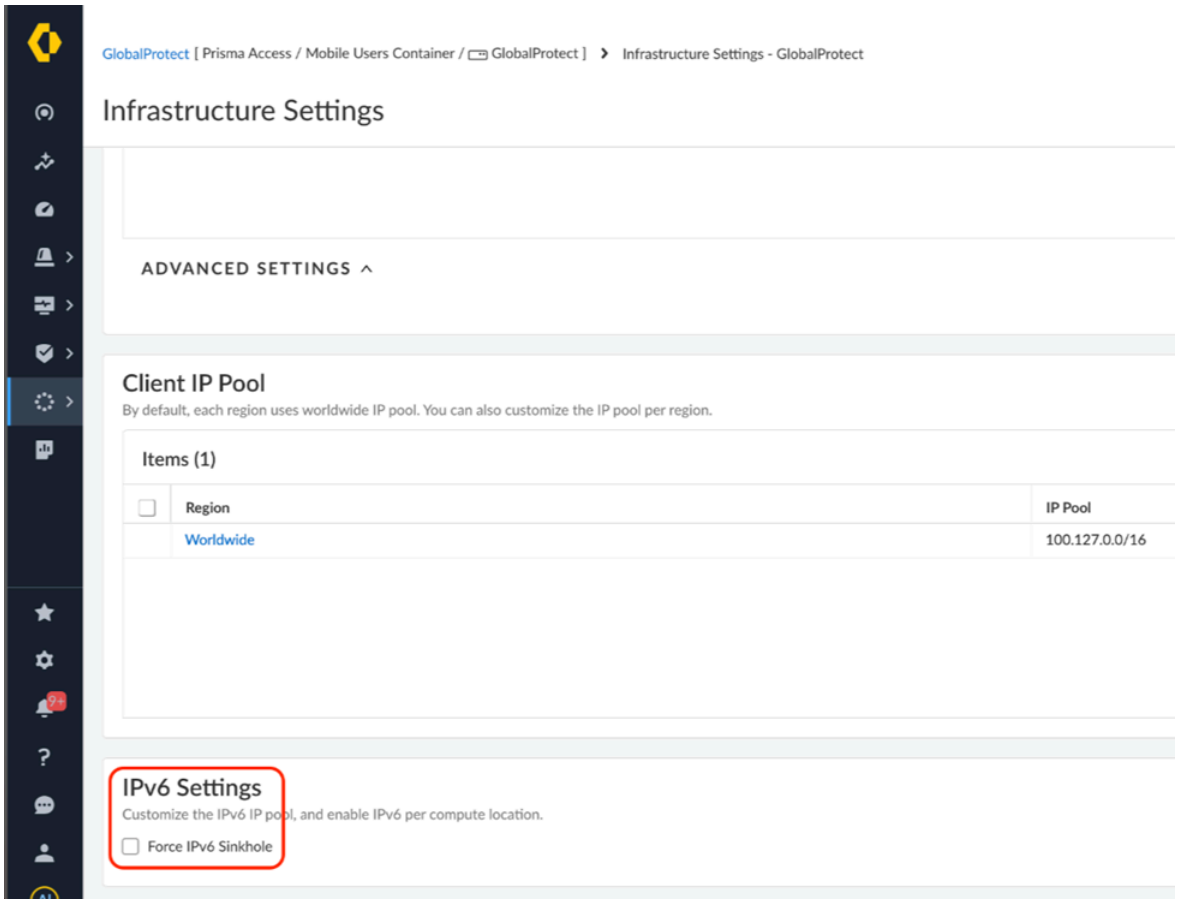

Gehen Sie wie folgt vor, um Prisma Access so zu konfigurieren, dass der gesamte IPv6-Datenverkehr für mobile Benutzer umgeleitet oder blockiert wird.

 ©2025 Palo Alto Networks, Inc.

- Prisma Access (Managed by Strata Cloud Manager)-Bereitstellungen:

  Wählen Sie **Workflows** > **Einrichtung Prisma Access** > **Mobile Benutzer** > **GlobalProtect-Einrichtung** > **Erweiterte Einstellungen** und **IPv6-Sinkhole erzwingen** aus.

  Prisma Access verwendet fc00:0:0:0:0:0:0:0/64 als Sinkhole-Adresse.




- Prisma Access (Managed by Panorama)-Bereitstellungen:

  1. Öffnen Sie eine sichere CLI-Sitzung mit Berechtigungen auf Administratorebene und verwenden Sie dieselbe IP-Adresse, mit der Sie sich bei der Panorama-Instanz anmelden, von der Prisma Access verwaltet wird.
  2. Geben Sie `configure` ein, um in den Konfigurationsmodus zu wechseln.
  3. Geben Sie den Befehl **`set plugins cloud_services mobile-users ipv6 yes`** ein.

     Wenn Sie diesen Befehl in Zukunft deaktivieren müssen, geben Sie **`set plugins cloud_services mobile-users ipv6 no`** ein.
  4. Geben Sie **`Commit`** ein, um Ihre Änderungen lokal zu speichern.
  5. Geben Sie **`exit`** ein, um den Konfigurationsmodus zu beenden.
  6. Geben Sie **`commit-all shared-policy include-template yes device-group Mobile_User_Device_Group`** ein, um Ihre Änderungen festzuschreiben, per Push zu übertragen und in Prisma Access zu aktivieren.

 ©2025 Palo Alto Networks, Inc.

## GlobalProtect so konfigurieren, dass der direkte Zugriff auf das lokale Netzwerk deaktiviert wird

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz<br>❑ Unterstützt auf allen GlobalProtect-Endpunkten unter macOS und Windows. Unterstützt auf Linux-Endpunkten ab GlobalProtect-App Version 6.0.0. |

Um sicherzustellen, dass der gesamte mobile Benutzerdatenverkehr an Prisma Access gesendet wird, können Sie das Senden von Daten über ausgehende Verbindungen, einschließlich des lokalen Subnetzdatenverkehrs, an den lokalen Adapter vollständig deaktivieren. Sie können alle ausgehenden Verbindungen zum lokalen Adapter deaktivieren, indem Sie Konfigurationsänderungen am GlobalProtect-Gateway vornehmen.

Sie können diese Schritte in Panorama oder auf einer lokalen Firewall ausführen, die als GlobalProtect-Gateway konfiguriert wurde.

*Aktivieren Sie die Einstellung **Kein direkter Zugriff auf das lokale Netzwerk**, um Risiken aufgrund nicht vertrauenswürdiger Netzwerke wie z. B. nicht zu kontrollierender WLAN-Zugangspunkte zu reduzieren.*

**STEP 1 |** Wählen Sie **Netzwerk** > **GlobalProtect** > **Gateways** aus.

**STEP 2 |** Wählen Sie ein vorhandenes GlobalProtect-Gateway aus oder **fügen** Sie ein neues Gateway hinzu.

**STEP 3 |** Wählen Sie **Agent** > **Clienteinstellungen** aus.

**STEP 4 |** Wählen Sie die Konfiguration **STANDARD** aus. Alternativ können Sie eine neue Konfiguration **hinzufügen**.

**STEP 5 |** Wählen Sie **Split-Tunnel** und dann **Kein direkter Zugriff auf lokales Netzwerk** aus.

*Durch das Deaktivieren des lokalen Netzwerkzugriffs wird das Senden des gesamten Datenverkehrs, einschließlich des IPv4- und IPv6-Datenverkehrs, an den lokalen Adapter verhindert. Darüber hinaus können Sie nicht auf Ressourcen im lokalen Subnetz, z. B. auf Drucker, zugreifen. Der Split-Tunnel-Datenverkehr auf Basis einer Zugriffsroute, Zieldomäne und einer Anwendung funktioniert weiterhin wie erwartet.*




 ©2025 Palo Alto Networks, Inc.

**STEP 6 |** (Nur Panorama- und Prisma Access-Bereitstellungen) Schreiben Sie Ihre Änderungen mit Commit lokal fest, um sie in Panorama zu aktivieren.

1. Wählen Sie **Commit** > **Commit in Panorama** aus.
2. Stellen Sie sicher, dass Ihre Änderung Teil des **Festschreibungsumfangs** ist.
3. Klicken Sie auf **OK**, um Ihre Änderungen im Übertragungsumfang zu speichern.
4. Übernehmen Sie mit **Commit** die Änderungen.

**STEP 7 |** Verwenden Sie **Commit** und **Push**, um Ihre Änderungen festzuschreiben und zu übertragen, sodass sie in Prisma Access aktiviert werden.

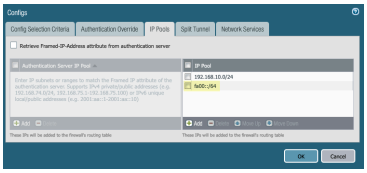
## IPv6-Sinkhole auf dem lokalen Gateway einrichten

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Wenn Sie über eine Hybrid-Bereitstellung verfügen, die Firewalls der nächsten Generation verwendet, die als Gateways mit Prisma Access konfiguriert sind, gehen Sie auf dem lokalen Gateway wie folgt vor, um den IPv6-Datenverkehr zu löschen.

**STEP 1 |** Fügen Sie Ihrer GlobalProtect-Agentkonfiguration IPv6-IP-Pools hinzu.

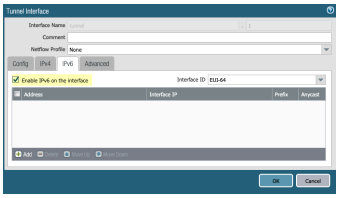
1. Wählen Sie **Netzwerk** > **GlobalProtect** > **Gateways** aus.
2. Wählen Sie ein vorhandenes GlobalProtect-Gateway aus oder **fügen** Sie ein neues Gateway hinzu.
3. Wählen Sie **Agent** > **Clienteinstellungen** aus.
4. Wählen Sie die zu ändernde Agent-Konfiguration aus. Alternativ können Sie auch eine neue Agent-Konfiguration **hinzufügen**.
5. Wählen Sie **IP-Pools** aus. Anschließend müssen Sie einen IPv6-Pool **hinzufügen**, der dem virtuellen Netzwerkadapter auf den Endpunkten zugewiesen werden soll, die eine Verbindung zum GlobalProtect-Gateway herstellen, der für den Netzwerkverkehr mobiler Benutzer verwendet wird, und klicken Sie auf **OK**.




 ©2025 Palo Alto Networks, Inc.

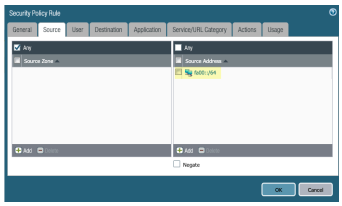
**STEP 2 |** Aktivieren Sie IPv6 auf der Schnittstelle.

1. Wählen Sie **Gerät** > **Schnittstelle** > **Tunnel** und schließlich die Tunnel-**Schnittstelle** aus, die Sie für den Datenverkehr des mobilen Benutzers verwenden.
2. Wählen Sie **IPv6** aus. Anschließend wählen Sie **IPv6 auf der Schnittstelle aktivieren** aus.

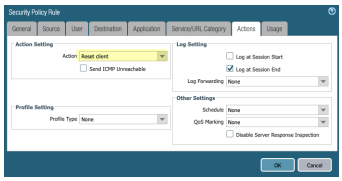


**STEP 3 |** Fügen Sie eine Sicherheitsrichtlinie hinzu, um eine Aktion zum Zurücksetzen des TCP festzulegen, mit der Sitzungen mit IPv6-Quelldatenverkehr beendet werden, die den IP-Pools entsprechen, die Sie in Schritt 1 konfiguriert haben.

1. Wählen Sie **Richtlinien** > **Sicherheit** aus, um eine neue Sicherheitsrichtlinie **hinzuzufügen**.
2. Legen Sie die **Quelladresse** in der Regel so fest, dass sie den IP-Pools entspricht, die Sie in Schritt 1 konfiguriert haben.



3. Wählen Sie **Aktionen** aus. Wählen Sie anschließend die **Aktionseinstellung Client zurücksetzen** aus und klicken Sie auf **OK**.



**STEP 4 |** Übernehmen Sie mit **Commit** die Änderungen.

**STEP 5 |** (Optional) Führen Sie diese Aufgabe auf allen Gateway-Firewalls in Ihrer Bereitstellung aus.

# HIP-Informationen mit Prisma Access weitergeben

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Zur Gewährleistung einer konsistenten Durchsetzung der Host Information Profile(HIP)-Richtlinien und zur Vereinfachung der Richtlinienverwaltung können Sie HIP-Informationen weitergeben, die Sie von mobilen Benutzern und Benutzern in Remote-Netzwerken erhalten

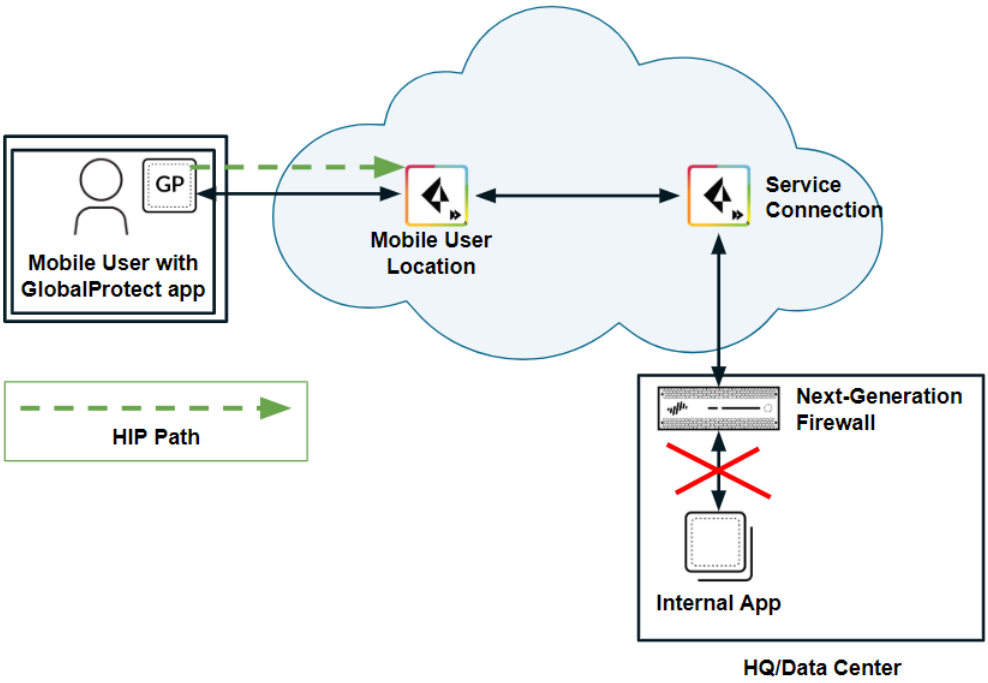
 ©2025 Palo Alto Networks, Inc.

haben. Diese werden von der GlobalProtect-App von Prisma Access für andere Gateways, Firewalls und Panorama-Appliances in Ihrem Unternehmen verwendet, darunter das von Prisma Access verwaltete Panorama.

Im folgenden Abschnitt werden einige gängige Prisma Access-Bereitstellungen beschrieben, bei denen die Weitergabe von HIP-Informationen für die konsistente Durchsetzung von Richtlinien und die Anzeige von HIP-Berichten nützlich ist:

- **Weitergabe von HIP-Informationen von Prisma Access an eine Firewall der nächsten Generation** – Wenn Sie im Rechenzentrum oder in der Zentrale Ihres Unternehmens über eine Firewall der nächsten Generation verfügen und diese Firewall mit HIP-basierten Sicherheitsrichtlinien konfiguriert haben, können Sie diese Richtlinien für mobile Prisma Access-Benutzer erst durchsetzen, wenn Sie die HIP-Informationen von Prisma Access an die Firewall weitergeben.

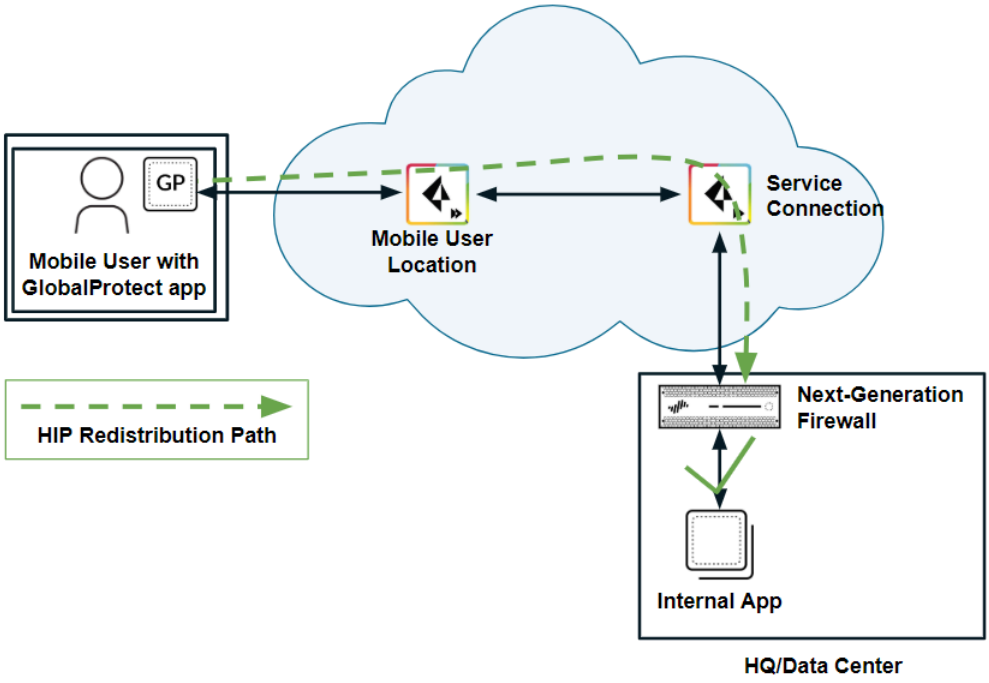
  Die folgende Abbildung zeigt einen mobilen Benutzer, dessen Endpunkt mit der GlobalProtect-App geschützt ist. Der Benutzer versucht, auf eine interne App in einer Zentrale / einem Rechenzentrum zuzugreifen, dessen Zugriff durch eine Firewall der nächsten Generation mit HIP-basierten Sicherheitsrichtlinien gesteuert wird. Wenn sich der Benutzer bei der GlobalProtect-App anmeldet, sammelt die App HIP-Informationen und sendet diese anPrisma Access. Prisma Access gibt diese Informationen jedoch nicht an die lokale Firewall weiter. Da die Firewall nicht über die HIP-Informationen des Benutzers verfügt, blockiert sie den Zugriff des Benutzers auf die App.



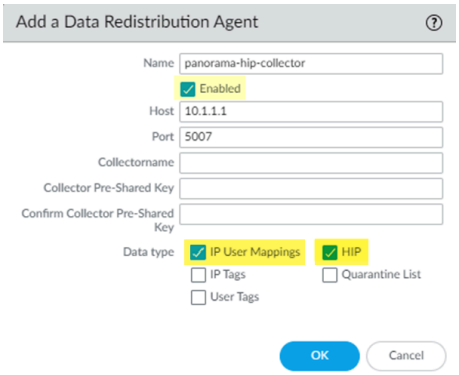

  Die Weitergabe von HIP-Informationen ermöglicht es Ihnen, die HIP-Informationen der mobilen Benutzer an die lokale Firewall weiterzugeben. Die Firewall kann dann die HIP-

 ©2025 Palo Alto Networks, Inc.

Informationen des Benutzers anhand der konfigurierten Sicherheitsrichtlinien überprüfen und dem Benutzer Zugriff auf die App gewähren.



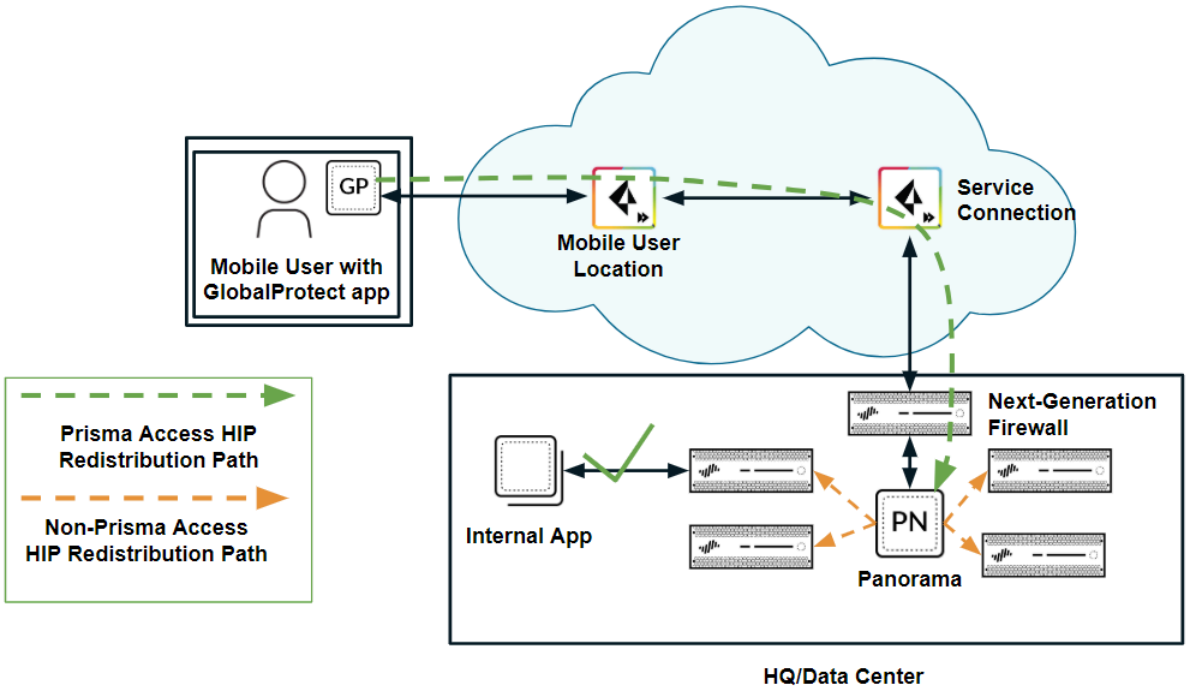

Wenn Sie HIP-Informationen von Prisma Access an die Firewall weitergeben möchten, erlauben Sie Prisma Access die Weitergabe von HIP-Informationen. **Fügen** Sie anschließend einen **Benutzer-ID-Agenten** (**Panorama** > **Benutzeridentifikation** > **Benutzer-ID-Agenten** für Panorama-Appliances der Version 9.1.*x* oder **Panorama** > **Datenweitergabe** für Panorama-Appliances der Version 10.*x*) in der Firewall hinzu und geben Sie diePrisma Access **Benutzer-ID-Agent-Adresse** (**Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Dienstverbindung** > **Benutzer-ID-Agent-Adresse**) als **Host** (im folgenden Beispiel: 10.1.1.1) und **5007** als **Port** an.




- **HIP-Weitergaben von Prisma Access an Panorama** – Wenn Sie in Ihrem Unternehmen mehrere Firewalls oder Gateways mit HIP-basierten Sicherheitsrichtlinien haben, können Sie die HIP-Informationen von Prisma Access an das Panorama weitergeben, das Prisma Access verwaltet. Erstellen Sie hierzu einen Benutzer-ID-Agenten in Panorama und geben Sie die **Benutzer-ID-Agent-Adresse** von Prisma Access als Benutzer-ID-**Host** an. Anschließend können Sie HIP-Berichte von dieser Panorama-Appliance an die anderen verwalteten

 ©2025 Palo Alto Networks, Inc.

Panorama-Appliances, Gateways, Firewalls und virtuellen Systeme in Ihrem Unternehmen weitergeben. Verwenden Sie dazu denselben Workflow, den Sie verwenden, um Benutzer-ID-Informationen an verwaltete Firewalls weiterzugeben und konsistente Richtlinien für interne Apps und Ressourcen durchzusetzen, wie in der folgenden Abbildung dargestellt.




Alternativ können Sie jede interne Firewall oder jedes Gateway in Ihrem Unternehmen so konfigurieren, dass HIP-Informationen direkt von Prisma Access erfasst werden, ohne Panorama als zentralen Standort zu verwenden. Hierzu erstellen Sie auf jedem Gerät einen Benutzer-ID-Agenten. Beachten Sie jedoch, dass Prisma Access Dienstverbindungen zum Senden von HIP-Informationen verwendet und der Bandbreitenverbrauch der Dienstverbindung steigen kann, wenn Prisma Access eine große Anzahl von HIP-Berichten sendet.

- **Weitergabe von HIP-Informationen von einem Benutzer in einem Remote-Netzwerk an Prisma Access** – In früheren Anwendungsfällen wurde gezeigt, wie Prisma Access HIP-Informationen von mobilen Benutzern sammelt. Wenn Sie HIP-basierte Richtlinien in Prisma Access für einen Benutzer an einem Remote-Netzwerkstandort anwenden möchten, müssen Sie einen Weg finden, die HIP-Informationen aus der GlobalProtect-App des Remote-Netzwerkbenutzers an Prisma Access weiterzugeben.

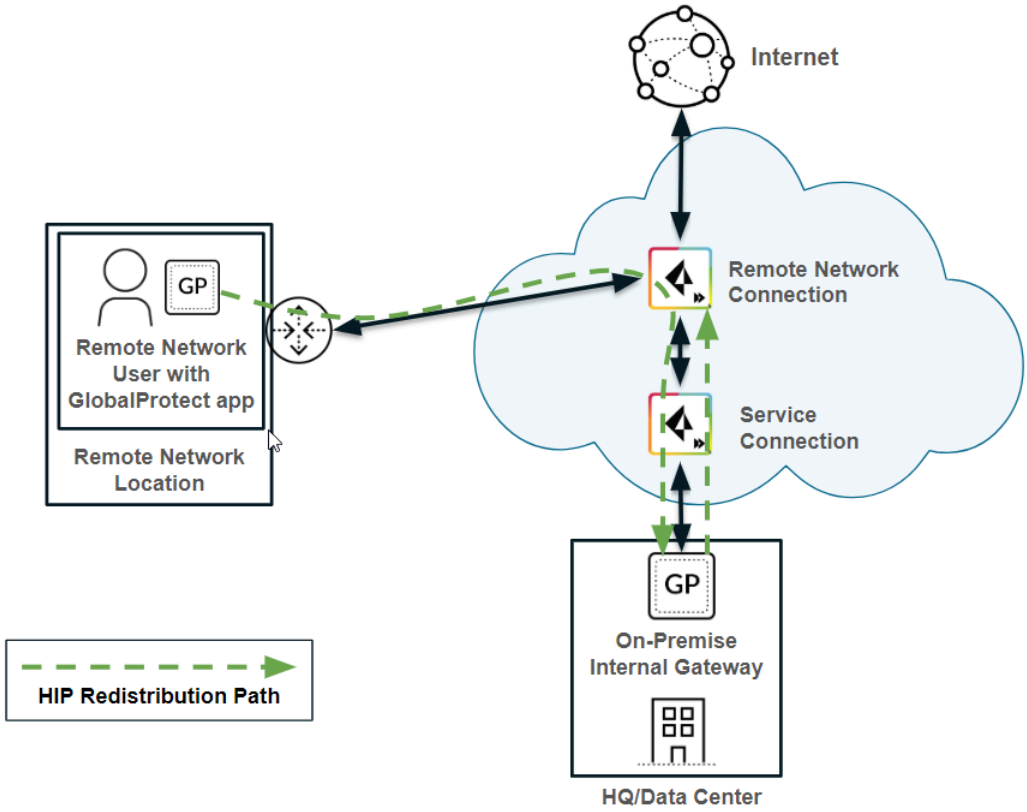
  Das folgende Beispiel zeigt einen Benutzer an einem Remote-Netzwerkstandort, dessen Internetzugang sich in der Remote-Netzwerkverbindung befindet. In Prisma Access steuern Sie den Internetzugang des Benutzers am Remote-Netzwerkstandort mit Sicherheitsrichtlinien, die in der **Remote_Network_Device_Group** oder in einer gemeinsam genutzten Gerätegruppe erstellt wurden. Für eine ordnungsgemäße Durchsetzung der Richtlinien am Remote-Netzwerkstandort für den Benutzer müssen Sie Prisma Access so konfigurieren, dass die HIP-Informationen des Benutzers vom internen Gateway abgerufen werden.

  In diesem Beispiel überprüft das GlobalProtect-Gateway in der Zentrale / im Rechenzentrum, die bzw. das über die interne Hosterkennung als internes Gateway konfiguriert ist, die HIP-Informationen des Benutzers aus der GlobalProtect-App des Benutzers. Das interne Gateway

 ©2025 Palo Alto Networks, Inc.

erkennt, dass sich der Benutzer innerhalb des Remote-Netzwerkstandorts befindet, und sammelt sowohl Benutzer-ID- als auch HIP-Informationen des Benutzers.

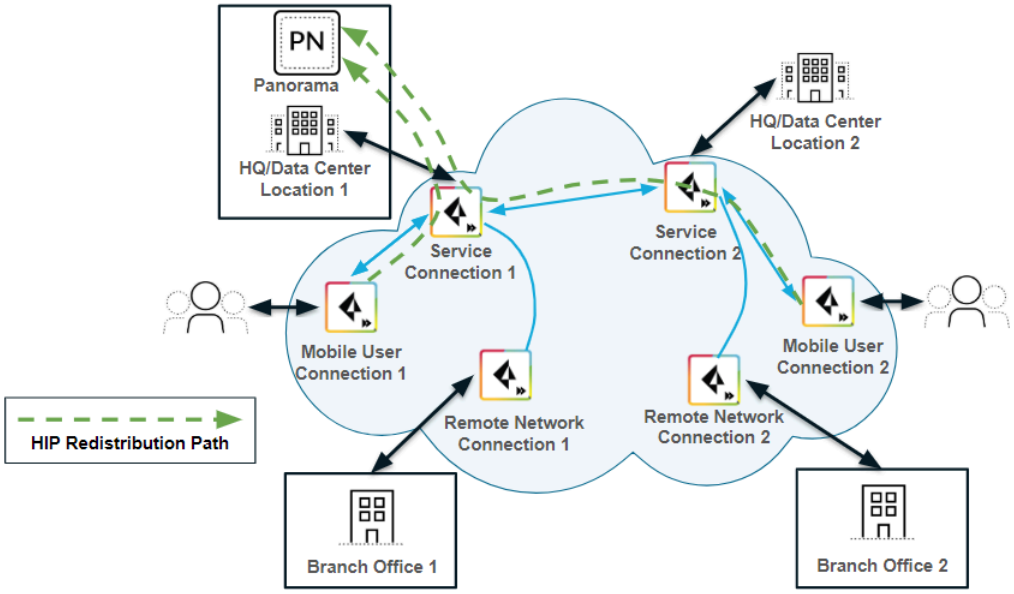
Erstellen Sie zur Weitergabe dieser HIP-Informationen vom internen Gateway an Prisma Access einen Benutzer-ID-Agenten in Panorama und geben Sie die IP-Adresse des internen Gateways als Host an.




- **Detaillierte HIP-Protokolle von Panorama anzeigen** – Wenn sich mobile Benutzer mit der GlobalProtect-App anmelden, sendet die App die HIP-Informationen an Prisma Access. Panorama ruft die Protokollergebnisse von Strata Logging Service ab, um die Ergebnisse der HIP-Übereinstimmungsprotokolle anzusehen (**Überwachen** > **Protokolle** > **HIP-Übereinstimmung**). Sie können jedoch erst dann detaillierte HIP-Berichte anzeigen, wenn Sie

 ©2025 Palo Alto Networks, Inc.

Panorama so konfiguriert haben, dass HIP-Berichtsdetails von Prisma Access an Panorama weitergegeben werden.

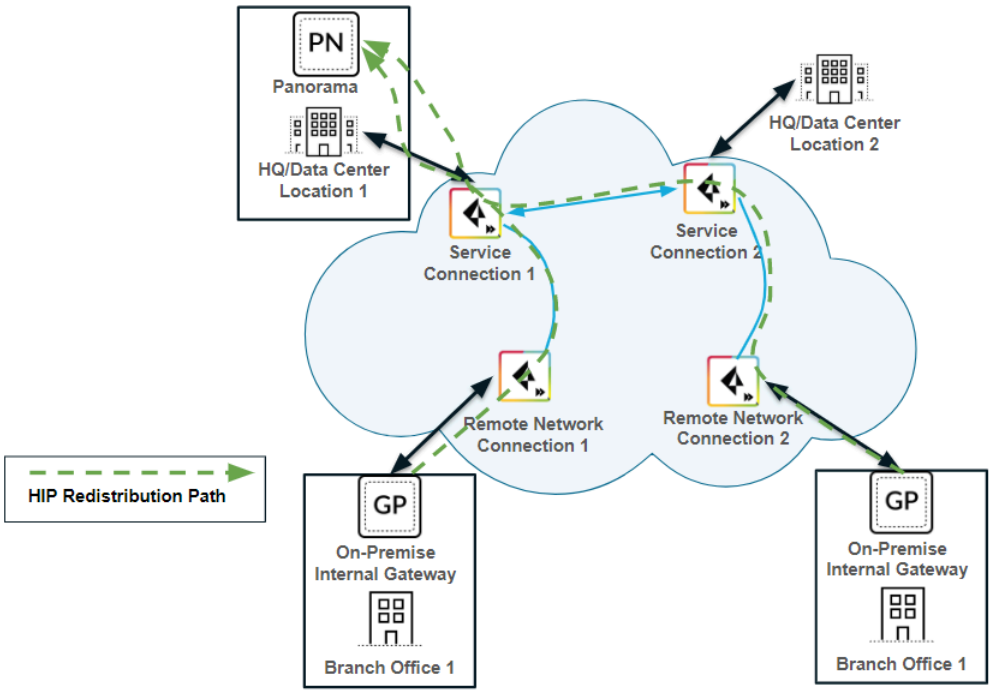



Erstellen Sie zur Weitergabe detaillierter HIP-Informationen von mobilen Benutzern an Panorama einen Benutzer-ID-Agenten in Panorama und geben Sie die **Benutzer-ID-Agent-Adresse** (**Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Dienstverbindung** > **Benutzer-ID-Agent-Adresse**) als Benutzer-ID-Host an.

Wenn Sie ein lokales Gateway als internes Gateway an einem Remote-Benutzerstandort konfiguriert haben, können Sie auch die HIP-Informationen für Benutzer in Remote-Netzwerken an Panorama senden, indem Sie in Panorama einen Benutzer-ID-Agenten erstellen

 ©2025 Palo Alto Networks, Inc.

und die **EBGP-Router-Adresse** des Remote-Netzwerks (**Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Remote-Netzwerke** > **EBGP-Router**) als Benutzer-ID-Host angeben.




Aktivieren und konfigurieren Sie die Weitergabe der HIP-Informationen inPrisma Access:

- Konfigurieren der HIP-Umverteilung in Prisma Access

## Konfigurieren der HIP-Umverteilung in Prisma Access

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

Wenn ein mobiler Benutzer, auf dessen Endpunkt die GlobalProtect-App installiert ist, eine Verbindung zu Prisma Access herstellt, erfasst Prisma Access die HIP-Informationen des Benutzers aus der GlobalProtect-App des Endpunkts, wodurch der HIP-Bericht in Prisma Access bereitgestellt wird.

*Um die HIP-Umverteilung verwenden zu können, müssen Benutzer die GlobalProtect-App auf ihrem Endpunkt installiert haben. Während Prisma Access Clientloses VPN unterstützt, können Sie HIP-Informationen für Benutzer eines clientlosen VPN nicht umverteilen.*

Die HIP-Umverteilung ist sowohl für mobile Benutzer als auch für Benutzer in Remote-Netzwerken anwendbar. Für Benutzer in Remote-Netzwerken muss ein lokales Gateway jedoch mithilfe der internen Hosterkennung feststellen, dass sich der Benutzer intern im Netzwerk der

 ©2025 Palo Alto Networks, Inc.

Organisation befindet, bevor das lokale Gateway HIP-Informationen an Prisma Access senden kann.

*In Prisma Access konfigurieren Sie die interne Hosterkennung, wenn Sie Ihre Bereitstellung für mobile Benutzer konfigurieren.*

Um eine konsistente Richtliniendurchsetzung zu gewährleisten, können Sie die HIP-Umverteilung verwenden, um Prisma Access das Verteilen der HIP-Informationen von Benutzern an andere Panorama-Appliances, Gateways, Firewalls und virtuelle Systeme in Ihrer Bereitstellung und die Verteilung von HIP-Informationen von diesen Geräten an Prisma Access in einigen Fällen zu erlauben. Mit dieser Funktion können Sie die HIP-basierte Richtliniendurchsetzung konsistent für den Datenverkehr der Benutzer anwenden. Dies gilt auch für Richtlinien für den internetgebundenen Datenverkehr oder für Datenverkehr, der auf eine interne Anwendung oder Ressource in der Zentrale oder im Rechenzentrum Ihrer Organisation zugreift. Durch die Umverteilung von HIP-Informationen an die Panorama-Appliance können Sie auch detaillierte HIP-Informationen für Prisma Access-Benutzer anzeigen, die von dieser Appliance stammen.

Beachten Sie, dass die internen und externen Gateways von GlobalProtect keine Unterstützung für die bidirektionale HIP-Umverteilung bieten. Daher hat es sich bewährt, die Panorama-Appliance als Umverteilungspunkt zu verwenden. In dieser Bereitstellung konfigurieren Sie Ihre internen und externen Gateways so, dass die HIP-Berichte an Panorama gesendet werden. Panorama leitet sie an Ihre Firewalls weiter, um eine konsistente Richtliniendurchsetzung in Ihrer Umgebung zu gewährleisten.

- Strata Cloud Manager
- Panorama

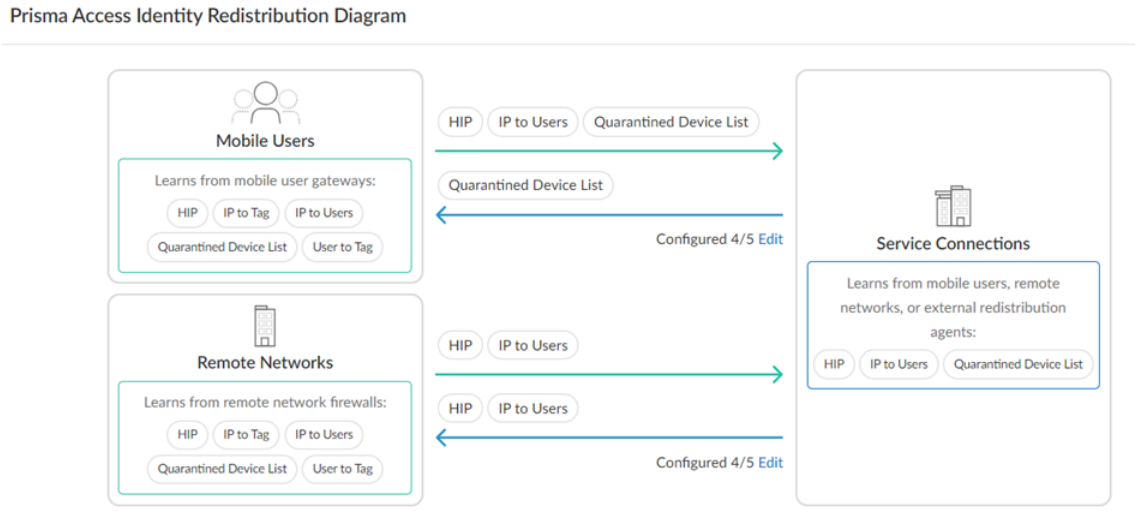
### Konfigurieren der HIP-Umverteilung in Prisma Access (Strata Cloud Manager)

Die HIP-Berichtsumverteilung ist in **Strata Cloud Manager** standardmäßig aktiviert. Führen Sie die folgenden Schritte aus, um die Umverteilungsdetails anzuzeigen oder die Umverteilung zu deaktivieren.


©2025 Palo Alto Networks, Inc.

**STEP 1 |** Wählen Sie in **Strata Cloud Manager** die Optionen **Verwalten** > **Konfiguration** > **NGFW und Prisma Access** > **Identitätsdienste** > **Umverteilung identifizieren** aus.

Das Prisma Access-Diagramm für die Identitätsweitergabe zeigt die Standardeinstellungen für die Umverteilung von HIP-Berichten zwischen mobilen Benutzern und Dienstverbindungen sowie zwischen Remote-Netzwerken und Dienstverbindungen an.




**STEP 2 |** Um die Umverteilung zwischen einem Segment zu deaktivieren, klicken Sie auf **Bearbeiten** und dann neben dem betreffenden Quell-Remote-Netzwerk auf **Bearbeiten**.

**STEP 3 |** Deaktivieren Sie **HIP**.

### Konfigurieren der HIP-Umverteilung in Prisma Access (Panorama)

Um Prisma Access das Sammeln und Umverteilen von HIP-Informationen zu erlauben, führen Sie die folgenden Schritte aus.

**STEP 1 |** Erlauben Sie Prisma Access die Umverteilung von HIP-Informationen.

1. Wählen Sie in Panorama **Panorama** > **Cloud Services** > **Konfiguration** > **Diensteinrichtung** aus.
2. Klicken Sie auf das Zahnradsymbol, um die Einstellungen zu bearbeiten.
3. Wählen Sie auf der Registerkarte **Erweitert** die Option **HIP-Umverteilung aktivieren** aus.

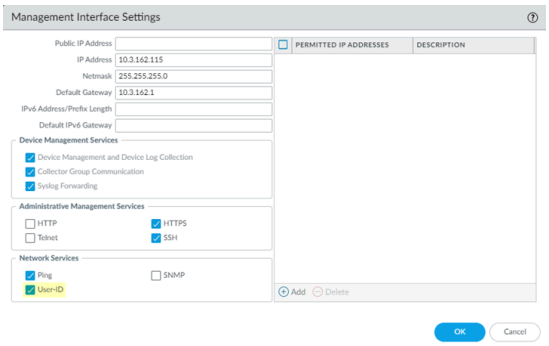
   Durch die Aktivierung der HIP-Umverteilung kann Prisma Access die von der GlobalProtect-App empfangenen HIP-Berichte an interne Firewalls und an Panorama umverteilen.




 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Konfigurieren Sie Panorama für den Empfang von HIP-Berichten von Prisma Access.

1. Wählen Sie **Panorama** > **Einrichtung** > **Schnittstellen** aus.
2. Wählen Sie die **Verwaltungsschnittstelle** aus.
3. Wählen Sie **Benutzer-ID** aus.




**STEP 3 |** Konfigurieren Sie Panorama so, dass die Benutzer-ID-Zuordnung von Prisma Accesserfasst wird.

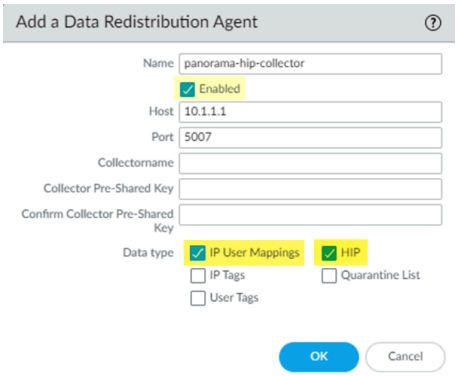
1. Wählen Sie in der Panorama-Software, die zum Verwalten von Prisma Accessverwendet wird, die Optionen **Panorama** > **Datenumverteilung** > **Agents** (für Panorama 10.*x*-Appliances) oder **Panorama** > **Benutzeridentifikation** > **Benutzer-ID-Agents** (für 9.1.*x*-Panorama-Appliances) aus.
2. **Fügen** Sie einen Benutzer-ID-Agent hinzu und geben Sie ihm einen **Namen**.
3. Geben Sie je nach Art der HIP-Informationen, die Sie sammeln möchten, einen der folgenden Werte in das Feld **Host** ein.
   - Um HIP-Informationen für mobile Benutzer zu sammeln, geben Sie die **Benutzer-ID-Agent-Adresse** (**Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Dienstverbindung** > **Benutzer-ID-Agent-Adresse**) ein.
   - Um HIP-Informationen von Benutzern an Standorten mit Remote-Netzwerken mit internem Gateway zu sammeln, geben Sie die IP-Adresse des internen Gateways ein.
   - Um HIP-Informationen von Benutzern zu sammeln, die über eine Remote-Netzwerkverbindung verfügen, geben Sie die Adresse für den **EBGP-Router** (**Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Remote-Netzwerke** > **EBGP-Router**) als Benutzer-ID-Host ein.

 ©2025 Palo Alto Networks, Inc.

4. Geben Sie in das Feld für den Port den Wert **5007** ein.

   Standardmäßig verwendet der Benutzer-ID-Agent Port 5007, um auf HIP-Informationsanfragen zu warten.

   *Stellen Sie sicher, dass Ihr Netzwerk den Zugriff auf diesen Port zwischen dem Prisma Access und dem Active Directory-Server oder dem Benutzer-ID-Agent nicht blockiert.*
5. Wählen Sie **Aktiviert** aus, damit Panorama mit dem Benutzer-ID-Agent kommunizieren kann.
6. Wählen Sie **IP-Benutzerzuordnungen** und **HIP** aus, damit Panorama Zuordnungen zwischen IP-Adresse und Benutzername und GlobalProtect-HIP-Daten von allen Standorten mobiler Benutzer empfangen kann.
7. Klicken Sie auf **OK**.




**STEP 4 |** Wiederholen Sie den Schritt 3 für jede Dienstverbindung, für die Sie die HIP-Berichterfassung konfigurieren möchten.

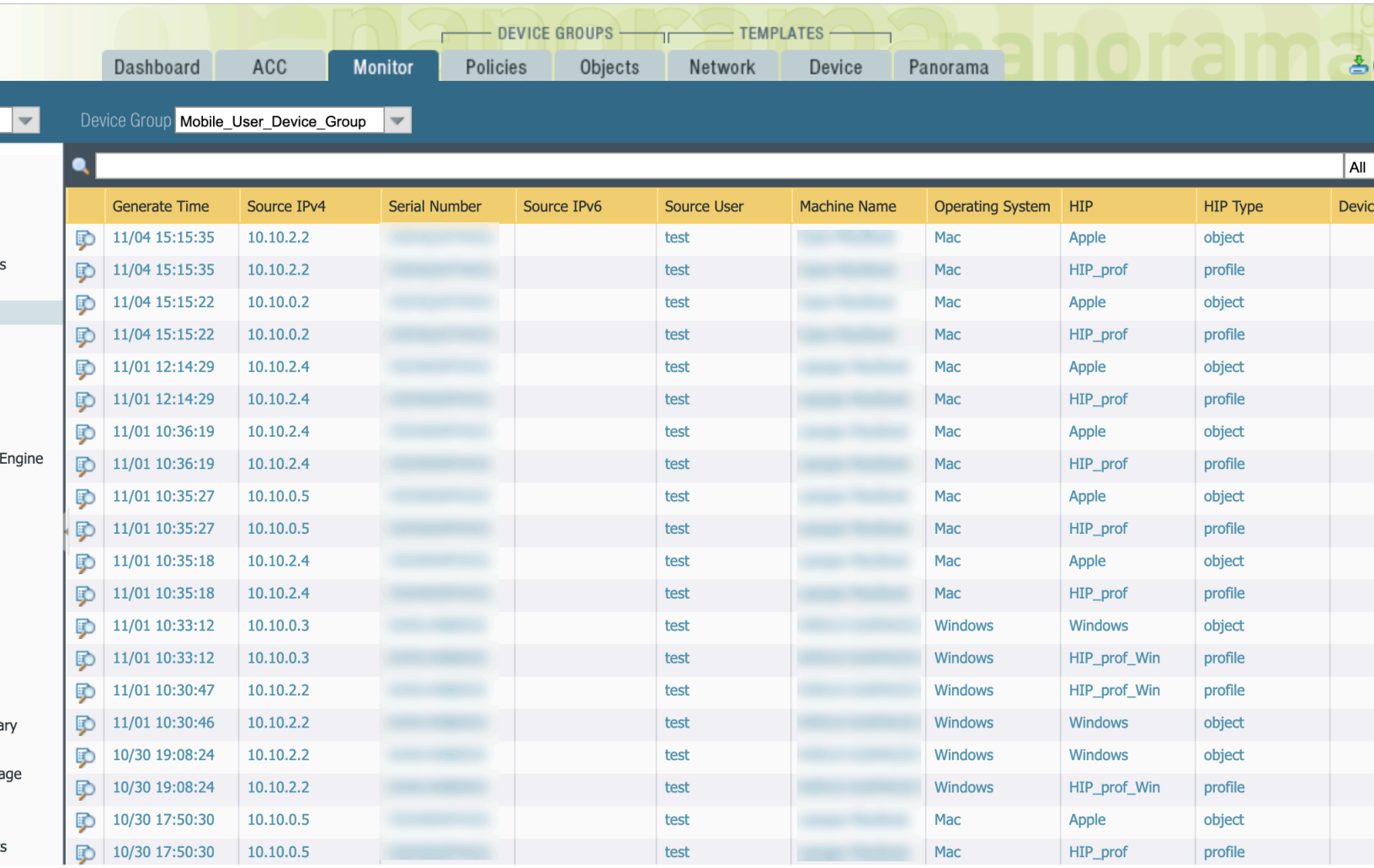
## Anzeigen von HIP-Berichten

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Nachdem Sie Prisma Access so konfiguriert haben, dass Sie HIP-Informationen sammeln und in Panorama umverteilen können, können Sie folgenden Workflow verwenden, um HIP-Informationen in Panorama anzuzeigen.


©2025 Palo Alto Networks, Inc.

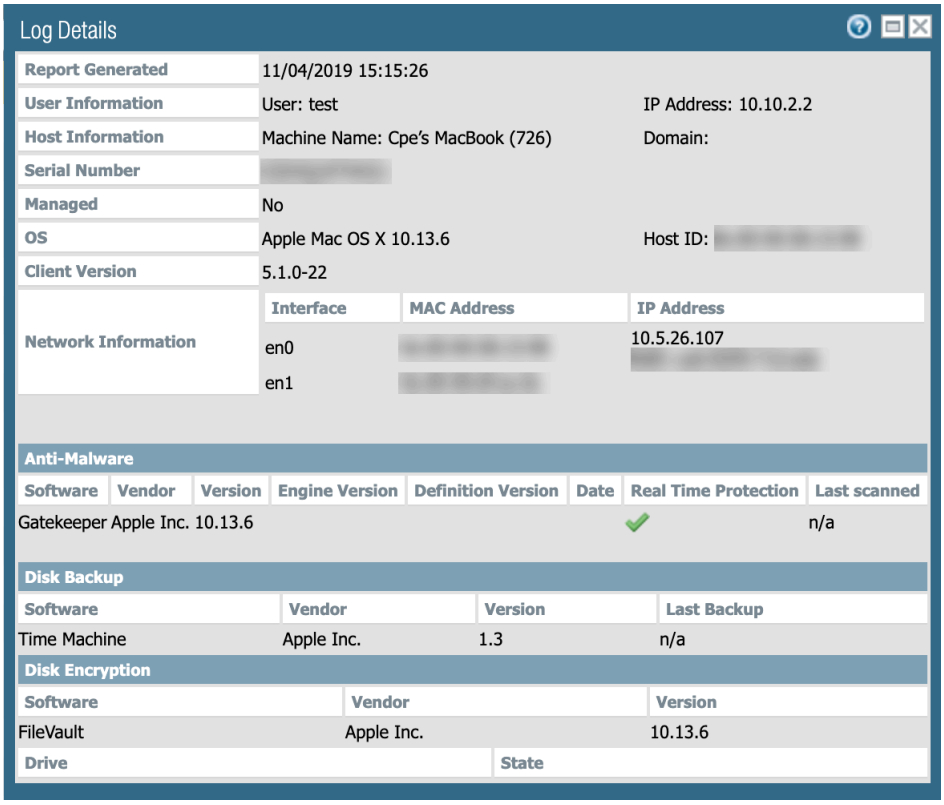
**STEP 1 |** Wählen Sie **Überwachen** > **Protokolle** > **HIP-Übereinstimmung** aus, um HIP-Informationen anzuzeigen.




| Generate Time | Source IPv4 | Serial Number | Source IPv6 | Source User | Machine Name | Operating System | HIP | HIP Type | Devic |
|---|---|---|---|---|---|---|---|---|---|
| 11/04 15:15:35 | 10.10.2.2 | | | test | | Mac | Apple | object | |
| 11/04 15:15:35 | 10.10.2.2 | | | test | | Mac | HIP_prof | profile | |
| 11/04 15:15:22 | 10.10.0.2 | | | test | | Mac | Apple | object | |
| 11/04 15:15:22 | 10.10.0.2 | | | test | | Mac | HIP_prof | profile | |
| 11/01 12:14:29 | 10.10.2.4 | | | test | | Mac | Apple | object | |
| 11/01 12:14:29 | 10.10.2.4 | | | test | | Mac | HIP_prof | profile | |
| 11/01 10:36:19 | 10.10.2.4 | | | test | | Mac | Apple | object | |
| 11/01 10:36:19 | 10.10.2.4 | | | test | | Mac | HIP_prof | profile | |
| 11/01 10:35:27 | 10.10.0.5 | | | test | | Mac | Apple | object | |
| 11/01 10:35:27 | 10.10.0.5 | | | test | | Mac | HIP_prof | profile | |
| 11/01 10:35:18 | 10.10.2.4 | | | test | | Mac | Apple | object | |
| 11/01 10:35:18 | 10.10.2.4 | | | test | | Mac | HIP_prof | profile | |
| 11/01 10:33:12 | 10.10.0.3 | | | test | | Windows | Windows | object | |
| 11/01 10:33:12 | 10.10.0.3 | | | test | | Windows | HIP_prof_Win | profile | |
| 11/01 10:30:47 | 10.10.2.2 | | | test | | Windows | HIP_prof_Win | profile | |
| 11/01 10:30:46 | 10.10.2.2 | | | test | | Windows | Windows | object | |
| 10/30 19:08:24 | 10.10.2.2 | | | test | | Windows | Windows | object | |
| 10/30 19:08:24 | 10.10.2.2 | | | test | | Windows | HIP_prof_Win | profile | |
| 10/30 17:50:30 | 10.10.0.5 | | | test | | Mac | Apple | object | |
| 10/30 17:50:30 | 10.10.0.5 | | | test | | Mac | HIP_prof | profile | |


©2025 Palo Alto Networks, Inc.

**STEP 2 |** Klicken Sie auf das Symbol links neben einem Datensatz, um detaillierte HIP-Informationen anzuzeigen.



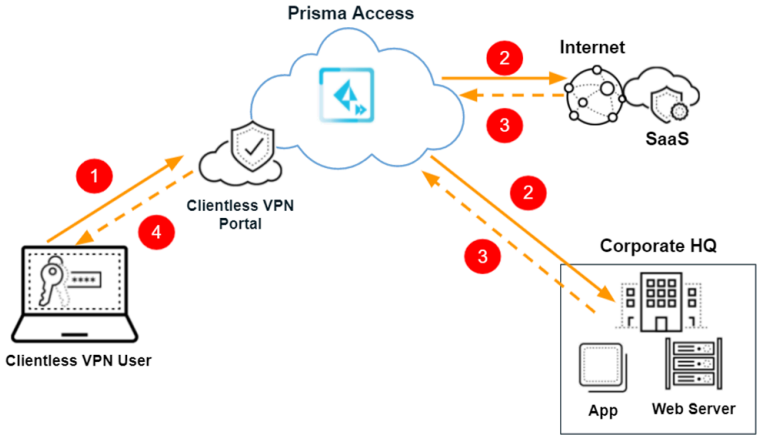

# Unterstützung für Gzip-Codierung in clientlosem VPN

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Panorama | • Prisma Access-Lizenz |

GlobalProtect Clientloses VPN bietet sicheren Remote-Zugriff auf gängige Webanwendungen von Unternehmen. Prisma Access Clientloses VPN ermöglicht mobilen Benutzern den Zugriff auf mit Gzip komprimierte Websites, um sowohl interne als auch SaaS-Anwendungen zu nutzen. Die Unterstützung für die Gzip-Codierung stellt sicher, dass die Gzip-Codierungsanfrage innerhalb des HTTP-Headers vom clientlosen VPN-Portal akzeptiert wird. Dadurch wird sichergestellt, dass der Inhalt der mit Gzip komprimierten Webseiten beim Zugriff über das clientlose VPN-Portal korrekt dargestellt wird.

Im folgenden Diagramm ist die erweiterte Unterstützung veranschaulicht, um Benutzern den Zugriff auf interne und SaaS-Anwendungen über clientloses VPN in Prisma Access zu ermöglichen.

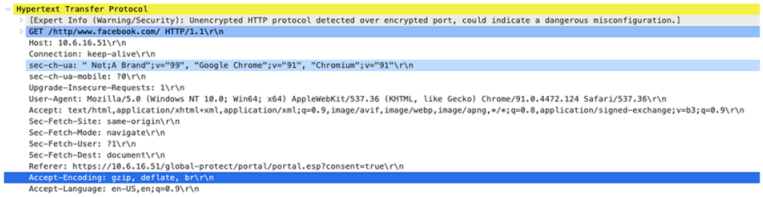
 ©2025 Palo Alto Networks, Inc.



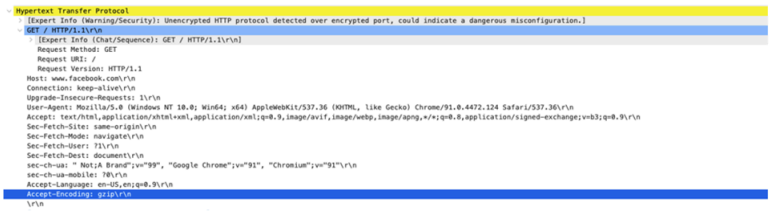

Das clientlose VPN kann basierend auf der HTTP-Anfrage des Clients und der entsprechenden Antwort der App bestimmen, ob die Gzip-Codierung verwendet werden soll. Der Wert **gzip** muss als einer der Werte im Header „Accept-Encoding“ enthalten sein, damit er vom clientlosen VPN akzeptiert wird.

Betrachten Sie z. B. die folgenden Szenarien, in denen das clientlose VPN die Gzip-Codierung verwendet:

1. Der Browser sendet eine HTTP-Anfrage an die Website, wobei die Werte im Header „Accept-Encoding“ auf **gzip**, **deflate**und **br** gesetzt sind, wie im folgenden Beispiel dargestellt.




2. Das clientlose VPN-Portal in Prisma Access analysiert die eingehende HTTP-Anfrage vom Browser und legt den Wert im Header „Accept-Encoding“ auf **gzip** fest. Dies gibt an, dass die Gzip-Codierung unterstützt wird wie im folgenden Beispiel dargestellt.

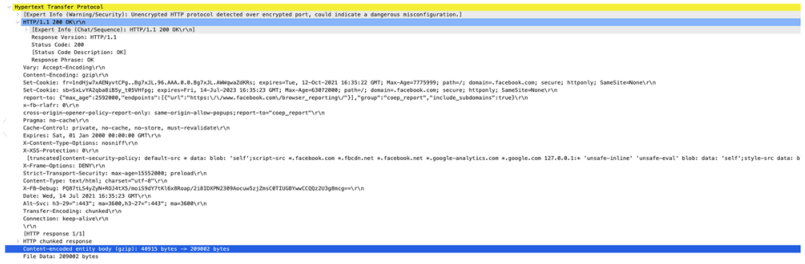



 ©2025 Palo Alto Networks, Inc.

3. Wenn die Website die Gzip-Codierung in der HTTP-Antwort unterstützt, sendet die Website den Header „Content-Encoding“ als **gzip**, was darauf hinweist, dass der Inhalt im Gzip-Format vorliegt, wie im folgenden Beispiel dargestellt.



4. Das clientlose VPN leitet die von der Website empfangene Antwort im gleichen Format an den Webbrowser weiter, wie im folgenden Beispiel dargestellt.



Wenn die vom clientlosen VPN empfangene HTTP-Anfrage **gzip** nicht als eine der Codierungsmethoden umfasst, akzeptiert das clientlose VPN auch keine Gzip-Codierung.

## Replikation des Datenverkehrs in Prisma Access

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz<br>❑ Add-on-Lizenz für Replikation des Datenverkehrs<br>❑ Replikation des Datenverkehrs erfordert mindestens Prisma Access Release 4.1 für den Datenverkehr mobiler Benutzer.<br>❑ Replikation des Datenverkehrs erfordert mindestens Prisma Access Release 5.0 für den Datenverkehr mobiler Benutzer und den Datenverkehr von Remote-Netzwerken.<br>❑ Die Unterstützung von TLS 1.3 für Remote-Netzwerke erfordert mindestens Prisma Access Release 5.2.<br>❑ PubSub erfordert mindestens Prisma Access Release 5.2.1. |

 ©2025 Palo Alto Networks, Inc.

Lokale Netzwerkrekorder sind ein leistungsstarkes Tool für Unternehmen, um forensische Analysen und Sicherheitslückenanalysen durchzuführen. In lokalen Topologien ist es üblich, eine parallele Infrastruktur mit TAP-Ports, SPAN-Ports oder Paketbrokern zu implementieren, die eine Kopie des Datenverkehrs für eine solche Out-of-Band-Analyse bereitstellen würde.

Gleichzeitig migrieren Unternehmen jedoch aufgrund der beschleunigten Einführung von Hybridarbeit und -clouds zu SASE-Architekturen, um diese Herausforderungen zu bewältigen. Die Einhaltung von SASE-Cloud-Sicherheitslösungen hat zu „blinden Flecken“ bei diesen forensischen Analysetools geführt, für die eine Kopie des Datenverkehrs von einem Remote-Benutzer zu einer SaaS-Anwendung nicht mehr verfügbar ist.

Prisma Access Replikation des Datenverkehrs bietet umfassende Einblicke in forensische und Post-Mortem-Analysen mit SASE-Architekturen und stellt dazu eine Kopie des durch Prisma Access verlaufenden Datenverkehrs zur Verfügung. Beispiele für häufige Anwendungsfälle, in denen Replikation des Datenverkehrs hilfreich ist:

- Forensische und Bedrohungsbekämpfungsanalysen, für die eine Paketerfassung unwiderlegbare Beweise für den Angriff und den verwendeten Ansatz bereitstellt
- Die Einhaltung bestimmter regulatorischer Vorschriften, wenn Paketerfassungen für eine bestimmte Zeit gespeichert werden müssen
- Weiterverwendung bevorzugter Tools von Drittanbietern, in die Ihr Unternehmen investiert hat
- Debugging der Netzwerk- und Anwendungsleistung auf Paketebene

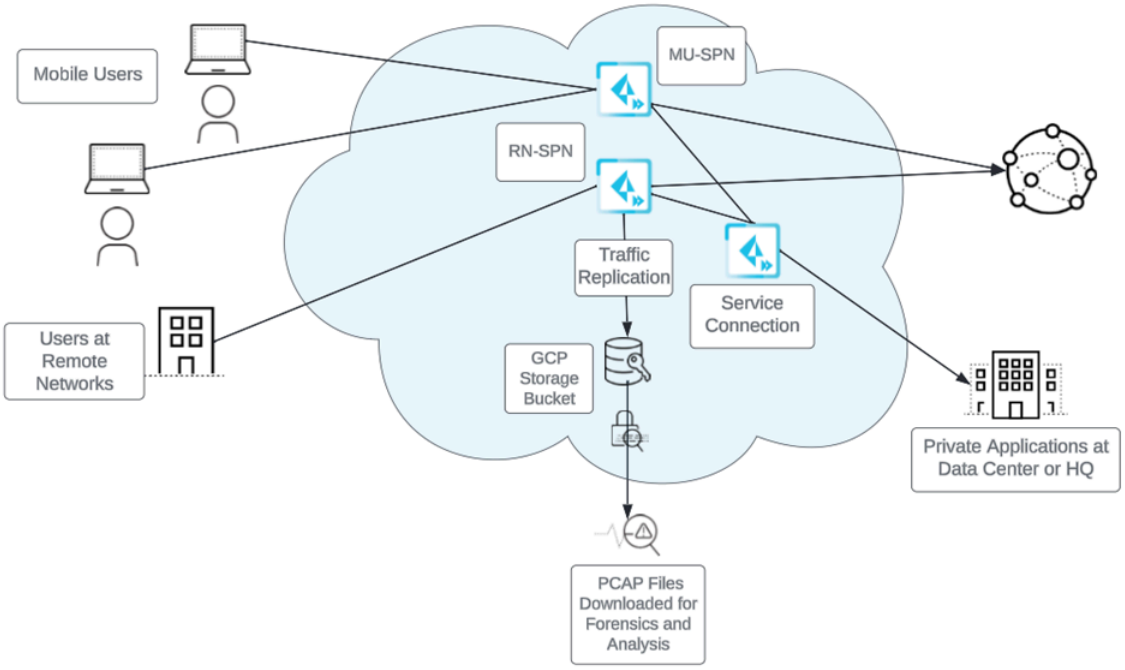
Replikation des Datenverkehrs bietet Zugriff auf Paketerfassungen (PCAPS) des realen Datenverkehrs von Benutzern und ermöglicht so die Erkennung und Bekämpfung von Bedrohungen, die sich über mehrere Sitzungen erstrecken könnten, oder die Identifikation anomaler Verhaltensweisen und das Ergreifen entsprechender Maßnahmen, um die Risiken zu verringern und das Unternehmen zu schützen.

Wenn Replikation des Datenverkehrs aktiviert ist, erstellt Prisma Access dedizierte Cloud-Speicher-Buckets an jedem Prisma Access-Compute-Standort, an dem diese Funktion aktiviert ist. Zudem werden PCAP-Dateien, die eine Replik des durch Prisma Access verlaufenden Datenverkehrs enthalten, kontinuierlich gespeichert.

Um benachrichtigt zu werden, wenn eine neue PCAP-Datei in den Speicher-Bucket hochgeladen wird, können Sie Pub/Sub-Benachrichtigungen abonnieren. Durch die Verwendung von Pub/Sub-Benachrichtigungen für neue PCAP-Dateien entfällt die Notwendigkeit, Tools zu entwickeln, über die Sie benachrichtigt werden, wenn den Buckets neue Dateien hinzugefügt werden.

Sie müssen ein Google-Cloud-Dienstkonto angeben, das für die Gewährung von Leserechten für diese Speicher-Buckets verwendet wird, um einen sicheren Zugriff auf die PCAP-Dateien zu ermöglichen. Eine zusätzliche Verschlüsselung der ruhenden PCAP-Dateien erfolgt mit einem öffentlichen Schlüssel, der über ein Zertifikat in Prisma Access freigegeben wird. Dabei hätten nur Sie den privaten Schlüssel, um die ursprünglichen PCAP-Dateien zu entschlüsseln und wiederherzustellen.

 ©2025 Palo Alto Networks, Inc.




### Voraussetzungen für Replikation des Datenverkehrs

Bevor Sie mit der Konfiguration der Replikation des Datenverkehrs beginnen, beachten Sie die folgenden Voraussetzungen.

- Stellen Sie sicher, dass Sie ein Dienstkonto in Google Cloud Platform (GCP) erstellt haben.
- Vergewissern Sie sich, dass Sie einen öffentlichen Schlüssel erstellt haben, der über ein Zertifikat auf der Seite **Objekte** > **Zertifikatverwaltung** > **Zertifikate** > **Benutzerdefinierte Zertifikate** > **Generieren** zur Verwendung für die SSL-Entschlüsselung freigegeben wird.
- Für die empfohlene Architektur muss sich der Rechner oder Dienst, der die PCAP-Dateien aus jedem Speicher-Bucket liest, in derselben GCP-Region befinden, aus der der Bucket die Daten liest. Zwar können PCAP-Dateien möglicherweise auch von einem Speicher-Bucket aus einer anderen GCP-Region oder sogar außerhalb der GCP-Cloud gelesen werden, doch diese Bereitstellungsmodelle werden nicht unterstützt.

### Richtlinien zur Replikation des Datenverkehrs

Befolgen Sie diese Richtlinien für die Replikation des Datenverkehrs:

- **TLS-Unterstützung** – TLS 1.2 wird für die Replikation des Datenverkehrs unterstützt, die in Bereitstellungen für mobile Benutzer verwendet wird. TLS 1.2 und 1.3 werden für die Replikation des Datenverkehrs unterstützt, die in Bereitstellungen für Remote-Netzwerke verwendet wird.
- **IPSec-Tunnelalgorithmen** – Alle IPSec-Tunnelalgorithmen, die für Bereitstellungen für mobile Benutzer und Remote-Netzwerke unterstützt werden, werden auch mit Replikation des Datenverkehrs unterstützt.

Erfahren Sie, wie Sie die Replikation des Datenverkehrs einrichten:

- Strata Cloud Manager
- Panorama

 ©2025 Palo Alto Networks, Inc.

## Replikation des Datenverkehrs in Prisma Access (Strata Cloud Manager)

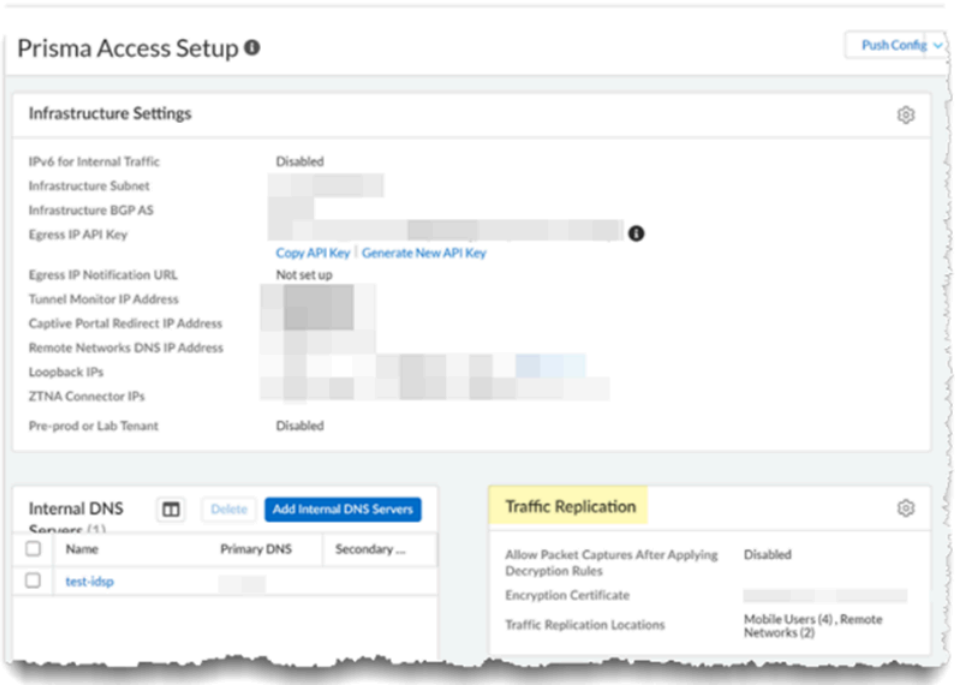
Gehen Sie wie folgt vor, um die Replikation des Datenverkehrs in den Paketerfassungsdateien (PCAP) zu konfigurieren und darauf zuzugreifen.

**STEP 1 |** Führen Sie die Schritte für Onboarding und Konfiguration von „Mobile Benutzer – GlobalProtect“ für die Standorte aus, an denen Sie die Replikation des Datenverkehrs aktivieren und Ihre Änderungen durch Auswählen von **Commit und Push** festschreiben und übertragen möchten.

Die Standorte für „Mobile Benutzer – GlobalProtect“ müssen aktiviert sein, bevor Sie die Replikation des Datenverkehrs für diese Standorte aktivieren können.

**STEP 2 |** (Optional) Wenden Sie SSL-Entschlüsselung auf die Paketerfassungen an.

1. Rufen Sie Prisma Access (Managed by Strata Cloud Manager) auf, wählen Sie **Einrichtung Prisma Access** > **Prisma Access** > **Replikation des Datenverkehrs** aus und klicken Sie auf das Zahnrad, um die **Einstellungen** zu bearbeiten.



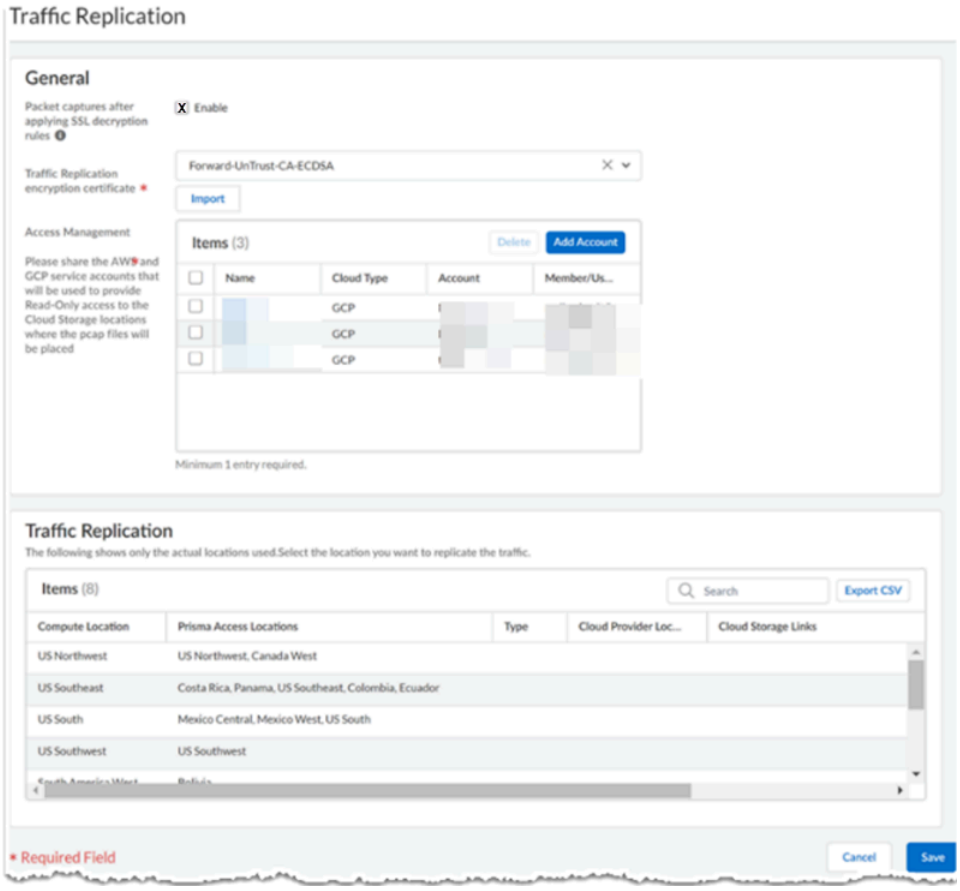

2. Aktivieren Sie **Paketerfassungen nach dem Anwenden von SSL-Entschlüsselungsregeln**, um Ihre bereits konfigurierten SSL-Entschlüsselungsrichtlinien auf die PCAP-Dateien anzuwenden.

   Nur Datenverkehr, der mit der Inline-SSL-Entschlüsselungsrichtlinie übereinstimmt, wird entschlüsselt.

   Wenn Sie diese Option auswählen, verwenden die PCAP-Dateien dieselben Entschlüsselungsregeln, die Sie in Ihrer Bereitstellung angegeben haben. Wenn Sie

 ©2025 Palo Alto Networks, Inc.

diese Option deaktivieren, wird keine Entschlüsselung der PCAP-Dateien durchgeführt, unabhängig von den Entschlüsselungsregeln, die Sie konfiguriert haben.




**STEP 3 |** Wählen Sie als **Verschlüsselungszertifikat für die Datenverkehrsreplikation** ein beliebiges Zertifikat aus, das Sie auf der Seite **Objekte** > **Zertifikatverwaltung** > **Zertifikate** > **Benutzerdefinierte Zertifikate** > **Generieren** hinzugefügt haben, oder wählen Sie **Importieren** aus, um das Zertifikat, das für die SSL-Entschlüsselung verwendet werden soll, zu importieren.

Das Zertifikat besteht aus einem öffentlichen und einem privaten Schlüssel. Laden Sie den öffentlichen Schlüssel in Prisma Access hoch. Sie behalten den privaten Schlüssel und verwenden ihn zum Entschlüsseln, wenn Sie die komprimierten PCAP-Dateien aus dem Speicher-Bucket herunterladen. Auf diese Weise garantieren Sie, dass nur Ihre Organisation auf den Speicher-Bucket zugreifen kann, in dem die PCAP-Dateien gespeichert sind.

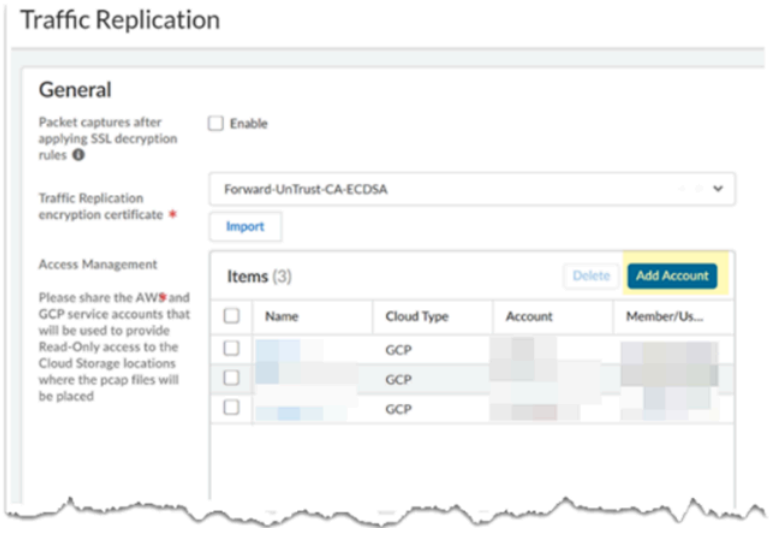
**STEP 4 |** Konfigurieren Sie das GCP-Dienstkonto, das Sie in Schritt 1 erstellt haben.

Die Replikation des Datenverkehrs wird nur für GCP-Konten unterstützt. Dieses Dienstkonto wird verwendet, um den schreibgeschützten Zugriff auf die Speicher-Buckets, in denen die PCAP-Dateien gespeichert sind, an den Standorten freizugeben, an denen Sie die Replikation des Datenverkehrs aktiviert haben. Sie können diese Dienstkonten in Ihrem GCP-Konto mithilfe normaler Verfahren zum Erstellen von GCP-Dienstkonten erstellen. Die Kontrolle, welche Benutzer Zugriff auf diese Dienstkonten haben, liegt in Ihrer Verantwortung. Alle

 ©2025 Palo Alto Networks, Inc.

Benutzer, die sowohl Zugriff auf die PCAP-Dateien als auch auf den privaten Schlüssel haben, hätten Zugriff auf die PCAP-Dateien.

1. Im Bereich **Zugriffsverwaltung** können Sie unter **Konto hinzufügen** Details zum Freigeben des schreibgeschützten Zugriffs auf die Speicher-Buckets eingeben, in denen die PCAP-Dateien gespeichert sind.




2. Geben Sie folgende Parameter ein:
   - Geben Sie dem Konto einen eindeutigen **Kontonamen**.
   - Geben Sie **GCP** als **Typ** für das Konto an.
   - Geben Sie die unter **Konto** Informationen zu dem von Ihnen erstellten GCP-Dienstkonto an.
   - Geben Sie unter **Mitglied/Benutzer** einen Namen für das GCP-Dienstkonto ein.

**STEP 5 |** (Optional) Wenn Sie Pub/Sub-Benachrichtigungen hinzufügen möchten, die Sie darüber informieren, wenn ein neuer Ordner oder neue Dateien zu einem Bucket hinzugefügt

 ©2025 Palo Alto Networks, Inc.

werden, richten Sie Pub/Sub-Benachrichtigungen in Ihrem Konto beim Google-Cloud-Dienst ein.

Prisma Access erstellt einen einzelnen Pub/Sub-Kanal pro Mandant für alle Standorte in diesem Mandanten.

*Pub/Sub-Benachrichtigungen werden ab Prisma Access 5.2 unterstützt. Wenn Sie bereits ein Konto haben und Pub/Sub-Benachrichtigungen hinzufügen möchten, aktualisieren Sie auf Prisma Access 5.2 und wählen Sie dann eine der folgenden Optionen aus, um Pub/Sub-Benachrichtigungen hinzuzufügen:*

- *Ändern Sie das bereits in Prisma Access konfigurierte Konto beim Google-Cloud-Dienst.*
- *Fügen Sie ein neues Konto für das bestehende Dienstkonto hinzu und geben Sie dieses Konto in Ihrer Prisma Access-Konfiguration an.*

  *Wenn Sie ein neues Konto hinzufügen, müssen Sie die Replikation des Datenverkehrs für das bestehende Konto deaktivieren und die Replikation des Datenverkehrs für das neue Konto aktivieren.*
- *Deaktivieren und aktivieren Sie die Replikation des Datenverkehrs am vorhandenen Standort.*

Prisma Access sendet Pub/Sub-Nachrichten mit der Überschrift `panw-traffic-replication-file- notifications-`<*tenantid*>, wobei <*tenantid*> die ID des Mandanten ist, der die Benachrichtigungen sendet. Die Nachrichten liegen im folgenden Format vor:

```
Nachricht { data: b'' ordering_key: '' attributes:
 { "bucketId": "xxxx-xx-xxx-xxxxxxxxx-us-west1", "eventTime":
 "2024-04-24T23:12:59.xxxxxxx", "eventType": "OBJECT_FINALIZE",
 "notificationConfig": "projects/_/buckets/xxxx-xx-xxx-
xxxxxxxxx-us-west1/notificationConfigs/1", "objectGeneration":
 "xxxxxxxxxxxxxxx", "objectId": "instance-group-
xxxxxx/12345678_190000_xxxxx.zip", "payloadFormat": "NONE" } }
```

Dabei gilt:

- `objectGeneration` ist die Generierungsnummer des geänderten Objekts.
- `objectID` ist der Name des geänderten Objekts.

**STEP 6 |** Konfigurieren Sie die Replikation des Datenverkehrs für einen oder mehrere Standorte mit mobilen Benutzern.

1. Wählen Sie im Bereich **Replikation des Datenverkehrs** die Standorte aus, an denen Sie die Replikation des Datenverkehrs aktivieren möchten. Wählen Sie anschließend **Mobile Benutzer** aus.

   Sie wählen den **Compute-Standort** aus, der mit **Prisma Access-Standorten** verknüpft ist. Die Replikation des Datenverkehrs ist für alle „Mobile Benutzer“-Clients aktiviert, die mit den ausgewählten Standorten verbunden sind.

 ©2025 Palo Alto Networks, Inc.

**STEP 7 |** Speichern Sie die Konfiguration mit **Save (Speichern)**.

**STEP 8 |** Führen Sie einen Commit aus und übertragen Sie die Änderung per Push.

1. Wählen Sie **Verwalten** > **Operation** > **Konfiguration übertragen** aus.
2. Wählen Sie **Container für mobile Benutzer** im **Übertragungsumfang** aus und wählen Sie anschließend **Konfiguration übertragen** und **Push** aus, um Ihre Änderungen per Push zu übertragen.
3. Überprüfen Sie die Übertragungsziele und wählen Sie **Übertragen**.

**STEP 9 |** Überprüfen Sie den Status der Replikation des Datenverkehrs, indem Sie zu **Prisma Access Einrichtung** > **Prisma Access** > **Replikation des Datenverkehrs** wechseln.

**STEP 10 |** Laden Sie die PCAP-Dateien herunter.

Verwenden Sie die **Cloud-Speicher-Links**, um auf die PCAP-Dateien in Ihren GCP-Speicher-Buckets zuzugreifen.

- Diese Speicher-Buckets unterstützen die gleichen regulären Vorgänge, Befehle und Abfragen wie alle anderen GCP-Speicher-Buckets.
- Sie können PCAP-Daten bis zu 72 Stunden lang herunterladen. Nach 72 Stunden werden die Dateien dauerhaft gelöscht.
- Dateien werden mit Ihrem öffentlichen Schlüssel verschlüsselt.
- Die maximale Dateigröße beträgt 200 MB oder 5 Minuten Paketerfassung, je nachdem, welcher Wert kleiner ist.

1. Listen Sie die Dateien in Ihrem Dienst auf, indem Sie `gsutil ls gs://<storage_bucket_link>/` eingeben, wobei *<storage_bucket_link>* der Speicher-Link in Ihrem GCP-Dienstkonto ist, in dem die Dateien gespeichert sind.
2. Laden Sie die Dateien von Ihrem Dienstkonto herunter, indem Sie `gsutil cp gs:///<storage_bucket_link>/<file_name> <destination folder>` eingeben. Dabei gilt:
   - *<storage_bucket_link>* ist der Speicher-Link in Ihrem GCP-Dienstkonto, in dem die Dateien gespeichert sind.
   - *<file_name>* ist der Name der PCAP-Datei.
   - *<destination folder>* ist der Ordner, in den die PCAP-Datei heruntergeladen werden soll.
3. Entpacken Sie die heruntergeladenen Dateien.
4. Entschlüsseln Sie die heruntergeladenen Dateien.

## Replikation des Datenverkehrs in Prisma Access (Panorama)

Gehen Sie wie folgt vor, um die Replikation des Datenverkehrs zu konfigurieren und auf die PCAP-Dateien zuzugreifen.

**STEP 1 |** Onboarding und Konfiguration von „Mobile Benutzer – GlobalProtect“ (wenn Sie die Replikation des Datenverkehrs für mobile Benutzer konfigurieren), Remote-Netzwerke (wenn Sie die Replikation des Datenverkehrs für Remote-Netzwerke konfigurieren) oder

 ©2025 Palo Alto Networks, Inc.

beides (wenn Sie die Replikation des Datenverkehrs sowohl für mobile Benutzer als auch für Remote-Netzwerke konfigurieren).

**STEP 2 |** (Optional) Wenden Sie SSL-Entschlüsselung auf die Paketerfassungen an.

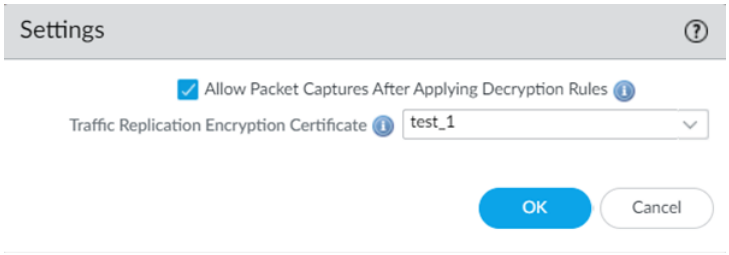
1. Gehen Sie zu **Panorama** > **Cloud Services** > **Konfiguration** > **Replikation des Datenverkehrs** und klicken Sie auf das Zahnrad, um die **Einstellungen** zu bearbeiten.
2. Wählen Sie **Zulassen von Paketerfassungen nach dem Anwenden von Entschlüsselungsregeln** aus, um Ihre bereits konfigurierten SSL-Entschlüsselungsrichtlinien auf die PCAP-Dateien anzuwenden.

   Wenn Sie diese Option auswählen, verwenden die PCAP-Dateien dieselben Entschlüsselungsregeln, die Sie in Ihrer Bereitstellung angegeben haben. Wenn Sie diese Option deaktivieren, wird keine Entschlüsselung der PCAP-Dateien durchgeführt, unabhängig von den Entschlüsselungsregeln, die Sie konfiguriert haben.

**STEP 3 |** Wählen Sie das **Verschlüsselungszertifikat für die Datenverkehrsreplikation** (öffentlicher Schlüssel) aus, das Sie in einem früheren Schritt in der Vorlage **Mobile_User_Template** (für Bereitstellungen für mobile Benutzer) oder in der Vorlage **Remote_Network_Template** (für Remote-Netzwerkbereitstellungen) erstellt haben, um es für die SSL-Entschlüsselung zu verwenden.

Dieser Schritt ist erforderlich. Sie können jedes Zertifikat auswählen, das Sie im Bereich **Gerät** > **Zertifikatverwaltung** > **Zertifikate** > **Gerätezertifikate** in der Vorlage **Mobile_User_Template** oder **Remote_Network_Template** hinzugefügt haben. Wenn Sie die Replikation des Datenverkehrs für mobile Benutzer und für Remote-Netzwerke aktivieren, legen Sie das Zertifikat sowohl in der Vorlage **Mobile_User_Template** als auch in der Vorlage **Remote_Network_Template** fest.

Das Zertifikat besteht aus einem öffentlichen und einem privaten Schlüssel. Laden Sie den öffentlichen Schlüssel in Prisma Access hoch. Sie behalten den privaten Schlüssel und verwenden ihn zum Entschlüsseln, wenn Sie die komprimierten PCAP-Dateien aus dem Speicher-Bucket herunterladen. Auf diese Weise garantieren Sie, dass nur Ihre Organisation auf den Speicher-Bucket zugreifen kann, in dem die PCAP-Dateien gespeichert sind.




**STEP 4 |** Konfigurieren Sie die Replikation des Datenverkehrs für einen oder mehrere „Mobile Benutzer – GlobalProtect“-Standorte und/oder Remote-Netzwerkstandorte, indem Sie den Standort im Bereich **Konfiguration** auswählen und die Standorte auswählen, an denen Sie die

 ©2025 Palo Alto Networks, Inc.

Replikation des Datenverkehrs aktivieren möchten. Wählen Sie anschließend **MU-GP** und/oder **RN** aus.

Wählen Sie den **Compute-Standort** aus, der mit **Prisma Access-Standorten** verknüpft ist. Die Datenverkehrsreplikation ist für alle Clients von „Mobile Benutzer – GlobalProtect“ und/oder Remote-Netzwerkbenutzer aktiviert, die mit den ausgewählten Standorten verbunden sind.

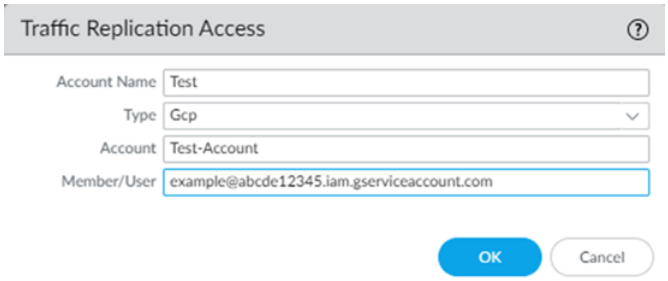



**STEP 5 |** Fügen Sie ein Konto hinzu, mit dem Sie auf Traffic Replication Package Capture-(PCAP-)Daten zugreifen können.

Dieses Dienstkonto wird verwendet, um den schreibgeschützten Zugriff auf die Speicher-Buckets, in denen die PCAP-Dateien gespeichert sind, an den Standorten freizugeben, an denen Sie die Replikation des Datenverkehrs aktiviert haben. Sie erstellen diese Dienstkonten in Ihrem GCP-Konto mithilfe normaler Verfahren zum Erstellen von GCP-Dienstkonten. Die Kontrolle, welche Benutzer Zugriff auf diese Dienstkonten haben, liegt in Ihrer Verantwortung. Alle Benutzer, die sowohl Zugriff auf die PCAP-Dateien als auch auf den privaten Schlüssel haben, hätten Zugriff auf die PCAP-Dateien.

1. Sie müssen unter „Replikation des Datenverkehrs“ im Bereich **Zugriffsverwaltung** ein **Konto hinzufügen**.
2. Geben Sie folgende Parameter ein:
   - Geben Sie dem Konto einen eindeutigen **Kontonamen**.
   - Geben Sie **GCP** als **Typ** für das Konto an.

     Die Replikation des Datenverkehrs wird nur für GCP-Konten unterstützt.
   - Geben Sie die unter **Konto** Informationen zu dem von Ihnen erstellten GCP-Dienstkonto an.
   - Geben Sie unter **Mitglied/Benutzer** einen Namen für das GCP-Dienstkonto ein.




**STEP 6 |** (Optional) Wenn Sie Pub/Sub-Benachrichtigungen hinzufügen möchten, die Sie darüber informieren, wenn ein neuer Ordner oder neue Dateien zu einem Bucket hinzugefügt

 ©2025 Palo Alto Networks, Inc.

werden, richten Sie Pub/Sub-Benachrichtigungen in Ihrem Konto beim Google-Cloud-Dienst ein.

Prisma Access erstellt einen einzelnen Pub/Sub-Kanal pro Mandant für alle Standorte in diesem Mandanten.

*Pub/Sub-Benachrichtigungen werden ab Prisma Access 5.2 unterstützt. Wenn Sie bereits ein Konto haben und Pub/Sub-Benachrichtigungen hinzufügen möchten, aktualisieren Sie auf Prisma Access 5.2 und wählen Sie dann eine der folgenden Optionen aus, um Pub/Sub-Benachrichtigungen hinzuzufügen:*

- *Ändern Sie das bereits in Prisma Access konfigurierte Konto beim Google-Cloud-Dienst.*
- *Fügen Sie ein neues Konto für das bestehende Dienstkonto hinzu und geben Sie dieses Konto in Ihrer Prisma Access-Konfiguration an.*

  *Wenn Sie ein neues Konto hinzufügen, müssen Sie die Replikation des Datenverkehrs für das bestehende Konto deaktivieren und die Replikation des Datenverkehrs für das neue Konto aktivieren.*
- *Deaktivieren und aktivieren Sie die Replikation des Datenverkehrs am vorhandenen Standort.*

Prisma Access sendet Pub/Sub-Nachrichten mit der Überschrift `panw-traffic-replication-file- notifications-`<*tenantid*>, wobei <*tenantid*> die ID des Mandanten ist, der die Benachrichtigungen sendet. Die Nachrichten liegen im folgenden Format vor:

```
Nachricht { data: b'' ordering_key: '' attributes:
 { "bucketId": "xxxx-xx-xxx-xxxxxxxxx-us-west1", "eventTime":
 "2024-04-24T23:12:59.xxxxxxx", "eventType": "OBJECT_FINALIZE",
 "notificationConfig": "projects/_/buckets/xxxx-xx-xxx-
xxxxxxxxx-us-west1/notificationConfigs/1", "objectGeneration":
 "xxxxxxxxxxxxxxx", "objectId": "instance-group-
xxxxxx/12345678_190000_xxxxx.zip", "payloadFormat": "NONE" } }
```

Dabei gilt:

- `objectGeneration` ist die Generierungsnummer des geänderten Objekts.
- `objectID` ist der Name des geänderten Objekts.

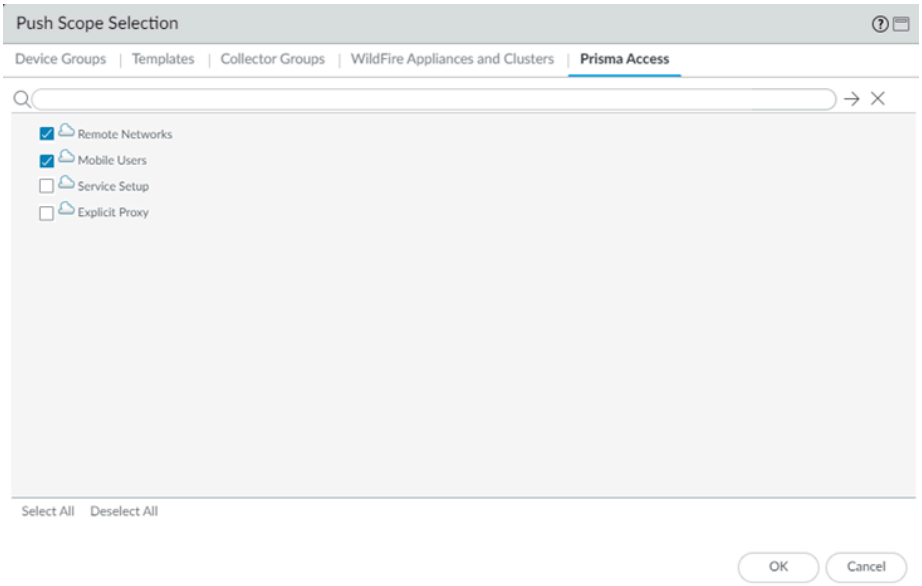
**STEP 7 |** Sie müssen Ihre Änderungen mit „Commit und Push“ festschreiben und übertragen. Nur so ist sichergestellt, dass **Mobile Benutzer** (für eine Bereitstellung für mobile Benutzer) und/oder **Remote-Netzwerke** (für eine Bereitstellung für Remote-Netzwerke) im **Übertragungsumfang** ausgewählt sind.

1. Klicken Sie auf **Commit** > **Commit und Push**.

 ©2025 Palo Alto Networks, Inc.

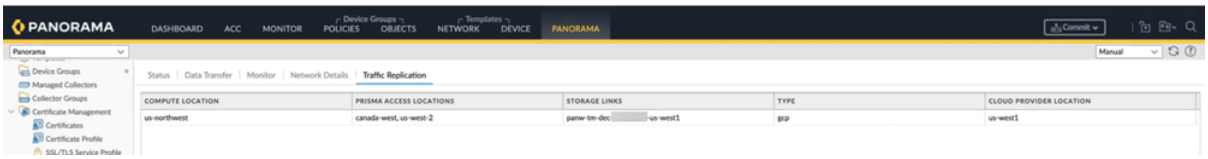
2. Wählen Sie **Auswahl bearbeiten** aus und vergewissern Sie sich, dass auf der Registerkarte **Prisma Access Mobile Benutzer** und **Remote-Netzwerke** im **Übertragungsumfang** ausgewählt sind, und klicken Sie dann auf **OK**.

   Der **Übertragungsumfang** wird möglicherweise nicht automatisch ausgewählt.




3. Klicken Sie auf **Commit und Push**.

**STEP 8 |** Überprüfen Sie den Status der Datenverkehrsreplikation, indem Sie zu **Panorama** > **Cloud Services** > **Status** > **Replikation des Datenverkehrs** wechseln.




**Speicher-Links** entspricht dem Namen des GCP-Speicher-Buckets, in dem Sie auf die PCAP-Dateien zugreifen können. Der **Standort des Cloud-Anbieters** ist der Speicherort, an dem die GCP-Instanz eingebunden ist.


©2025 Palo Alto Networks, Inc.

**STEP 9 |** Laden Sie die PCAP-Dateien mit dem privaten Schlüssel herunter, den nur Sie besitzen.

Verwenden Sie die **Speicher-Links**, um auf die PCAP-Dateien in Ihren GCP-Speicher-Buckets zuzugreifen.

- Diese Speicher-Buckets unterstützen die gleichen regulären Vorgänge, Befehle und Abfragen wie alle anderen GCP-Speicher-Buckets.
- Sie können PCAP-Daten bis zu 72 Stunden lang herunterladen. Nach 72 Stunden werden die Dateien dauerhaft gelöscht.
- Dateien werden mit Ihrem öffentlichen Schlüssel verschlüsselt.
- Die maximale Dateigröße beträgt 200 MB oder 5 Minuten Paketerfassung, je nachdem, welcher Wert kleiner ist.

1. Listen Sie die Dateien in Ihrem Dienst auf, indem Sie `gsutil ls gs://<storage_bucket_link>/` eingeben, wobei *<storage_bucket_link>* der Speicher-Link in Ihrem GCP-Dienstkonto ist, in dem die Dateien gespeichert sind.
2. Laden Sie die Dateien von Ihrem Dienstkonto herunter, indem Sie `gsutil cp gs:///<storage_bucket_link>/<file_name> <destination folder>` eingeben. Dabei gilt:
   - *<storage_bucket_link>* ist der Speicher-Link in Ihrem GCP-Dienstkonto, in dem die Dateien gespeichert sind.
   - *<file_name>* ist der Name der PCAP-Datei.
   - *<destination folder>* ist der Ordner, in den die PCAP-Datei heruntergeladen werden soll.
3. Entpacken Sie die heruntergeladenen Dateien.
4. Entschlüsseln Sie die heruntergeladenen Dateien mit dem privaten Schlüssel, den nur Sie besitzen.

 ©2025 Palo Alto Networks, Inc.

# Erweiterte Bereitstellungen für Prisma Access-Remote-Netzwerke

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Die folgenden Abschnitte zeigen Ihnen die erweiterten Bereitstellungen, die für Prisma Access-Remote-Netzwerke verfügbar sind:

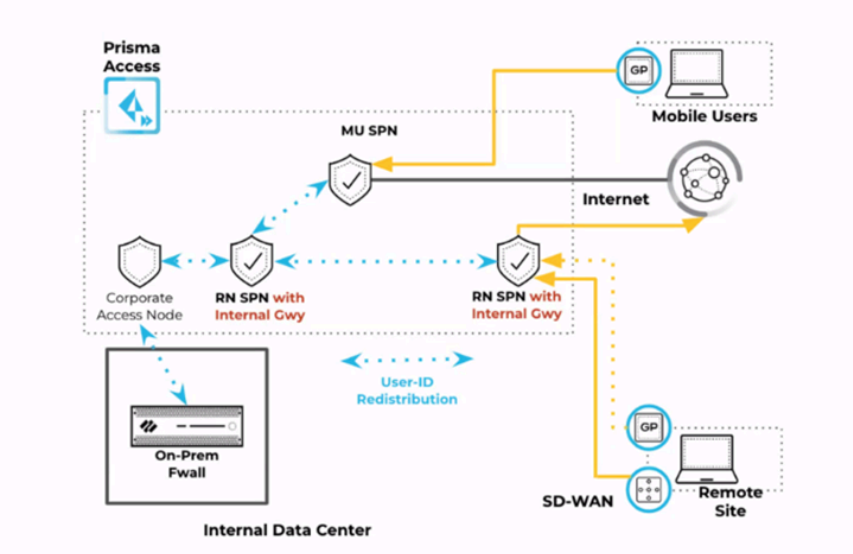
- Sicheren eingehenden Zugriff auf Remote-Netzwerkstandorte gewähren
- Netzwerk mit hoher Bandbreite für einen Remote-Standort erstellen

## Internes Gateway von Prisma Access

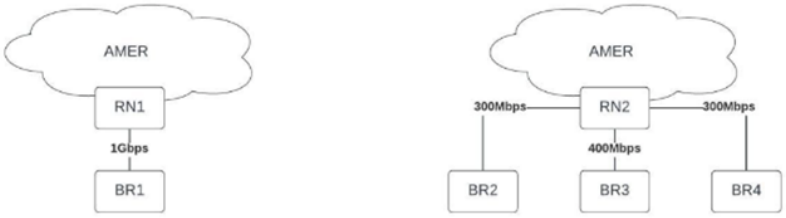
| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | ❑ Prisma Access und eine Mobile-Benutzer-Lizenz<br>❑ Minimum Required Prisma Access Version: 5.1<br>❑ Mindestens erforderliche Dataplane-Version für Prisma Access (Managed by Panorama): 10.2.4<br>❑ Mindestens erforderliche GlobalProtect-Clientversion: 6.0 |

Wenn Sie IP-Benutzerzuordnungen und HIP für Hosts mit GlobalProtect-Clientsoftware in Remote-Netzwerken von Prisma Access generieren möchten, müssen Sie zuvor eine lokale NGFW als internes Gateway bereitstellen. Diese Lösung ist nicht Cloud-nativ. Mit dem Cloud-nativen internen Gateway von Prisma Access können Sie die Verwendung interner Gateways vor Ort vermeiden, und das interne Gateway von Prisma Access generiert die IP-Benutzerzuordnungen und HIPs lokal in Remote-Netzwerken. Remote-Netzwerke verwenden IP-Benutzerzuordnungen und HIPs aus der lokalen Datenbank für Statusprüfungen, anstatt sie von anderen Firewalls zu übernehmen.


©2025 Palo Alto Networks, Inc.

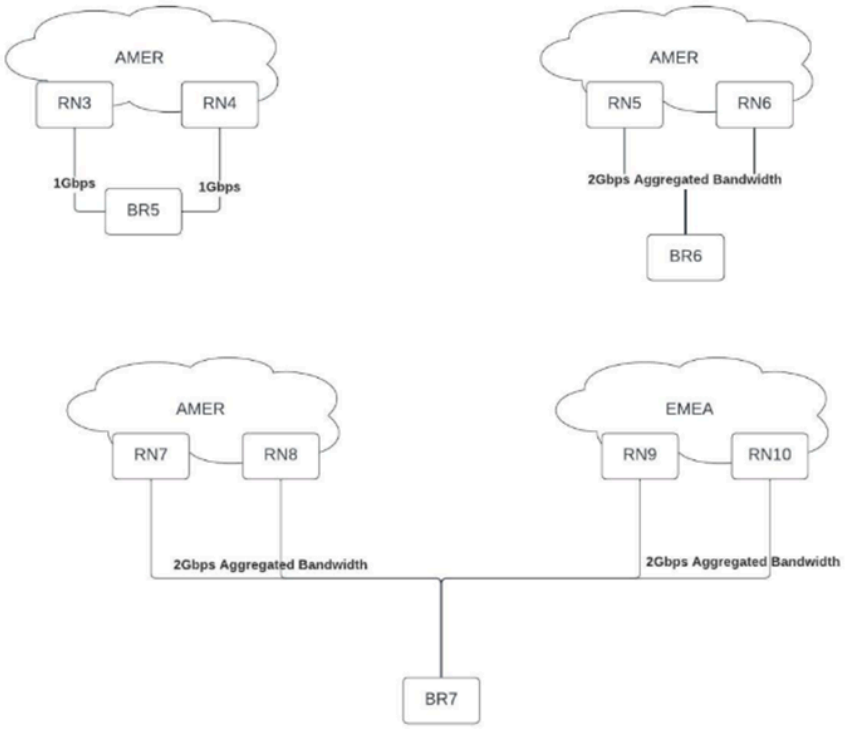



Beachten Sie, dass Sie kein internes Gateway bereitstellen können, wenn ein Remote-Standort mehrere IPsec-Tunnel für verschiedene Remote-Netzwerkstandorte (z. B. einen Aktiv/Aktiv-Tunnel) oder einen Standort mit hoher Bandbreite aufweist. Das folgende Diagramm zeigt ein Beispiel für eine unterstützte Umgebung für die Bereitstellung eines internen Gateways.




Das folgende Diagramm enthält Beispiele für Bereitstellungen, bei denen interne Gateways nicht unterstützt werden.

 ©2025 Palo Alto Networks, Inc.




Binden Sie Ihre mobilen Benutzer ein, bevor Sie das interne Gateway von Prisma Access einrichten.

- Strata Cloud Manager
- Panorama

## Internes Gateway von Prisma Access (Strata Cloud Manager)

Gehen Sie wie folgt vor, um das interne Gateway von Prisma Access einzurichten.

**STEP 1 |** In Strata Cloud Manager können Sie GlobalProtect einrichten, App-Einstellungen hinzufügen und Remote-Netzwerke einbinden.

Beachten Sie, dass es derzeit keine Konfigurationen für die interne Hosterkennung und interne Gateways gibt.

**STEP 2 |** Notieren Sie sich die **DNS-IP-Adresse des Remote-Netzwerks** aus **Workflows** > **Einrichtung Prisma Access** > **Prisma Access**.

**STEP 3 |** Notieren Sie sich die **Gateway-FQDNs** aus **Workflows** > **Einrichtung Prisma Access** > **GlobalProtect** > **Infrastruktur** > **Infrastruktureinstellungen** > **Gateway-FQDNs**.

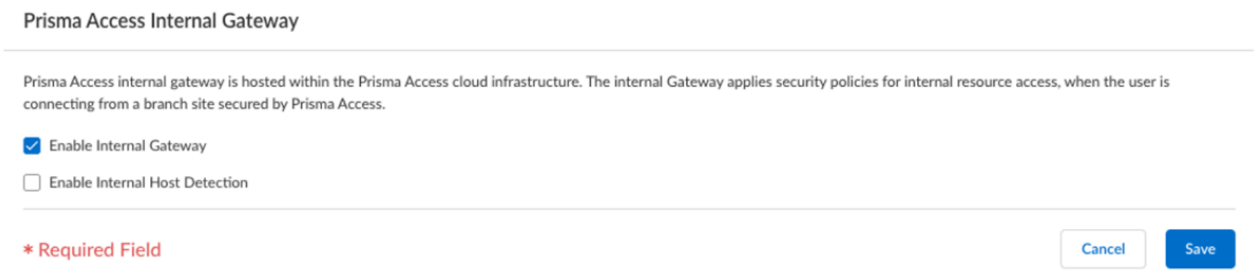
**STEP 4 |** Wählen Sie **Workflows** > **Einrichtung Prisma Access** > **Remote-Netzwerke** > **Erweiterte Einstellungen** aus.

 ©2025 Palo Alto Networks, Inc.

**STEP 5 |** Bearbeiten Sie die Einstellungen des **Prisma Access internen Gateways**, um das interne Gateway zu aktivieren, und **speichern** Sie die Änderungen.

(Optional) **Aktivieren Sie die interne Hosterkennung** für IPv4, wenn Sie Ihren eigenen DNS-Server nicht verwenden möchten. Sie können die interne Hosterkennung erst aktivieren, nachdem Sie **Internes Gateway aktivieren** ausgewählt haben.

*Prisma Access unterstützt die interne Hosterkennung nur für die **Always On**-Verbindungsmethode.*

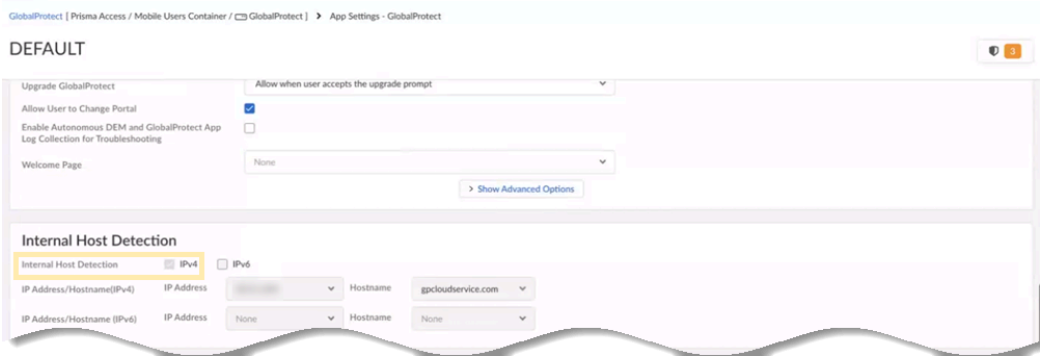



Wenn Sie das interne Gateway aktivieren, fungieren die Remote-Netzwerkinstanzen als interne Gateways. Wenn Sie die interne Hosterkennung aktivieren, erstellt Prisma Access PTR-Datensätze auf den DNS-Proxyservern des Remote-Netzwerks für den Prozess der internen Hosterkennung.

**STEP 6 |** Wählen Sie **Workflows** > **Einrichtung Prisma Access** > **GlobalProtect** > **GlobalProtect-App** aus.

**STEP 7 |** Wählen Sie eine App-Einstellung aus und sehen Sie sich die Details zur internen Hosterkennung und zum internen Gateway an.

Wenn Sie das interne Gateway und die interne Hosterkennung in Schritt 5 aktivieren, aktiviert Prisma Access hier auch die Erkennung interner IPv4-Hosts und das interne Gateway. Prisma Access füllt den Wert **DNS-IP-Adresse der Remote-Netzwerke** aus Schritt 2 als IP-Adresse aus.

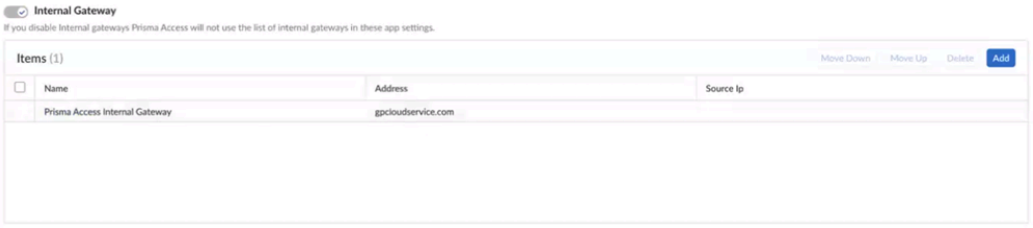



Beachten Sie, dass die Erkennung interner IPv6-Hosts auf DNS-Proxyservern von Prisma Access nicht unterstützt wird.

Sie können diesen Eintrag **Internes Gateway von Prisma Access** nicht entfernen. Sie können jedoch die internen Gateways hinzufügen, die Sie selbst bereitgestellt haben. Sie können Ihre eigenen DNS-Server im internen Netzwerk für die interne Hosterkennung bereitstellen. Stellen

 ©2025 Palo Alto Networks, Inc.

Sie jedoch sicher, dass Sie PTR-Datensätze hinzufügen, damit die interne Hosterkennung möglich ist. Prisma Access hängt den Wert **Gateway-FQDNS** aus Schritt 3 an die Adresse an.




Sie können die Details zur IP-Adresse des DNS-Proxyservers anzeigen, indem Sie **Workflows** > **Einrichtung Prisma Access** > **Prisma Access** auswählen.

Wenn Sie **Interne Hosterkennung** aktivieren, überprüfen Sie, ob die DNS-Auflösung funktioniert, führen Sie ein Reverse-DNS-Lookup von Ihrem internen Netzwerk zur IP-Adresse des DNS-Proxyservers durch und stellen Sie sicher, dass ein FQDN zurückgegeben wird, der mit **`any-igw`** beginnt.

**STEP 8 |** Übertragen Sie die Änderungen zur gleichen Zeit per **Push** an mobile Benutzer und Remote-Netzwerke.

**STEP 9 |** Melden Sie sich am Endpunkt an.

Wenn Sie eine Verbindung mit GlobalProtect herstellen, authentifizieren Sie sich zunächst beim GlobalProtect-Portal. Die interne Hosterkennung löst aus, dass GlobalProtect eine Verbindung mit dem internen Gateway herstellt. Wenn der GlobalProtect-Agent dann weiterhin im Nicht-Tunnelmodus arbeitet, erscheint die zweite Authentifizierung und sendet die Hostinformationen an das interne Gateway in Remote-Netzwerken.

## Internes Gateway von Prisma Access (Panorama)

**STEP 1 |** In Panorama können Sie GlobalProtect einrichten, App-Einstellungen hinzufügen und Remote-Netzwerke einbinden.

Beachten Sie, dass es derzeit keine Konfigurationen für die interne Hosterkennung und interne Gateways gibt.

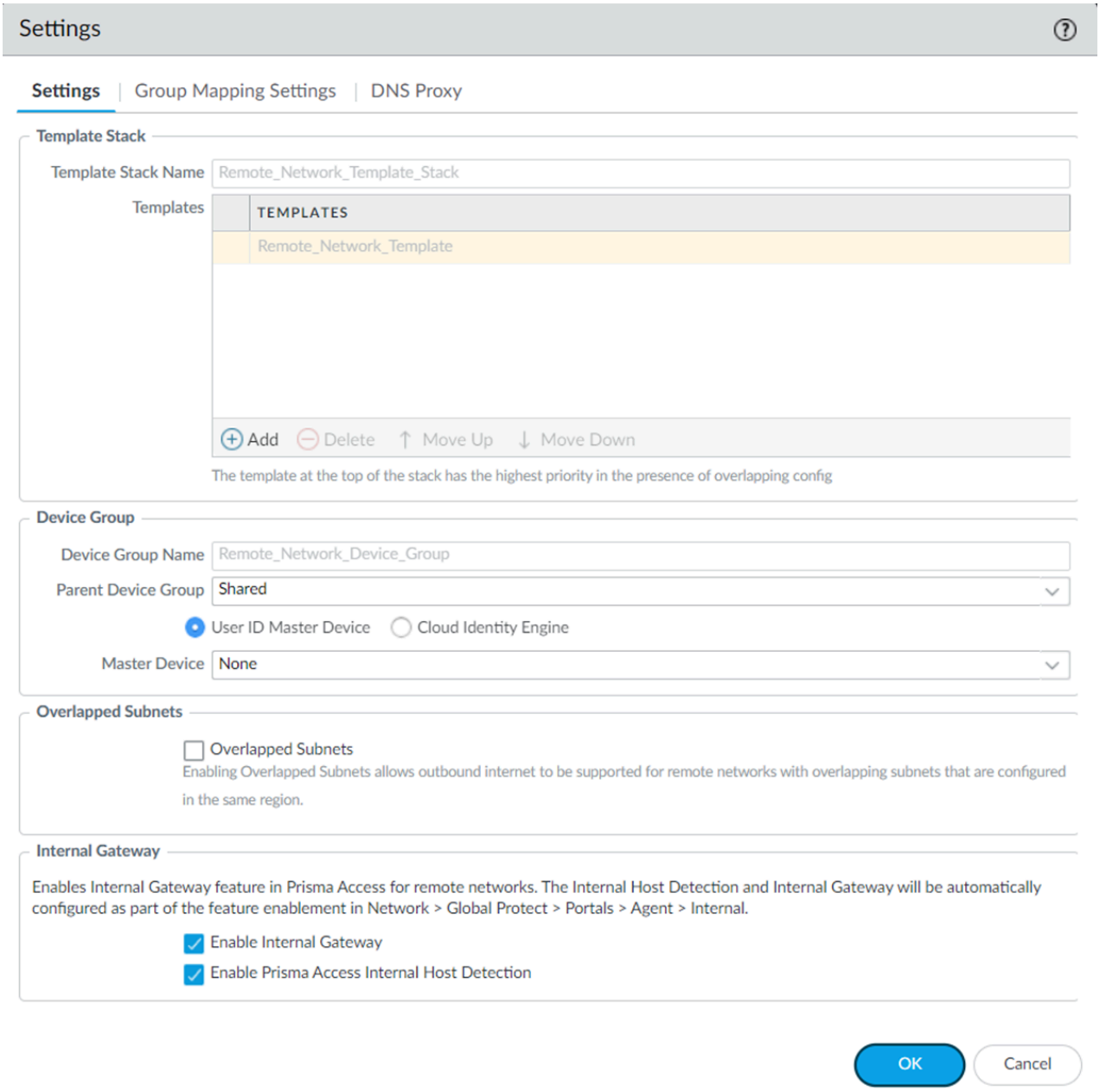
**STEP 2 |** Gehen Sie zu **Panorama** > **Cloud Services** > **Konfiguration** > **Remote-Netzwerke** > **Einstellungen**.

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** **Aktivieren Sie „Internes Gateway“** und speichern Sie die Änderungen.

(Optional) Wenn Sie keinen eigenen DNS-Server verwenden möchten, **aktivieren Sie die interne Hosterkennung von Prisma Access** für IPv4. Sie können die interne Hosterkennung erst aktivieren, nachdem Sie **Internes Gateway aktivieren** ausgewählt haben.

*Prisma Access unterstützt die interne Hosterkennung nur für die **Always On**-Verbindungsmethode.*




Wenn Sie das interne Gateway aktivieren, fungieren die Remote-Netzwerkinstanzen als interne Gateways. Wenn Sie die interne Hosterkennung aktivieren, erstellt Prisma Access auf

 ©2025 Palo Alto Networks, Inc.

den DNS-Proxyservern des Remote-Netzwerks PTR-Datensätze für den Prozess der internen Hosterkennung.

Wenn Sie das interne Gateway aktivieren, erstellt Prisma Access in einer Remote-Netzwerkvorlage eine interne Gateway-Konfiguration.

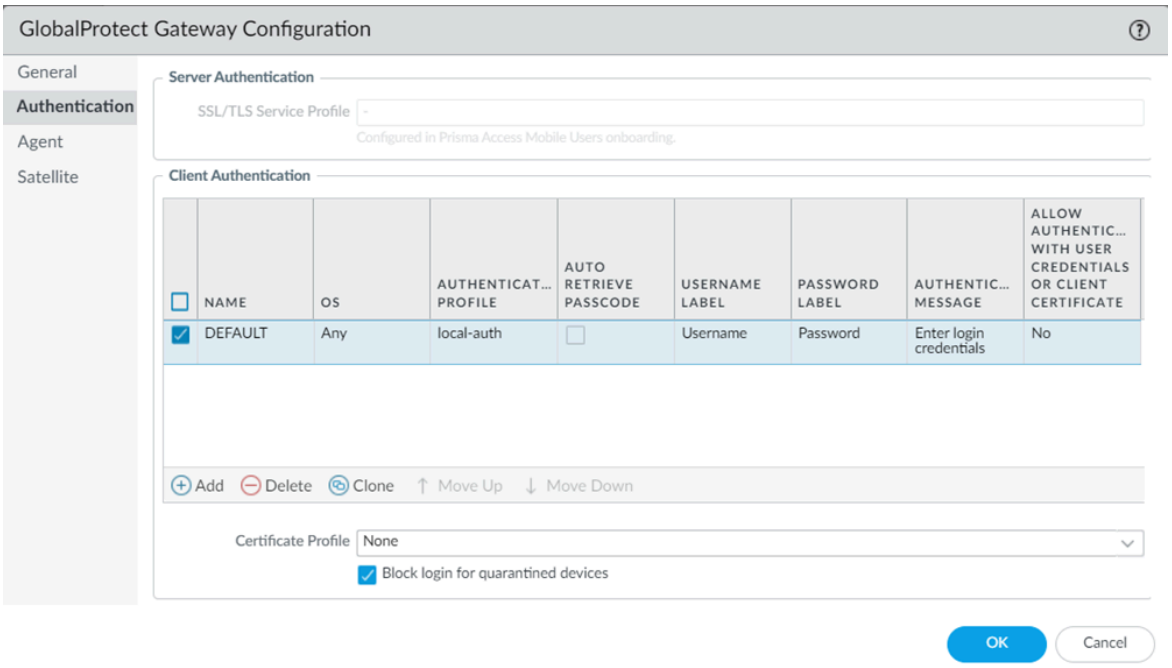
**STEP 4 |** Gehen Sie zu **Vorlagen** > **Netzwerk** > **GlobalProtect** > **Gateways** und wählen Sie **Remote_Network_Template** aus.

Dort werden Sie die Vorlage **GlobalProtect_Internal_Gateway** finden, die für das interne Gateway erstellt wurde.

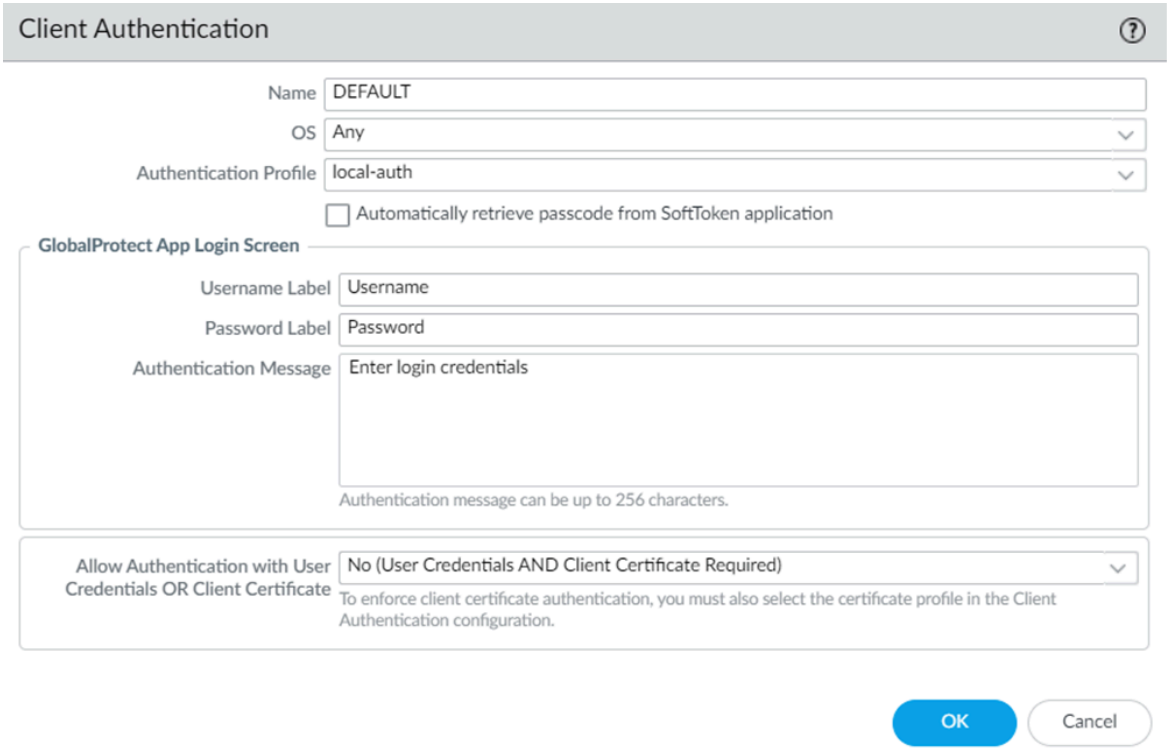
 ©2025 Palo Alto Networks, Inc.

**STEP 5 |** Erstellen Sie ein Authentifizierungsprofil für diese Remote-Netzwerkvorlage ähnlich dem Authentifizierungsprofil in der Vorlage für mobile Benutzer.

1. Wählen Sie die Vorlage für Remote-Netzwerke aus, dann die Vorlage **GlobalProtect_Internal_Gateway** und den Hyperlink.
2. Gehen Sie zu **Authentifizierung** > **Clientauthentifizierung**.

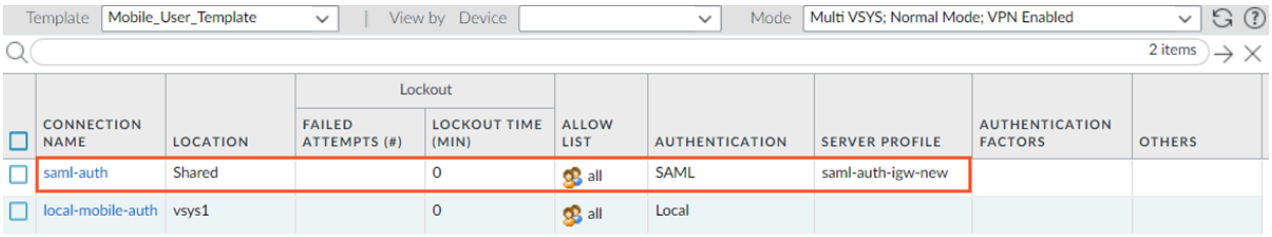



3. Bearbeiten Sie die Authentifizierungsprofildetails der **STANDARD**-Clientauthentifizierung.

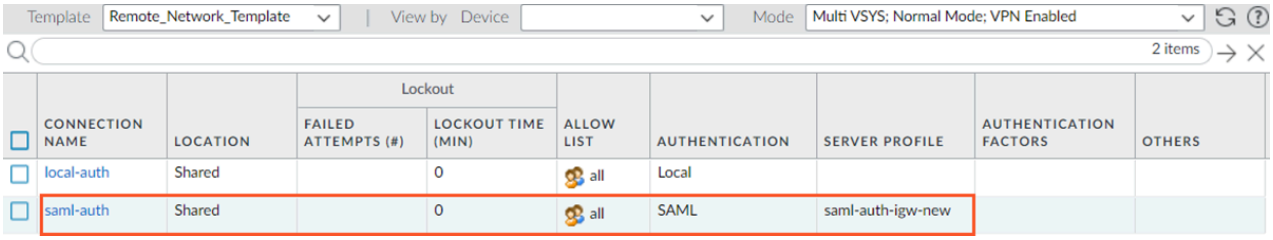



 ©2025 Palo Alto Networks, Inc.

Erstellen Sie ein Authentifizierungsprofil, das dem in der Vorlage für mobile Benutzer entspricht. Das in der Vorlage für mobile Benutzer verwendete Authentifizierungsprofil finden Sie unter **Vorlage** > **Gerät** > **Authentifizierungsprofil**. Stellen Sie sicher, dass Sie **Mobile_User_Template** auswählen.



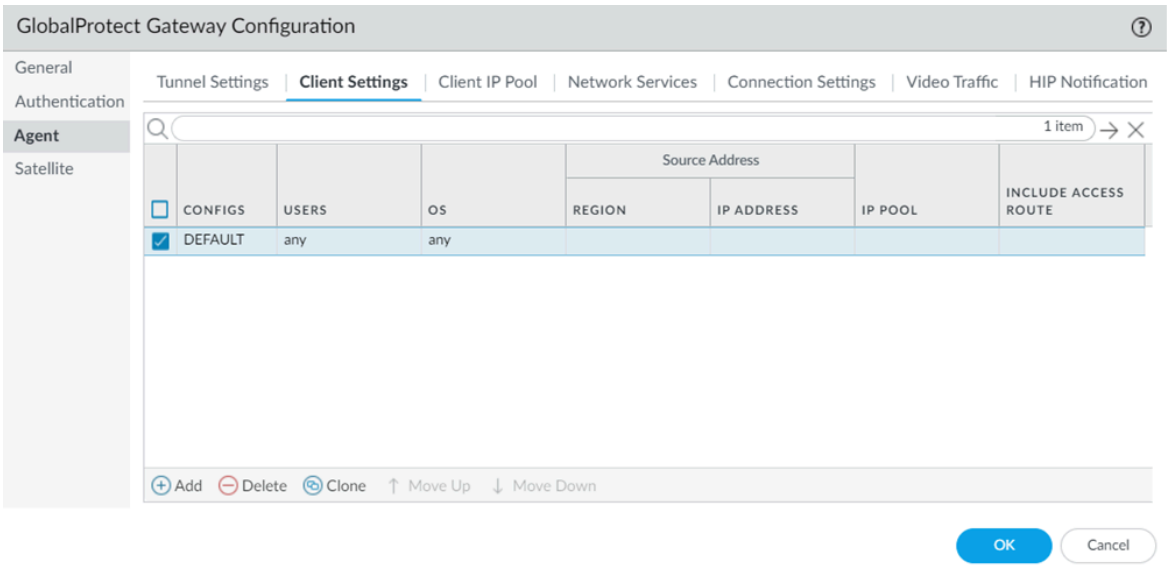

*Sie können auch das Authentifizierungsprofil für die Remote-Netzwerkvorlage anzeigen, indem Sie **Vorlagen** > **Gerät** > **Authentifizierungsprofil**auswählen. Wählen Sie **Remote_Network_Template** aus.*



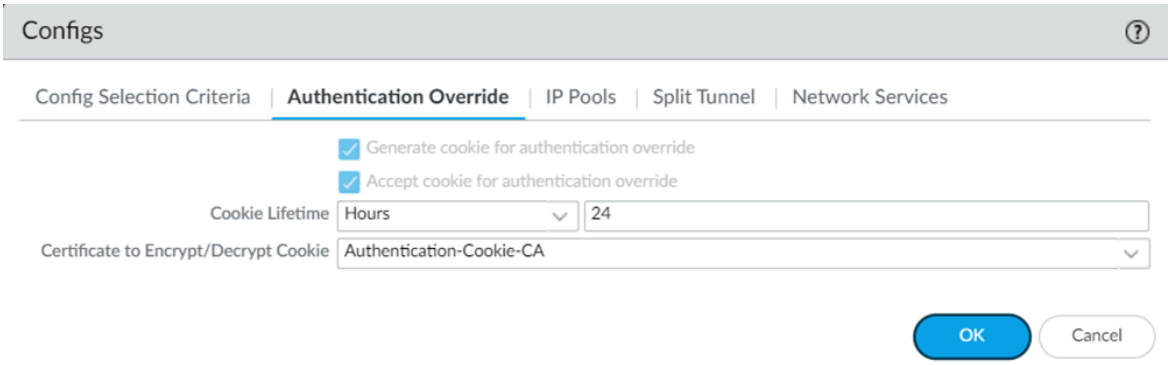

 ©2025 Palo Alto Networks, Inc.

**STEP 6 |** Erstellen Sie ein Gerätezertifikat für die Vorlage für Remote-Netzwerke ähnlich dem Gerätezertifikat in der Vorlage für mobile Benutzer.

1. Wählen Sie die Vorlage für Remote-Netzwerke aus, dann **GlobalProtect_Internal_Gateway** und den Hyperlink.
2. Gehen Sie zu **Agent** > **Clienteinstellungen**.



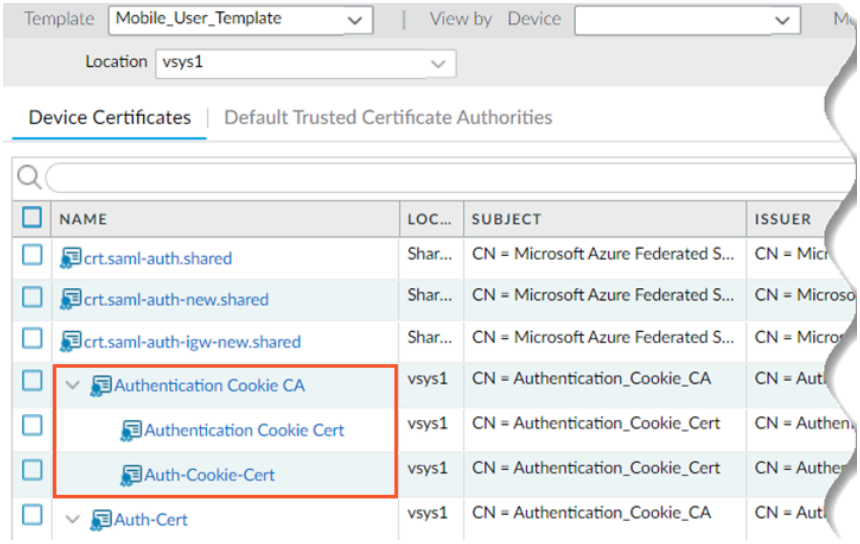

3. Wählen Sie die **STANDARD**-Konfiguration aus und gehen Sie zu den Einstellungen für die **Authentifizierungsüberschreibung**.
4. Bearbeiten Sie die Einstellungen für **Zertifikat zum Ver-/Entschlüsseln von Cookies** und erstellen Sie ein neues Gerätezertifikat.



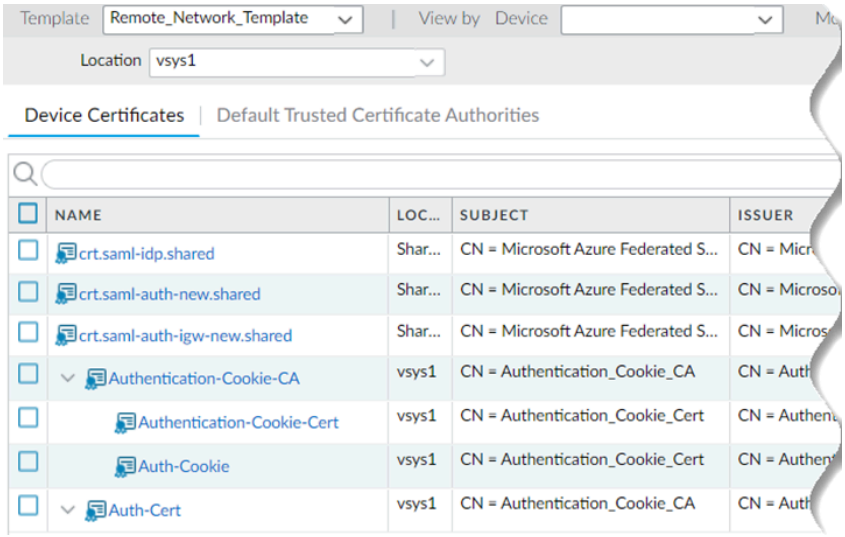

Erstellen Sie ein Gerätezertifikat wie in der Vorlage für mobile Benutzer. Sie finden das in der Vorlage für mobile Benutzer verwendete Gerätezertifikat unter **Vorlage** > **Gerät** > **Zertifikatverwaltung** > **Zertifikate** > **Gerätezertifikate**. Wählen Sie **Mobile_User_Template** aus. Die **STANDARD**-Konfiguration verweist auf das

 ©2025 Palo Alto Networks, Inc.

Zertifikat **Authentifizierungscookie CA**. Folgen Sie der gleichen Hierarchie wie in **Mobile_User_Template** für eine erfolgreiche Authentifizierung.




*Sie können das Gerätezertifikat für die Vorlage für Remote-Netzwerke auch anzeigen, indem Sie **Vorlage** > **Gerät** > **Zertifikatverwaltung** > **Zertifikate** > **Gerätezertifikate** auswählen. Wählen Sie **Remote_Network_Template** aus.*




**STEP 7 |** Übertragen Sie die Änderungen zur gleichen Zeit per **Push** an mobile Benutzer und Remote-Netzwerke.

 ©2025 Palo Alto Networks, Inc.

# Sicheren eingehenden Zugriff auf Remote-Netzwerkstandorte gewähren

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz, die Net Interconnect für Site-to-Site- und User-to-Site-Zugriff umfasst |

Wenn Ihr Unternehmen an einem Remote-Netzwerkstandort internetfähige Anwendungen hostet, setzt die Bereitstellung des Zugriffs auf diese Anwendungen Ihr Netzwerk allen Bedrohungen eines offenen Internets aus. In diesem Abschnitt wird beschrieben, wie Prisma Access sicheren Zugriff auf diese Anwendungen bietet, wann Sie ihn implementieren sollten und wie Sie ihn konfigurieren.

- Sicherer eingehender Zugriff für Remote-Netzwerkstandorte
- Secure Inbound Access – Beispiele
- Richtlinien für die Verwendung von Secure Inbound Access
- Konfigurieren des sicheren eingehenden Zugriffs für Remote-Netzwerkstandorte

## Sicherer eingehender Zugriff für Remote-Netzwerkstandorte

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz mit Net Interconnect für Zugriff zwischen Standorten und zwischen Benutzern und Standorten |

Prisma Access für Remote-Netzwerke ermöglicht den ausgehenden Zugriff auf mit dem Internet verbundene Anwendungen. In einigen Fällen muss in Ihrer Organisation möglicherweise eingehender Zugriff auf eine Anwendung oder Website an einem Remote-Standort bereitgestellt werden, und Sie müssen allen Benutzern, die mit dem Internet verbunden sind, sicheren Zugriff auf diese Anwendung gewähren – nicht nur Benutzern, die durch Prisma Access geschützt sind. Beispiel:

- Sie hosten eine öffentlich zugängliche, benutzerdefinierte Anwendung oder ein Portal an einem Remote-Netzwerkstandort.
- Sie verfügen über eine Labor- oder Staging-Umgebung, für die Sie sicheren Zugriff bereitstellen möchten.
- Sie müssen Benutzern, die nicht Mitglied einer Organisationsdomäne sind, Zugriff auf eine Anwendung oder Website gewähren.
- Sie verfügen über IoT-Geräte, die Zugriff auf eine interne Asset-Management-, Nachverfolgungs- oder Statusanwendung benötigen.

Erstellen Sie dazu ein Remote-Netzwerk, das einen sicheren eingehenden Zugriff ermöglicht. Wenn Sie sowohl ausgehenden als auch eingehenden Zugriff für einen Remote-Netzwerkstandort

 ©2025 Palo Alto Networks, Inc.

benötigen, erstellen Sie zwei Remote-Netzwerke am selben Standort – eines für den eingehenden Zugriff und eines für den ausgehenden Zugriff.

*Obwohl diese Lösung Zugriff für bis zu 50.000 gleichzeitige eingehende Sitzungen pro Remote-Netzwerk bieten kann, empfiehlt Palo Alto Networks die Verwendung dieser Lösung nicht, um den Zugriff auf eine Anwendung oder Website mit hohem Volumen zu ermöglichen.*

## Secure Inbound Access – Beispiele

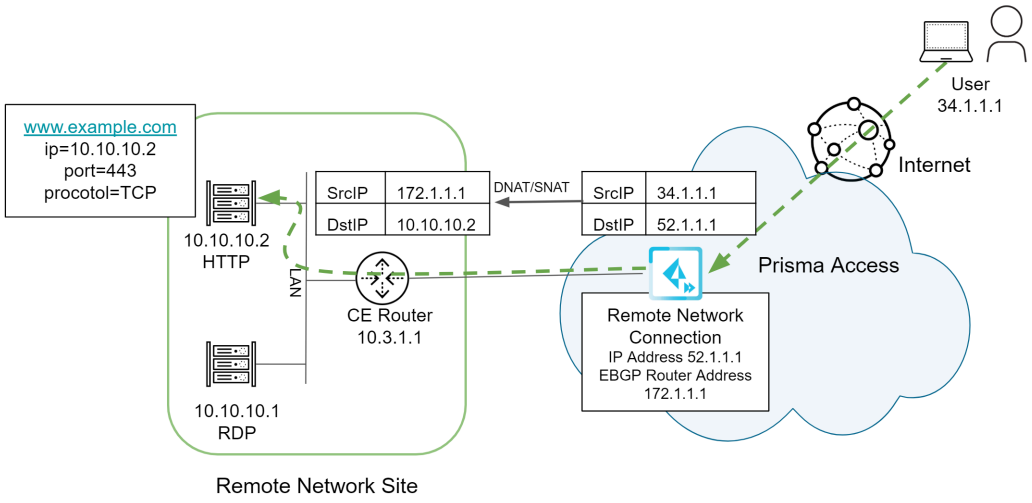
| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Die Prisma Access-Lizenz mit Net Interconnect für Site-to-Site- und User-to-Site-Zugriff |

In diesem Abschnitt finden Sie Beispiele für Inbound Access sowie die IP-Adressen, die Prisma Access in verschiedenen Bereitstellungen zuweist.

Das folgende Beispiel zeigt eine Beispielkonfiguration zur Aktivierung von Inbound Access für eine Anwendung (www.example.com) an einem Remote-Netzwerkstandort. Sie weisen der Anwendung die IP-Adresse 10.10.10.2, den Port 443 und das Protokoll TCP zu. Diese Werte geben Sie dann in Prisma Access ein, wenn Sie Inbound Access konfigurieren. Nachdem Sie Ihre Änderungen gespeichert und übernommen haben, weist Prisma Access der von Ihnen definierten Anwendung eine öffentliche IP-Adresse zu, in diesem Fall 52.1.1.1.

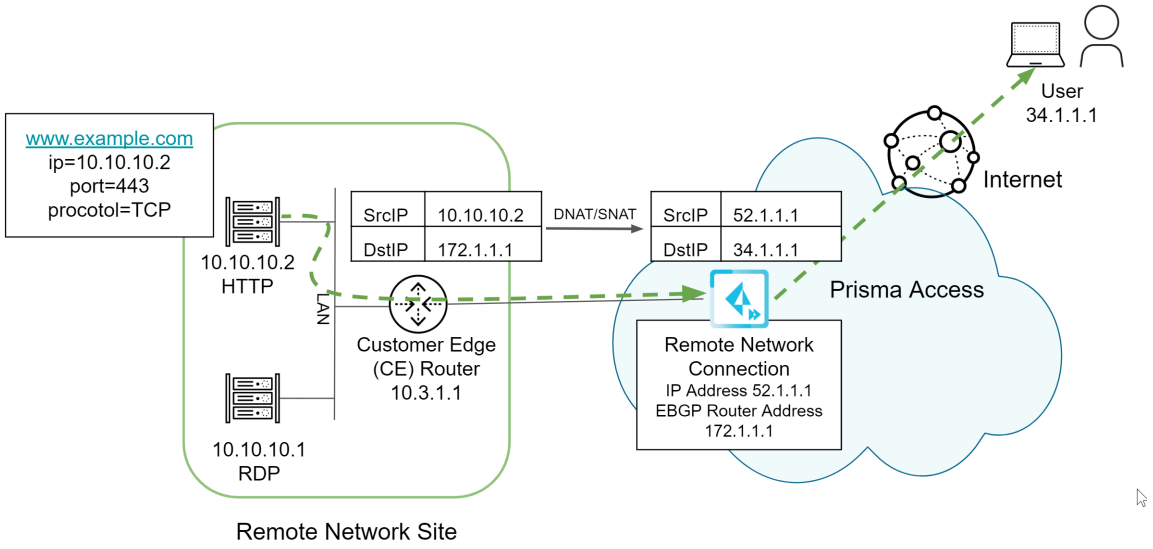
Prisma Access führt standardmäßig eine Quellnetzwerkadressübersetzung (Quell-NAT) für die Pakete durch. Wenn das IPSec-fähige Gerät an Ihrem Remote-Netzwerkstandort symmetrische Rückgaben durchführen kann (z. B. eine Next-Generation Firewall von Palo Alto Networks), können Sie Quell-NAT deaktivieren.

Die folgende Abbildung zeigt den Datenverkehr von Benutzern zu Anwendungen. Da Quell-NAT aktiviert ist, ändert sich die Quell-IP-Adresse in der Routingtabelle von der IP des Geräts des Benutzers (34.1.1.1) zur **EBGP-Routeradresse** des Remote-Netzwerks (**Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Remote-Netzwerke** > **EBGP-Router**). (172.1.1.1).

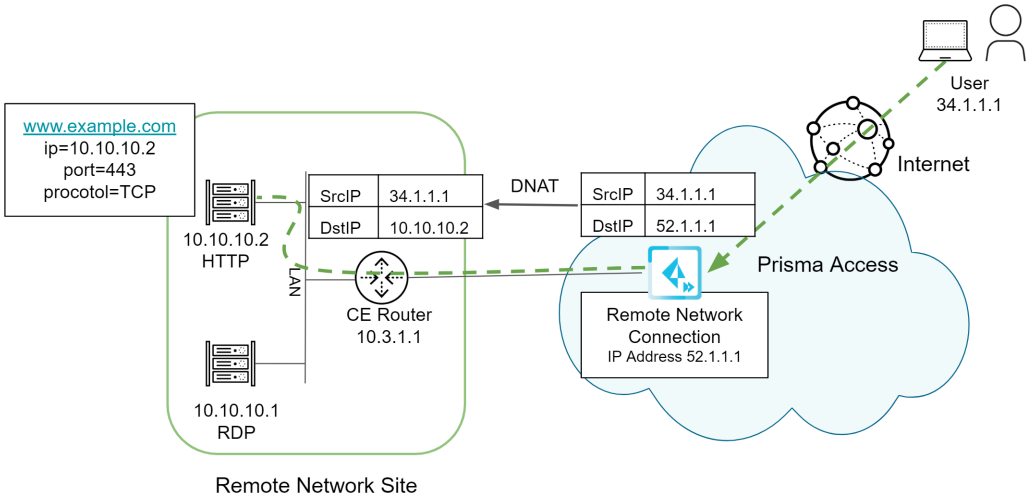



 ©2025 Palo Alto Networks, Inc.

Die folgende Abbildung zeigt den Rückweg des Datenverkehrs mit aktiviertem Quell-NAT.

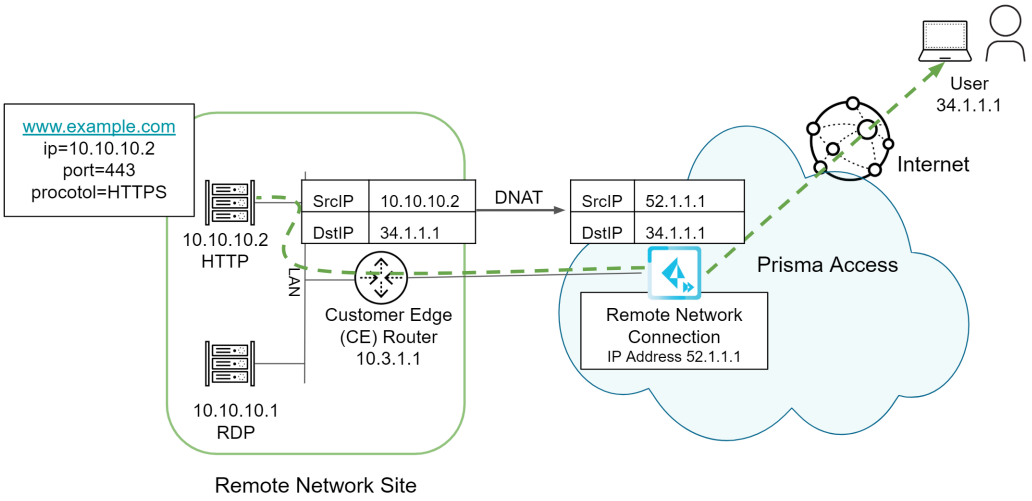



Wenn Sie Quell-NAT deaktivieren, führt Prisma Access weiterhin Ziel-NAT aus, aber die Quell-IP-Adresse der Anforderung bleibt unverändert.




Für den zurückfließenden Datenverkehr ist SNAT deaktiviert. Die Zieladresse für alle Routingtabellen ist die IP-Adresse des Benutzers (34.1.1.1).

 ©2025 Palo Alto Networks, Inc.




Wenn Sie über eine Ressource verfügen, die sich an einem Remote-Netzwerkstandort mit aktiviertem Inbound Access befindet, und Sie Benutzern an Standorten ohne Inbound Access den Zugriff auf diese Ressource einrichten möchten, dann wählen Sie hierzu **Eingehenden Verkehr an andere Remote-Netzwerke über Prisma Access-Backbone zulassen** aus, wenn Sie das Remote-Netzwerk ohne Inbound Access konfigurieren.

*Wenn Sie eingehenden Verkehr von anderen Remote-Netzwerken zulassen möchten, müssen Sie Quell-NAT aktivieren.*




## Richtlinien für die Verwendung von Secure Inbound Access

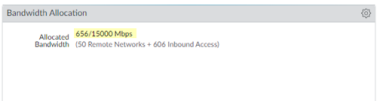
| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz, die Net Interconnect für Site-to-Site- und User-to-Site-Zugriff umfasst |

Verwenden Sie die folgenden Richtlinien und Einschränkungen, wenn Sie ein Remote-Netzwerk für die Verwendung von sicherem eingehendem Zugriff konfigurieren:

- Wenn Sie ein Remote-Netzwerk für eingehenden Zugriff konfigurieren, fügen Sie Einheiten (Mbit/s) aus Ihrer Lizenz für die von Ihnen zugewiesenen IP-Adressen hinzu (150 Mbit/s für 5 IP-Adressen und 300 Mbit/s für 10 IP-Adressen). Vergewissern Sie sich daher zunächst, dass Sie über genügend verbleibende lizenzierte Bandbreite verfügen, um die Remote-Netzwerke für eingehenden Zugriff einzubinden. Um Ihre verfügbare Bandbreite zu überprüfen, wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Remote-Netzwerke** aus und sehen Sie sich

 ©2025 Palo Alto Networks, Inc.

Ihre lizenzierte **Bandbreitenzuweisung** an. In diesem Bereich wird die bereits zugewiesene Bandbreite zusammen mit der gesamten lizenzierten Bandbreite angezeigt.




- Der sichere eingehende Zugriff verwendet eine Teilmenge der Prisma Access-Standorte.
- Sie können ein vorhandenes Remote-Netzwerk nicht ändern, um einen sicheren eingehenden Zugriff bereitzustellen. Stattdessen können Sie ein neues Remote-Netzwerk erstellen.
- Die Funktion für eingehenden Zugriff ist in Remote-Netzwerken, die ECMP-Lastausgleich verwenden, nicht verfügbar.
- Anwendungsportübersetzung wird nicht unterstützt.
- Die Funktion für den Massenimport zum Onboarding von Remote-Netzwerken unterstützt keinen eingehenden Zugriff. Verwenden Sie Panorama, um neue Remote-Netzwerke für eingehenden Zugriff einzubinden.
- Verwenden Sie eingehenden Zugriff von Remote-Netzwerken nicht mit Verkehrsweiterleitungsregeln für Dienstverbindungen.
- Ausgehender Datenverkehr, der von der Zweigstelle abgeht, ist auf dem Remote-Netzwerk mit eingehendem Zugriff nicht erlaubt.
- Benutzer-ID und Anwendungsauthentifizierung werden nicht unterstützt.
- Prisma Access setzt folgende Grenzwerte für den Hochwasserschutz durch und misst die Rate in Verbindungen pro Sekunde (Connections per Second, CPS):

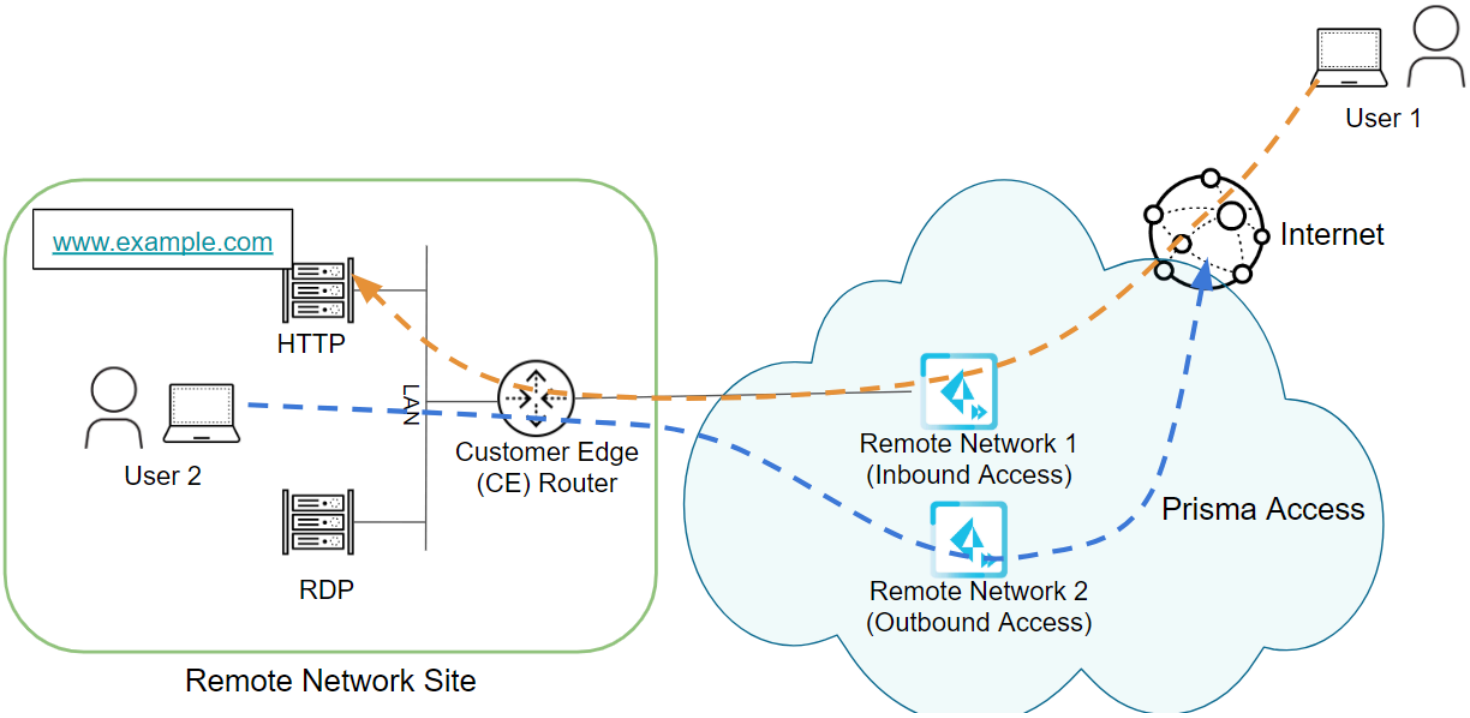
| Flood-Schutz-Typ | Alarmrate in CPS | Aktivierungsrate in CPS |
|---|---|---|
| SYN-Flood | 10000 | 15000 |
| ICMP-Flood | 20 | 20 |

Wenn Sie einen besseren Schutz vor dem Flooding mit neuen Sitzungen benötigen, wenden Sie sich an Ihr Palo Alto Networks Team.

- Remote-Netzwerke, die für einen sicheren eingehenden Zugriff konfiguriert sind, können nur zu diesem Zweck verwendet werden. Wenn Sie sowohl ausgehenden Zugriff als auch eingehenden Zugriff für einen Remote-Netzwerkstandort benötigen, erstellen Sie zwei Remote-Netzwerkstandorte am selben Standort – einen für eingehenden Zugriff und einen für ausgehenden Zugriff – wie in der folgenden Abbildung gezeigt. In diesem Beispiel verwendet Benutzer 1 das Remote-Netzwerk 1 für den eingehenden Zugriff auf www.example.com,

 ©2025 Palo Alto Networks, Inc.

während Benutzer 2 das Remote-Netzwerk 2 für den ausgehenden Internetzugang vom Remote-Netzwerkstandort verwendet.




- Wenn Sie mit einer benutzerdefinierten Prisma Access-Bereitstellung arbeiten, bei der einer der Cloud-Anbieter ausgeschlossen ist, wird der eingehende Zugriff möglicherweise nicht unterstützt. In diesem Fall können Sie den Standort beim Onboarding des Remote-Netzwerks nicht auswählen.
- Sicherer eingehender Zugriff wird mit Evaluierungslizenzen nicht unterstützt.

## Konfigurieren des sicheren eingehenden Zugriffs für Remote-Netzwerkstandorte

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz mit Net Interconnect für Site-to-Site- und User-to-Site-Zugriff |

Ihre Bereitstellung kann Bandbreite nach Compute-Standort oder nach Standort einbinden. Beide Methoden werden für die Konfiguration von eingehendem Remote-Netzwerkzugriff unterstützt. Wenn Sie den eingehenden Zugriff für ein Remote-Netzwerk konfigurieren, das Bandbreite nach Compute-Standort zuweist, geben Sie die Bandbreite pro Standort an. Um einen Remote-Netzwerkstandort zu erstellen, der sicheren eingehenden Zugriff zulässt, verwenden Sie einen der folgenden Workflows:

- Zum Konfigurieren eines sicheren eingehenden Zugriffs für eine Remote-Netzwerkbereitstellung, die Bandbreite nach Compute-Standort zuweist, verwenden Sie diesen Workflow.

 ©2025 Palo Alto Networks, Inc.

- Zum Konfigurieren des sicheren eingehenden Zugriffs für eine Remote-Netzwerkbereitstellung, die Bandbreite nach Standort zuweist, verwenden Sie diesen Workflow.

### Konfigurieren des sicheren eingehenden Zugriffs für Remote-Netzwerke

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Strata Cloud Manager)<br>• Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz mit Net Interconnect für Site-to-Site- und User-to-Site-Zugriff |

Um internetfähige Anwendungen von einem Remote-Netzwerkstandort aus verfügbar zu machen, erstellen Sie zunächst eine Liste der Anwendungen, für die Sie Zugriff gewähren möchten, und weisen Sie für jede Anwendung eine Kombination aus privater IP-Adresse, Portnummer und Protokoll zu. Wenn Sie dieselbe IP-Adresse für mehrere Anwendungen verwenden, muss die Port/Protokoll-Kombination für jede Anwendung eindeutig sein. Wenn Sie dieselbe Port/Protokoll-Kombination für mehrere Anwendungen verwenden, muss jede IP-Adresse eindeutig sein.

Wählen Sie zu Beginn der Konfiguration aus, wie viele öffentliche IP-Adressen Sie den Anwendungen zuordnen möchten. Sie können entweder fünf oder zehn öffentliche IP-Adressen pro Remote-Netzwerkstandort angeben. Jede öffentliche IP-Zuweisung verbraucht Bandbreite (Einheiten) Ihrer Lizenz für Remote-Netzwerke sowie Bandbreite, die Sie für den Compute-Standort zugewiesen haben, der mit dem Remote-Netzwerk verknüpft ist. Fünf IP-Adressen verbrauchen 150 Mbit/s der zugewiesenen Bandbreite Ihrer Lizenz für Remote-Netzwerke und zehn IP-Adressen verbrauchen 300 Mbit/s.

Nachdem Sie die Anzahl der öffentlichen IP-Adressen ausgewählt haben, geben Sie die Anwendung mit der zugehörigen Kombination aus privater IP-Adresse, Portnummer und Protokoll ein, für die Sie einen sicheren eingehenden Zugriff konfigurieren möchten.

Sie können festlegen, wie Sie Ihre Anwendung den öffentlichen IP-Adressen zuordnen möchten. Standardmäßig weist Prisma Access die öffentlichen IP-Adressen den von Ihnen angegebenen Anwendungen zu, und es können mehrere Anwendungen einer einzigen IP-Adresse zugewiesen werden. Wenn Sie eine einzelne Anwendung einer einzigen öffentlichen IP-Adresse zuordnen müssen, können Sie während der Systemkonfiguration **Dedizierte IP** auswählen. Sie können bis zu 100 eingehende Anwendungen für jede Gruppe der bereitgestellten öffentlichen IP-Adressen (fünf oder zehn) konfigurieren.

- Strata Cloud Manager
- Panorama

*Konfigurieren des sicheren Inbound Access für Remote-Netzwerke (Strata Cloud Manager)*

So ermöglichen Sie den Zugriff auf eine Anwendung über einen Remote-Netzwerkstandort für alle mit dem Internet verbundenen Benutzer (nicht nur Prisma Access-Benutzer).

**STEP 1 |** Falls Sie die Richtlinien für den Inbound Access bei Remote-Netzwerken noch nicht gelesenen haben, dann holen Sie dies jetzt nach.

 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Sammeln Sie die Anwendungsdetails, die Sie benötigen, um zu beginnen.

Erstellen Sie eine Liste der Anwendungen, auf die der Zugriff eingerichtet werden soll, und weisen Sie für jede Anwendung eine private IP-, Portnummern- und Protokollkombination zu. Wenn Sie dieselbe IP-Adresse für mehrere Anwendungen benutzen, muss die Port/Protokoll-Kombination für jede Anwendung eindeutig sein. Wenn Sie dieselbe Port/Protokoll-Kombination für mehrere Anwendungen benutzen, muss jede IP-Adresse eindeutig sein.

**STEP 3 |** Rufen Sie in Strata Cloud Manager **Workflows** > **Prisma Access-Einrichtung** > **Remote-Netzwerke** > **Inbound Access** > **Inbound Access hinzufügen** auf.

**STEP 4 |** Geben Sie die erforderlichen Details ein.

Wählen Sie die **Anzahl der öffentlichen IPs** aus, die Sie für die Anwendungen benutzen möchten (entweder fünf oder zehn).

Jede öffentliche IP-Zuweisung benötigt Bandbreite aus Ihrer Lizenz für Remote-Netzwerke, und zwar zusätzlich zu den Lizenzkosten für das Remote-Network. Fünf IP-Adressen verbrauchen 150 MB des zugewiesenen Volumens Ihrer Lizenz für Remote-Netzwerke und zehn IP-Adressen verbrauchen 300 MB.

Ab Prisma Access Version 4.1 können Sie für Ressourcen, die sich an einem Remote-Netzwerkstandort mit aktiviertem Inbound Access befinden, den Zugriff für Benutzer an Standorten ohne Inbound Access auf diese Ressource einrichten. Wählen Sie hierzu **Eingehenden Verkehr an andere Remote-Netzwerke über Prisma Access-Backbone zulassen** aus, wenn Sie das Remote-Netzwerk ohne Inbound Access konfigurieren.

Ab Prisma Access Version 5.0 können Sie eingehenden Datenverkehr zu anderen Remote-Netzwerken über das Dienstanbieter-Backbone zulassen, wenn Sie das Remote-Netzwerk ohne Inbound Access konfigurieren.

*Die Dienstanbieterverbindung unterstützt nur Folgendes:*

- *GCP-Regionen*
- *Neue Prisma Access-Bereitstellungen*
- *Ausgangsverkehr für expliziten Proxy*

**STEP 5 |** Fügen Sie die **Inbound Access-Anwendungen** hinzu, für die Sie den Zugriff sichern möchten.

Fügen Sie die zugehörige Kombination aus privater IP, Portnummer und Protokoll für die Anwendung hinzu.

**STEP 6 |** Entscheiden Sie, wie Sie Anwendungen den öffentlichen IP-Adressen zuordnen möchten.

Standardmäßig weist Prisma Access die öffentlichen IP-Adressen den von Ihnen angegebenen Anwendungen zu, und es können mehrere Anwendungen einer einzigen IP-Adresse zugewiesen werden. Wenn Sie eine einzelne Anwendung einer einzigen öffentlichen IP-Adresse zuordnen müssen, können Sie während der Systemkonfiguration **Dedizierte IP zuweisen** angeben. Sie können bis zu 100 eingehende Anwendungen für jede Gruppe der bereitgestellten öffentlichen IP-Adressen (fünf oder zehn) konfigurieren.

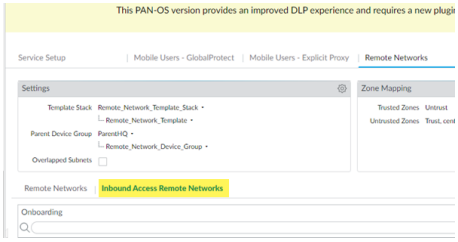
**STEP 7 |** Beenden Sie die Einrichtung des Remote-Netzwerks mit Inbound Access auf die gleiche Weise, wie Sie es von einem regulären Remote-Netzwerkstandort gewohnt sind.

 ©2025 Palo Alto Networks, Inc.

*Konfigurieren des sicheren Inbound Access für Remote-Netzwerke (Panorama)*

Wenn Sie über eine Prisma Access-Bereitstellung verfügen, die Bandbreite des Remote-Netzwerks nach Compute-Standort zuweist, konfigurieren Sie den Inbound Access, indem Sie die folgenden Schritte ausführen.

**STEP 1 |** Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Remote-Netzwerke** aus und anschließend **Remote-Netzwerke mit Inbound Access**.




**STEP 2 |** **Fügen** Sie ein Remote-Netzwerk für den Inbound Access hinzu.

**STEP 3 |** Geben Sie die Einstellungen für die Verbindung zum Remote-Netzwerk mit Inbound Access an.

1. Geben Sie unter **Name** einen Namen für die Inbound Access-Verbindung ein.
2. Geben Sie einen **Standort** ein.

   Der Inbound Access unterstützt eine Teilmenge der Standorte.
3. Geben Sie eine **Bandbreite** an, die für die Inbound Access-Verbindung verwendet werden soll.

   Sie weisen die Bandbreite für Inbound Access-Verbindungen für jeden einzelnen Standort zu.
4. Geben Sie die **Anzahl der öffentlichen IPs** an, die für die Inbound Access-Verbindung verwendet werden soll.

   Geben Sie entweder fünf oder zehn öffentliche IP-Adressen an. Jede Zuweisung einer öffentlichen IP verbraucht Bandbreite (Einheiten) Ihrer Lizenz für Remote-Netzwerke sowie Bandbreite, die Sie für den Compute-Standort zugewiesen haben, der mit dem Remote-Netzwerk verknüpft ist.
5. Wählen Sie den IPSec-Tunnel aus, der mit der Inbound Access-Verbindung verwendet werden soll.
6. Wählen Sie aus, ob Sie **Eingehenden Verkehr an andere Remote-Netzwerke über das Prisma Access-Backbone zulassen** wollen.

   Wenn Sie über eine Ressource verfügen, die sich an einem Remote-Netzwerkstandort mit aktiviertem Inbound Access befindet, und Sie Benutzern an Standorten ohne Inbound Access den Zugriff auf diese Ressource einrichten möchten, dann wählen Sie hierzu **Eingehenden Verkehr an andere Remote-Netzwerke über Prisma Access-Backbone zulassen** aus, um das Remote-Netzwerk ohne Inbound Access zu konfigurieren. Wenn Sie eingehenden Datenverkehrsfluss von anderen Remote-Netzwerken zulassen wollen, müssen Sie die Quell-NAT aktivieren.
7. (Optional) Wenn Sie über einen sekundären WAN-Link an diesem Standort verfügen, dann wählen Sie **Sekundäres WAN aktivieren** aus und geben Sie dann einen **IPSec-Tunnel** an, der nicht mit dem primären IPSec-Tunnel identisch ist.

 ©2025 Palo Alto Networks, Inc.

**STEP 4 |** Konfigurieren Sie **Statische Routen**, **BGP**, und **QoS** für Ihre Bereitstellung.

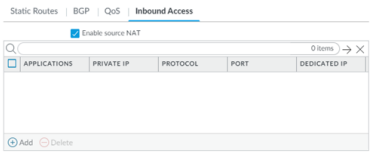
Diese Konfiguration ist identisch mit der Konfiguration für eine Remote-Netzwerkverbindung ohne Inbound Access.

**STEP 5 |** Klicken Sie auf die Registerkarte für **Inbound Access**, um die Optionen für den Inbound Access zu konfigurieren.

1. (Optional) Wählen Sie zum Deaktivieren der Quell-NAT die Option **Quell-NAT aktivieren** ab.

   Standardmäßig ist die Quell-NAT aktiviert. Wenn das IPSec-fähige Gerat an Ihrem Remote-Netzwerkstandort in der Lage ist, eine symmetrische Rückkehr auszuführen (z. B. eine Firewall der nächsten Generation von Palo Alto Networks) oder wenn Sie die Option **Eingehenden Verkehr an andere Remote-Netzwerke über das Prisma Access-Backbone zulassen** nicht ausgewählt haben, dann wählen Sie die Option **Quell-NAT aktivieren** ab.

   *Wenn Sie dieses Kontrollkästchen aktivieren, müssen Sie auf der Registerkarte **Inbound Access** die Option **Quell-NAT aktivieren** aktivieren. Die Quell-NAT ist eine Voraussetzung, um eingehenden Verkehr zu anderen Remote-Netzwerken zuzulassen.*




2. Sie müssen die Anwendungen **hinzufügen**, um sicheren Inbound Access zu ermöglichen.

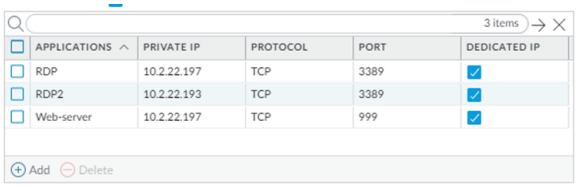
   Sie können bis zu 100 eingehende Anwendungen für jede Gruppe der bereitgestellten öffentlichen IP-Adressen (fünf oder zehn) konfigurieren. Geben Sie für jede Anwendung eine eindeutige Kombination aus **privater IP**-Adresse, **Protokoll** und **Port** an. Es ist akzeptabel, doppelte private IP-Adressen und Ports für zwei Anwendungen zu verwenden, solange Sie **TCP** für eine Anwendung und **UDP** für die andere Anwendung angeben.

   Legen Sie die folgenden Werte fest:

   - Geben Sie den Namen der **Anwendung** an.
   - Geben Sie die **private IP**-Adresse an, die mit dieser Anwendung verwendet werden soll.
   - Geben Sie das **Protokoll** an, das mit der Anwendung verwendet werden soll (**TCP** oder **UDP**).
   - Geben Sie den **Port** an, der mit der Anwendung verwendet werden soll.

 ©2025 Palo Alto Networks, Inc.

- Wählen Sie aus, ob Sie eine einzelne öffentliche IP-Adresse für eine einzelne Anwendung festlegen möchten. Wählen Sie dazu **Dedizierte IP** aus.

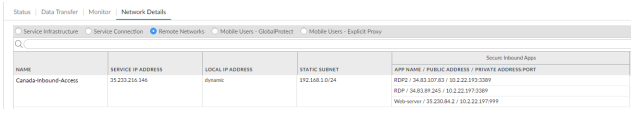



**STEP 6 |** Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

**STEP 7 |** **Speichern** Sie Ihre Anwendungen und führen Sie einen **Commit** aus.

**STEP 8 |** Warten Sie circa 30 Minuten, bis die öffentlichen IP-Adressen von Prisma Access generiert wurden. Wählen Sie dann **Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Remote-Netzwerke** aus und notieren Sie sich die **öffentliche Adresse**, die mit dem **App-Namen** der von Ihnen erstellten Anwendung verknüpft ist.

Wenn Sie **Dedizierte IP** ausgewählt haben, suchen Sie nach der einzelnen Anwendung, die der **öffentlichen Adresse** zugeordnet ist.




**STEP 9 |** Erstellen Sie Sicherheitsrichtlinien, um Datenverkehr von eingehenden Internetbenutzern zuzulassen.

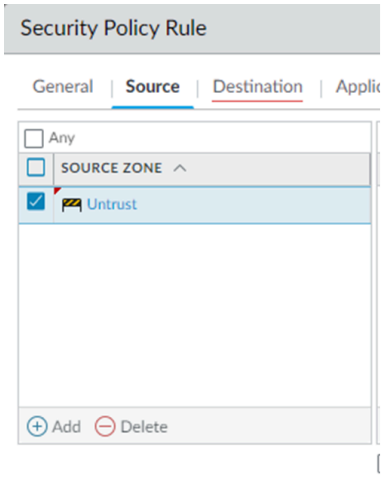
Weil die Standardsicherheitsrichtlinie von Prisma Access nur nicht vertrauenswürdigen Datenverkehr zu nicht vertrauenswürdigem Datenverkehr zulässt, müssen Sie Sicherheitsrichtlinien konfigurieren, um nicht vertrauenswürdigen Datenverkehr zu vertrauenswürdigem Datenverkehr für Ihre Anwendungen mit Inbound Access zuzulassen. Palo Alto Networks empfiehlt, den von Ihnen zugelassenen Zugriffstyp auf eingehende Anwendungen zu beschränken. Die folgenden Beispiele bieten Zugriff auf SSH-Server, Webportale und RDP-Server.

1. Wählen Sie **Richtlinien** > **Sicherheit** aus, um eine Richtlinie **hinzuzufügen**.

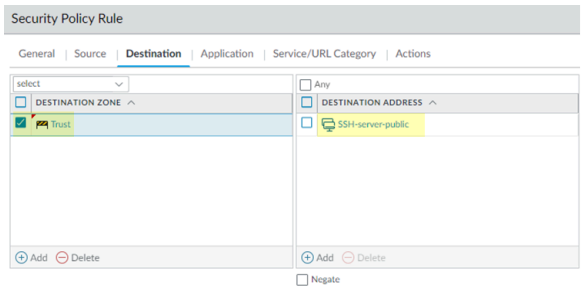
   Stellen Sie sicher, dass Sie diese Richtlinie unter der Gerätegruppe **Remote_Network_Device_Group** erstellen.

 ©2025 Palo Alto Networks, Inc.

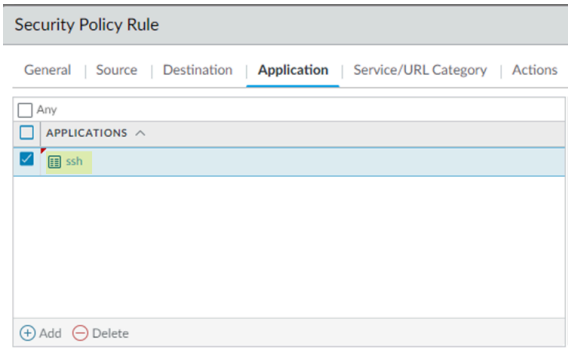
2. Legen Sie den **Quellverkehr** als **nicht vertrauenswürdig** fest.




3. Erstellen Sie eine Richtlinie, um SSH-Serverdatenverkehr zuzulassen, indem Sie die Option **Zielzone** für den Zielverkehr als **vertrauenswürdig** festlegen und als **Zieladresse SSH-server-public** auswählen. Dies ist ein von Ihnen erstelltes Adress- oder Adressgruppenobjekt mit einer Liste aller öffentlichen IP-Adressen, die für die SSH-Anmeldung verwendet werden.

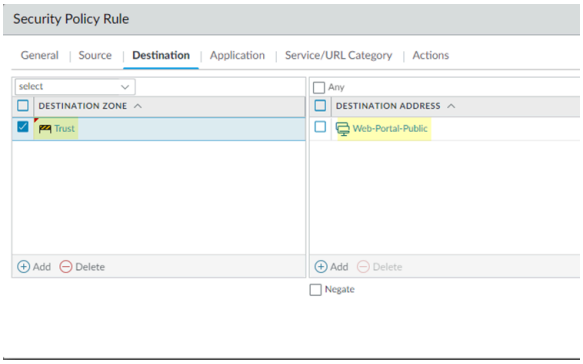



4. Wählen Sie unter **Anwendung** die Option **ssh** aus.

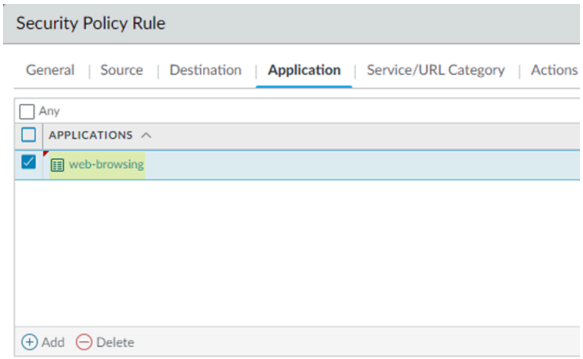



 ©2025 Palo Alto Networks, Inc.

5. Wählen Sie für **Dienst/URL-Kategorie** die Option **Anwendungsstandard** aus, um Anwendungen, wie von Palo Alto Networks definiert, ausschließlich abhängig von ihren Standardports zuzulassen oder abzulehnen.
6. Wählen Sie unter **Aktionen** die Option **Zulassen** aus.
7. Klicken Sie auf **OK**, um die Richtlinie zu speichern.
8. Erstellen Sie eine Richtlinie, um den Zugriff auf das Webportal zuzulassen, indem Sie wie in den vorherigen Schritten eine Richtlinie erstellen, aber die folgenden Einstellungen auf den Registerkarten **Ziel** und **Anwendung** ersetzen:
   - Wählen Sie als **Zieladresse** die Adresse oder Adressgruppe **Web-Portal-Public** aus, die alle öffentlichen IP-Adressen des Webportals enthält.

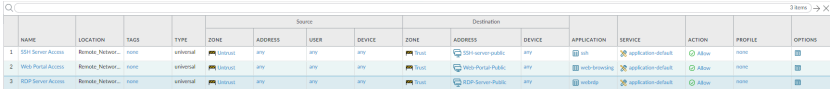



   - Wählen Sie unter **Anwendung** die Option **web-browsing** aus.




9. Erstellen Sie eine Sicherheitsrichtlinie für den RDP-Serverzugriff, indem Sie die gleichen Einstellungen wie für die anderen Richtlinien verwenden, aber ein Adress- oder Adressgruppenobjekt mit dem Namen **RDP-Server-Public**, das die öffentlichen IP-Adressen für den RDP-Server enthält, als **Zieladresse** und **webrdp** als **Anwendung** erstellen.

   Danach stehen Ihnen drei verschiedene Richtlinien zur Verfügung, um den SSH-Serverzugriff, den Webportalzugriff und den RDP-Serverzugriff zuzulassen.

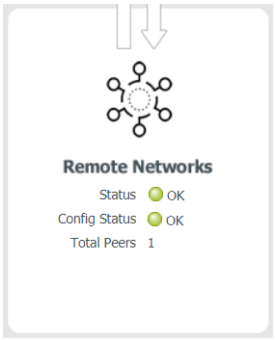


**STEP 10 | Speichern** Sie Ihre Anwendungen und führen Sie einen **Commit** aus.

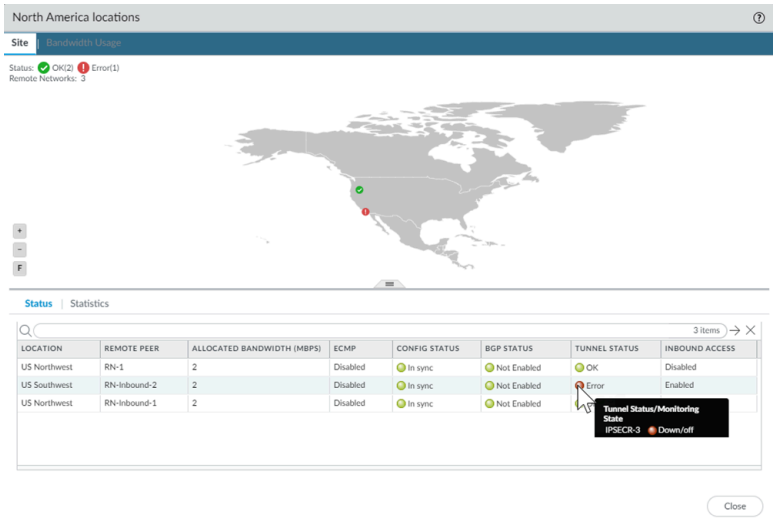
 ©2025 Palo Alto Networks, Inc.

**STEP 11 |** Überprüfen Sie, ob die Remote-Netzwerkverbindung betriebsbereit ist und eingehenden Datenverkehr ordnungsgemäß verarbeitet.

1. Wählen Sie **Panorama** > **Cloud Services** > **Status** > > **Status** > **Remote-Netzwerke** aus und bewegen Sie den Mauszeiger über die Bereiche **Status** und **Konfigurationsstatus**, um den Status des Tunnels anzuzeigen.




2. Wenn es Hinweise auf Probleme gibt, wählen Sie **Panorama** > **Cloud Services** > **Status** > > **Überwachen** > **Remote-Netzwerke** aus, wählen Sie den Speicherort des Remote-Netzwerktunnels in der Übersicht aus, und fahren Sie mit der Maus über den Bereich **Tunnelstatus**, um die Ursache des Fehlers zu ermitteln.




## Konfigurieren des sicheren eingehenden Zugriffs für Remote-Netzwerkstandorte an Standorten, die Bandbreite nach Standort zuweisen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz inklusive Net Interconnect für Site-to-Site- und User-to-Site-Zugriff |

Wenn Sie mit einer Prisma Access-Bereitstellung arbeiten, die Remote-Netzwerkbandbreite nach Standort zuweist, konfigurieren Sie den eingehenden Zugriff mithilfe der folgenden Schritte.

 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Remote-Netzwerke** aus, um eine Verbindung **hinzuzufügen**, und konfigurieren Sie das Remote-Netzwerk, einschließlich Routing- und IPSec-Tunneloptionen.

Weitere Einzelheiten finden Sie unter Prisma Access-Remote-Netzwerke. Ihre Bereitstellung kann die Bandbreite nach Compute-Standort oder nach Standort integrieren. Beide Methoden werden für den eingehenden Zugriff unterstützt.

*Stellen Sie sicher, dass Sie einen der für den eingehenden Zugriff unterstützten Standorte auswählen.*

**STEP 2 |** Klicken Sie auf das Symbol für **Inbound Access**, um die Optionen für den eingehenden Zugriff zu konfigurieren.

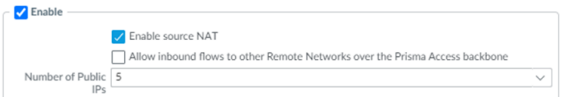
1. Wählen Sie **Aktivieren** aus, um den eingehenden Zugriff für das Remote-Netzwerk zu aktivieren.

   Wenn Sie einen Speicherort ausgewählt haben, der für den eingehenden Zugriff nicht unterstützt wird, werden Sie von Prisma Access aufgefordert, eine unterstützte Version auszuwählen.

2. (Optional) Deaktivieren Sie zum Deaktivieren von Quell-NAT die Option **Quell-NAT aktivieren**.

   Standardmäßig ist Quell-NAT aktiviert. Wenn das IPSec-fähige Gerät an Ihrem Remote-Netzwerkstandort in der Lage ist, eine symmetrische Rückkehr auszuführen (z. B. eine Firewall der nächsten Generation von Palo Alto Networks), oder wenn Sie die Option **Eingehenden Verkehr an andere Remote-Netzwerke über Prisma Access-Backbone zulassen** nicht ausgewählt haben, deaktivieren Sie die Option **Quell-NAT aktivieren**.

   *Wenn Sie dieses Kontrollkästchen aktivieren, müssen Sie auf der Registerkarte **Inbound Access** die Option **Quell-NAT aktivieren** aktivieren. Quell-NAT ist eine Voraussetzung, um eingehenden Verkehr zu anderen Remote-Netzwerken zuzulassen.*




**STEP 3 |** Sie müssen die Anwendungen **hinzufügen**, um sicheren eingehenden Zugriff zu ermöglichen.

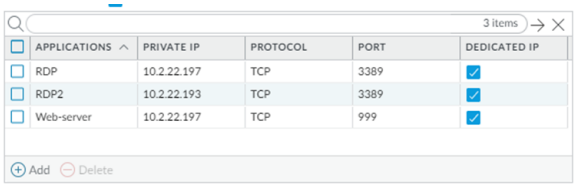
Sie können bis zu 100 eingehende Anwendungen für jede Gruppe der bereitgestellten öffentlichen IP-Adressen (fünf oder zehn) konfigurieren. Geben Sie für jede Anwendung eine eindeutige Kombination aus **privater IP**-Adresse, **Protokoll** und **Port** an. Es ist akzeptabel,

 ©2025 Palo Alto Networks, Inc.

doppelte private IP-Adressen und Ports für zwei Anwendungen zu verwenden, solange Sie **TCP** für eine Anwendung und **UDP** für die andere Anwendung angeben.

Legen Sie die folgenden Werte fest:

- Geben Sie den Namen der **Anwendung** an.
- Geben Sie die **private IP**-Adresse an, die mit dieser Anwendung verwendet werden soll.
- Geben Sie das **Protokoll** an, das mit der Anwendung verwendet werden soll (**TCP** oder **UDP**) an.
- Geben Sie den **Port** an, der mit der Anwendung verwendet werden soll.
- Wählen Sie aus, ob Sie eine einzelne öffentliche IP-Adresse für eine einzelne Anwendung festlegen möchten. Wählen Sie dazu **Dedizierte IP** aus.

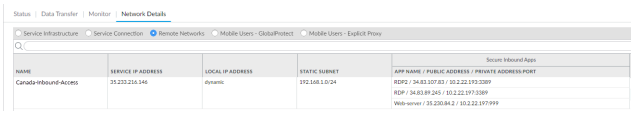



**STEP 4 |** Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

**STEP 5 |** **Speichern** Sie Ihre Anwendungen und führen Sie einen **Commit** aus.

**STEP 6 |** Warten Sie ca. 30 Minuten, bis die öffentlichen IP-Adressen von Prisma Access generiert wurden. Wählen Sie dann **Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Remote-Netzwerke** aus und notieren Sie sich die **öffentliche Adresse**, die mit dem **App-Namen** der von Ihnen erstellten Anwendung verknüpft ist.

Wenn Sie **Dedizierte IP** ausgewählt haben, suchen Sie nach der einzelnen Anwendung, die der **öffentlichen Adresse** zugeordnet ist.




**STEP 7 |** Erstellen Sie Sicherheitsrichtlinien, um Datenverkehr von eingehenden Internetbenutzern zuzulassen.

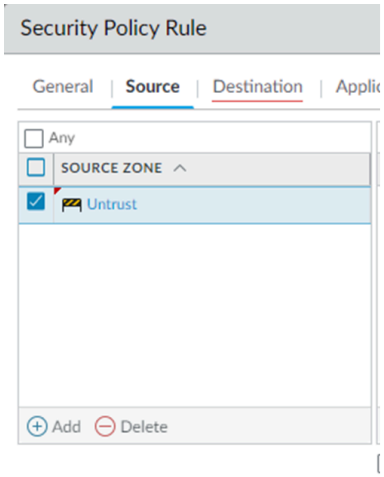
Weil die Standardsicherheitsrichtlinie von Prisma Access nur nicht vertrauenswürdigen Datenverkehr zu nicht vertrauenswürdigem Datenverkehr zulässt, müssen Sie Sicherheitsrichtlinien konfigurieren, um nicht vertrauenswürdigen Datenverkehr zu vertrauenswürdigem Datenverkehr für Ihre Anwendungen mit eingehendem Zugriff zuzulassen. Palo Alto Networks empfiehlt, den von Ihnen zugelassenen Zugriffstyp auf eingehende Anwendungen zu beschränken. Die folgenden Beispiele bieten Zugriff auf SSH-Server, Webportale und RDP-Server.

1. Wählen Sie **Richtlinien** > **Sicherheit** aus, um eine Richtlinie **hinzuzufügen**.

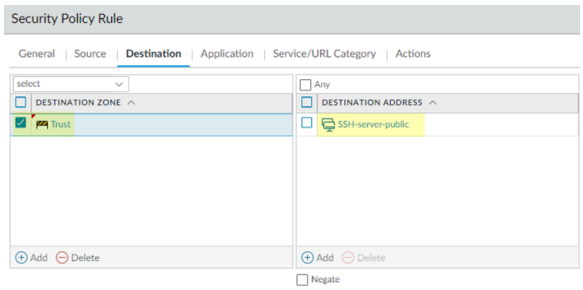
   Stellen Sie sicher, dass Sie diese Richtlinie unter der Gerätegruppe **Remote_Network_Device_Group** erstellen.

 ©2025 Palo Alto Networks, Inc.

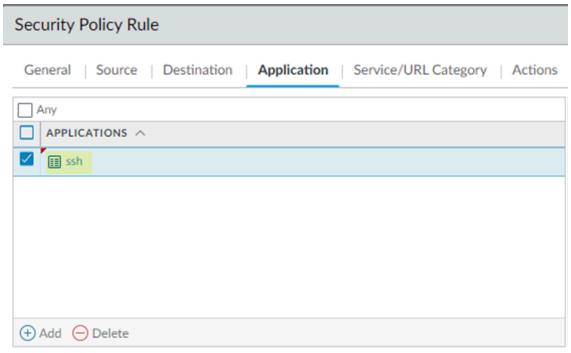
2. Legen Sie den **Quellverkehr** als **nicht vertrauenswürdig** fest.




3. Erstellen Sie eine Richtlinie, um SSH-Serverdatenverkehr zuzulassen, indem Sie die Option **Zielzone** für den Zielverkehr als **vertrauenswürdig** festlegen und als **Zieladresse SSH-server-public** auswählen. Dies ist ein von Ihnen erstelltes Adress- oder Adressgruppenobjekt mit einer Liste aller öffentlichen IP-Adressen, die für die SSH-Anmeldung verwendet werden.

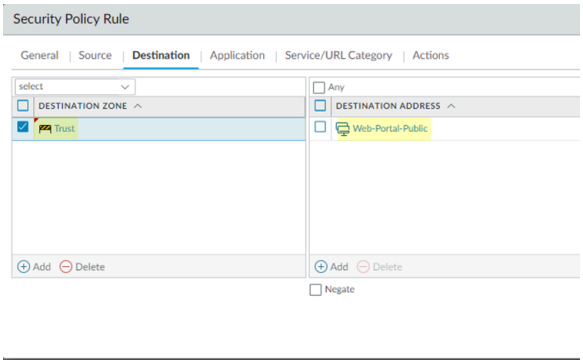



4. Wählen Sie unter **Anwendung** die Option **ssh** aus.

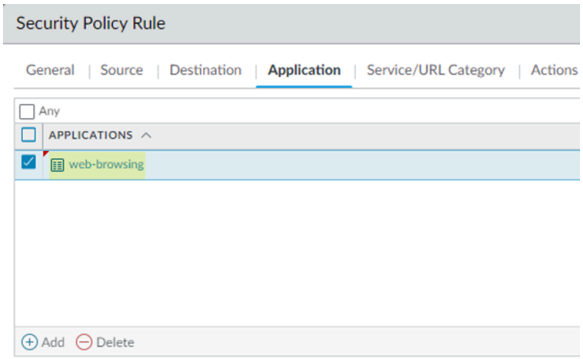



 ©2025 Palo Alto Networks, Inc.

5. Wählen Sie für **Dienst/URL-Kategorie** die Option **application-default** aus, um Anwendungen, wie von Palo Alto Networks definiert, ausschließlich abhängig von ihren Standardports zuzulassen oder abzulehnen.
6. Wählen Sie unter **Aktionen** die Option **Zulassen** aus.
7. Klicken Sie auf **OK**, um die Richtlinie zu speichern.
8. Erstellen Sie eine Richtlinie, um den Zugriff auf das Webportal zuzulassen, indem Sie wie in den vorherigen Schritten eine Richtlinie erstellen, aber die folgenden Einstellungen auf den Registerkarten **Ziel** und **Anwendung** ersetzen:
   - Wählen Sie als **Zieladresse** die Adresse oder Adressgruppe **Web-Portal-Public** aus, die alle öffentlichen IP-Adressen des Webportals enthält.

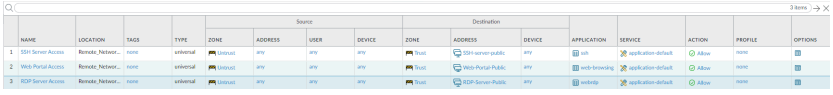



   - Wählen Sie unter **Anwendung** die Option **web-browsing** aus.




9. Erstellen Sie eine Sicherheitsrichtlinie für den RDP-Serverzugriff, indem Sie die gleichen Einstellungen wie für die anderen Richtlinien verwenden, aber ein Adress- oder Adressgruppenobjekt mit dem Namen **RDP-Server-Public**, das die öffentlichen IP-Adressen für den RDP-Server enthält, als **Zieladresse** und **webrdp** als **Anwendung** erstellen.

   Danach stehen Ihnen drei verschiedene Richtlinien zur Verfügung, um den SSH-Serverzugriff, den Webportalzugriff und den RDP-Serverzugriff zuzulassen.

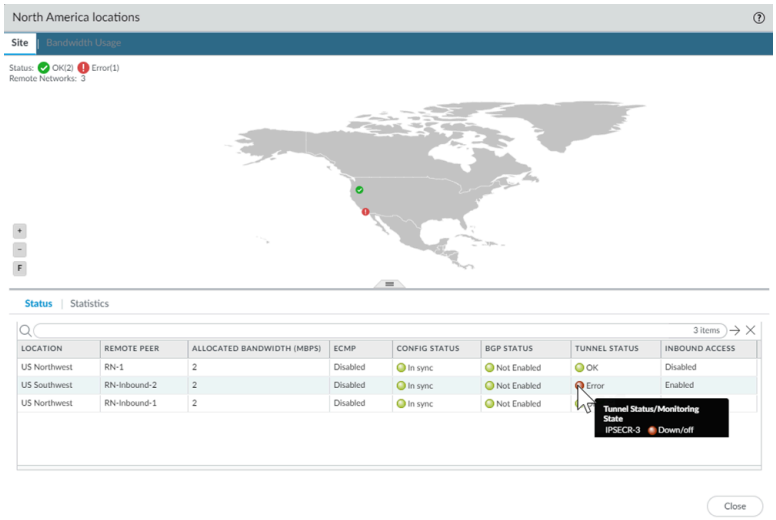


**STEP 8 |** **Speichern** Sie Ihre Anwendungen und führen Sie einen **Commit** aus.

 ©2025 Palo Alto Networks, Inc.

**STEP 9 |** Überprüfen Sie, ob die Remote-Netzwerkverbindung betriebsbereit ist und eingehenden Datenverkehr ordnungsgemäß verarbeitet.

1. Wählen Sie **Panorama** > **Cloud Services** > **Status** > > **Status** > **Remote-Netzwerke** aus und bewegen Sie den Mauszeiger über die Bereiche **Status** und **Konfigurationsstatus**, um den Status des Tunnels anzuzeigen.
2. Wenn es Hinweise auf Probleme gibt, wählen Sie **Panorama** > **Cloud Services** > **Status** > > **Überwachen** > **Remote-Netzwerke** aus, wählen Sie den Speicherort des Remote-Netzwerktunnels in der Übersicht aus, und fahren Sie mit der Maus über den Bereich **Tunnelstatus**, um die Ursache des Fehlers zu ermitteln.




## Netzwerk mit hoher Bandbreite für einen Remote-Standort erstellen

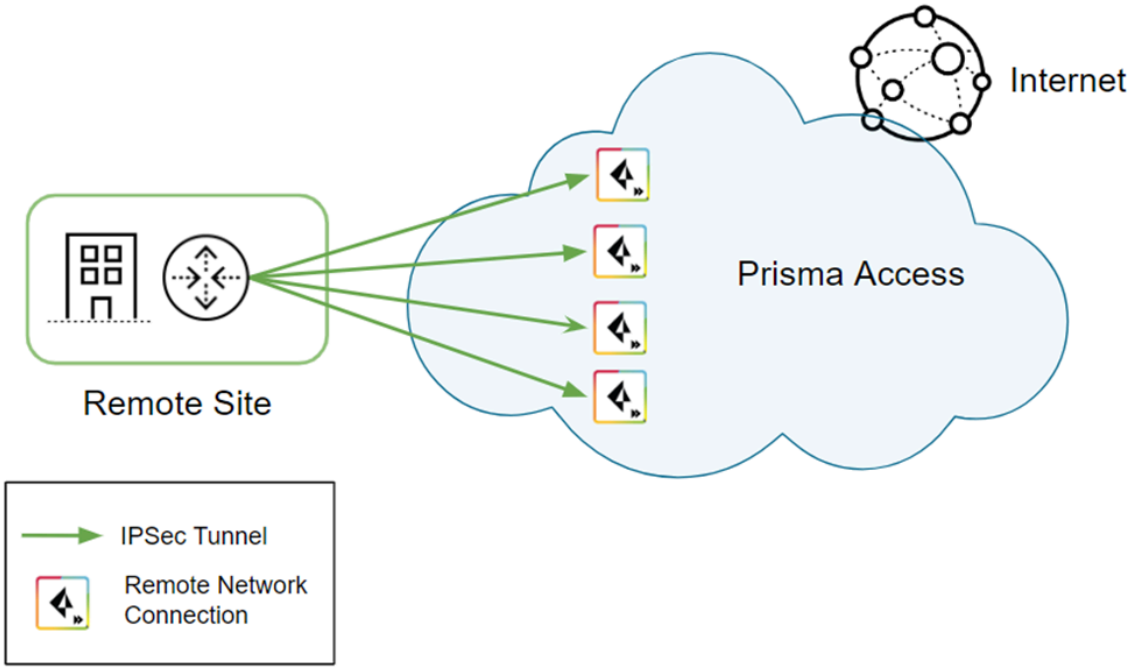
| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Wenn Sie Ihr Zweigstellenbüro oder Ihren Standort für ausgehenden Internetzugang mit einer Breitbandverbindung zu Prisma Access sichern möchten, können Sie einen Lastausgleich des Datenverkehrs von Ihrem Zweigstellenbüro oder Ihrem Standort mithilfe mehrerer IPSec-Tunnel konfigurieren, indem Sie die Schritte in diesem Abschnitt ausführen.

Im folgenden Diagramm sind vier Remote-Netzwerkverbindungen dargestellt, die denselben Remote-Standort verwenden. Weisen Sie vor dem Onboarding dem Compute-Standort, der in diesem Beispiel Südkorea ist und dem Remote-Standort entspricht, 4 Gbit/s (4000 Mbit/s) zu. 4000 Mbit/s stellen vier IPSec-Terminierungsknoten bereit, wobei jeder IPSec-Terminierungsknoten maximal 1000 Mbit/s Bandbreite bereitstellt. Weisen Sie jeder Remote-Netzwerkverbindung während des Onboarding-Prozesses einen eigenen IPSec-Terminierungsknoten zu, um die gesamte Bandbreite zu nutzen.

*In diesem Beispiel sind vier Tunnel dargestellt. Die maximale Anzahl von Tunneln, die Sie in Prisma Access für eine Verbindung mit hoher Bandbreite verwenden können, basiert auf der maximalen Anzahl von IPSec-Tunneln, die Ihre Kundenendgeräte (Customer Premises Equipment, CPE) mit dem von Ihnen verwendeten Lastausgleichsprotokoll unterstützen.*

 ©2025 Palo Alto Networks, Inc.




Beachten Sie die folgenden Einschränkungen und Empfehlungen, bevor Sie diese Konfiguration bereitstellen:

- Verwenden Sie BGP-Routing für die IPSec-Tunnel. Statisches Routing wird nicht unterstützt.
- Verwenden Sie diese Konfiguration ausschließlich für ausgehenden Internetzugang.
- Verwenden Sie auf Prisma Access oder dem CPE keine Tunnelüberwachung. Die Verfügbarkeit des IPSec-Tunnels wird durch BGP-Peering zwischen dem CPE und dem Prisma Access-Remote-Netzwerk bestimmt. Wenn ein IPSec-Tunnel ausfällt und die BGP-Verbindung unterbrochen wird, werden die über BGP erlernten Routen auf diesem Tunnel automatisch aus ECMP entfernt.
- Da Sie BGP verwenden, um festzustellen, wann ein Tunnel ausfällt, berücksichtigen Sie den HoldTime-Wert, den Sie auf Ihrem CPE konfiguriert haben. Der Hold-Timer bestimmt, wie lange der Tunnel ausfällt, bevor die Route entfernt wird. Prisma Access verwendet den BGP-HoldTime-Standardwert von 90 Sekunden wie durch RFC 4271 definiert. Wenn Sie eine kürzere Haltezeit für das BGP-CPE am Remote-Netzwerkstandort konfigurieren, verwendet BGP den niedrigeren Haltezeitwert. Palo Alto Networks empfiehlt für Ihr CPE mit dieser Bereitstellung einen KeepAlive-Wert von 10 Sekunden und einen HoldTime-Wert von 30 Sekunden.

Gehen Sie wie folgt vor, um eine Remote-Netzwerkverbindung mit hoher Bandbreite zu erstellen.

 ©2025 Palo Alto Networks, Inc.

**STEP 1 |** Konfigurieren Sie in Panorama die Prisma Access-Remote-Netzwerktunnel.

1. (Optional) Falls noch nicht geschehen, richten Sie IKE-Gateways, Profile für die IKE-Verschlüsselung und IPSec-Verschlüsselung sowie IPSec-Tunnel für die erstellten Remote-Netzwerkverbindungen ein.

   Notieren Sie die kryptografischen Profile von IKE und IPSec. Sie geben dieselben Einstellungen auf dem CPE an, das Sie zum Beenden der Remote-Netzwerkverbindung am Remote-Netzwerkstandort verwenden.

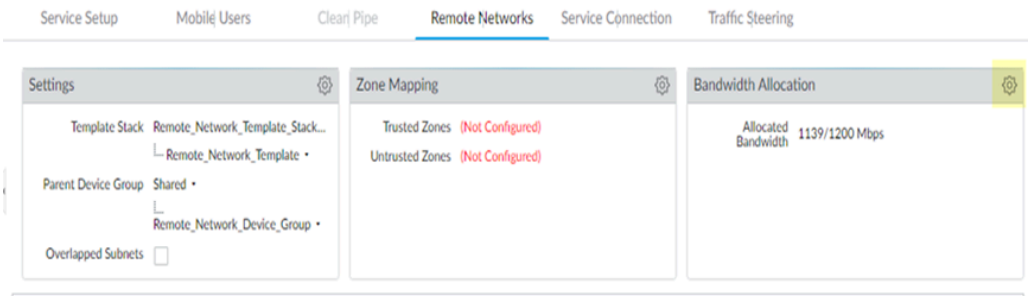
2. Bestimmen Sie den Typ der vorliegenden Remote-Netzwerkbereitstellung.

   Prisma Access-Bereitstellungen weisen Bandbreite zu, indem sie Bandbreite pro Compute-Standort zuweisen oder indem sie Bandbreite nach Standort zuweisen.

3. Binden Sie das Remote-Netzwerk ein.

   - So binden Sie das Remote-Netzwerk ein, das Bandbreite nach Compute-Standort zuweist:

     1. Weisen Sie den Standorten, die Sie einbinden möchten, Bandbreite zu, indem Sie auf das Zahnradsymbol im Bereich **Bandbreitenzuweisung** klicken.

     2. Geben Sie die **Bandbreitenzuweisung** an, die Sie für jeden **Compute-Standort** verwenden möchten, der den **Prisma Access-Standorten** zugeordnet ist, die Sie einbinden möchten.
     3. Warten Sie, bis die Bandbreite im Feld **Gesamt zugewiesen** oben auf der Seite angezeigt wird und klicken Sie dann auf **OK**.

   - Um das Remote-Netzwerk, das Bandbreite nach Standort zuweist, einzubinden, fahren Sie mit dem nächsten Schritt fort: Sie weisen Bandbreite beim Onboarding des Remote-Netzwerks zu.

4. Wählen Sie **Panorama** > **Cloud Services** > **-Konfiguration** > **Remote-Netzwerke** aus und erstellen Sie vier Remote-Netzwerkverbindungen mit den folgenden Einstellungen:

   - Wählen Sie für jede Verbindung den gleichen **Standort** aus.
   - Wählen Sie den **IPSec-Terminierungsknoten** aus.

     Wählen Sie für jede Remote-Netzwerkverbindung einen separaten IPSec-Terminierungsknoten aus.

     *Wenn Sie mit einer Bereitstellung arbeiten, die Bandbreite nach Standort zuweist, wählen Sie eine **Bandbreite** von **500 Mbit/s** aus.*

     Die von Ihnen ausgewählte Bandbreite darf die gesamte, von Ihnen lizenzierte Bandbreite nicht überschreiten. Verwenden Sie diese Einstellung, um den Wert der

 ©2025 Palo Alto Networks, Inc.

gesamten lizenzierten Bandbreite festzulegen, die Sie diesem Standort zuweisen möchten.

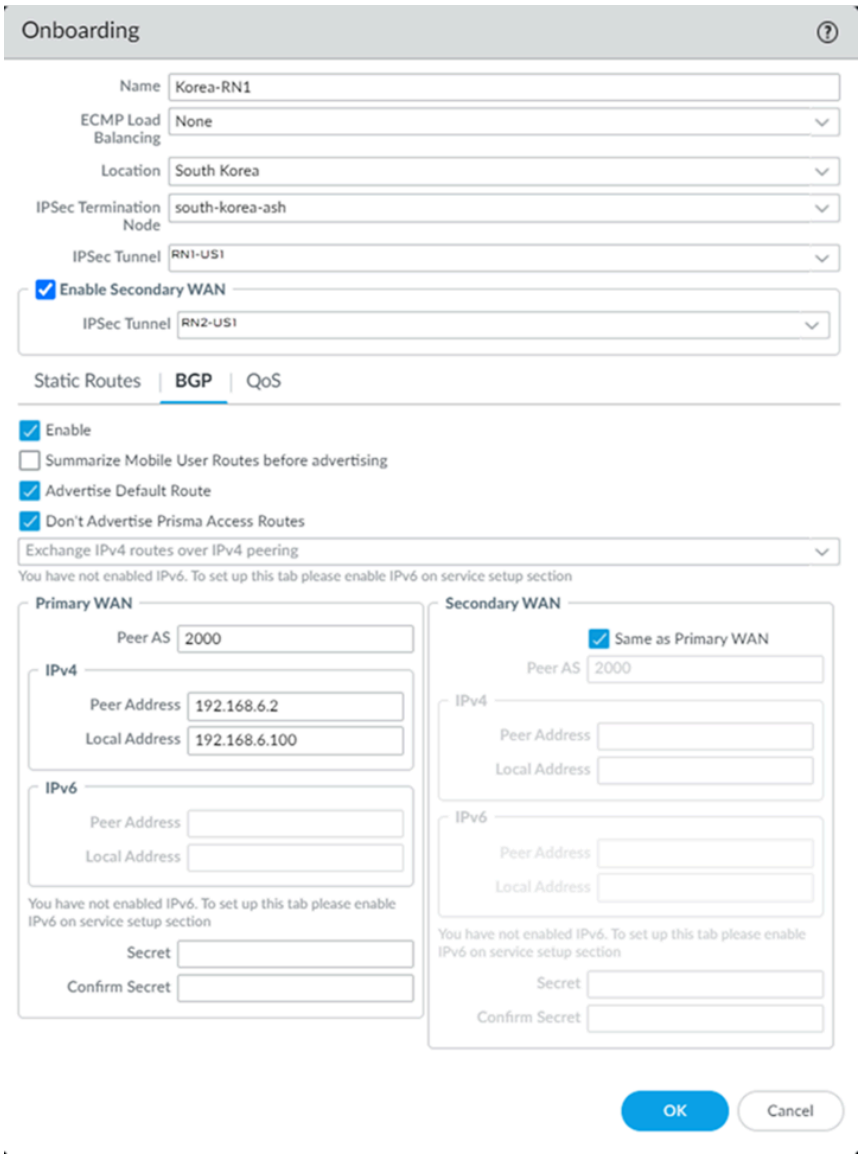
- **Aktivieren** Sie BGP, wählen Sie **Standardroute mitteilen** aus und wählen Sie **Keine Prisma Access-Routen mitteilen** aus.
- Geben Sie dasselbe **Peer-AS** für alle Remote-Netzwerkverbindungen an.

  In diesem Beispiel ist ein **Peer-AS** von 2000 dargestellt. Wählen Sie für dieses Beispiel ein **Peer-AS** von 2000 für alle vier Verbindungen aus.
- (Optional) Wenn Sie ein Backup-Remote-Netzwerk erstellen möchten, wählen Sie **Sekundäres WAN aktivieren** aus. Anschließend wählen Sie den **IPSec-Tunnel** aus, den Sie für den Backup-Tunnel erstellt haben.

Die Konfiguration eines sekundären WAN wird in den folgenden Bereitstellungen nicht unterstützt:

- Wenn Ihr sekundäres WAN im Aktiv-Aktiv-Modus mit dem primären IPSec-Tunnel eingerichtet ist.
- Wenn Ihre Kundenendgeräte (Customer Premises Equipment, CPE) in einer Equal Cost Multipath-(ECMP-)Konfiguration mit dem primären und sekundären IPSec-Tunnel eingerichtet sind.

 ©2025 Palo Alto Networks, Inc.

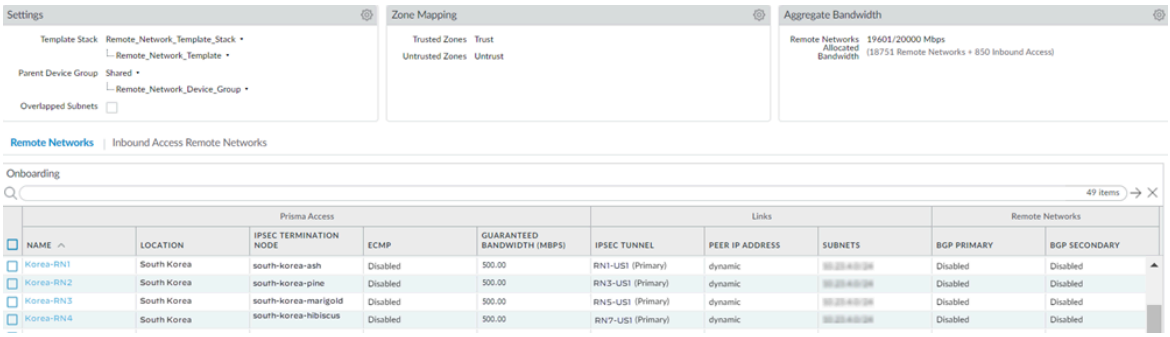



Nach Abschluss stehen vier 1000-Mbit/s-Remote-Netzwerkverbindungen für denselben Standort zur Verfügung.

Da Bereitstellungen, die Bandbreite nach Standort zuweisen, eine maximale Bandbreite von 500 Mbit/s haben, würden Sie mit dieser Konfiguration 500 Mbit/s für jeden Standort erhalten.

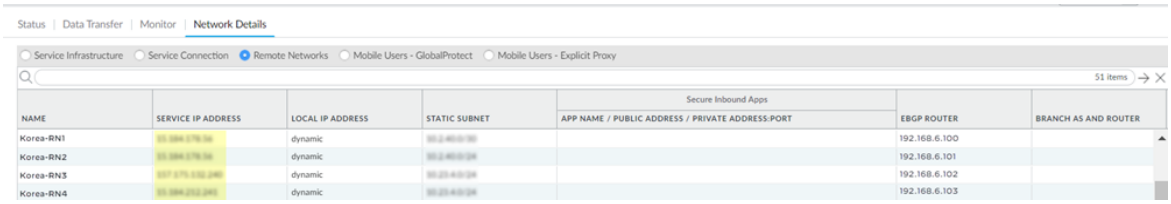
Wenn Sie Backup-Tunnel konfiguriert haben, stehen Ihnen auch vier sekundäre Tunnel zur Verfügung, die für Failover-Zwecke verwendet werden können.

 ©2025 Palo Alto Networks, Inc.




5. Wählen Sie **Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Remote-Netzwerke** aus und notieren Sie sich die **Dienst-IP-Adresse** und die **EBGP-Router**-Adressen.

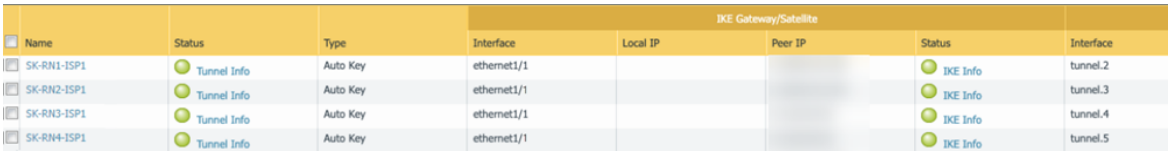
   Wenn Sie den IPSec-Tunnel auf dem CPE am Remote-Netzwerkstandort konfigurieren, verwenden Sie die **Service-IP-Adresse** als Peer IP-Adresse. Zudem verwenden Sie diese Adressen sowie die **EBGP-Router**-Adressen, wenn Sie statische Routen auf dem CPE erstellen.




**STEP 2 |** Konfigurieren Sie auf dem CPE am Remote-Netzwerkstandort die Remote-Netzwerktunnel.

- *Die Konfiguration in diesen Schritten verwendet Palo Alto Networks Firewalls der nächsten Generation. Sie können für diese Bereitstellung jedes CPE-Gerät verwenden, das IPSec-Tunnel und ECMP unterstützt.*
- *Der Bandbreitenausgleich hängt vom CPE-Hashing für ECMP ab. Prisma Access sorgt jedoch für eine symmetrische Rückkehr des Datenverkehrs.*

1. Erstellen Sie vier aktive Tunnel vom aktiven CPE zu jeder der vier Netzwerkverbindungen. Geben Sie für die **Peer-IP**-Adresse die **Dienst-IP-Adresse** des Remote-Netzwerks ein, die Sie in einem vorherigen Schritt von Prisma Access erhalten haben.




2. (Optional) Erstellen Sie Backup-Tunnel aus dem aktiven CPE zu allen vier Netzwerkverbindungen. Geben Sie für die **Peer-IP**-Adresse die **Dienst-IP-Adresse** des

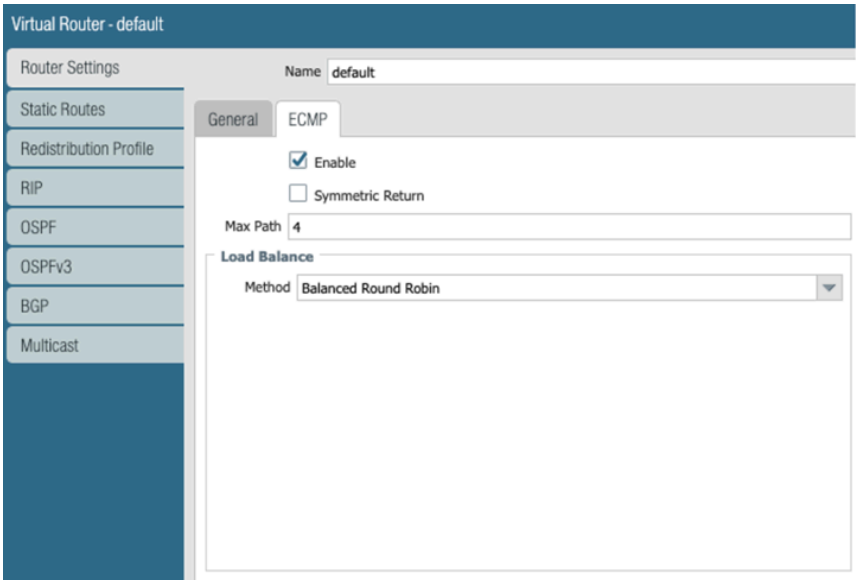
 ©2025 Palo Alto Networks, Inc.

Remote-Netzwerks ein, die Sie in einem vorherigen Schritt von Prisma Access erhalten haben.

| | | | IKE Gateway/Satellite | | | | |
|---|---|---|---|---|---|---|---|
| Name | Status | Type | Interface | Local IP | Peer IP | Status | Interface |
| SK-RN1-ISP2 | Tunnel Info | Auto Key | ethernet1/1 | | | IKE Info | tunnel.2 |
| SK-RN2-ISP2 | Tunnel Info | Auto Key | ethernet1/1 | | | IKE Info | tunnel.3 |
| SK-RN3-ISP2 | Tunnel Info | Auto Key | ethernet1/1 | | | IKE Info | tunnel.4 |
| SK-RN4-ISP2 | Tunnel Info | Auto Key | ethernet1/1 | | | IKE Info | tunnel.5 |

**STEP 3 |** Konfigurieren Sie ECMP auf dem CPE am Remote-Netzwerkstandort.

1. Wählen Sie **Netzwerk** > **Virtuelle Router** aus.
2. Wählen Sie den virtuellen **Standard**-Router aus. Alternativ können Sie einen neuen virtuellen Router **hinzufügen**.
3. Wählen Sie **Router-Einstellungen** > **Aktivieren** > **ECMP** aus, **aktivieren** Sie ECMP und geben Sie für **Maximaler ECMP-Pfad** den Wert **4** und als **Methode** für den Lastausgleich **Ausgeglichenes Ringmodell** ein.




**STEP 4 |** Erstellen Sie auf dem CPE am Remote-Netzwerkstandort statische Routen zur Prisma Access **Dienst-IP-Adresse** und zu den **EBGP-Router**-IP-Adressen, die Sie in einem vorherigen Schritt abgerufen haben.

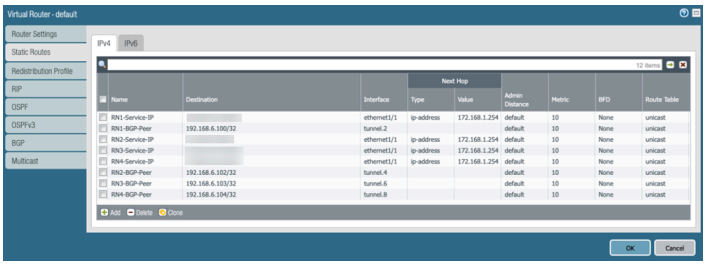
Wie bereits erwähnt, ist für diese Konfiguration dynamisches Routing mit BGP erforderlich. Um die BGP-Verbindung zwischen dem CPE und dem eBGP-Router von Prisma Access zu erleichtern, müssen Sie eine statische Route für die IP-Adresse des eBGP-Routers auf dem CPE hinzufügen. Der nächste Hop muss die Tunnelschnittstelle auf dem CPE sein. Sie

 ©2025 Palo Alto Networks, Inc.

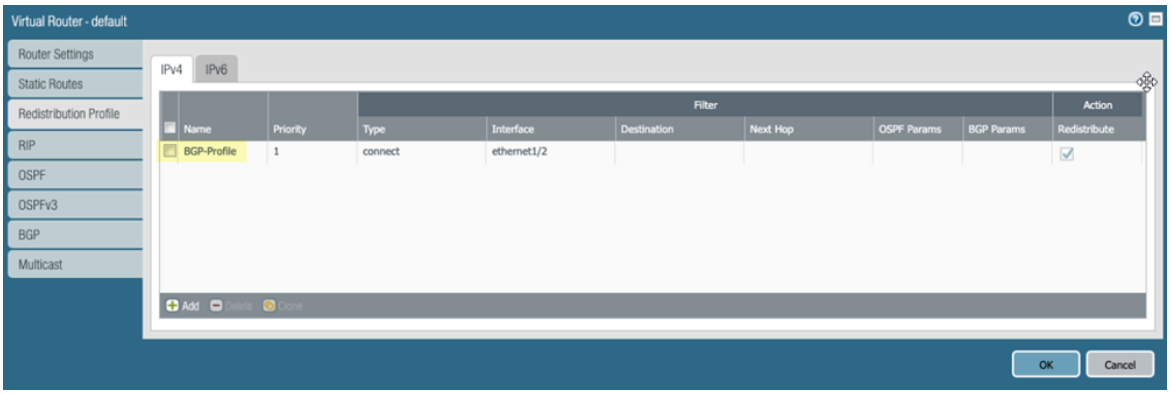
müssen diesen Schritt für alle anderen IP-Adressen des Remote-Netzwerk-EBGP-Routers auf verbleibenden Tunneln wiederholen.

Im folgenden Beispiel ist die Route auf dem aktiven CPE dargestellt. Wenn Sie Backup-Tunnel auf einem Standby-CPE erstellt haben, erstellen Sie dasselbe Routing auf dem Standby-CPE.

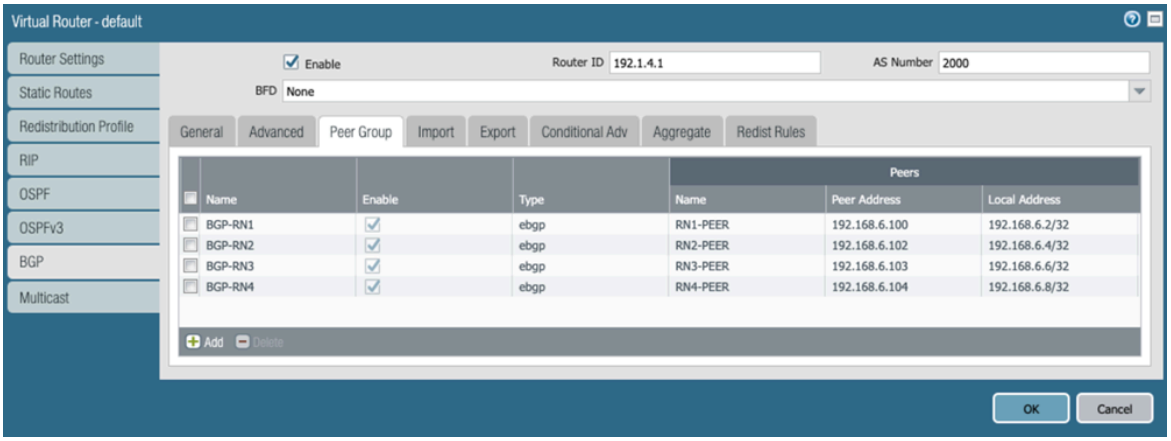
Wenn Sie eine Palo Alto Networks Firewall der nächsten Generation konfigurieren, wählen Sie **Statische Routen** > **IPv4** aus, um die statischen Routen hinzuzufügen.




**STEP 5 |** Aktivieren Sie die Routenumverteilung auf dem CPE, indem Sie **das Umverteilungsprofil** > **IPv4** auswählen und dann ein IPv4-Routenumverteilungsprofil **hinzufügen**.

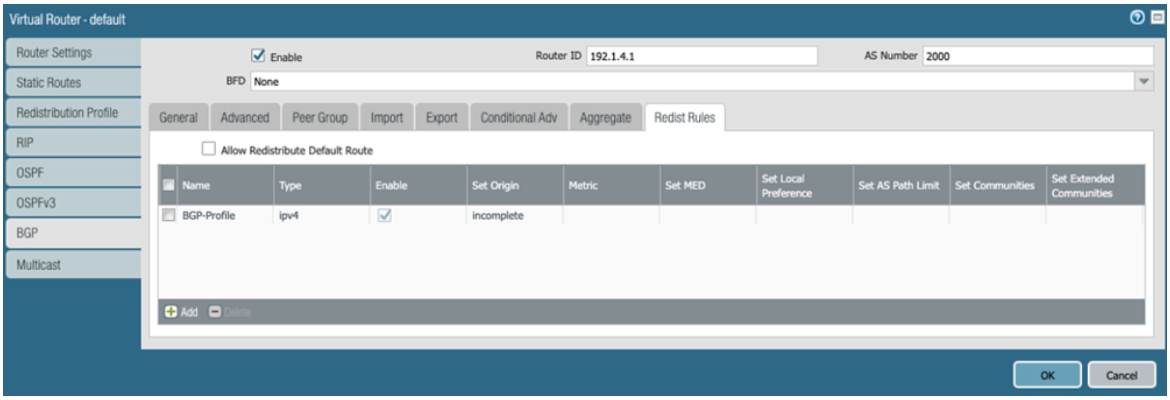



**STEP 6 |** Wählen Sie **BGP** > **Peer-Gruppe** aus und **aktivieren** Sie BGP auf der virtuellen Router-Instanz. Anschließend müssen Sie Remote-Netzwerk-BGP-Peers **hinzufügen**.




 ©2025 Palo Alto Networks, Inc.

**STEP 7 |** Wählen Sie **BGP** > **Regeln zum erneuten Verteilen** aus und hängen Sie anschließend das Routenumverteilungsprofil an, das Sie in einem vorherigen Schritt erstellt haben.

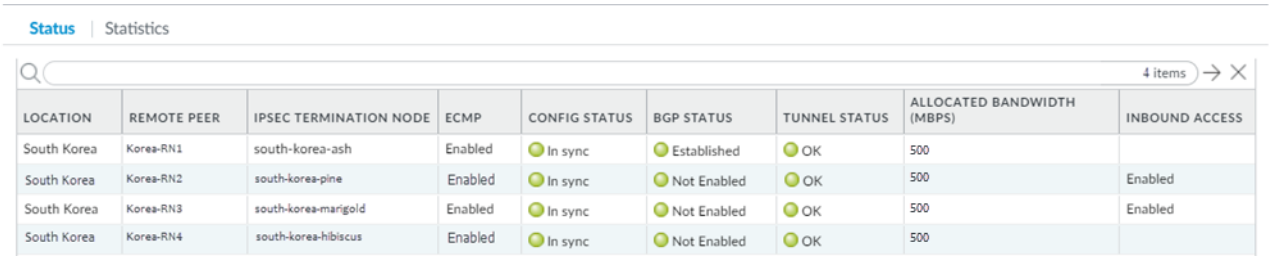



**STEP 8 |** Prüfen Sie, ob das CPE den Datenverkehr auf allen vier Tunneln weiterleitet.

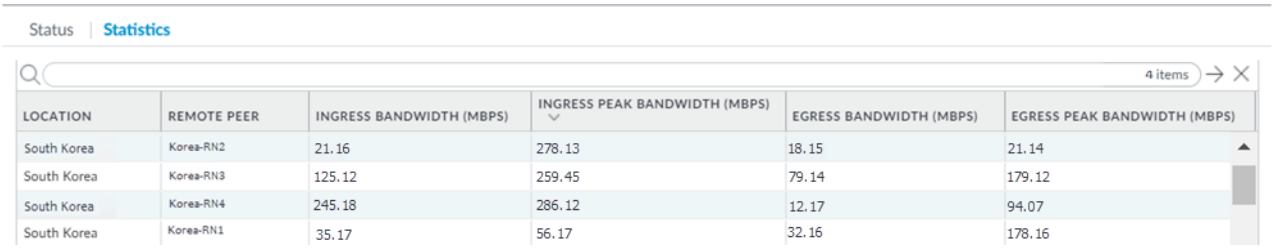
**STEP 9 |** Überprüfen Sie den Status der ECMP-fähigen Verbindungen von Prisma Access.

- Wählen Sie **Panorama** > **Cloud Services** > **Monitor** > **Remote-Netzwerke** und die Region aus, in der Sie die ECMP-Verbindungen bereitgestellt haben, und wählen Sie dann **Status** aus.

  - *In diesem Bereich wird für **ECMP Nein** angezeigt. Dies wird erwartet, weil Sie die Prisma Access-Funktion ECMP-Lastausgleich nicht konfigurieren.*
  - *ECMP ist vom CPE auf Prisma Access gerichtet und Prisma Access gewährleistet eine symmetrische Rückführung des Datenverkehrs vom CPE.*




- Wählen Sie **Statistiken** aus, um zu sehen, dass der Datenverkehr jeden Remote-Netzwerktunnel durchläuft.




Wenn Sie diesen Workflow abgeschlossen haben, liegt eine Konfiguration mit hoher Bandbreite für das Remote-Netzwerk vor. Beachten Sie, dass diese Lösung nur für ausgehenden Datenverkehr unterstützt wird.

 ©2025 Palo Alto Networks, Inc.

 ©2025 Palo Alto Networks, Inc.

# Prisma Access für Clean Pipe

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Verwenden Sie *Prisma Access für Clean Pipe*, um schnell und einfach mehrere Instanzen bereinigter ausgehender Internetverbindungen zu konfigurieren.

*Diese Funktion wird für Prisma Access (Managed by Strata Cloud Manager) nicht unterstützt.*

# Prisma Access für Clean Pipe – Übersicht

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Damit Organisationen, die die IT-Infrastruktur anderer Organisationen verwalten, wie z. B. Dienstleister, MSSPs oder Telcos, den ausgehenden Internetverkehr für ihre Mandanten schnell und einfach schützen können, bietet Palo Alto Networks Prisma Access für Clean Pipe. Ein Dienstleister, MSSP oder Telco kann seine Kunden (konfiguriert als Mandanten) über Partner Interconnect an Prisma Access für Clean Pipe weiterleiten. Nachdem der Datenverkehr über die Partner Interconnect-Verbindung übertragen wurde, wird er zur Sicherheit an eine für den Mandanten eingerichtete Instanz der Clean Pipe gesendet und dann ins Internet weitergeleitet.

Prisma Access für Clean Pipe bietet auch eine API, mit der Sie schnell und einfach Clean Pipes für Ihre Mandanten erstellen können.

## Clean Pipe-Anwendungsfälle

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Verwenden Sie Prisma Access für Clean Pipe, wenn alle folgenden Anwendungsfälle für Sie zutreffen:

- Sie verwalten eine Netzwerkbereitstellung mit einer großen Anzahl von Mandanten.

  Sie sind beispielsweise als Dienstanbieter, Telco oder MSSP tätig, der die Netzwerke vieler verschiedener Organisationen (bis zu mehreren Zehntausend) verwaltet und wartet.
- Sie möchten für jeden Mandanten in Ihrer Bereitstellung die Sicherheit des ausgehenden Internetverkehrs sicherstellen.
- Sie benötigen eine schnelle und skalierbare Möglichkeit, Clean Pipes für die Organisationen einzubinden, deren Netzwerke Sie verwalten.
- Mit Ausnahme der ausgehenden Internetsicherheit haben Sie keine zusätzlichen Anforderungen zum Schutz der mobilen Benutzer, der Zentrale oder der Niederlassungsstandorte der von Ihnen verwalteten Netzwerke.

  Wenn Sie zusätzliche Sicherheitsanforderungen haben, empfehlen wir Ihnen, in Prisma Access mehrere Mandanten zu erstellen, anstatt Clean Pipe zu implementieren. Dadurch haben Sie die Möglichkeit, Sicherheitsprofile für getrennte Gruppen von Remote-Netzwerken und mobilen Benutzern zu erstellen und durchzusetzen.

 ©2025 Palo Alto Networks, Inc.

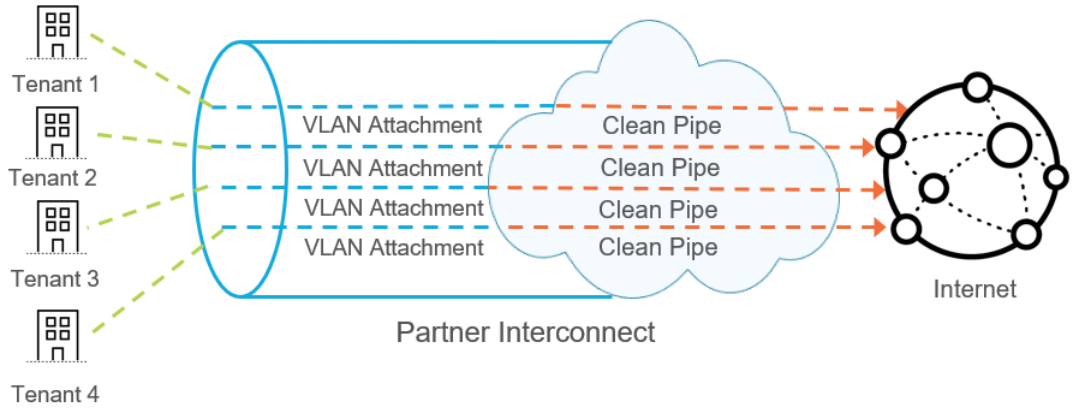
# Beispiele für Clean Pipe

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

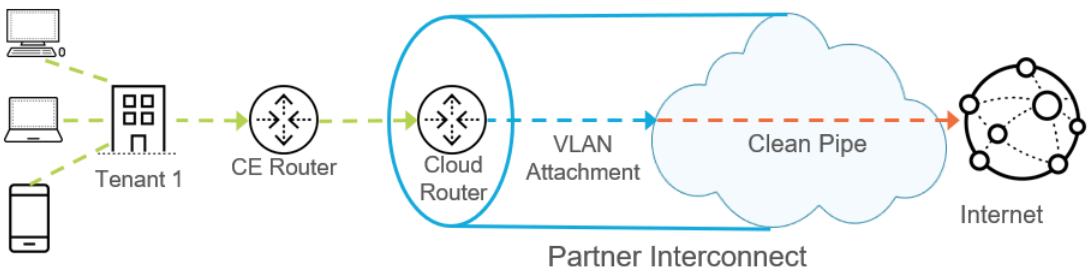
Die folgende Abbildung zeigt ein Beispiel für mehrere Clean Pipes, die für einen einzelnen Mandanten konfiguriert wurden, wobei für den Mandanten mehrere Clean Pipes vorhanden sind.

In diesem Beispiel verwaltet der Dienstanbieter die Internetkonnektivität für vier Organisationen und möchte für diese Organisationen den Ausgangsinternetzugang schützen. Der Dienstanbieter erstellt ein System mit Google Cloud Platform (GCP) Partner Interconnect und erstellt für jeden Mandanten einen VLAN-Anschluss. Der Dienstanbieter konfiguriert Prisma Access für Clean Pipe mithilfe von Panorama, um die Sicherheit des VLAN-Anschlusses zu gewährleisten.

Im Beispiel ist eine einzelne Clean Pipe pro Mandant dargestellt. Sie können auch mehrere Clean Pipes für einen einzelnen Mandanten erstellen. Vergewissern Sie sich, dass jede Clean Pipe, die Sie für einen Mandanten angeben, einen anderen Standort verwendet.




Die folgende Abbildung zeigt eine detaillierte Darstellung einer einzelnen Clean Pipe für einen Mandanten, der eine bereinigte Verbindung zum Internet erhalten möchte. Der CE-Router (Customer Edge) bietet WAN-Konnektivität für den Mandanten. Der CE-Router verbindet sich mit einem Cloud-Router und der Cloud-Router bietet Konnektivität für Partner Interconnect. Der Dienstanbieter erstellt einen VLAN-Anschluss für den Mandanten und konfiguriert Prisma Access für Clean Pipe in Panorama, um die Sicherheit für den VLAN-Anschluss zu gewährleisten, wodurch der internetbasierte Datenverkehr des Mandanten geschützt wird.




 ©2025 Palo Alto Networks, Inc.

# Clean Pipe- und Partner Interconnect-Anforderungen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama) | ❑ Prisma Access-Lizenz |

Bevor Sie beginnen, sollten Sie die folgenden Anforderungen an die Bereitstellung von Clean Pipe beachten und sich über die folgenden Unterschiede zwischen Prisma Access für Clean Pipe und anderen Prisma Access-Bereitstellungen informieren:

- Sie müssen über eine Prisma Access für Clean Pipe-Lizenz verfügen.

  Die Prisma Access für Clean Pipe-Lizenz unterscheidet sich von anderen Prisma Access-Produkten und ist eine separate Lizenz. Für Clean Pipe gelten jedoch die gleichen Anforderungen in Bezug auf den Kauf und die Installation von Panorama- und Strata Logging Service-Lizenzen.
- Prisma Access für Clean Pipe hat die folgenden GCP-Partner Interconnect-Anforderungen:
  - Sie müssen in der Lage sein, eine Partner Interconnect-Verbindung in GCP zu erstellen.
  - Sie müssen die Möglichkeit haben, VLAN-Verbindungen in GCP zu erstellen.
  - Für Layer-2(L2)-Partnerverbindungen müssen Sie Zugriff auf den CE-Router (Customer Edge) auf der MSSP-Seite haben und Konfigurationsänderungen an dieser Komponente vornehmen können.

  Weitere Informationen zur GCP-Konfiguration finden Sie in der GCP-Dokumentation.
- Beachten Sie für die Bereitstellung von Clean Pipe die Mindestanforderungen in Bezug auf die Bandbreite.

  Die Mindestlizenz, die Sie erwerben können, umfasst 1000 Mbit/s. Die Mindestbandbreitenzuweisung für jeden Clean Pipe-Mandanten beträgt 100 Mbit/s.

  Nachdem Sie einen Mandanten erstellt haben, können Sie in diesem Mandanten Clean Pipes erstellen. Jede Clean Pipe muss über eine Mindestkapazität von 100 Mbit/s verfügen. Jede Clean Pipe teilt die Zugriffsdomänen, Vorlagen, den Vorlagenstack und die Gerätegruppe des Mandanten.
- Wenn Sie mehrere Clean Pipes für einen einzelnen Mandanten konfigurieren, muss jede Clean Pipe ein eindeutiger Standort sein. Wenn Sie zwei VLAN-Anschlüsse für einen einzelnen Clean Pipe-Standort in einer Aktiv/Backup-Konfiguration für die Redundanz innerhalb der Zonen konfigurieren möchten, geben Sie die Option **REDUNDANT** an, wenn Sie eine neue Clean Pipe-Instanz hinzufügen.
- Wenn Sie eine Verbindung innerhalb eines Clean Pipe-Mandanten erstellen, passen Sie die Bandbreitenzuweisung an die des VLAN-Anschlusses an. Erstellen Sie keinen VLAN-Anschluss, dessen Bandbreite höher oder niedriger als die Bandbreite der Verbindung ist.
- Nachdem Sie die Unterstützung mehrerer Mandanten aktiviert haben, konfigurieren Sie Ihre Clean Pipe-Bereitstellung nicht über eine der anderen Registerkarten im Bereich „Konfiguration“. Eine Ausnahme bildet hierbei der Link **API-Schlüssel generieren** auf der Registerkarte **Diensteinrichtung**, über den Sie einen API-Schlüssel zum Abrufen von Clean Pipe-IP-Adressen generieren können. Alle Konfigurationen sind für Prisma Access für Clean

 ©2025 Palo Alto Networks, Inc.

Pipe eindeutig und arbeiten getrennt von anderen Prisma Access-Bereitstellungen wie beispielsweise Prisma Access für Netzwerke oder Prisma Access für Benutzer.

- Nach der Festschreibung (Commit) einer Clean Pipe-Konfiguration dürfen keine Änderungen mehr vorgenommen werden. Wenn Sie eine Clean Pipe nach dem Commit ändern, erhalten Sie einen Commit-Fehler, wenn Sie erneut eine Festschreibung durchführen. Löschen Sie stattdessen die vorhandene Clean Pipe und fügen Sie eine neue hinzu. Planen Sie diese Änderung während eines Systemausfallzeitfensters. Wenn Sie bereits Änderungen vorgenommen und noch nicht festgeschrieben haben, können Sie die Änderungen zurücksetzen, indem Sie für die Clean Pipe-Konfiguration wieder die vorherigen Werte einstellen.
- Beachten Sie, dass die von Clean Pipe verwendeten Standorte von denen anderer Prisma Access-Bereitstellungen abweichen. Prisma Access für Clean Pipe unterstützt die folgenden Standorte:
  - asia-east1
  - asia-east2
  - asia-northeast1
  - asia-south1
  - asia-southeast1
  - australia-southeast1
  - europe-north1
  - europe-west2
  - europe-west3
  - europe-west4
  - northamerica-northeast1
  - southamerica-east1
  - us-central1
  - us-east1
  - us-east4
  - us-west1
  - us-west2
- Beachten Sie die folgenden Netzwerkbeschränkungen für Clean Pipe:
  - QoS für Clean Pipe wird nur beim Eingang (in der Richtung aus dem Internet zu Clean Pipe) unterstützt.
  - User-ID (Benutzeridentifikation) wird nicht unterstützt.
  - Clean Pipe unterstützt die Sitzungsaffinität basierend auf Quell- und Ziel-IP-Adressen und ist nicht konfigurierbar.
  - Trust-to-Trust-Richtlinien sind für Clean Pipe ungültig, da der Datenverkehr immer internetgebunden ist. Verwenden Sie ausschließlich Trust-to-Untrust-Richtlinien.

 ©2025 Palo Alto Networks, Inc.

# Clean Pipe-Konfiguration abschließen

| Wo kann ich das verwenden? | Was brauche ich? |
|---|---|
| • Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

Um die Konfiguration von Prisma Access for Clean Pipe abzuschließen, führen Sie die Konfiguration in Partner Interconnect und in Panorama durch.

*Vergewissern Sie sich, dass Sie auf der Partner Interconnect-Seite (ohne Prisma Access) auf die CE- und Cloud-Router zugreifen und diese konfigurieren können.*

**STEP 1 |** Erstellen Sie auf der Partner Interconnect-Seite der Konfiguration einen VLAN-Anschluss mithilfe des **Kopplungsschlüssels**, den Sie von Panorama abgerufen haben.

Weitere Informationen zum Erstellen von VLAN-Anschlüssen mit Partner Interconnect und zum Konfigurieren von CE-Routern (Customer Edge) für die Kommunikation mit Cloud-Routern finden Sie in der Google-Cloud-Dokumentation unter https://cloud.google.com/interconnect/docs/

Stellen Sie sicher, dass der von Ihnen gewählte Standort und die ausgewählte Bandbreite mit dem **Standort** übereinstimmen, den Sie in Panorama angegeben haben. Der Dienstanbieter, den Sie für Partner Interconnect verwenden, benutzt den Kopplungsschlüssel zusammen mit Ihrem angeforderten Verbindungsstandort und der Kapazität, um die Konfiguration Ihres VLAN-Anschlusses abzuschließen.

**STEP 2 |** Nachdem die Verbindung hergestellt wurde, kehren Sie zu Panorama zurück, wählen Sie **Panorama** > **Cloud Services** > **Status** > **Netzwerkdetails** > **Clean Pipe** aus und notieren Sie sich die **MSSP CE**- und die **Cloud-Router-IP-Adressen**.

Diese Werte werden ausgefüllt, nachdem Sie den **Kopplungsschlüssel** auf der anderen Seite des VLAN-Anschlusses eingegeben haben.




**STEP 3 |** Melden Sie sich beim CE-Router an und führen Sie die folgende Konfiguration durch.

1. Geben Sie die **MSSP CE**-Adresse als lokale IP-Adresse ein.
2. Geben Sie die **Cloud-Router-IP**-Adresse als Peer-IP-Adresse ein.
3. Geben Sie eine BGP-ASN ein, die der **BGP-Peer-ASN** entspricht, die Sie bei der Konfiguration von Clean Pipe in Panorama eingegeben haben.

   Vergewissern Sie sich, dass Sie diese Werte korrekt eingegeben haben; Sie können sie nicht ändern.


©2025 Palo Alto Networks, Inc.

**STEP 4 |** Überprüfen Sie den Clean Pipe-Status.

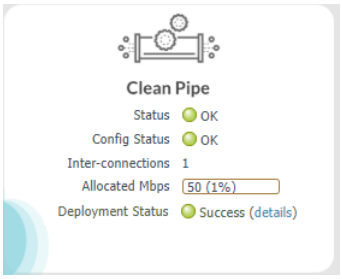
1. Wählen Sie in Panorama **Panorama** > **Cloud Services** > **Status** aus und dann in der Dropdown-Liste einen Wert für **Mandant** und überprüfen Sie anschließend den **Status** von Clean Pipe.

   Zulässige Werte finden Sie in der Liste der Prisma Access-Standorte.

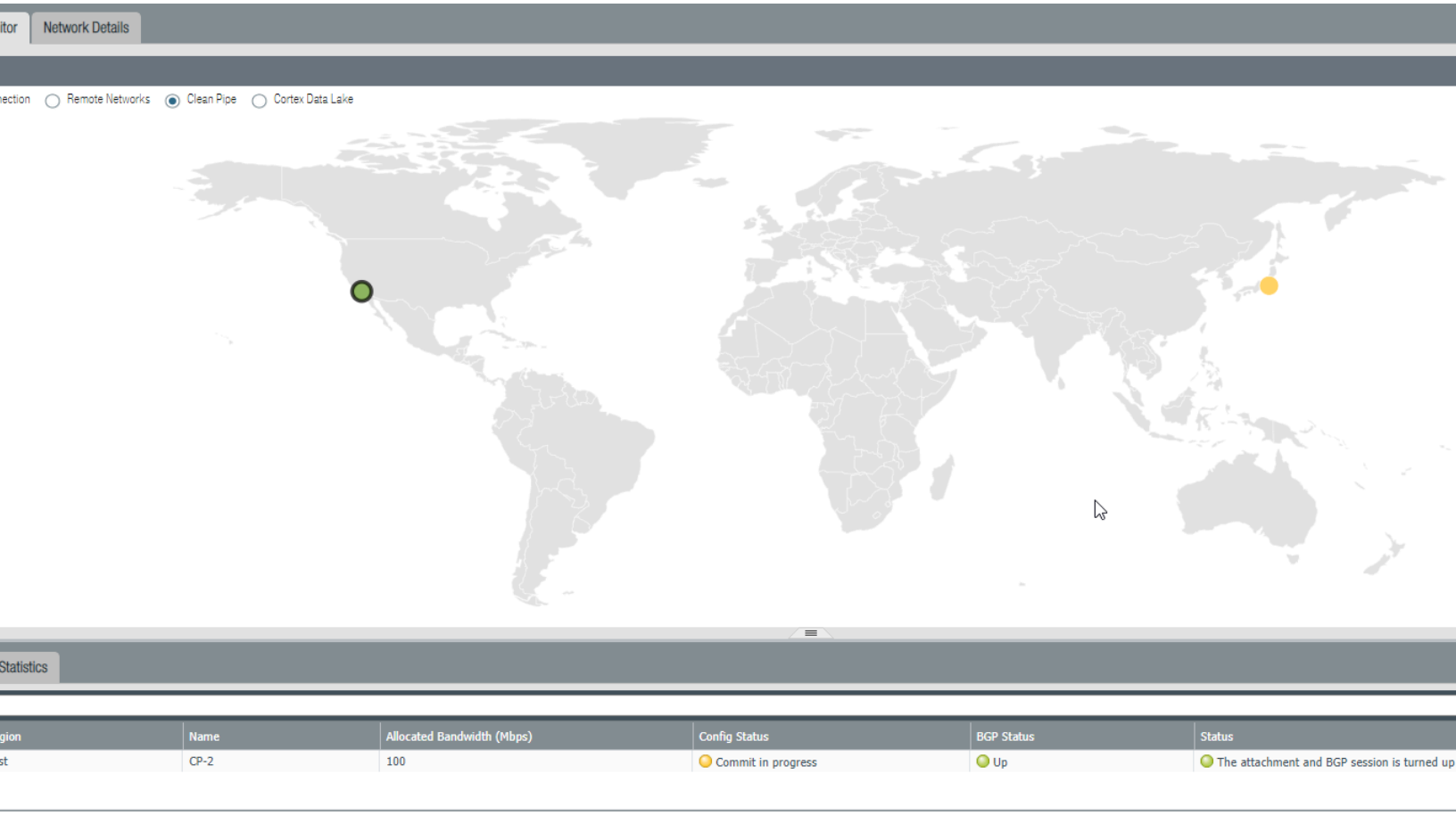
   Im Bereich **Bereitstellungsstatus** können Sie den Fortschritt der Onboarding- und Bereitstellungsaufträgen verfolgen, bevor sie abgeschlossen sind. Außerdem erhalten Sie

 ©2025 Palo Alto Networks, Inc.

weitere Informationen zum Status abgeschlossener Jobs. Einzelheiten finden Sie unter Fortschritt und Status der Bereitstellung.




2. Wählen Sie **Panorama** > **Cloud Services** > **Status** > **Clean Pipe** aus und klicken Sie dann auf die Registerkarte **Überwachen**, um eine Karte mit dem Status der bereitgestellten Clean Pipes anzuzeigen.




Klicken Sie auf die Registerkarten unter der Karte, um zusätzliche Statistiken für die Clean Pipes anzuzeigen.

Registerkarte **Status**:

- **Rechenregion** – Die Rechenregion, in der Ihre Cloud-Service-Infrastruktur für die Clean Pipe-Instanz bereitgestellt wird.
- **Name** – Der Name der Clean Pipe-Instanz.
- **Zugewiesene Bandbreite (Mbit/s)** – Die Bandbreite, die Sie der Clean Pipe-Instanz zugewiesen haben.

 ©2025 Palo Alto Networks, Inc.

- **Konfigurationsstatus** – Der Status Ihrer letzten Übertragungsaktion für die Konfiguration an den Dienst. Wenn Sie lokal eine Änderung vorgenommen und die Konfiguration noch nicht in die Cloud übertragen haben, lautet der Status **Nicht synchron**. Bewegen Sie den Mauszeiger über die Statusanzeige, um detailliertere Informationen zu erhalten. Nachdem Sie die Konfiguration mit „Commit und Push“ festgeschrieben und an Prisma Access übertragen haben, ändert sich der Konfigurationsstatus in **Synchron**.
- **BGP-Status** – Zeigt Informationen über den BGP-Status zwischen der Firewall oder dem Router in der Clean Pipe-Instanz und in Prisma Access an. Obwohl der Status beim Durchlaufen der verschiedenen BGP-Status nur kurz angezeigt wird (**Inaktiv**, **Aktiv**, **Offen Senden**, **Offen Anstehend**, **Offen Bestätigen**), wird der BGP-Status meist angezeigt:
  - **Verbinden** – Der Router an der Clean Pipe-Instanz versucht, die BGP-Peer-Beziehung zur Cloud-Firewall herzustellen.
  - **Eingerichtet** – Die BGP-Peer-Beziehung wurde eingerichtet.

    In diesem Feld wird auch angezeigt, ob sich die BGP-Verbindung in einem Fehlerzustand befindet:
  - **Warnung** – Seit mehr als acht Minuten wurde der BGP-Status nicht aktualisiert. Dies kann auf einen Ausfall der Firewall hindeuten.

 ©2025 Palo Alto Networks, Inc.

  - **Fehler** – Der BGP-Status ist unbekannt.
- **Status** – Der Betriebsstatus der Verbindung zwischen Prisma Access und der Clean Pipe-Instanz.

Registerkarte **Statistiken**:

- **Region** – Die Region, in der Ihre Cloud-Service-Infrastruktur für die Clean Pipe-Instanz bereitgestellt wird.
- **Name** – Der Name der Clean Pipe-Instanz.
- **Zugewiesene Bandbreite (Mbit/s)** – Die Bandbreite, die Sie dem Standort des Remote-Netzwerks zugewiesen haben.
- **QoS** – Wählen Sie **QoS** aus, um eine Seite mit grafischen QoS-Statistiken anzuzeigen.
- **Durchschnittliche Bandbreite für ausgehenden Datenverkehr 5 Minuten (Mbit/s)** – Die durchschnittliche Bandbreite von Clean Pipe für ausgehenden Datenverkehr im Durchschnitt über 5 Minuten.
- **Durchschnittliche Bandbreite für ausgehenden Datenverkehr 60 Minuten (Mbit/s)** – Die durchschnittliche Bandbreite von Clean Pipe für ausgehenden Datenverkehr im Durchschnitt über 60 Minuten.
- **Durchschnittliche Bandbreite für eingehenden Datenverkehr 5 Minuten (Mbit/s)** – Die durchschnittliche Bandbreite von Clean Pipe für eingehenden Datenverkehr im Durchschnitt über 5 Minuten.
- **Durchschnittliche Bandbreite für eingehenden Datenverkehr 60 Minuten (Mbit/s)** – Die durchschnittliche Bandbreite von Clean Pipe für eingehenden Datenverkehr im Durchschnitt über 60 Minuten.
- **Spitzenausgangsbandbreite 1 Stunde (Mbit/s)** – Die Höhe der Spitzenausgangsbandbreite für die Clean Pipe-Instanz in der letzten 1 Stunde.
- **Spitzenausgangsbandbreite 24 Stunden (Mbit/s)** – Die Höhe der Spitzenausgangsbandbreite für die Clean Pipe-Instanz in den letzten 24 Stunden.
- **Spitzenausgangsbandbreite 7 Tage (Mbit/s)** – Die Höhe der Spitzenausgangsbandbreite für die Clean Pipe-Instanz in den letzten 7 Tagen.
- **Spitzenausgangsbandbreite 30 Tage (Mbit/s)** – Die Höhe der Spitzenausgangsbandbreite für die Clean Pipe-Instanz in den letzten 30 Tagen.
- **Spitzeneingangsbandbreite 1 Stunde (Mbit/s)** – Die Höhe der Spitzeneingangsbandbreite für die Clean Pipe-Instanz in der letzten 1 Stunde.
- **Spitzeneingangsbandbreite 24 Stunden (Mbit/s)** – Die Höhe der Spitzeneingangsbandbreite für die Clean Pipe-Instanz in den letzten 24 Stunden.
- **Spitzeneingangsbandbreite 7 Tage (Mbit/s)** – Die Höhe der Spitzeneingangsbandbreite für die Clean Pipe-Instanz in den letzten 7 Tagen.
- **Spitzeneingangsbandbreite 30 Tage (Mbit/s)** – Die Höhe der Spitzeneingangsbandbreite für die Clean Pipe-Instanz in den letzten 30 Tagen.

 ©2025 Palo Alto Networks, Inc.

# Mehrmandantenfähigkeit aktivieren und einen Mandanten erstellen

| Wo kann ich das verwenden? | Was brauche ich? |
| --- | --- |
| • Prisma Access (Managed by Panorama) | • Prisma Access-Lizenz |

Für die Clean Pipe-Konfiguration erstellen Sie in Panorama eine Mehrmandantenbereitstellung und dann einen oder mehrere Mandanten.

**STEP 1 |** Installieren und aktivieren Sie Prisma Access für Clean Pipe.

Prisma Access für Clean Pipe erfordert eine separate Lizenz. Durch die Aktivierung werden Clean Pipe-spezifische Registerkarten im Cloud-Services-Plug-in erstellt. Das Verfahren zum Installieren von Prisma Access für Clean Pipe ist dasselbe wie das Verfahren zum Aktivieren und Installieren einer Prisma Access-Lizenz, einschließlich der Installation des Cloud-Services-Plug-ins.

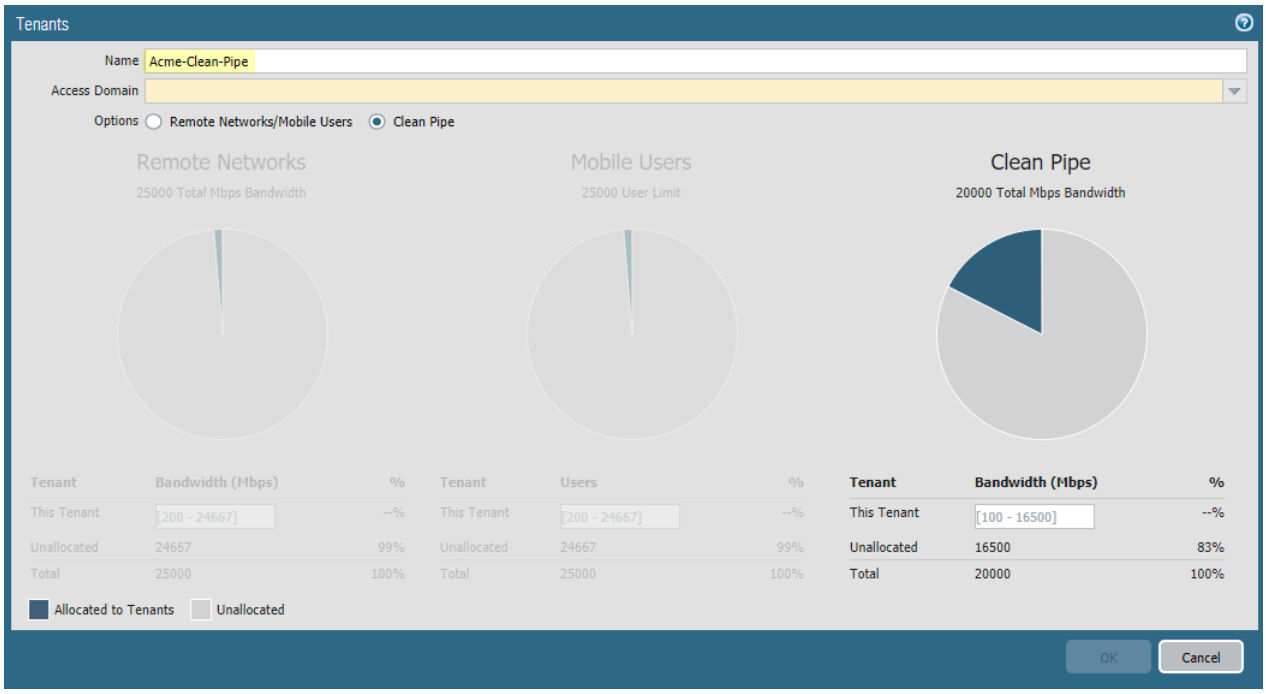
 ©2025 Palo Alto Networks, Inc.

**STEP 2 |** Aktivieren Sie Mehrmandantenfähigkeit, falls Sie dies noch nicht getan haben.

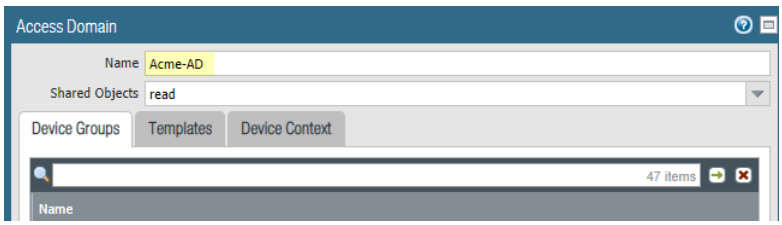
1. Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** aus.
2. Wählen Sie **Mehrmandantenfähigkeit aktivieren** aus (oben rechts auf der Seite).
3. Klicken Sie auf **OK**.

   Die Seite **Mandanten** wird angezeigt.
4. Wählen Sie im Bereich **Optionen** die Option **Clean Pipe** aus.

   Informationen zum Konfigurieren eines Mandanten für Remote-Netzwerke, mobile Benutzer oder beides finden Sie unter „Mehrere Mandanten in Prisma Access verwalten“.




5. Geben Sie einen **Namen** für den ersten Mandanten ein.
6. Erstellen und konfigurieren Sie eine neue **Zugriffsdomäne** für den ersten Mandanten und klicken Sie auf **OK**.




7. Geben Sie im Bereich **Clean Pipe** eine **Bandbreite (Mbit/s)** für **diesen Mandanten** ein.

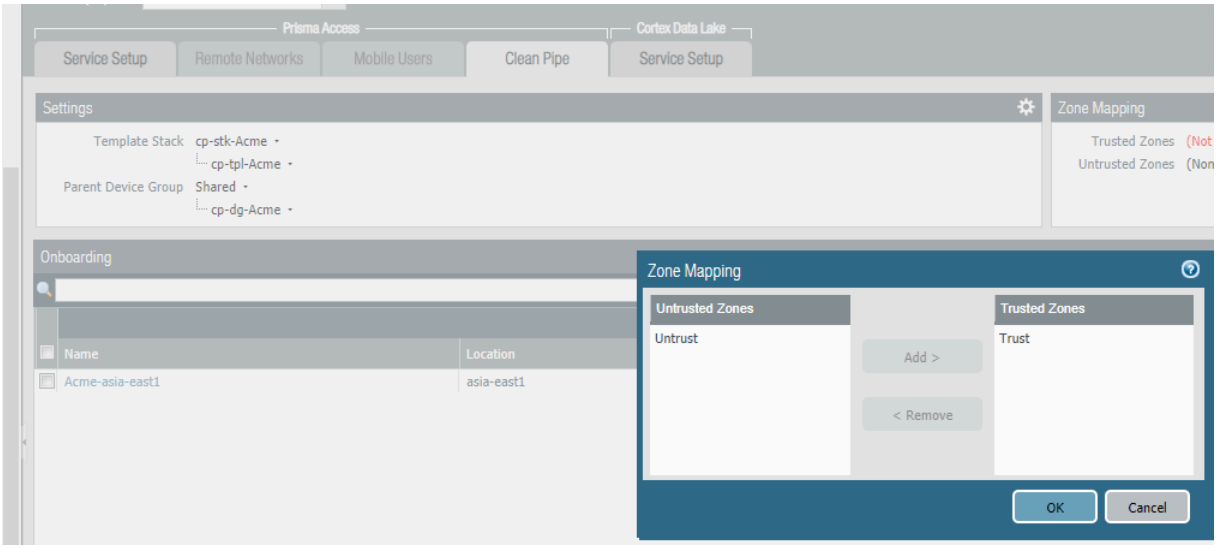
   Geben Sie mindestens 100 Mbit/s für jeden Mandanten ein, den Sie erstellen.
8. Klicken Sie auf **OK**.

 ©2025 Palo Alto Networks, Inc.

**STEP 3 |** Erstellen Sie Zonen für den Mandanten und ordnen Sie diese Zonen dem Mandanten zu.

1. Wählen Sie **Netzwerk** > **Zonen** aus.

   Stellen Sie sicher, dass Sie die Clean Pipe-**Vorlage** für den von Ihnen erstellten Mandanten (**cp-tpl-***tenant*) ausgewählt haben.
2. Erstellen Sie Zonen für den Mandanten (z. B. **Vertrauenswürdig** und **Nicht vertrauenswürdig**).
3. Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** und dann den **Mandanten** aus der Dropdownliste aus.
4. Wählen Sie die Registerkarte **Clean Pipe** aus.
5. Klicken Sie auf das Zahnradsymbol neben **Zonenzuordnung**, um die Einstellungen zu bearbeiten.
6. **Fügen** Sie Zonen hinzu und **entfernen** Sie Zonen, die Sie erstellt haben, um sie vertrauenswürdigen und nicht vertrauenswürdigen Zonen zuzuordnen.




**STEP 4 |** Binden Sie eine neue Clean Pipe-Instanz ein.

1. Wählen Sie **Panorama** > **Cloud Services** > **Konfiguration** > **Clean Pipe** aus.
2. **Fügen** Sie eine neue Clean Pipe-Instanz für den Mandanten hinzu und geben Sie folgende Informationen ein:

   - **Name** – Geben Sie einen Namen für die Clean Pipe-Instanz an.
   - **Bandbreite** – Wählen Sie die Bandbreite aus, die der Clean Pipe-Instanz zugewiesen werden soll.

     Sie können Clean Pipe-Instanzen in Schritten von 100 Mbit/s, 200 Mbit/s, 300 Mbit/s, 400 Mbit/s, 500 Mbit/s, 1.000 Mbit/s, 2.000 Mbit/s, 5.000 Mbit/s und 10.000 Mbit/s einbinden. Die von Ihnen angegebene Bandbreite muss innerhalb der

 ©2025 Palo Alto Networks, Inc.

lizenzierten Bandbreitenzuweisung liegen und mit der Bandbreite der VLAN-Anlage übereinstimmen, die Sie in Partner Interconnect erstellen.

- **Edge-Verfügbarkeitsdomäne** – Wählen Sie die gewünschte Verfügbarkeitsdomäne für die Clean Pipe-Instanz aus. Sie können **1**, **2**, **BELIEBIG** oder **REDUNDANT** auswählen.
  - Geben Sie **BELIEBIG** für eine nicht redundante Clean Pipe-Bereitstellung an.

    Stellen Sie sicher, dass Ihr Cloud-Anbieter diese Wahl unterstützt. Sie müssen **BELIEBIG** auch auf der Cloud-Anbieterseite der Partnerverbindung auswählen. Wenn diese Option für Ihren Cloud-Anbieter nicht verfügbar ist, treffen Sie eine andere Wahl.
  - Um zwei VLAN-Anschlüsse am selben Standort in einer Active/Backup-Konfiguration am selben Standort anzugeben, wählen Sie **REDUNDANT** aus.

    Prisma Access erstellt zwei Kopplungsschlüssel für eine **REDUNDANT**-Konfiguration (einen für jede Verfügbarkeitszone) und fügt den Namen der Clean Pipe-Instanz mit `zone1` für die erste Verfügbarkeitszone und `zone2` für die zweite Verfügbarkeitszone an. Wenn Sie als **Name** z. B. **San Francisco** angeben, erstellt Prisma Access zwei Zonen mit den Namen **San Francisco-zone1** und **San Francisco-zone2**.

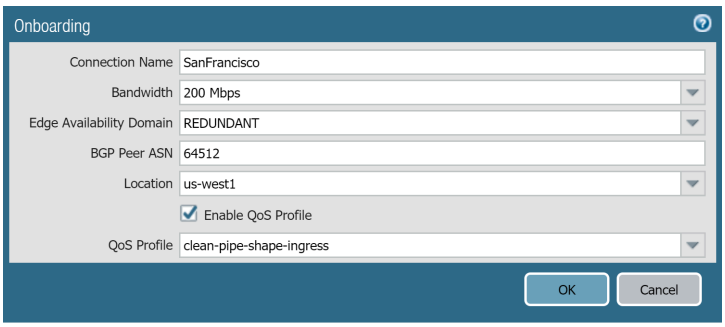
    *Stellen Sie sicher, dass Sie die erste Verfügbarkeitszone (zone1) als primäre Zone auf Ihrem CPE konfigurieren.*

  Sie können auch ein Paar von Clean Pipe-Instanzen für eine Redundanz eines einzelnen Mandanten an verschiedenen Standorten erstellen. Geben Sie dazu **1** für die erste Clean Pipe-Instanz an einem Standort und **2** für die zweite Clean Pipe-Instanz an einem anderen Standort an.
- **BGP-Peer-ASN** – Geben Sie die autonome Systemnummer (ASN) von BGP ein.

  Sie können entweder eine private oder öffentliche BGP-ASN angeben.

  Notieren Sie sich diesen Wert. Sie konfigurieren ihn auf dem CE-Router (Customer Edge), wenn Sie die Clean Pipe-Konfiguration abgeschlossen haben.
- **Standort** – Wählen Sie den Standort aus.

  Wir empfehlen Ihnen, den gleichen Standort zu verwenden, den Sie beim Erstellen des VLAN-Anschlusses für die Partnerverbindung verwenden.
- Um QoS zu aktivieren, wählen Sie **QoS** und dann das QoS-Profil aus, das mit der Clean Pipe-Instanz verwendet werden soll. Clean Pipe-QoS-Formen beim Eingang.



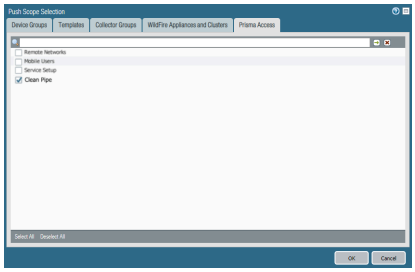

 ©2025 Palo Alto Networks, Inc.

**STEP 5 |** Fügen Sie nach Bedarf weitere Clean Pipe-Instanzen hinzu, indem Sie Schritt 4 wiederholen.

Achten Sie darauf, dass jede weitere Clean Pipe-Instanz einen anderen Standort verwendet.

**STEP 6 |** Führen Sie die Aktion „Commit und Push“ aus, um Ihre Änderungen festzuschreiben und zu übertragen und sie so in Prisma Access zu aktivieren.

1. Wählen Sie **Commit** > **Commit und Push** und **Auswahl bearbeiten** im Übertragungsumfang aus.
2. Wählen Sie **Prisma Access** und dann **Clean Pipe** aus.



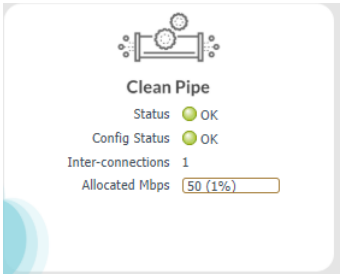
3. Klicken Sie auf **OK**, um Ihre Änderungen im Übertragungsumfang zu speichern.
4. Führen Sie einen **Commit** aus und übertragen Sie die Änderung per **Push**.

**STEP 7 |** Überprüfen Sie, ob Ihre Clean Pipe-Instanz bereitgestellt wurde.

1. Wählen Sie **Panorama** > **Cloud Services** > **Status** aus.
2. Wählen Sie den **Mandanten** aus der Dropdown-Liste oben auf der Seite aus.
3. Klicken Sie auf **Status**.

   Der Clean Pipe-Status wird angezeigt.
4. Bewegen Sie den Mauszeiger über den **Konfigurationsstatus** für die Clean Pipe-Instanz und warten Sie, bis der Status von **Bereitstellung in Bearbeitung** auf **Bereitgestellt** wechselt.

   Diese Bereitstellung kann bis zu 30 Minuten dauern.




**STEP 8 |** Klicken Sie auf die Registerkarte **Netzwerkdetails**, klicken Sie auf das Optionsfeld **Clean Pipe** und notieren Sie sich den **Kopplungsschlüssel**.

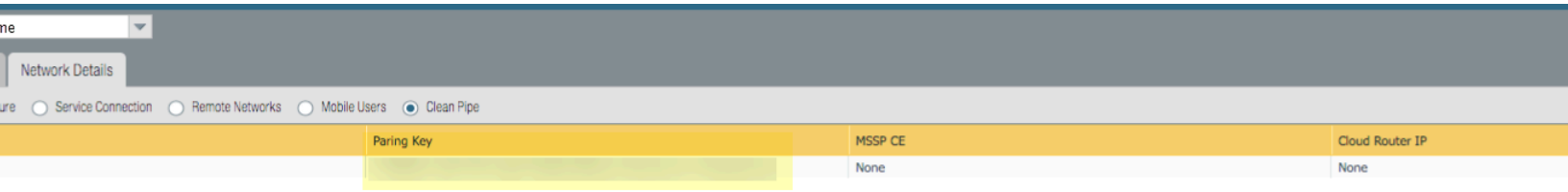
Die Felder **MSSP-CE** und **Cloud-Router-IP** sind leer, wenn Sie mit der Konfiguration der Clean Pipe-Instanz beginnen. Diese Felder werden ausgefüllt, nachdem Sie den VLAN-Anschluss erstellt haben, wenn Sie die Clean Pipe-Konfiguration abgeschlossen haben.

Wenn Sie eine **REDUNDANTE** Verbindung angegeben haben, erstellt Prisma Access zwei Kopplungsschlüssel, einen für jede Verfügbarkeitszone, und hängt den Namen der Clean Pipe-Verbindung mit `zone1` für die erste Verfügbarkeitszone und `zone2` für die zweite

 ©2025 Palo Alto Networks, Inc.

Verfügbarkeitszone an. Der folgende Screenshot zeigt die Clean Pipe-Instanz **SanFrancisco** mit redundanter Konfiguration. Prisma Access hat zwei Kopplungsschlüssel erstellt, einen für **SanFrancisco-zone1** und einen für **SanFrancisco-zone2**.

*Stellen Sie sicher, dass Sie die erste Verfügbarkeitszone (zone1) als primäre Zone auf Ihrem CPE konfigurieren.*




**STEP 9 |** Schließen Sie die Clean Pipe-Konfiguration ab.

 ©2025 Palo Alto Networks, Inc.