paloalto TECHDOCS

Prisma Access 管理

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 23, 2025

Table of Contents

Prisma Access 概述 13

使用 Prisma Access 确保互联网流量的安全 16

网络安全的重要性 16

Prisma Access 云安全 Web 网关 (SWG) 16

使用 Prisma Access 保护用户和终端 16

如何管理 Prisma Access 18

通过 Strata Cloud Manager 实现对 Prisma Access 的可见性和监控 22

Prisma Access 位置 24

计算位置、城市和国家/地区 25

大区和位置组 30

按地区划分的位置 34

显式代理位置 39

Colo-Connect 位置 40

支持的 Strata Logging Service 区域 41

远程网络—高性能、流量复制和安全入站访问位置 42

Prisma Access China 位置 45

FedRAMP 中等和高等位置 45

北美地区地图 45

本地区域位置 46

Prisma Access 及相关服务处理位置 47

Prisma Access 基础设施管理 49

Prisma Access API 51

适用于 Prisma Access (Managed by Strata Cloud Manager) 的 API 51

适用于 Prisma Access (Managed by Panorama) 的 API 51

使用浏览器和 Web 界面访问 Prisma Access (Managed by Panorama) API 51

使用 curl 命令检索 Panorama 托管 API 命令 53

将 CLI 命令用于 Prisma Access (Managed by Panorama) 54

Prisma Access Insights APIs 54

将 Prisma Access 从 Panorama 迁移到 Strata Cloud Manager 56

准备迁移到 Prisma Access (Managed by Strata Cloud Manager) 56

将 Prisma Access (Managed by Panorama) 部署迁移到 Strata Cloud Manager 57

Prisma Access 版本和升级 69

Prisma Access 版本类型 70

紧急计划升级 71

Prisma Access 升级类型 72

 ©2025 Palo Alto Networks, Inc.

Prisma Access 的软件和内容更新频率 74
Prisma Access 数据平面升级 79
获取升级提醒和更新 84
查看 Prisma Access 软件版本 89
Prisma Access (Managed by Strata Cloud Manager) 89
Prisma Access (Managed by Panorama) 90
Prisma Access 设置 95
设置 Prisma Access 97
配置 Prisma Access 服务基础架构 104
移动用户：IP 地址分配 117
示例：公共 IP 地址扩展示例（移动用户） 117
回环 IP 地址分配（移动用户） 120
远程网络：IPSec 终止节点和服务 IP 地址 123
远程网络：与带宽分配相关的 IP 地址变化 124
远程网络： IP 地址和传出 IP 地址分配 127
检索 Prisma Access 的 IP 地址 128
针对“移动用户—GlobalProtect”部署部署的 IP 优化 150
检索 Prisma Access IP 地址的 API 示例 152
在 Prisma Access IP 地址更改时收到通知 154
使用旧脚本检索 IP 地址 156
检索移动用户 IP 地址 158
检索公共、环回和传出 IP 地址 159
Prisma Access 区域 162
Prisma Access 的 DNS 164
Prisma Access 的高可用性 170
预定义模板：接入服务连接或远程网络 173
常见 SD-WAN 设备支持的 IKE 和 IPSec 加密配置文件 178
Prisma Access 服务连接 181
规划服务连接。 183
收集总部或数据中心信息 183
配置 Prisma Access 中的服务连接 185
使用服务连接实现移动用户和远程网络之间的访问 211
服务连接的动态路由注意事项 213
工作原理 — 路由服务连接流量 213
Prisma Access 默认路由 213
热土豆路由 216
Prisma Access ZTNA 连接器 221

©2025 Palo Alto Networks, Inc.

ZTNA 连接器组件 222
ZTNA 连接器用例 223
服务连接和 ZTNA 连接器的支持用例 227
ZTNA 连接器 2.0 原则 228
ZTNA 连接器要求和指南 229
支持的 Prisma Access 版本和要求 229
应用程序支持 229
特性和功能限制 230
扩缩和吞吐量注意事项 231
支持的应用程序托管环境 231
网络要求 232
允许 ZTNA 连接器使用的 IP 地址和 FQDN 234
证书管理 237
启用 ZTNA 连接器 238
配置 ZTNA 连接器 244
升级 ZTNA 连接器 253
ZTNA 连接器诊断工具 256
删除连接器 IP 块 263
使用 Cloud Identity Engine 设置应用程序的自动发现 268
私有应用程序目标发现 269
启用 ZTNA 连接器的应用程序的安全策略 276
在您的数据中心内接入 ZTNA Connector 虚拟机 292
支持的 ZTNA 连接器部署 292
ZTNA 连接器支持的 Microsoft Azure 部署 294
ZTNA 连接器支持的 Google Cloud Platform 部署 310
ZTNA 连接器支持的 Amazon Web Services 部署 320
Prisma Access ZTNA 连接器支持的 VMware ESXi 部署 326
Prisma Access ZTNA 连接器支持的 KVM 部署 337
Prisma Access ZTNA 连接器支持的 Hyper-V 部署 342
监控 ZTNA 连接器 355
查看 ZTNA 连接器日志 358
保留使用源 NAT 的 ZTNA 连接器连接的 User-ID 映射 361
配置动态特权访问设置 371
什么是动态特权访问？ 372
通过 Common Services 为 Prisma Access 启用动态权限访问 373
在 Cloud Identity Engine 中授权用户组映射进行动态特权访问 375
启用访问客户端。 383
为动态权限访问设置代理基础设施 385

 ©2025 Palo Alto Networks, Inc.

配置基础架构设置 385
选择 Prisma Access 地点 386
为动态权限访问启用 SC-NAT 支持 390
为动态特权访问启用路由汇总 391
创建代码段 393
配置项目特定的 Prisma Access Agent 设置 403
配置转发配置文件以管理动态特权访问代理的代理流量 403
为动态特权访问配置 Prisma Access Agent 应用程序设置 417
为动态特权访问配置 DNS 设置 423
为动态特权访问配置 HIP 数据收集设置 424
创建项目 429
动态特权访问的流量控制 432
为动态特权访问设置 Prisma Access Agent 434
为 Prisma Access Agent 配置分阶段推出 434
配置 Prisma Access Agents 的常规全局设置 442
为动态特权访问 Prisma Access Agent 配置 HIP 通知 445
推送 Prisma Access Agent 配置 455
下载启用动态权限访问的 Prisma Access Agent 软件包 458
使用 Prisma Access Agent 访问您的项目 460
安装 Prisma Access Agent 460
登录到已启用动态特权访问的 Prisma Access Agent 468
更改启用动态特权访问的 Prisma Access Agent 的首选项 473
将启用动态特权访问的 Prisma Access Agent 连接到不同的地点 475
切换到不同的项目 476
将启用动态特权访问的 Prisma Access Agent 连接到不同的服务器 478
在 GlobalProtect 应用程序和 Prisma Access Agent 之间切换 480
查看和监控动态权限访问用户 486
已连接用户 486
查看和监控动态权限访问项目 491
项目 491

Prisma Access Colo-Connect 495

Colo-Connect 用例 497
对私有应用程序的高带宽访问 497
私有应用程序的专用连接 497
使用第三方 NaaS 提供商 497
Colo-Connect 与服务连接和 ZTNA 连接器有何不同？ 498
Colo-Connect 不支持的特性和功能 499
Prisma Access Colo-Connect 的要求和先决条件 500

 ©2025 Palo Alto Networks, Inc.

配置 Prisma Access Colo-Connect 502

Prisma Access 中的 App Acceleration 553

App Acceleration 要求和准则 555
配置 App Acceleration 558

Prisma Access 移动用户 581

移动用户：GlobalProtect 583
Prisma Access 上的 GlobalProtect 规划清单 583
设置“GlobalProtect—移动用户” 586
GlobalProtect—自定义隧道设置 619
GlobalProtect—自定义应用程序设置 624
禁用 GlobalProtect 的工单请求 632
GlobalProtect 预登录 637
GlobalProtect — 无客户端 VPN 652
监控 GlobalProtect 移动用户 654
GlobalProtect 移动用户部署的 IP 地址池 659
GlobalProtect 应用程序如何为移动用户选择 Prisma Access 接入位置 665
允许列出 GlobalProtect 移动用户 667
GlobalProtect 应用程序升级 678
将 Prisma 访问与本地 GlobalProtect 网关集成 686
移动用户：显式代理 704
显式代理配置准则 706
代理模式下的 GlobalProtect 710
隧道和代理模式下的 GlobalProtect 723
基于代理的代理流量的专用 IP 地址可见性和实施 745
用于显式代理的 SAML 身份验证 747
设置 Explicit Proxy 750
用于显式代理部署的 Kerberos 身份验证 771
用于显式代理部署的 Cloud Identity Engine 身份验证 804
远程网络的代理模式 809
显式代理如何识别用户 818
显式代理转发配置文件 819
PAC 文件指南 828
显式代理最佳实践 834
监控显式代理并排除故障 835
显式代理的阻止设置 838
使用特殊对象将显式代理互联网流量限制到特定 IP 地址 841
使用显式代理访问数据中心 842
基于应用程序的 Office 365 与显式代理集成 847

 ©2025 Palo Alto Networks, Inc.

使用 Blue Coat 代理配置代理链 851
在 GlobalProtect（或第三方 VPN）中使用显式代理 856
显式代理用户的 IP 地址优化 - 代理部署 869
“移动用户 — 显式代理”部署的 DNS 解析 869
查看用户到IP地址或用户组的映射 873
报告移动用户站点访问问题 878
允许移动用户向 Prisma Access 进行身份验证 880
身份验证支持和功能 881
设置身份验证 885
让移动用户能够访问公司资源 891
Prisma Access 远程网络 895
远程网络规划清单 896
分配远程网络带宽 901
规划向新模式的迁移 917
迁移后聚合带宽部署的带宽分配 920
QoS迁移指南 921
迁移您的带宽管理设置 926
加入远程网络 933
将远程网络站点连接到 Prisma Access 961
添加主要和辅助 IPSec VPN 隧道 961
更多 IKE 选项 962
更多 IPSec 选项 963
为远程网络启用路由 965
站点连接故障排除 968
接入多个远程网络 970
远程网络表中的字段 971
验证远程网络是否已连接到 Prisma Access 980
验证远程连接 BGP 状态 983
配置通过 WAN 链路连接的远程网络和服务连接 984
远程网络的 QoS 986
更改保证带宽 1003
远程网络 — 高性能 1006
“远程网络—高性能”部署的性能和指南 1006
使用终端服务器将共享桌面 VDI 与 Prisma Access 集成 1025
Prisma Access 监控和可见性 1033
Prisma Access日志 1034
外部日志和其他数据 1035
Prisma Access 活动指示板和报告 1036

 ©2025 Palo Alto Networks, Inc.

在 Strata Cloud Manager 中查看和监控 Prisma Access 1037
在 Strata Cloud Manager 中使用 Prisma Access Monitoring 入门 1038
查看和监控应用程序 1040
查看和监控应用加速 1043
查看移动用户 1044
查看和监视移动用户的 IPv6 1044
查看和监控分支站点 1046
查看和监视数据中心 1055
查看和监控网络服务 1071
查看订阅使用情况 1076
查看和监控 Prisma 访问位置 1078
查看和监控第三方设备 ID 1079
查看和监控远程浏览器隔离 1081
Prisma Access 和自主 DEM 1083

Prisma Access 基于用户的策略 1085

为 Prisma Access 配置基于用户的策略 1086
将 Cloud Identity Engine 与 Prisma Access 集成 1089
检索 Prisma Access 的 User-ID 组映射 1095
身份重新分发 1104
在 Prisma Access 中配置第三方 Device-ID 1121
第三方 Device-ID API 1128
更新判定 1128
删除所有判定 1130
查询判定 1131
按 IP 地址查询判定结果 1133
查询判定统计信息 1135

Prisma Access 多租户 1137

多租户配置概述 1138
规划您的多租户部署 1142
创建全新的多租户部署 1144
启用多租户并迁移第一个租户 1145
向 Prisma Access 添加租户 1151
删除租户 1157
创建租户级管理用户 1162
控制租户级管理用户的基于角色的访问权限 1166
删除租户级管理用户的插件访问权限 1167
在多租户部署中按设备组 ID 对日志进行排序 1171

 ©2025 Palo Alto Networks, Inc.

FedRAMP 环境中的 Prisma Access 1173
Prisma Access FedRAMP 要求 1174
预安装和产品激活要求 1174
所需的 Panorama、插件和 PAN-OS 数据平面版本 1175
支持的 Prisma Access FedRAMP 位置 1176
Prisma Access FedRAMP 部署中支持和不支持的功能 1177
在 FedRAMP 环境中配置 Prisma Access 1178
Prisma Access 高级部署 1185
为已部署的 Prisma Access 位置添加新的计算位置 1187
IPv6 支持 1189
原生 IPv6 支持概述 1191
在 Prisma Access 基础设施中启用和配置 IPv6 网络和 IP 池 1194
为“移动用户 — GlobalProtect 部署”启用 IPv6 网络 1201
为服务连接启用 IPv6 网络 1205
为远程网络启用 IPv6 网络 1212
“移动用户 — GlobalProtect”和远程网络部署的 DNS 解析 1220
“移动用户 — GlobalProtect”部署的 DNS 解析 1222
远程网络的 DNS 解析 1223
BGP 如何为服务连接和远程网络连接通告移动用户 IP 地址池 1225
Prisma Access 和 Strata Logging Service 对代理的支持情况 1227
阻止来自特定国家/地区的传入连接 1228
确保来自 AWS WorkSpace 的互联网流量安全 1229
在 AWS WorkSpace 客户端上配置 PAC 文件 1229
在 AWS 和 Prisma Access 之间配置站点到站点隧道 1231
适用于无默认路由网络的 Prisma Access 1232
什么是无默认路由网络？ 1232
无默认路由网络注意事项 1232
关于保护无默认路由网络的互联网访问安全的部署建议 1232
关键注意事项 1233
Prisma Access 服务连接高级部署 1234
服务连接多云冗余 1234
使用流量导向将互联网绑定流量转发到服务连接 1243
服务连接流量的路由 1264
使用多个服务连接创建高带宽网络 1277
为具有源 NAT 的服务连接保留 User-ID 和 Device-ID 映射 1290
Prisma Access 移动用户—GlobalProtect 高级部署 1298
在 Prisma Access 中配置多个门户 1298
支持动态 DNS 注册，实现远程故障排查与更新 1307

 ©2025 Palo Alto Networks, Inc.

对“移动用户—GlobalProtect”的动态 DNS 注册支持 1322
在 Prisma Access GlobalProtect 部署中识别和隔离感染设备 1328
移动用户中的 IPv6 流量陷坑 — GlobalProtect 部署 1337
使用 Prisma Access 重新分发 HIP 信息 1342
查看 HIP 报告 1350
无客户端 VPN 中支持 Gzip 编码 1352
Prisma Access 中的流量复制 1354
Prisma Access 远程网络高级部署 1366
Prisma Access 内部网关 1366
提供对远程网络地点的安全入站访问 1375
Prisma Access for Clean Pipe 1403
Prisma Access for Clean Pipe 概述 1404
Clean Pipe 用例 1404
Clean Pipe 示例 1404
Clean Pipe 和合作伙伴互连要求 1405
完成 Clean Pipe 配置 1408
启用多租户并创建一个租户 1411

 ©2025 Palo Alto Networks, Inc.

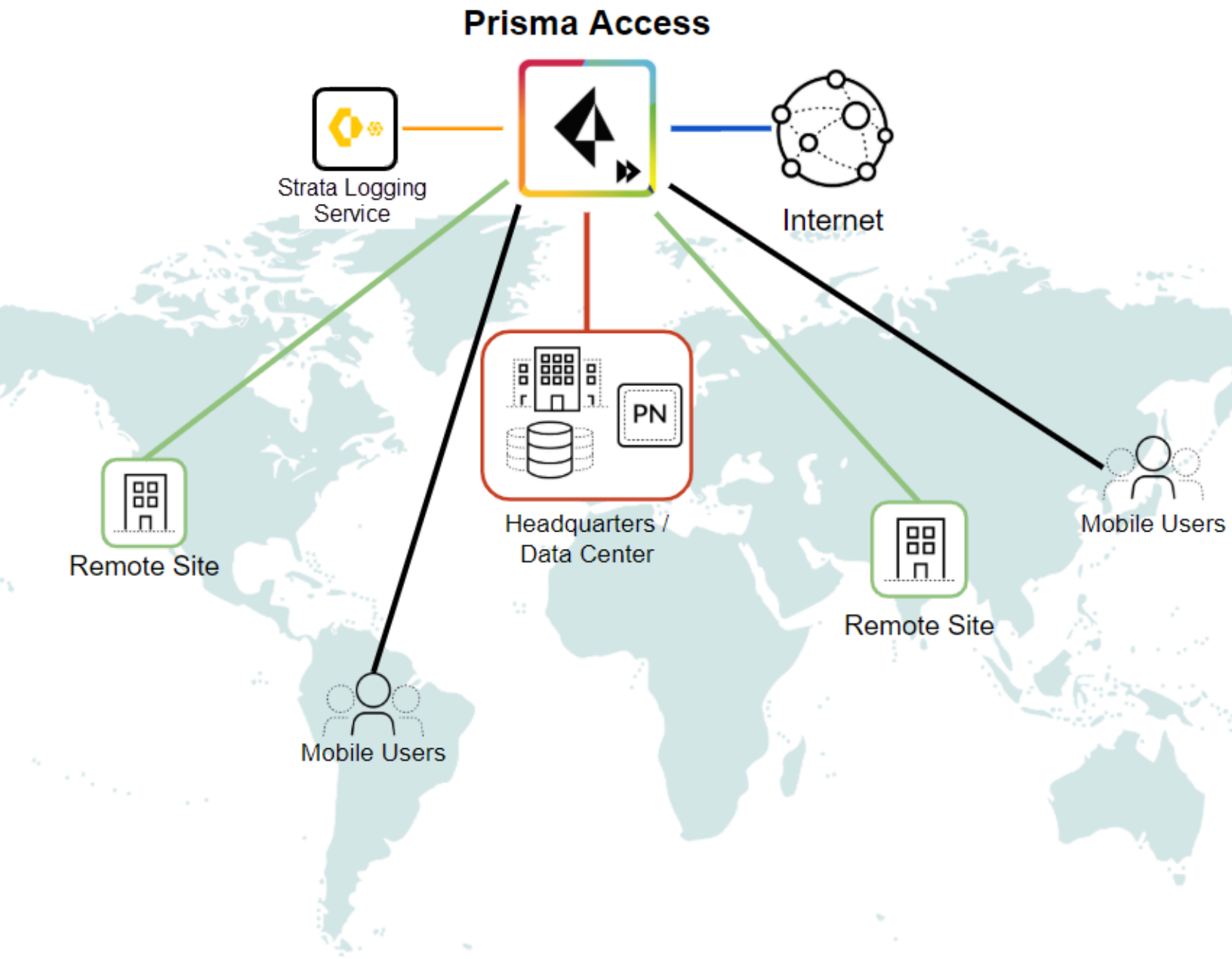
©2025 Palo Alto Networks, Inc.

Prisma Access 概述

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

为了保障您的应用程序和数据安全，必须始终确保所有地点的所有用户都得到安全防护。但是，随着您的业务版图在全球范围内不断拓展，越来越多的用户处于移动状态，并且您的应用程序和数据正从你的网络迁移到云端时，如何能做到这一点呢？Prisma Access 让您的用户能够安全地访问云端和数据中心应用程序以及互联网，从而实现这种一致的安全保障，无论他们是在总部、分支机构，还是在旅途中。Prisma Access 会持续检查所有端口的所有流量，从而实现对互联网、所批准的 SaaS 应用程序、公共云环境、数据中心以及总部的安全访问。系统内置了威胁预防、恶意软件防范、URL 过滤、SSL 解密以及基于应用程序的策略管控等功能。无论您的用户身在何处，也不管他们正在访问何种资源，这些功能都能为您提供同等水准的安全保障。所有 Prisma Access 日志都存储在 Strata Logging Service 中，提供跨所有用户、应用程序和位置的集中分析、报告和取证。

Prisma Access 借助全球覆盖能力实现大规模防护，您无需担心硬件防火墙在分支机构的部署和选型，也不必在托管设施中搭建和管理设备。Prisma Access 提供网络基础设施，用于连接您所有的远程分支机构、总部站点、数据中心和移动用户，您不必自己构建全球安全基础设施和扩充运营能力。



借助 Prisma Access，Palo Alto Networks 可在全球范围内部署和管理安全基础设施，以保障您的远程网络和移动用户的安全。Prisma Access 会对以下连接之间的数据进行端到端加密：移动用户安全处理节点 (MU-SPN) 与远程网络安全处理节点之间 (RN-SPN)、SPN 与服务连接企业接入节点之间 (SC-CAN) 以及 SC-CAN 与数据中心之间。

- 服务基础设施—Prisma Access使用内部服务基础设施来保护您组织的网络。您为基础设施提供一个子网，然后 Prisma Access 会使用该子网内的 IP 地址，在您的远程网络地点与移动用户之间建立网络基础设施，并建立与您内部网络资源的服务连接（如果适用）。云中的内部通信是使用动态路由建立的。

 ©2025 Palo Alto Networks, Inc.

- 服务连接—如果您的 Prisma Access 许可证包含此功能，您可以选择建立 IPSec 隧道，以允许网络中的内部资源与移动用户和远程网络位置的用户之间进行通信。例如，您可以创建到组织总部或数据中心的身份验证服务器的服务连接。

  即使您的总部或数据中心不需要服务连接，我们也建议您创建一个服务连接，以允许移动用户和远程网络位置之间以及不同地理位置的移动用户之间的网络通信。
- 移动用户—为您的移动用户提供一致的安全性，无论他们是访问数据中心的应用程序、使用 SaaS 应用程序还是浏览互联网。可通过以下方式让用户连接到 Prisma Access：
  - **GlobalProtect**

    你可以将 GlobalProtect 应用程序部署到您的用户（该应用程序适用于运行 Microsoft Windows、Apple macOS 和 iOS、Android、Google Chrome OS 以及 Linux 系统的智能手机、平板电脑或笔记本电脑），这样用户就可以将流量通过隧道传输至 Prisma Access，以实现策略执行和威胁防范。GlobalProtect 应用程序还提供主机信息配置文件 (HIP) 报告，以便您可以根据设备状态创建精细策略，以确保端点只有遵守您的安全标准（例如，它们配备了最新的补丁程序、加密和病毒定义）才能访问您最敏感的应用程序。或者，要对非托管设备上的用户启用安全访问，可以启用 无客户端 **VPN**。Prisma Access 根据用户当前所处的位置，按区域动态扩展。
  - 显式代理

    如果您组织的现有网络已使用显式代理并在客户端端点上部署了 PAC 文件，则可以顺利迁移到 Prisma Access 以保护移动用户的出站互联网流量。
- 远程网络—使用基于云的下一代防火墙，使用远程网络保护远程网络位置（如分支机构）和这些分支机构中的用户。您可以使用静态路由、使用 BGP 的动态路由或静态和动态路由的组合来启用对每个远程网络位置的子网的访问。上线的所有远程网络位置都是完全网格化的。
- **ZTNA** 连接器—零信任网络访问 (ZTNA) 连接器可让您简单安全地连接到组织的私有应用程序。ZTNA 连接器借助自动安全隧道，为移动用户和分支机构的用户提供访问您的私有应用程序的途径，您无需再设置 IPsec 隧道和路由定义来访问这些私有应用程序。ZTNA 连接器不需要从客户基础设施进行任何路由，并且可以提供对网络中使用重叠 IP 地址的应用程序的访问。
- **Strata Logging Service**—Prisma Access将所有日志转发到 Strata Logging Service；作为激活 Prisma Access 的一部分，您将指定要将 Prisma Access 日志转发到的 Strata Logging Service 实例。日志流量不会使用您为 Prisma Access 购买的许可带宽。

 ©2025 Palo Alto Networks, Inc.

使用 Prisma Access 确保互联网流量的安全

在何处可以使用？	需要提供什么？
• Prisma Access	❑ Prisma Access 许可证

网络安全的重要性

确保互联网访问安全从未如此重要且具有挑战性。现有的传统解决方案难以检测规避性和有针对性的网络钓鱼以及其他基于网络的攻击，同时忽略了不安全的 DNS 流量带来的新威胁。Palo Alto Networks Prisma Access 拥有业界首创的由机器学习驱动的高级 URL 过滤和 DNS 安全服务，从而实现互联网安全。使用 Prisma Access，您可以实时阻止规避性和针对性的网络钓鱼和无文件攻击，并防范最新的基于 DNS 的复杂攻击。

Prisma Access 云安全 Web 网关 (SWG)

由于网络威胁的复杂性和爆发频率不断上升，安全 Web 网关已经成为当今数字环境下的关键要素。网络犯罪分子不断设计新的策略和技术来突破安全防御，其中之一就是将恶意代码伪装在看似合法的网站中。当用户访问这些受感染的网站时，他们可能会在无意中泄露凭据或导致有害代码入侵组织，如果不注意，可能会造成严重破坏。

在这种充满风险的环境中，缺少强大的安全网关会大大增加组织数字资产的风险。这种风险可能导致未经授权的访问、数据窃取和业务运营中断，尤其是在网络钓鱼和勒索软件攻击日益猖獗的情况下。如果没有 SWG 提供的安全屏障，勒索软件攻击可能会有效地劫持组织，导致财务和声誉损失。

现在，加密流量的使用很普遍，其中 HTTPS 构成了网络流量的主要部分。如果组织缺乏能够有效解密和检查流量的 SWG，则组织将面临隐藏在加密通道内的安全威胁的风险。

但是，为 SWG、私有应用程序访问和 CASB 多个点产品只会让事情复杂化。将分散的产品拼凑在一起作为一项服务，会导致功能上的差距和较差的安全性后果，使您容易受到攻击。通过这些解决方案，对于互联网和私有应用程序，您获得的安全性不一致。

为了应对这些挑战，Prisma Access 提供了统一的产品，将所有用户和应用程序的管理、策略和数据融合在一起，并且涵盖所有功能，包括 ZTNA、SWG、NG-CASB、FWaaS、DLP 等。

客户可以轻松地从传统的本地和基于云的代理解决方案迁移到 Prisma Access，以便通过行业领先的人工智能安全保护获得互联网和 SaaS 应用流量的在线可视性和控制性。

使用 Prisma Access 保护用户和终端

Prisma Access 旨在防止网络攻击取得成功，因此，它的作用不仅仅是保护网络安全。为了阻止网络攻击，有必要检查所有流量。如果不对所有流量进行全面检查，任何措施都会导致严重的安全漏洞。Prisma Access 持续保护所有端口和所有应用程序的所有流量，使您的组织能够：

- 利用经过验证的安全理念和威胁情报来防止网络攻击取得成功，从而实现整个组织的深度可视性和精确控制性。

 ©2025 Palo Alto Networks, Inc.

- 在所有端口上全面双向检查所有应用程序流量（包括 SSL 或 TLS 加密流量），无论是与互联网、云还是分支机构之间的通信。
- 从 Palo Alto Networks 和数百个第三方源提供的自动威胁数据提供的全面威胁情报受益。

了解 Prisma Access 及其解决方案。

 ©2025 Palo Alto Networks, Inc.

如何管理 Prisma Access

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

可以通过两种方式管理 Prisma Access，但在激活 Prisma Access 许可证后，便无法在这两种管理界面之间进行切换（使用迁移工作流程从 Prisma Access (Managed by Panorama) 部署模式转换到 Prisma Access (Managed by Strata Cloud Manager) 部署模式的情况除外）。因此，在开始之前，您必须决定如何管理 Prisma Access：

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

  要从云端管理 Prisma Access，则使用 Strata Cloud Manager。借助云管理，可以通过任务驱动的工作流快速接入分支机构和移动用户，几分钟即可设置和测试您的环境。使用 Strata Cloud Manager 进行云管理可以提供基于最佳实践的预定义互联网访问和解密策略规则，从而简化接

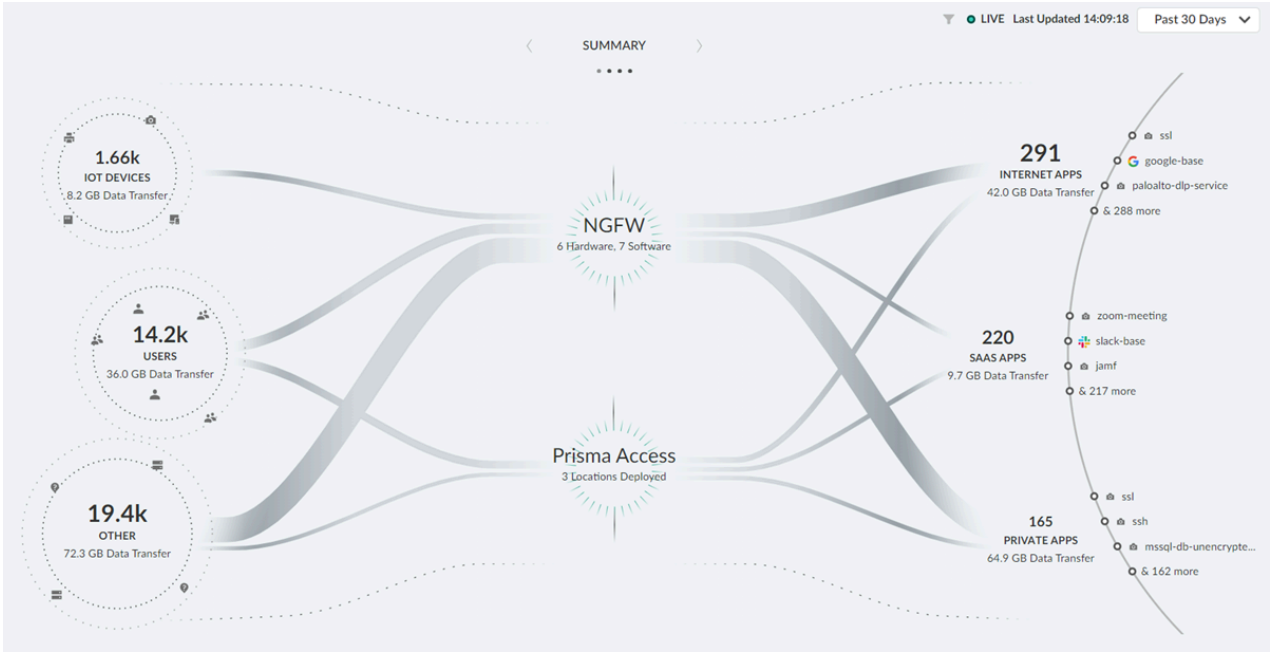
 ©2025 Palo Alto Networks, Inc.

入过程。使用默认设置（适用于最常见的支持 IPSec 的设备）快速设置 IPSec 隧道，并为推荐的 URL 类别开启 SSL 解密。

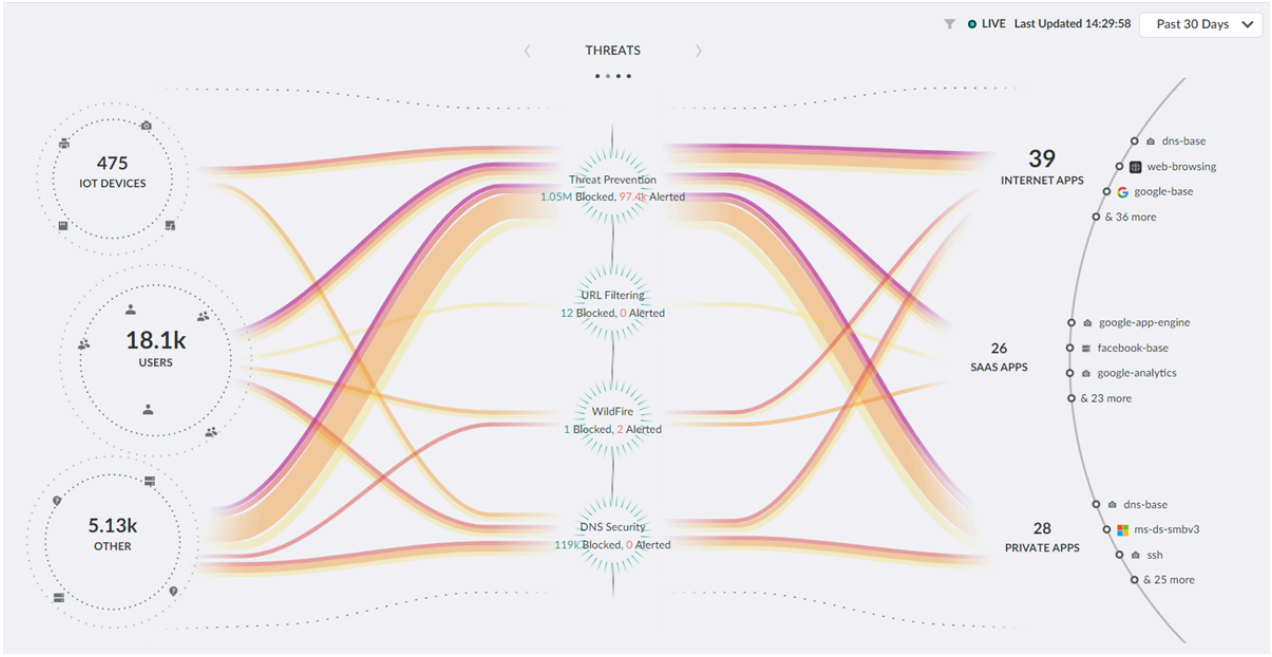
Strata Cloud Manager 命令中心

在您启动 Strata Cloud Manager 后，便会出现 Strata Cloud Manager 的命令中心页面。该命令中心可帮助您评估网络的运行状况、改善可见性，并有助于您全面了解您的数据。命令中心包含不同的指示板，可用于查看不同类型的报告。

- 摘要：在摘要指示板中，您可以查看不同类型的数据源、平台基础设施（如 NGFW 或 Prisma Access），数据会通过这些基础设施从各种数据源流向您网络中的不同应用程序。

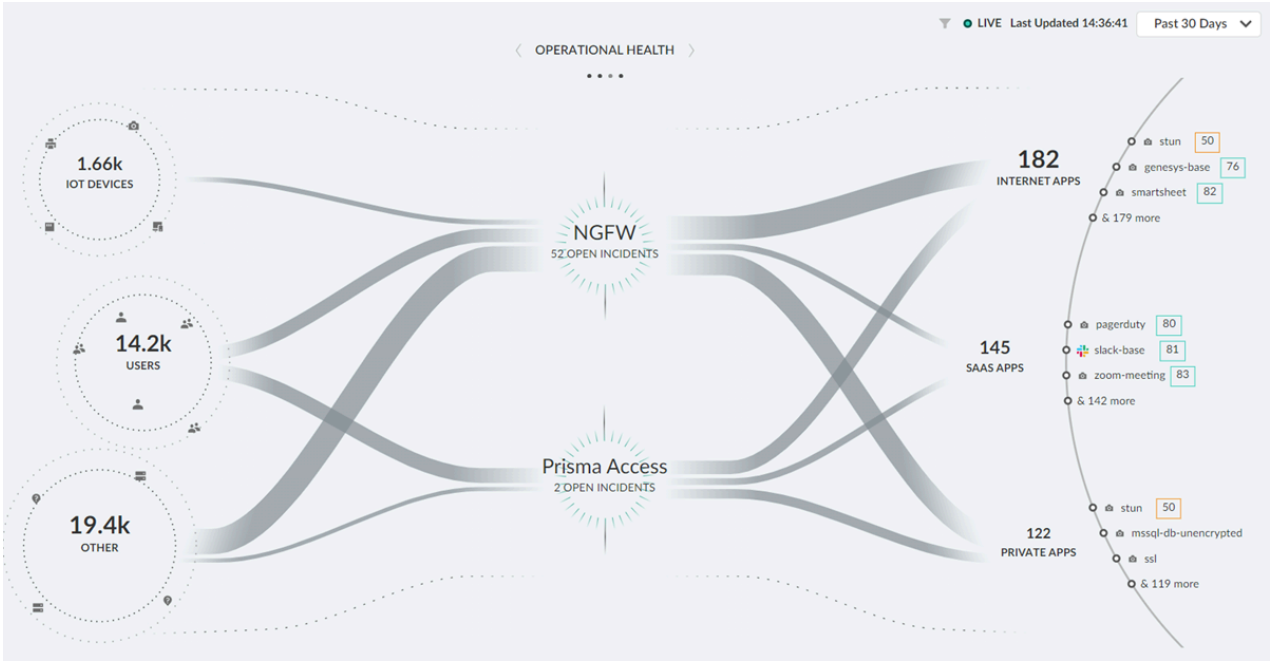


- 威胁：在您的威胁指示板中，您可以查看安全应用程序检测到的威胁。你可以使用此指示板来监控网络上被阻止和被允许的威胁，或者调查网络中可能存在流量检查比例较低的区域。



 ©2025 Palo Alto Networks, Inc.

- 操作运行状况：显示 ADEM 监控的网络运行状况和用户体验。可以使用此视图来监控网络上的用户体验并查看未解决事件的严重性。



- 数据安全性：显示在您的网络中，已被 DLP 和 SaaS 安全订阅标记为含有敏感数据的流量。可以使用此视图来监控流经防火墙和连接的 SaaS 应用程序的数据以及网络上任何数据风险的严重性。



单击指示板中的任意类别即可相应地筛选结果。

©2025 Palo Alto Networks, Inc.

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

  使用 Panorama 上的云服务插件来设置和管理 Prisma Access。如果您已经在使用 Panorama 来管理新一代防火墙，并且有一个用于访问公司应用程序的通用策略，那么这是个不错的选择。



即使正在使用 *Panorama* 来管理 *Prisma Access*，仍然可以使用 *Strata Cloud Manager* 来实现 *Prisma Access* 许多方面的可见性和监控功能。了解详情。

决定要使用哪个管理选项后，请按照您选择的选项的许可和激活工作流程开始操作：

- 要开始使用 Prisma Access (Managed by Panorama) Access，请从客户支持门户 (CSP) 执行许可证激活，并在 Panorama 上安装云服务插件。
- 要开始使用 Cloud Managed Prisma Access，请从中心执行许可证激活。



Panorama 与云管理之间的功能一致性

Prisma Access (Managed by Panorama) Access 与 *Prisma Access (Managed by Strata Cloud Manager)* 支持的功能存在一些差别。有关 *Prisma Access (Managed by Panorama)* 和 *Prisma Access (Managed by Strata Cloud Manager)* 中支持的功能的列表，请参阅兼容性一览表。

 ©2025 Palo Alto Networks, Inc.

通过 Strata Cloud Manager 实现对 Prisma Access 的可见性和监控

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access（Panorama 托管）	• Prisma Access 许可证

您可以选择两种方式来管理 Prisma Access：

- 对于 Prisma Access (Managed by Strata Cloud Manager)，可以使用 **Strata Cloud Manager**
- 也可以使用 **Panorama** 来管理 Prisma Access

这两个管理界面是您处理 Prisma Access 环境接入、配置和安全策略实施的方式。但是，Prisma Access 还为您的 Prisma Access 环境提供了强大的可见性和监控功能，这些功能在 Strata Cloud Manager 上提供。

重要的是：

无论您为 Prisma Access 使用何种管理界面（Strata Cloud Manager 或 Panorama），您都可以将 Strata Cloud Manager 用于许多 Prisma Access 可见性功能，并与附加订阅（如 AI 驱动的自主 DEM）进行交互。

Strata Cloud Manager 上的 Prisma Access 可见性和监控功能	
自主 DEM	为您的安全访问服务边缘 (SASE) 环境中的所有用户流量提供本机、端到端的可见性和洞察力。ADEM 功能已原生集成到 GlobalProtect 应用程序和 Prisma Access 中，因此不需要部署任何其他设备或代理。您可以快速隔离数字体验问题的来源，并简化修复过程。 此功能需要 Autonomous DEM 附加许可证才能使用 *Prisma Access (Managed by Panorama)* 使用权。
Strata Cloud Manager 中的指示板和报告	Strata Cloud Manager 中的可见性功能可识别关键发现，您可以使用这些发现来通知您的策略更新，并缩小企业安全和用户生产力差距。 • 交互式指示板 探索网络中应用程序、威胁、用户、安全订阅的数据 • 报告 许多指示板支持报告，您可以在其中离线共享数据并安排定期更新
Strata Cloud Manager 命令中心	命令是您网络上物联网设备、用户、主机和流量的交互式可视化摘要。利用云交付的安全和 ADEM 订阅中的数据，命令中心可显示有关威胁、用户体验和网络数据安全性的重要信息。

©2025 Palo Alto Networks, Inc.

Strata Cloud Manager 上的 Prisma Access 可见性和监控功能	
	通过命令中心，您能够与数据交互，查看网络上的事件之间的关系，以便发现异常情况，寻找增强网络安全的方法。

©2025 Palo Alto Networks, Inc.

Prisma Access 位置

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证

您可以根据数据位置首选项和您拥有最多用户的位置，在您选择的位置部署 Prisma Access。Prisma Access 在全球提供了 100 多个位置，以便您的用户获得适合其区域设置的体验。根据优化的性能和延迟，所有 Prisma Access 位置都映射到一个安全计算位置。这意味着某些国家的流量将被定向到这个定义的计算位置。

如果您需要将计算位置限制在特定国家/地区，请参阅显示 *Prisma Access* 及其相关服务的处理国家/地区的表格。

有不同的 Prisma Access 位置类型：

- 按计算位置排序的位置—配置远程网络时，可以按计算位置分配带宽。在地理位置上彼此相近的至少两个（通常更多）Prisma Access 位置被分组为计算位置。这是您分配带宽的层级，这种方式不是为各个 Prisma Access 位置或特定的远程网络站点分配带宽，而是允许 Prisma Access 根据负载或需求，动态地为计算位置中的各个站点分配带宽。
- 大区和位置组—在“移动用户—GlobalProtect”部署中分配 IP 地址池时，您可以按位置组（一个比大区小的位置集合）、大区或全球范围来指定 IP 地址池。如果您拥有一些依赖于用户源 IP 地址来识别用户详细信息的服务（例如基于位置的服务，或基于用户组或功能的服务），以便您能够应用访问控制策略，或者当不同国家处于不同的计算区域时，需要对这些国家执行路由或策略操作，则使用特定于位置组的 IP 地址池。
- 按地区划分的位置—每个 Prisma Access 位置都有相关区域。
- 显式代理位置—显式代理有自己的一组位置，这些位置是 Prisma Access 位置的子集。
- **Colo-Connect** 位置—Colo-Connect 有自己的一组位置，这些位置是 Prisma Access 位置的子集。
- **Strata Logging Service** 区域—Prisma Access 支持 Strata Logging Service 区域的子集。
- 远程网络—高性能、流量复制和安全入站访问位置—高性能远程网络、流量复制和安全入站访问部署使用 Prisma Access 位置的子集。
- **Prisma Access China** 位置—Prisma Access China 部署使用中国大陆的位置。
- **FedRAMP** 中等和高等位置—Prisma Access FedRAMP 中级和高级部署使用 Prisma Access 位置的子集。
- 北美地区地图—为了帮助您选择北美地区的位置，请参考这张地图，其中显示了北美地区位置的地理覆盖范围。

 ©2025 Palo Alto Networks, Inc.

- 本地区域—本地区域将计算、存储、数据库和其他服务放置在靠近大型人口和工业中心的位置。这些位置有自己的计算位置。

  要添加本地区域，请联系您的 *Palo Alto Networks* 代表。

  部署本地区域时请牢记以下准则：

  - 本地区域位置不支持 IPv6。
  - 本地区域位置不使用 Palo Alto Networks 注册的 IP 地址。
  - 对远程网络不支持 1 Gbps 速度。
  - 如果您将远程网络和服务连接节点部署在同一个本地区域内，那么跨可用区的节点冗余将不可用，因为这两个节点都设置在单一区域中。
  - 这些本地区域不使用 Palo Alto Networks 注册的 IP。如果您在访问 URL 时遇到问题，可以使用 https://reportasite.gpcloudservice.com/ 网址来报告网站问题，也可以联系 Palo Alto Networks 支持。

查看 Prisma Access Privacy 数据表，详细了解 *Prisma Access* 位置以及 *Prisma Access* 处理流量的位置。

计算位置、城市和国家/地区

每个计算位置列出的第一个位置（以粗体显示）显示该计算位置所在的城市和国家/地区。

用两个星号 (**) 表示的位置是本地区域，不一定支持所有 Prisma Access 功能。

计算位置	**Prisma Access** 位置	国家/地区和城市
亚洲东北部	日本中部	日本东京
亚洲南部	印度西部 孟加拉国 印度南部 巴基斯坦南部 巴基斯坦西部	印度孟买 孟加拉国，达卡 印度，钦奈 巴基斯坦，卡拉奇 巴基斯坦，拉合尔
亚洲东南部（印度尼西亚）	印度尼西亚	印度尼西亚，雅加达
东南亚（新加坡）	新加坡 柬埔寨 马来西亚 缅甸 巴基斯坦西部 (II)	新加坡 柬埔寨，金边 马来西亚，吉隆坡 缅甸，仰光 巴基斯坦，伊斯兰堡

©2025 Palo Alto Networks, Inc.

计算位置	Prisma Access 位置	国家/地区和城市
	菲律宾	菲律宾，奎松城
	斯里兰卡	斯里兰卡，科伦坡
	泰国	泰国，曼谷
	越南	越南，胡志明市
澳大利亚南部	澳大利亚南部	澳大利亚墨尔本
澳大利亚东南部	澳大利亚东南部	澳大利亚悉尼
	澳大利亚东部	澳大利亚，布里斯班
	新西兰	新西兰，奥克兰
	巴布亚新几内亚	巴布亚新几内亚，莫尔兹比港
澳大利亚西部（珀斯）**	澳大利亚西部（珀斯）**	澳大利亚，珀斯
巴林	巴林	巴林，麦纳麦
比利时	比利时	比利时，圣吉斯兰
	拉脱维亚	拉脱维亚，里加
	塞内加尔	塞内加尔，达喀尔
加拿大中部（蒙特利尔）	加拿大东部	加拿大，魁北克
加拿大中部（多伦多）	加拿大中部	加拿大，多伦多
加拿大西部（卡尔加里）	加拿大西部	加拿大，卡尔加里
欧洲中部	德国中部	德国法兰克福
	奥地利	奥地利，维也纳
	保加利亚	保加利亚，索非亚
	克罗地亚	克罗地亚，萨格勒布
	捷克共和国	捷克共和国，布拉格
	埃及	埃及，开罗
	德国北部	德国，汉堡
	德国南部	德国，慕尼黑
	希腊	希腊，雅典
	匈牙利	匈牙利，布达佩斯
	科威特	科威特，艾哈迈迪

©2025 Palo Alto Networks, Inc.

计算位置	Prisma Access 位置	国家/地区和城市
	列支敦士登	列支敦士登，沙恩
	卢森堡	卢森堡，卢森堡城
	摩尔多瓦	摩尔多瓦，基希讷乌
	尼日利亚	尼日利亚，拉各斯
	罗马尼亚	罗马尼亚，布加勒斯特
	斯洛伐克	斯洛伐克，布拉迪斯拉发
	斯洛文尼亚	斯洛文尼亚，卢布尔雅那
	土耳其	土耳其，伊斯坦布尔
	乌克兰	乌克兰，基辅
	乌兹别克斯坦	乌兹别克斯坦，塔什干
欧洲中部（华沙）	波兰	波兰，华沙
欧洲北部	芬兰	芬兰，哈米纳
	白俄罗斯	白俄罗斯，明斯克
	哈萨克斯坦	哈萨克斯坦，阿斯塔纳
	立陶宛	立陶宛，维尔纽斯
	挪威	挪威，奥斯陆
	俄罗斯中部	俄罗斯，莫斯科
	俄罗斯西北部	俄罗斯圣，彼得堡
欧洲北部（斯德哥尔摩）	瑞典	瑞典，斯德哥尔摩
欧洲西北部	英国	英国，伦敦
	加纳	加纳，阿克拉
欧洲西北部（巴黎）	法国南部	法国巴黎
欧洲南部	意大利	意大利，米兰
	约旦	约旦，安曼
	肯尼亚	肯尼亚，蒙巴萨
	摩纳哥	摩纳哥
欧洲西南部	西班牙中部	西班牙，马德里
	安道尔	安道尔，安道尔城
	葡萄牙	葡萄牙，里斯本

©2025 Palo Alto Networks, Inc.

计算位置	Prisma Access 位置	国家/地区和城市
	西班牙东部	西班牙，巴塞罗那
欧洲西部	荷兰中部 丹麦 荷兰南部	荷兰，埃姆斯哈文 丹麦，哥本哈根 荷兰，鹿特丹
法国北部	法国北部	法国巴黎
中国香港	中国香港	中国香港
印度北部	印度北部	印度，新德里
爱尔兰	爱尔兰	爱尔兰，都柏林
日本南部	日本南部	日本，大阪
中东中部（卡塔尔）	卡塔尔	卡塔尔，多哈
中东中部（沙特阿拉伯）	沙特阿拉伯	沙特阿拉伯，利雅得
中东中部（阿联酋）	阿拉伯联合酋长国	阿拉伯联合酋长国，迪拜
中东西部	以色列	以色列，特拉维夫
尼日利亚（拉各斯）**	尼日利亚（拉各斯）**	尼日利亚，拉各斯
新西兰（奥克兰）**	新西兰（奥克兰）**	新西兰，奥克兰
南非中部	南非中部	南非，约翰内斯堡
南非西部	南非西部	南非开普敦
南美洲东部	巴西南部 巴西中部 巴西东部 巴拉圭 委内瑞拉	巴西，圣保罗 巴西利亚，巴西 巴西，里约热内卢 巴拉圭，亚松森 委内瑞拉，加拉加斯
南美洲西部	智利 阿根廷 玻利维亚 秘鲁	智利，圣地亚哥 阿根廷，布宜诺斯艾利斯 玻利维亚，圣克鲁斯德拉谢拉 秘鲁，利马

©2025 Palo Alto Networks, Inc.

计算位置	Prisma Access 位置	国家/地区和城市
	乌拉圭	乌拉圭，蒙得维的亚
南美西部（利马）**	南美西部（利马）**	秘鲁，利马
韩国	韩国	韩国，首尔
瑞士	瑞士 乌干达	瑞士，苏黎世 乌干达，坎帕拉
中国台湾	中国台湾	台湾，彰化
美国中部	美国中部	美国，康瑟尔布拉夫斯
美国中部（芝加哥）**	美国中部（芝加哥）**	美国，芝加哥
美国中西部	美国中西部	美国，盐湖城
美国东部	美国东部 美国东北部 危地马拉	美国，阿什本 美国，纽约市 危地马拉，危地马拉城
美国西北部	美国西北部	美国，达尔斯
美国南部	美国南部 墨西哥中部 墨西哥西部	美国，达拉斯 墨西哥，墨西哥城 墨西哥，瓜达拉哈拉
美国东南部	美国东南部 哥伦比亚 哥斯达黎加 厄瓜多尔 巴拿马	美国，蒙克斯科纳 哥伦比亚，波哥大 哥斯达黎加，圣何塞 厄瓜多尔，瓜亚基尔 巴拿马，巴拿马城
美国东南部（迈阿密）**	美国东南部（迈阿密）**	美国，迈阿密
美国西南部	美国西南部 美国西部	美国，洛杉矶 美国，旧金山

©2025 Palo Alto Networks, Inc.

大区和位置组

大区/位置组	IP 池组 ID
哥伦比亚 哥斯达黎加 厄瓜多尔 危地马拉 墨西哥中部 巴拿马 美国东部 美国东南部 美国中部 哥斯达黎加 美国中北部 美国东北部 美国南部 美国东南部 委内瑞拉	1
加拿大东部 加拿大中部	2
爱尔兰	3
法国南部 加纳 英国	4
法国北部	5
亚洲、澳大利亚和日本	6
安道尔 奥地利 保加利亚 克罗地亚	7

©2025 Palo Alto Networks, Inc.

大区/位置组	IP 池组 ID
捷克共和国	
埃及	
德国中部	
德国北部	
德国南部	
希腊	
匈牙利	
以色列	
意大利	
约旦	
肯尼亚	
科威特	
列支敦士登	
卢森堡	
摩尔多瓦	
摩纳哥	
尼日利亚	
波兰	
葡萄牙	
罗马尼亚	
斯洛伐克	
斯洛文尼亚	
沙特阿拉伯	
南非中部	
西班牙中部	
西班牙东部	
土耳其	
乌克兰	
阿拉伯联合酋长国	
乌兹别克斯坦	
白俄罗斯	8

©2025 Palo Alto Networks, Inc.

大区/位置组	IP 池组 ID
芬兰 哈萨克斯坦 立陶宛 挪威 俄罗斯中部 俄罗斯西北部 瑞典	
丹麦 荷兰中部 荷兰南部	9
非洲、欧洲和中东	10
瑞士 乌干达	11
比利时 拉脱维亚 塞内加尔	12
巴西中部 巴西东部 巴西南部 巴拉圭 委内瑞拉	13
澳大利亚东部 澳大利亚南部 澳大利亚东南部 新西兰 巴布亚新几内亚	14
柬埔寨 印度尼西亚 马来西亚	15

©2025 Palo Alto Networks, Inc.

大区/位置组	IP 池组 ID
缅甸 菲律宾 新加坡 泰国 越南	
中国香港	16
中国台湾	17
韩国	18
孟加拉国 印度北部 印度南部 印度西部 巴基斯坦西部 巴基斯坦南部 卡塔尔	19
南非西部 瑞典 南非西部	20
日本中部 日本南部	21
巴林	22
加拿大西部 墨西哥中部 墨西哥西部 美国中西部 美国西北部 美国西南部 美国西部	23

©2025 Palo Alto Networks, Inc.

大区/位置组	IP 池组 ID
阿根廷 玻利维亚 智利 秘鲁 乌拉圭	24

按地区划分的位置

位置
非洲地区
肯尼亚
尼日利亚
塞内加尔
南非中部
南非西部
亚洲地区
孟加拉国
柬埔寨
中国香港
印度北部
印度南部
印度西部
印度尼西亚
哈萨克斯坦
马来西亚
缅甸

©2025 Palo Alto Networks, Inc.

位置
巴基斯坦南部
巴基斯坦西部
巴基斯坦西部 (II)
巴布亚新几内亚
菲律宾
新加坡
韩国
斯里兰卡
中国台湾
泰国
越南
澳新地区
澳大利亚东部
澳大利亚南部
澳大利亚东南部
新西兰
欧洲地区
安道尔
奥地利
白俄罗斯
比利时
保加利亚
克罗地亚
捷克共和国

©2025 Palo Alto Networks, Inc.

位置
丹麦
芬兰
法国北部
法国南部
德国中部
德国北部
德国南部
加纳
希腊
匈牙利
爱尔兰
意大利
拉脱维亚
列支敦士登
立陶宛
卢森堡
摩尔多瓦
摩纳哥
荷兰中部
荷兰南部
挪威
波兰
葡萄牙
罗马尼亚

©2025 Palo Alto Networks, Inc.

位置
俄罗斯中部
俄罗斯西北部
斯洛伐克
斯洛文尼亚
西班牙中部
西班牙东部
瑞典
瑞士
乌干达
英国
乌克兰
乌兹别克斯坦
日本地区
日本中部
日本南部
中东地区
巴林
埃及
以色列
约旦
科威特
卡塔尔
沙特阿拉伯
土耳其

©2025 Palo Alto Networks, Inc.

位置
阿拉伯联合酋长国
北美地区
加拿大中部
加拿大东部
加拿大西部
哥斯达黎加
墨西哥中部
墨西哥西部
巴拿马
美国中部
美国中西部
美国东部
美国东北部
美国西北部
美国南部
美国东南部
美国西南部
美国西部
南美地区
阿根廷
玻利维亚
巴西中部
巴西东部
巴西南部

©2025 Palo Alto Networks, Inc.

位置
智利
哥伦比亚
厄瓜多尔
巴拉圭
秘鲁
乌拉圭
委内瑞拉

显式代理位置

Prisma Access 在以下位置支持显式代理。显式代理使用 GeoDNS 解析并将移动用户连接到距离最近的 Prisma Access 部署位置。

- 非洲、欧洲和中东：
  - 比利时
  - 芬兰
  - 法国南部
  - 德国中部
  - 以色列
  - 意大利
  - 荷兰中部
  - 波兰
  - 卡塔尔
  - 沙特阿拉伯
  - 南非中部
  - 西班牙中部
  - 瑞士
  - 英国

 ©2025 Palo Alto Networks, Inc.

- 亚洲、澳大利亚和日本：
  - 澳大利亚南部
  - 澳大利亚东南部
  - 中国
  - 中国香港
  - 日本中部
  - 日本南部
  - 印度北部
  - 印度西部
  - 印度尼西亚
  - 新加坡
  - 韩国
  - 中国台湾
- 北美和南美：
  - 巴西南部
  - 智利
  - 加拿大中部
  - 加拿大东部
  - 美国中部
  - 美国东部
  - 美国西北部
  - 美国南部
  - 美国东南部
  - 美国西南部
  - 美国中西部

Colo-Connect 位置

Prisma Access Colo-Connect 支持以下 Prisma Access 位置。创建服务连接以支持 Colo-Connect 时，请确保仅在以下位置创建服务连接。

对于专用互连链路，请使用位置的 GCP 列表，您可以在这些位置中创建“专用互联”连接。

- 澳大利亚南部
- 澳大利亚东南部
- 比利时
- 巴西南部

©2025 Palo Alto Networks, Inc.

- 加拿大中部
- 加拿大东部
- 智利
- 芬兰
- 法国南部
- 德国中部
- 中国香港
- 印度北部
- 印度西部
- 印度尼西亚
- 意大利
- 日本中部
- 日本南部
- 荷兰中部
- 卡塔尔
- 沙特阿拉伯
- 新加坡
- 南非中部
- 西班牙中部
- 瑞士
- 中国台湾
- 英国
- 美国中部
- 美国中西部
- 美国东部
- 美国西北部
- 美国南部
- 美国东南部
- 美国西南部

支持的 Strata Logging Service 区域

Prisma Access 支持以下 Strata Logging Service 区域：

- 澳大利亚
- 加拿大
- 法国

©2025 Palo Alto Networks, Inc.

- 德国
- 日本
- 印度
- 印度尼西亚
- 以色列
- 荷兰—欧洲
- 卡塔尔
- 沙特阿拉伯
- 新加坡
- 瑞士
- 中国台湾
- 英国
- 美国—美洲

远程网络—高性能、流量复制和安全入站访问位置

Prisma Access 支持以下高性能远程网络位置：

- 安道尔
- 阿根廷
- 澳大利亚东部
- 澳大利亚南部
- 澳大利亚东南部
- 奥地利
- 孟加拉国
- 白俄罗斯
- 比利时
- 玻利维亚
- 巴西中部
- 巴西东部
- 巴西南部
- 保加利亚
- 柬埔寨
- 加拿大中部
- 加拿大东部
- 智利
- 哥伦比亚

 ©2025 Palo Alto Networks, Inc.

- 哥斯达黎加
- 克罗地亚
- 捷克共和国
- 丹麦
- 厄瓜多尔
- 埃及
- 芬兰
- 法国北部
- 法国南部
- 德国中部
- 德国北部
- 德国南部
- 加纳
- 希腊
- 危地马拉
- 中国香港
- 匈牙利
- 印度北部
- 印度南部
- 印度西部
- 印度尼西亚
- 以色列
- 意大利
- 日本中部
- 日本南部
- 约旦
- 哈萨克斯坦
- 肯尼亚
- 科威特
- 拉脱维亚
- 列支敦士登
- 立陶宛
- 卢森堡
- 马来西亚
- 墨西哥中部

©2025 Palo Alto Networks, Inc.

- 墨西哥西部
- 摩尔多瓦
- 摩纳哥
- 缅甸
- 荷兰中部
- 荷兰南部
- 新西兰
- 尼日利亚
- 挪威
- 巴基斯坦南部
- 巴基斯坦西部
- 巴基斯坦西部 (II)
- 巴拿马
- 巴布亚新几内亚
- 巴拉圭
- 秘鲁
- 菲律宾
- 波兰
- 葡萄牙
- 卡塔尔
- 罗马尼亚
- 俄罗斯中部
- 俄罗斯西北部
- 沙特阿拉伯
- 塞内加尔
- 新加坡
- 斯洛伐克
- 斯洛文尼亚
- 南非中部
- 韩国
- 西班牙中部
- 西班牙东部
- 斯里兰卡
- 瑞士
- 中国台湾

 ©2025 Palo Alto Networks, Inc.

- 泰国
- 土耳其
- 乌干达
- 英国
- 乌克兰
- 乌拉圭
- 美国中部
- 美国中西部
- 美国东部
- 美国东北部
- 美国西北部
- 美国南部
- 美国东南部
- 美国西南部
- 美国西部
- 乌兹别克斯坦
- 委内瑞拉
- 越南

Prisma Access China 位置

Prisma Access China 支持中国大陆地区的以下位置：

- 华北—北京（使用华北计算位置）
- 西北—宁夏（使用西北计算位置）

FedRAMP 中等和高等位置

可在 Prisma SASE FedRAMP 文档中找到 FedRAMP 位置的列表。

北美地区地图

使用以下地图作为参考，以帮助您在北美选择 Prisma Access 位置。

©2025 Palo Alto Networks, Inc.



本地区域位置

Prisma Access 中的 IPv4 支持以下本地区域：

- 要申请在下列其中一个本地区域中部署，您需要与您的 *Palo Alto Networks* 代表合作。
- 不支持 *IPv6*。

- 澳大利亚西部（珀斯）
- 新西兰（奥克兰）
- 尼日利亚（拉各斯）
- 南美洲西部（利马）
- 美国中部（芝加哥）
- 美国东南部（迈阿密）

©2025 Palo Alto Networks, Inc.

Prisma Access 及相关服务处理位置

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证

Prisma Access 在全球 100 多个位置提供本地体验，并根据优化的性能和延迟将每个位置映射到安全计算位置。

如果您需要将计算位置限制在特定国家/地区，请查看每个 Prisma Access 位置的国家/地区映射，并在 Prisma Access 配置过程中仅部署与这些国家/地区关联的位置。

下表提供了 Strata Logging Service 区域、Strata Cloud Manager（用于 Prisma Access (Managed by Strata Cloud Manager)）、Prisma Access Insights、自主 DEM 和 SaaS 安全内联的国家/地区处理位置）。

Strata Logging Service	Strata Cloud Manager 配置	Prisma Access Insights 数据	Autonomous DEM	SaaS Security Inline
英国	英国	英国	英国	英国
荷兰	德国	荷兰	荷兰	德国（欧盟）
德国	德国	德国	德国	德国（欧盟）
瑞士	瑞士	瑞士	瑞士	德国（欧盟）
法国	德国	法国	法国	德国（欧盟）
新加坡	新加坡	新加坡	新加坡	新加坡
印度	印度	印度	印度	印度
日本	日本	日本	日本	日本
加拿大	加拿大	加拿大	加拿大	美国
美国	美国	美国	美国	美国
澳大利亚	澳大利亚	澳大利亚	澳大利亚	澳大利亚
以色列	德国	以色列	以色列	德国（欧盟）
卡塔尔	卡塔尔	卡塔尔	卡塔尔	德国（欧盟）
沙特阿拉伯	德国	沙特阿拉伯	沙特阿拉伯	德国（欧盟）

©2025 Palo Alto Networks, Inc.

Strata Logging Service	Strata Cloud Manager 配置	Prisma Access Insights 数据	Autonomous DEM	SaaS Security Inline
中国台湾	新加坡	中国台湾	中国台湾	新加坡
印度尼西亚	新加坡	印度尼西亚	印度尼西亚	新加坡

©2025 Palo Alto Networks, Inc.

Prisma Access 基础设施管理

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access（Panorama 托管）	❑ Prisma Access 许可证

Prisma Access 使用共享所有权模型。Palo Alto Networks 管理底层的安全基础设施，确保其安全可靠、具有弹性、保持最新状态，并且在您有需求时随时可用。您组织的责任是接入位置和用户，推送策略，进行更新，查询日志并生成报告。

Palo Alto Networks 管理安全基础设施的以下部分。除了安全基础设施之外，Prisma Access 还管理版本和升级：

- **Prisma Access**
- **Strata Logging Service**—我们管理日志的交付机制。
- 内容更新—我们管理发布和升级，包括 PAN-OS 更新。对于您的移动用户，Prisma Access 托管多个版本的 GlobalProtect 应用程序，您可以从该列表中选择活动的 GlobalProtect 应用程序版本。
- 容错—我们管理服务的可用性。
- 自动扩展—当您添加服务连接或远程网络，或当额外的移动用户登录到单个区域中的一个或多个网关时，我们会自动扩展服务。
- 配置—我们为基础设施配齐一切所需。
- 服务监控—我们监控服务状态并保持其正常运行。
- 计算位置映射—每个 Prisma Access位置根据优化的性能和延迟映射到安全计算位置，这意味着，除非系统管理员另行修改，否则某些国家/地区的流量将被定向到定义的计算位置。有关位置到计算位置的映射，请参阅 Prisma Access 隐私数据表。

您的组织管理以下安全基础设施组件。

- 用户—您管理移动用户的接入。
- 身份验证—您管理这些用户的身份验证。
- 移动设备管理 **(MDM)**—您可以使用自己的 MDM 软件控制您组织中受 Prisma Access 保护的移动设备。
- （仅限 Prisma Access (Managed by Panorama)）**Panorama** 和云服务插件—确保安装了云服务插件的 Panorama 正在运行支持云服务插件的 Panorama 版本。此外，在我们通知您有新插件可用后，您可以在 Panorama 中升级云服务插件。
- 政策创建和管理—您在 Panorama 中规划和创建策略以与 Prisma Access 一起使用。
- 日志分析和取证—Prisma Access 提供日志，您提供分析和报告，使用我们或其他供应商提供的集成工具。

©2025 Palo Alto Networks, Inc.

- 本地安全—您在本地网络的微分段之间提供本地安全。在某些部署中，您还可以指示所有流量都由 Prisma Access 进行保护。
- 网络连接—您提供到 Prisma Access 的网络连接。
- 监控—您监控本地网络的状态。
- 服务连接—为移动用户提供到 Prisma Access 网关的连接（例如，提供 ISP），并提供本地设备，这些设备用作服务连接和远程网络连接所使用的 IPSec 隧道的终止点。
- 接入—您接入移动用户、总部/数据中心网站和分支站点。
- （仅限 Prisma Access (Managed by Panorama)）备份—您管理全景配置的备份。

 ©2025 Palo Alto Networks, Inc.

Prisma Access API

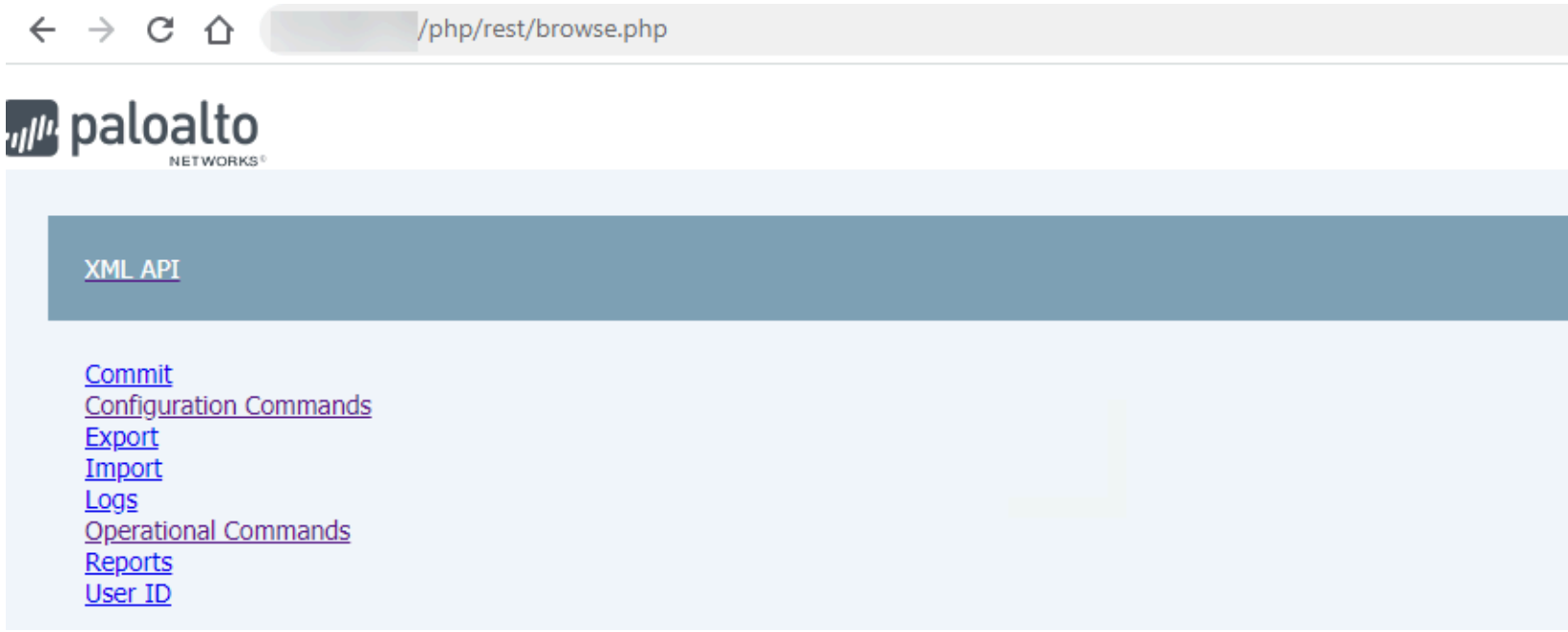
在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

适用于 Prisma Access (Managed by Strata Cloud Manager) 的 API

您可以在 pan.dev （Palo Alto Networks 开发人员文档的站点）上找到有关 Prisma Access (Managed by Strata Cloud Manager) API 的更多信息。Prisma Access (Managed by Strata Cloud Manager) 使用这些 API 来进行服务接入、配置和操作。

适用于 Prisma Access (Managed by Panorama) 的 API

除了可用于在 Panorama 中进行配置和管理的 XML API 外，您还可以使用云服务插件的 XML API 来执行特定于 Prisma Access 的任务。通过第三方服务、应用程序或脚本使用这些 API 来自动执行 Prisma Access 的配置和报告任务。



使用浏览器和 Web 界面访问 Prisma Access (Managed by Panorama) API

要使用浏览器访问 API，请使用管理员权限登录到管理 Prisma 访问的 Panorama，然后在 URL 末尾输入 /api。URL更改为 XML API 浏览器界面。

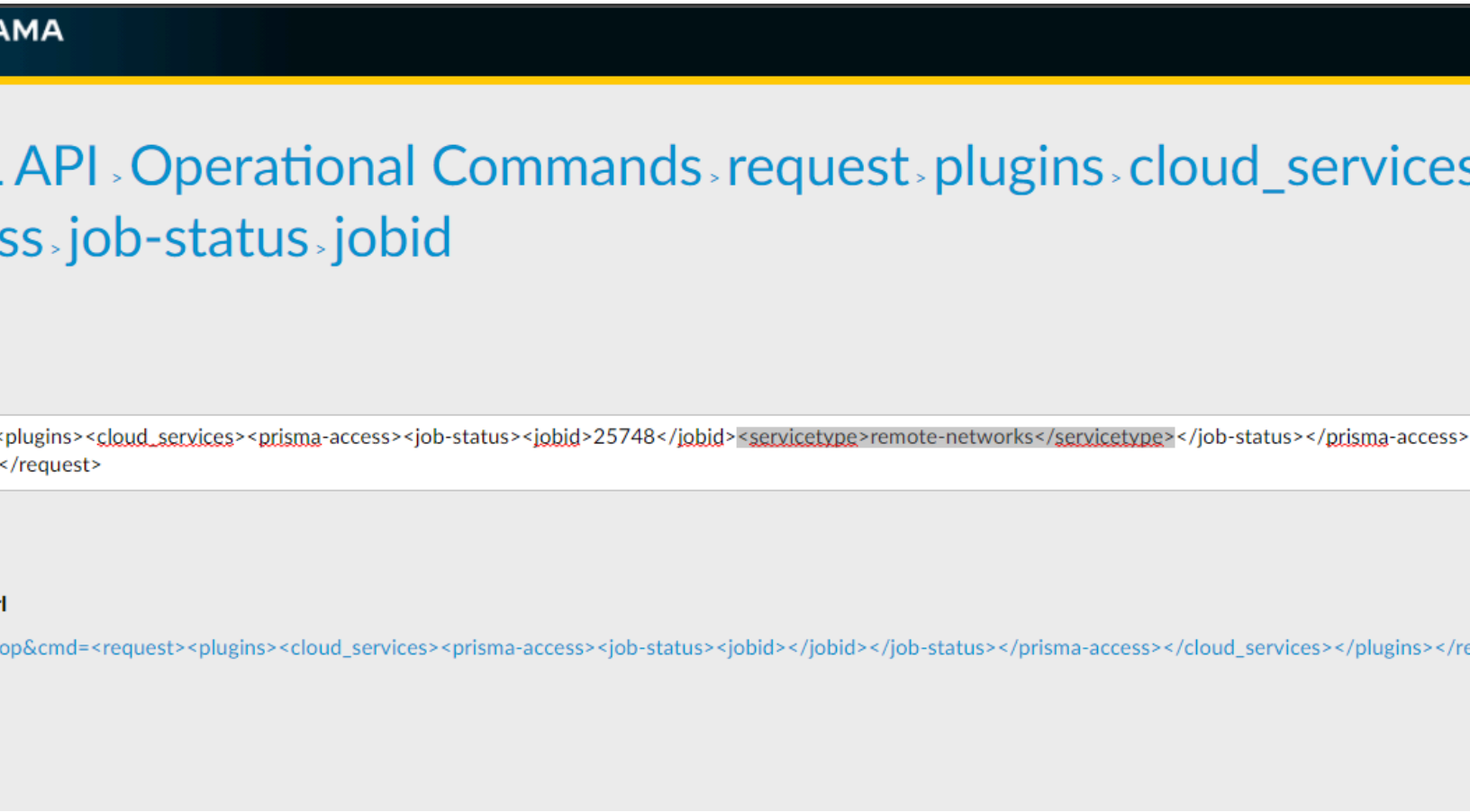
Prisma Access API 位于 XML 树中的以下 XML 路径语言 (XPath) 节点中：

 ©2025 Palo Alto Networks, Inc.

- 配置命令：**XML API** > 配置命令 > **devices** > **entry[@name='localhost.localdomain']** > **plugins** > **cloud_services**
- 操作命令：**XML API** > 操作命令 > **request** > **plugins** > **cloud_services** > **prisma-access**

当您在 XML 树中导航时，Prisma Access 将填充 **XML** 区域中的树。您可以在 **XML** 区域输入所需的值，然后单击 **Submit**（提交）以处理 XML 请求。例如，要请求某个作业的接入状态，请导航到 **XML API** > **Operational Commands**（操作命令） > **request** > **plugins** > **cloud_services** > **prisma-access** > **job-status** > **jobid**，在 **jobid** 字段中输入作业 ID，在 **servicetype** 区域输入服务类型，然后单击 **Submit**（提交）以提交请求。

此 *XML* 仅检索作业的接入状态。要检索所有提交操作的状态，请使用 *Prisma Access UI*。



Prisma Access 以 XML 格式返回输出。

 ©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>
```


您还可以使用 Web 界面在 Panorama 中查找 API。

使用 curl 命令检索 Panorama 托管 API 命令

如果更喜欢使用 CLI 来检索 API 命令结果，则可以将 API 与用于检索 Prisma Access 的公共和基础设施 IP 地址的 API 结合使用。为此，请使用以下命令：

配置命令：

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

操作命令：

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

其中：

- *<panorama-ip-address>* 是管理 Prisma Access 的 Panorama 的 IP 地址。

 ©2025 Palo Alto Networks, Inc.

- *<api-key>* 是 API 密钥，用于检索 Prisma Access 的 IP 地址（**Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Service Setup**（服务设置） > **Generate API Key**（生成 **API** 密钥））。
- *<api-parameters>* 和 *</api-parameters>* 是用于从 API 检索所请求信息的 API 参数。

如果您有一个多租户部署，您可以将要检索其 API 信息的租户的名称添加到 API 中。

例如，给定具有以下参数的 Prisma Access 部署：

- **Panorama IP** 地址：1.2.3.4
- **API** 密钥：12345abcde
- 租户名称：tenant-1

如果要检索该租户的活跃移动用户数量，可以输入以下 curl 命令：

```
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>"
```

将 CLI 命令用于 Prisma Access (Managed by Panorama)

Prisma Access 允许您使用 CLI 命令来检索 Prisma Access 数据。要访问 CLI，请使用管理 Prisma Access 的 Panorama 的 IP 地址建立 SSH 连接。

除了为多租户部署输入租户名称外，CLI 使用与 PAN-OS 命令相同模式并且行为也相同；您将使用 `tenant-name` *tenant-name* 命令输入租户名称。例如，给定租户名称 *tenant-1*，输入以下命令以检索多租户部署中的活跃用户数量：

```
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

Prisma Access Insights API 允许您查询您的 Prisma Access Insights 租户以获取数据资源。有两个版本的 API。Prisma Access Insights 2.0 和 1.0 API 都允许您查询 Prisma Access 租户以了解 Prisma Access 网络部署的运行状况。这两个版本的 API 调用是相同，但每个版本使用的访问令牌不同，并且获取访问令牌的机制在每个版本中也各不相同。

要开始使用 Prisma Access Insights API，请转到位于欢迎使用 Prisma SASE 的开发人员指南。

Prisma Access Insights API 介绍了特定于 Prisma Access Insights API 的内容，还提供了有关 API 版本 2.0、API 版本 1.0、Prisma Access Insights API 示例和 PAI 常见问题解答的信息。

关于 2.0 API

Prisma Access Insights 2.0 API 适用于 Prisma Access (Managed by Strata Cloud Manager) 客户，其中租户已经由 Palo Alto Networks 使用租户服务组 (TSG) 标识符登录。要查看您的租户是否使

 ©2025 Palo Alto Networks, Inc.

用 TSG ID，请前往 Prisma Access 中心，单击 **Prisma Access Insights** 应用程序名称，然后查看 **Manage Apps**（管理应用程序）部分。

Prisma Access (Managed by Panorama) 客户也可以使用 2.0 API。在这种情况下，如果 Prisma Access (Managed by Panorama) 部署是多租户部署，则只有超租户具有 TSG ID，而子租户包含在具有 Strata Logging Service 租户 ID 的标头中。

API 2.0 案例

超级租户迁移到 TSG ID 后，查询子租户时：

标头需要以下信息：`Prisma-Tenant:tsg_id:sub_tenant_id`

关于 1.0 API

Prisma Access Insights 1.0 API 适用于所有 Prisma Access (Managed by Strata Cloud Manager) 单租户客户以及 Prisma Access (Managed by Panorama) 单租户和多租户客户。

API 1.0 案例

在超级租户迁移到 TSG ID 之前，使用 1.0 API 查询子租户信息时，请在端点上包含超级租户 ID：

`/api/sase/v1.0/resource/tenant/{super_tenant_id}/`

在呼叫中包括以下标头：`Prisma-Tenant: {tenant_id}: {sub_tenant_id}`

 ©2025 Palo Alto Networks, Inc.

将 Prisma Access 从 Panorama 迁移到 Strata Cloud Manager

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证 要开始从 Prisma Access (Managed by Panorama) 迁移到 Prisma Access (Managed by Strata Cloud Manager)，请联系您的 Palo Alto Networks 客户团队。

如果您有一个现有的 Prisma Access 部署，其配置由 Panorama 管理，并希望迁移到 Strata Cloud Manager 进行配置管理，Palo Alto Networks 可提供了一个产品内工作流，用于将现有 Prisma Access 配置迁移到 Strata Cloud Manager。

使用 Strata Cloud Manager 代替 Panorama 来管理您的 Prisma Access 配置有以下优势：

- 持续的最佳实践评估
- 安全的默认配置
- 基于机器学习 (ML) 的配置优化
- 简化 Web 安全工作流
- 交互式可视化摘要（命令中心），可帮助您评估网络的运行状况、安全性和效率
- 用于复杂任务的直观工作流
- 简单安全的管理 API
- 云原生架构提供可扩展性、弹性和全球覆盖
- 无需管理硬件，也无需维护软件

准备迁移到 Prisma Access (Managed by Strata Cloud Manager)

在开始迁移之前，应了解最低软件要求以及可以迁移的 Prisma Access (Managed by Panorama) 部署类型。

- 何时迁移—切勿在数据平面或基础设施升级期间执行升级。检查升级首选项，确认是否有即将进行的数据平面升级。
- 从 **Panorama** 到 **Prisma Access (Managed by Strata Cloud Manager)** 的单向迁移—您只能从 Prisma Access (Managed by Panorama) 部署迁移到 Prisma Access (Managed by Strata Cloud Manager) 部署。迁移到 Strata Cloud Manager 后，便无法再回到使用 Panorama 管理 Prisma Access 部署的场景。
- **Panorama** 最低版本—至少需要 Panorama 版本 10.0。
- 所需的管理员角色—您必须以超级用户身份登录 Strata Cloud Manager 才能开始迁移。
- 许可要求—需要有效的 Prisma Access 许可证。

©2025 Palo Alto Networks, Inc.

- **Cloud Identity Engine**—在迁移之前，必须将 Cloud Identity Engine 的目录同步组件与当前的 Prisma Access (Managed by Panorama) 租户集成。
- 不支持的功能—迁移程序不支持 Prisma Access 的以下功能：
  - 多租户部署
  - IoT 安全
  - 数据过滤（可使用 Enterprise DLP 代替）
  - SSH 代理
  - GlobalProtect 门户和网关的单独身份验证
- 配置差异问题—在迁移期间运行配置差异时，请忽略显示以下对象名称的任何差异，因为这些差异不会影响您的配置：
  - Clientless-vpn crypto-settings
  - Hip-profiles rename
  - Mobile-user-redundancy
  - Exclude-video-traffic

将 Prisma Access (Managed by Panorama) 部署迁移到 Strata Cloud Manager

若要将 Prisma Access (Managed by Panorama) 迁移到 Prisma Access (Managed by Strata Cloud Manager) 部署，请完成以下步骤。

总体来说，您需要：

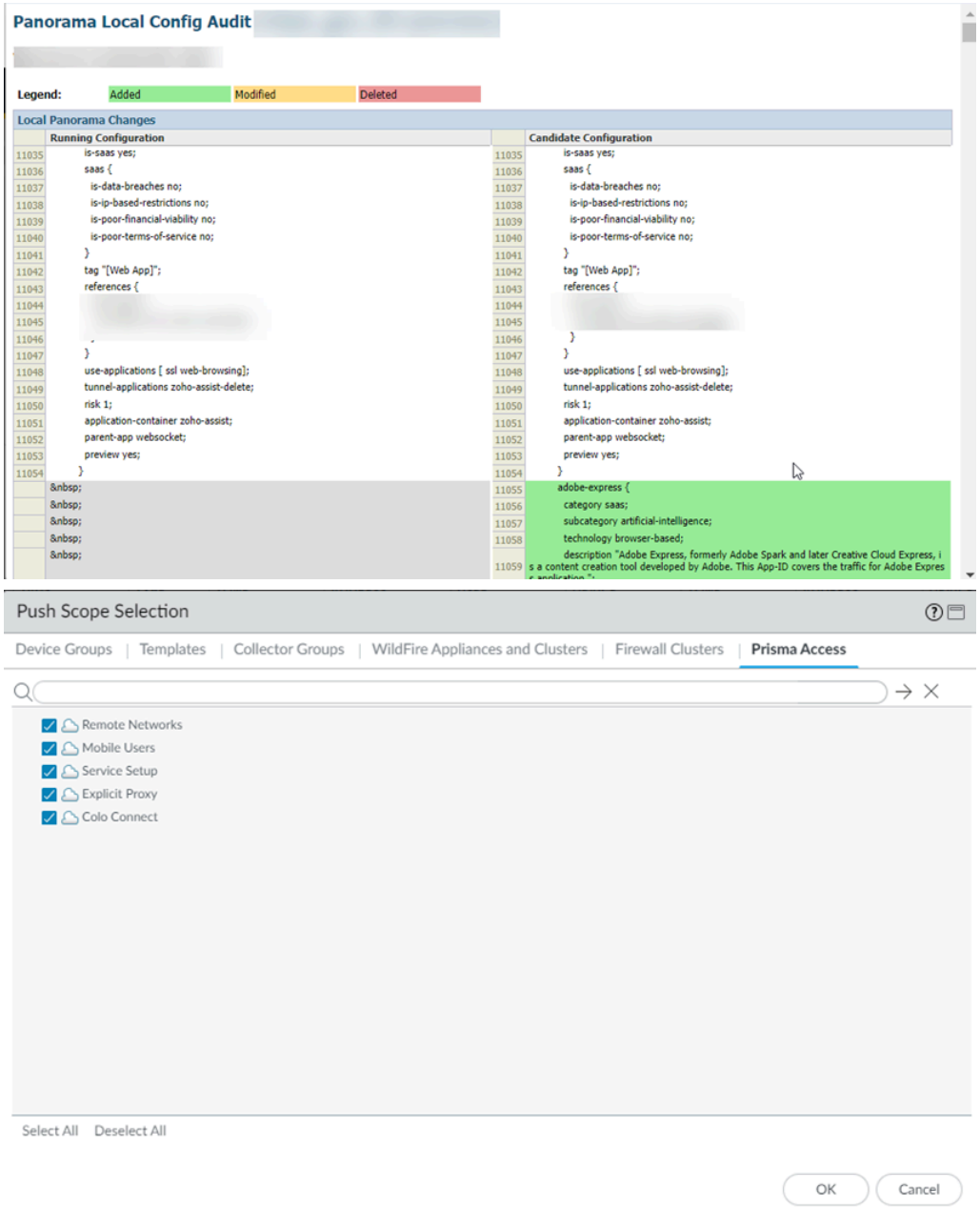
1. 请确保您已成功将最新配置推送到 Prisma Access，已保存最新配置，并已从管理 Prisma Access 的 Panorama 中导出了 .xml 配置文件。
2. 从 Strata Cloud Manager 启动迁移程序。
3. 检查 Panorama 配置与迁移的 Strata Cloud Manager 配置之间的配置差异（即“差异”）。
4. 解决差异并完成迁移。

©2025 Palo Alto Networks, Inc.

STEP 1 | 准备好 Panorama 的迁移工作

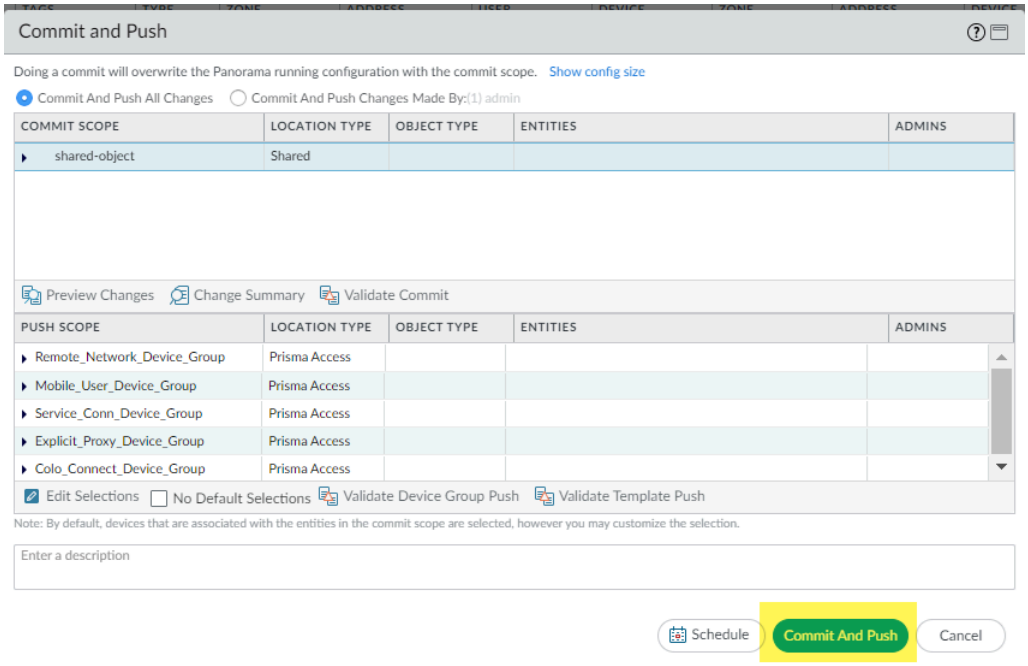
1. 登录到管理 Prisma Access 的 Panorama，并且要使用被分配了超级用户角色的管理帐户。
2. (可选) 如果您已为 Panorama 和 Prisma Access 配置了自定义主密钥，请记下来。

   如果您的部署使用默认主密钥，则不需要执行此步骤。
3. 确保您当前的 Panorama 配置是最新的，并且您已通过转到 **Commit**（提交） > **Commit & Push**（提交并推送） 以及 **Preview Changes**（预览更改），将所有更改提交并推送到 Panorama 和 Prisma Access。
4. （可选）检查运行配置和候选配置之间的差异，并确定是否要推送这些更改。如果您想要提交并推送这些更改，请单击 **Edit Selections**（编辑选择项），然后在 **Push Scope**（推送范围）中选择您想要推送的 Prisma Access 组件。



 ©2025 Palo Alto Networks, Inc.

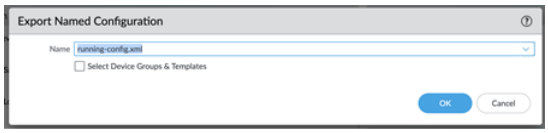
5. （可选）选择 **Commit and Push**（提交并推送）以提交并推送更改。



6. 转到 **Panorama** > **Setup**（设置） > **Operations**（操作），然后单击 **Export named Panorama configuration snapshot**（导出命名的 **Panorama** 配置快照）。

   在迁移过程中，需要将此 .xml 文件上传到 Strata Cloud Manager。请勿上传技术支持文件或除 **.xml** 配置文件以外的任何其他文件。

7. 选择 **running-config.xml** 配置文件，然后单击 **OK**（确定）。

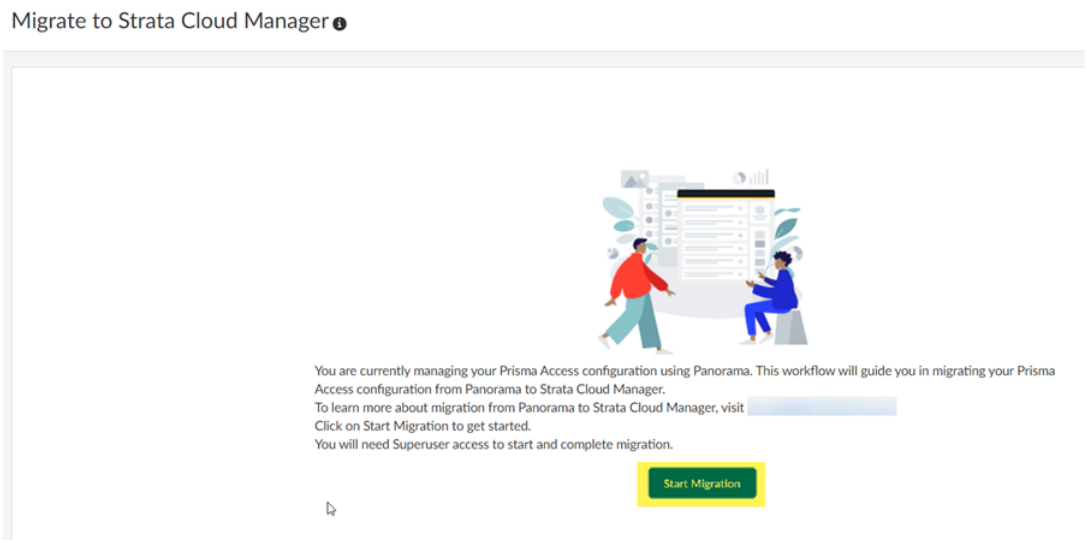


STEP 2 | 使用具有超级用户角色的管理员身份登录到 Strata Cloud Manager，然后转到 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（新一代防火墙和**Prisma Access**）。

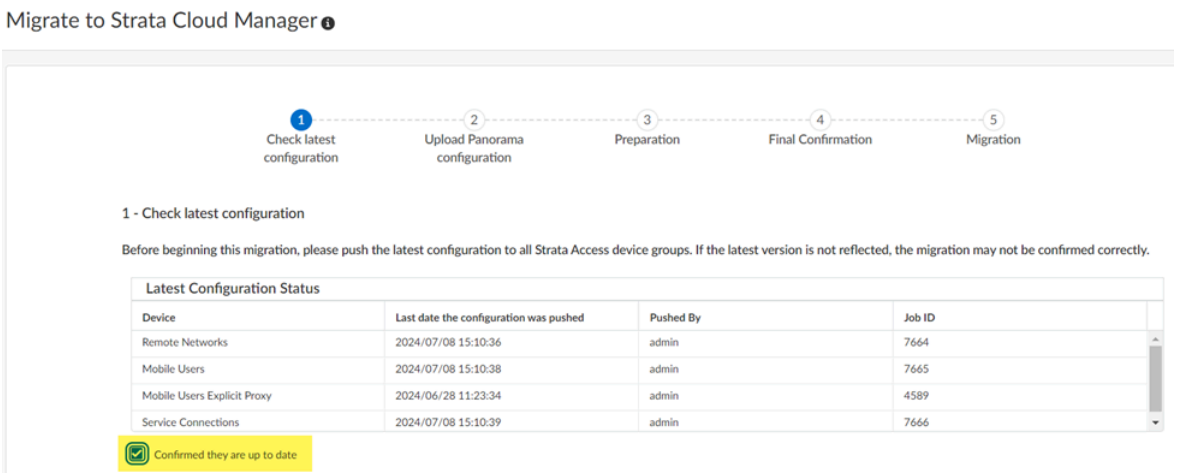
迁移程序检测到您采用了 Panorama 托管部署。

 ©2025 Palo Alto Networks, Inc.

STEP 3 | 开始迁移。



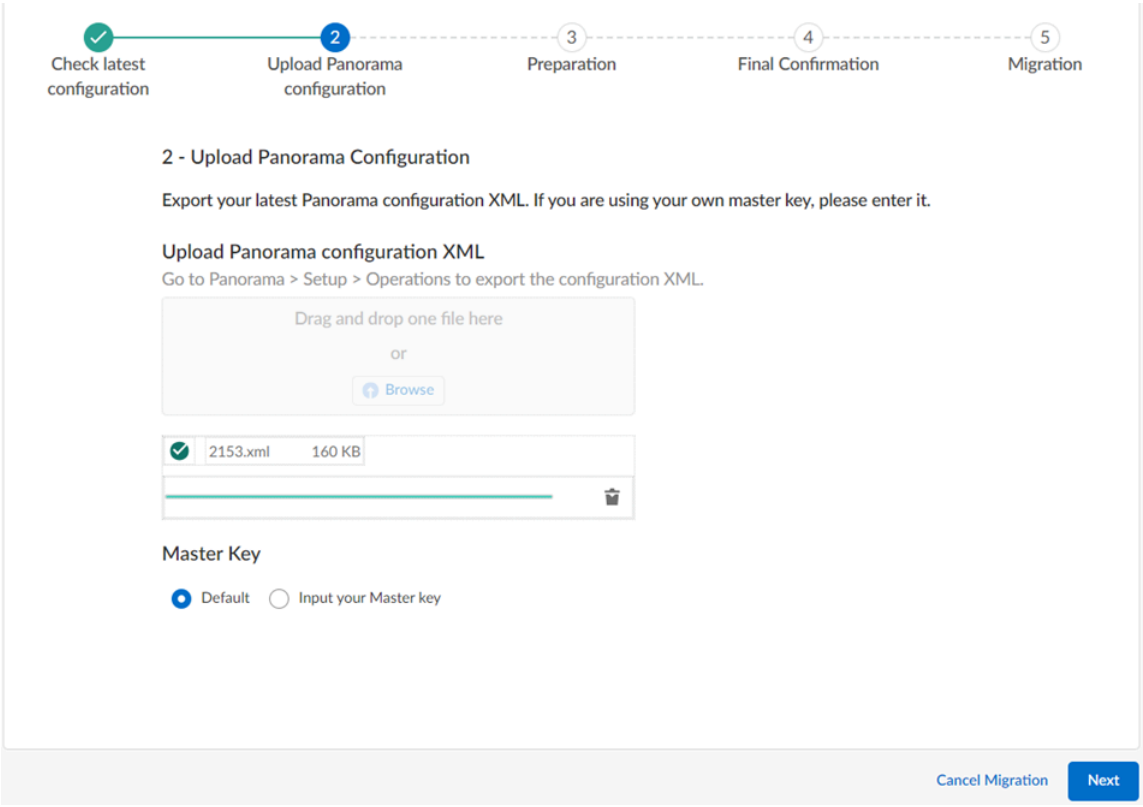
STEP 4 | 迁移程序要求您确保配置是最新的，并显示上次更新配置的用户。在您确认此配置包含了最新的更改之后，选择 **Confirmed they are up to date**（已确认它们是最新的），然后单击 **Next**（下一步）。



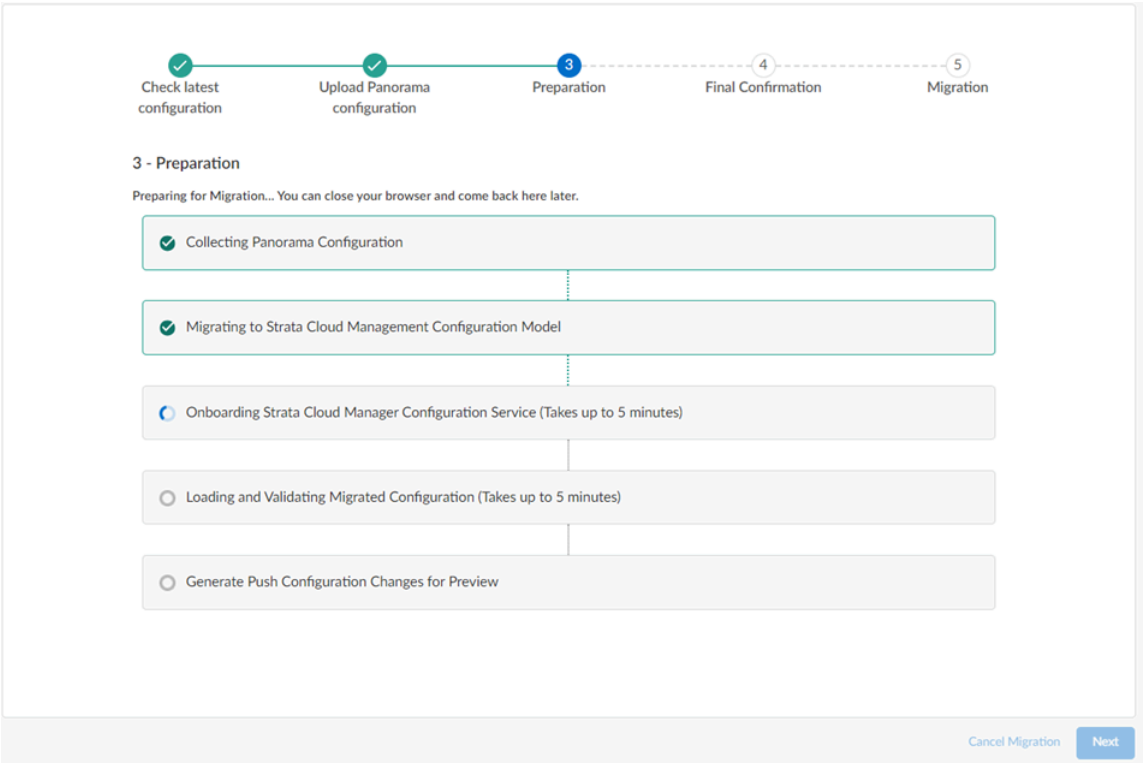
STEP 5 | 通过拖放操作，或者单击 **Choose File**（选择文件），来选择您在之前步骤中下载的 Panorama 配置 .xml 文件。

 ©2025 Palo Alto Networks, Inc.

STEP 6 | 在 **Master Key**（主密钥）中输入您的主密钥，如果您没有创建自定义的主密钥，请让 Strata Cloud Manager 使用 **Default**（默认值）主密钥，然后单击 **Next**（下一步）。



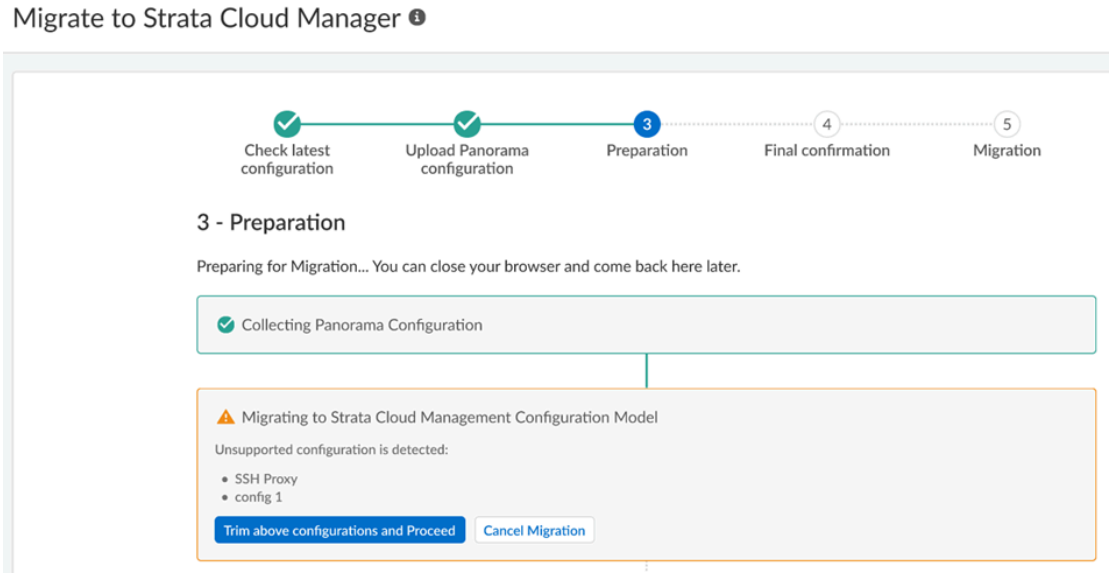
迁移程序随即开始。



©2025 Palo Alto Networks, Inc.

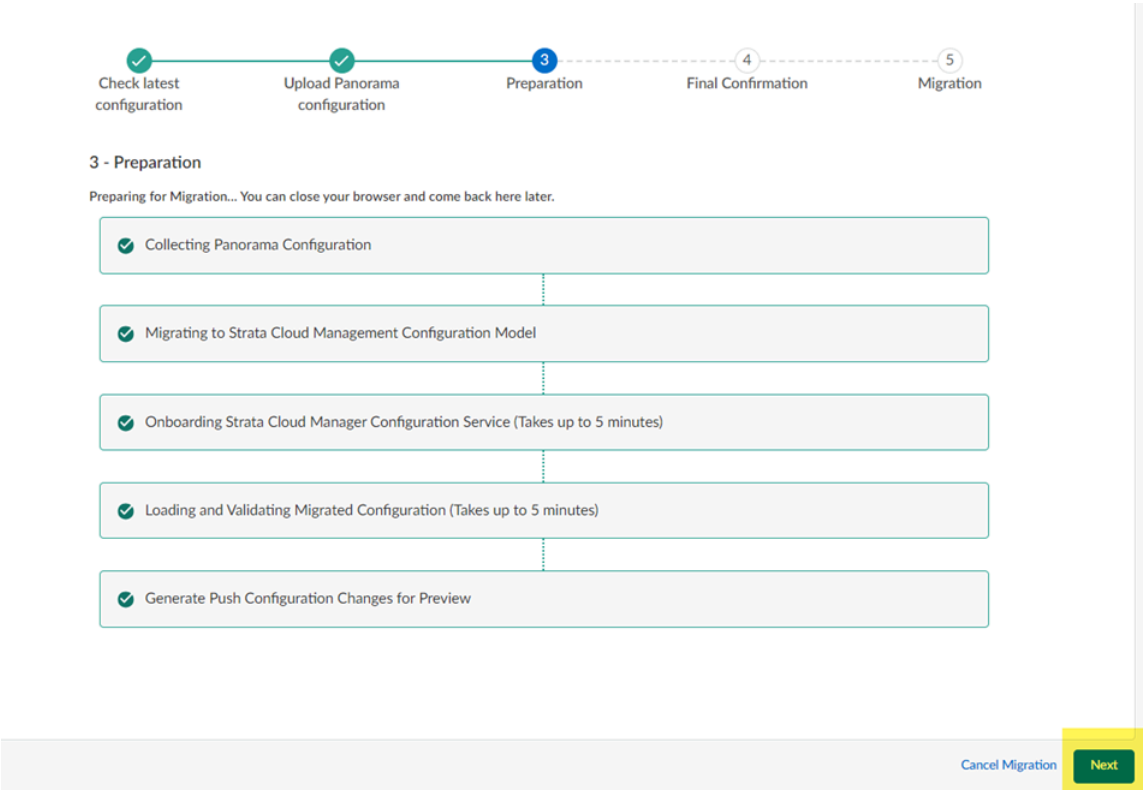
等待所有步骤完成。

STEP 7 | 如果在迁移过程中，程序显示它遇到了一个不支持的配置，可以单击 **Trim the above configurations and proceed**（修剪上述配置并继续），或者单击 **Cancel migration**（取消迁移）。



一些不支持的配置（例如多租户配置）会导致取消迁移，并且迁移程序无法解决该问题；在这种情况下，请单击 **Cancel Migration**（取消迁移）。

STEP 8 | 迁移完成后，单击 **Next**（下一步）。



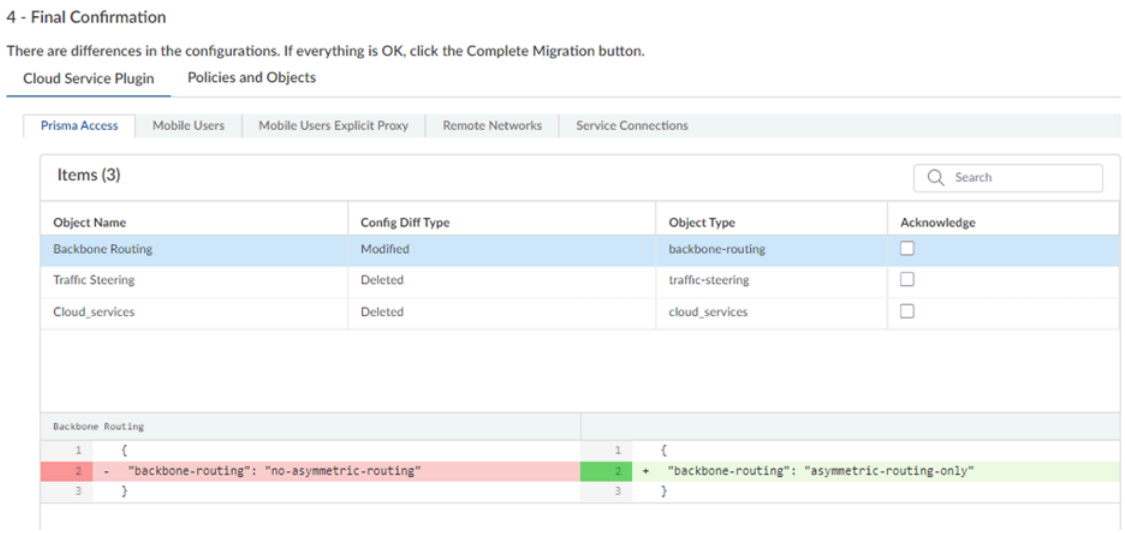
 ©2025 Palo Alto Networks, Inc.

STEP 9 | 如果迁移程序进行了更改，请在最终确认屏幕中查看这些更改。

迁移程序可能会对您的配置进行更改，以处理 Panorama 和 Strata Cloud Manager 配置之间的差异，或者修复不被支持的功能。如果需要进行更改，迁移程序会在差异视图中显示这些更改内容，新增的行以绿色显示，删除的行以红色显示。

忽略显示以下对象名称的任何差异；它们不会影响您的配置：

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



STEP 10 | （可选）对差异进行更改。

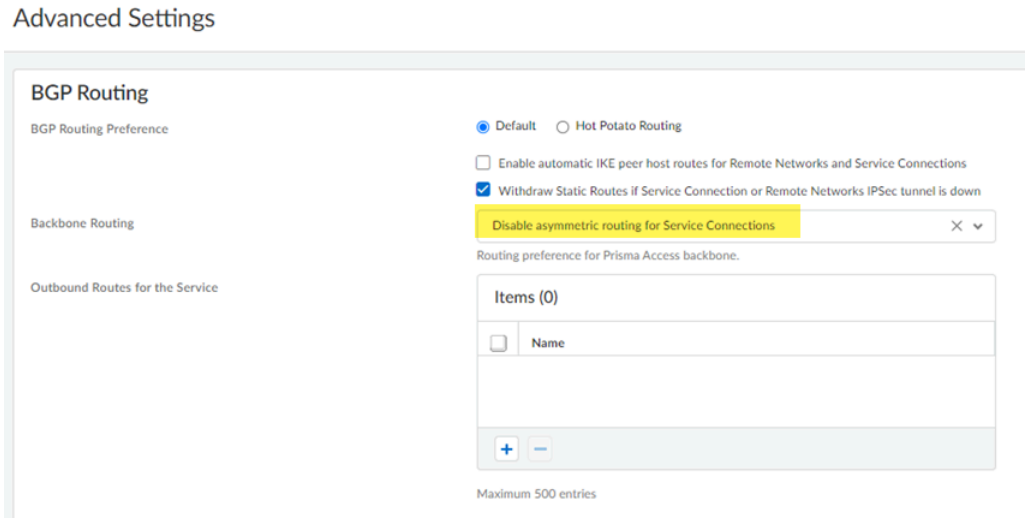
在您完成迁移并将更改推送到 Strata Cloud Manager 之前，您所做的任何更改都不会提交到配置中。

1. 导航到 Prisma Access 配置中找到差异的区域，并对配置进行更改。

   对于上一步中的示例，迁移程序对骨干网路由进行了更改（从 **no-asymmetric-routing** 更改为 **asymmetric-routing-only**）。要将此设置改回您原来的配置，请转到 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Service Connections**（服务连接） > **Advanced Settings**（高级设置） >，然后将 **Backbone**

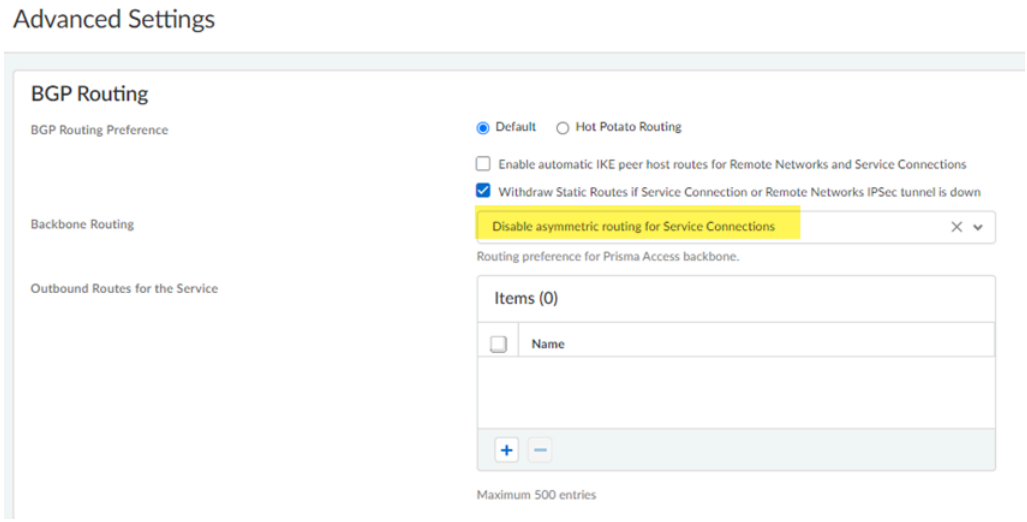
 ©2025 Palo Alto Networks, Inc.

Routing（骨干网路由） 配置更改为 **Disable Asymmetric Routing for Service Connections**（禁用服务连接的非对称路由）。



2. （可选）要跟踪您的更改，请在完成更改时单击 **Acknowledge**（确认）。

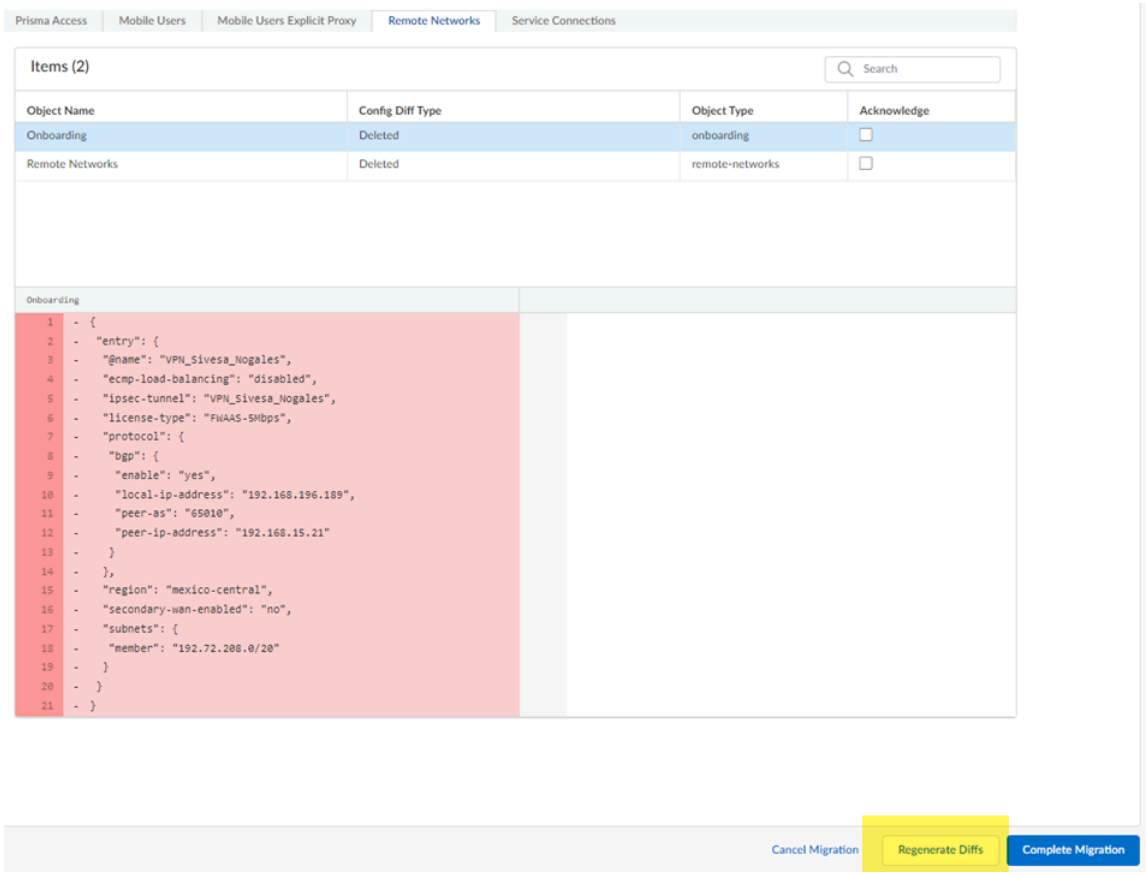
   虽然并非必需操作，但在您进行每一项更改时确认一下这些更改会很有用，这样您就可以跟踪更改。



3. 继续检查更改并进行更改和确认。

 ©2025 Palo Alto Networks, Inc.

STEP 11 | （可选）如果对配置进行了任何更改，请单击 **Regenerate Diffs**（重新生成差异）以查看更新的差异。

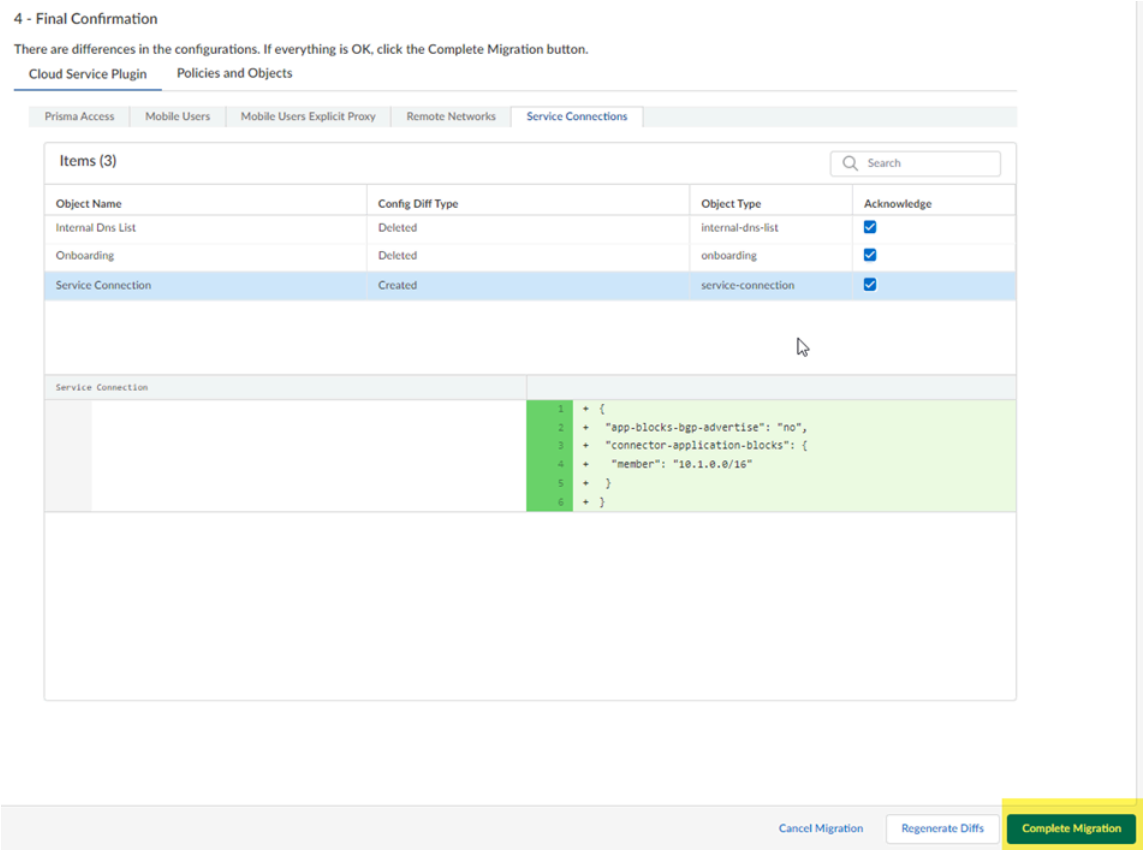


 ©2025 Palo Alto Networks, Inc.

STEP 12 | 完成迁移。

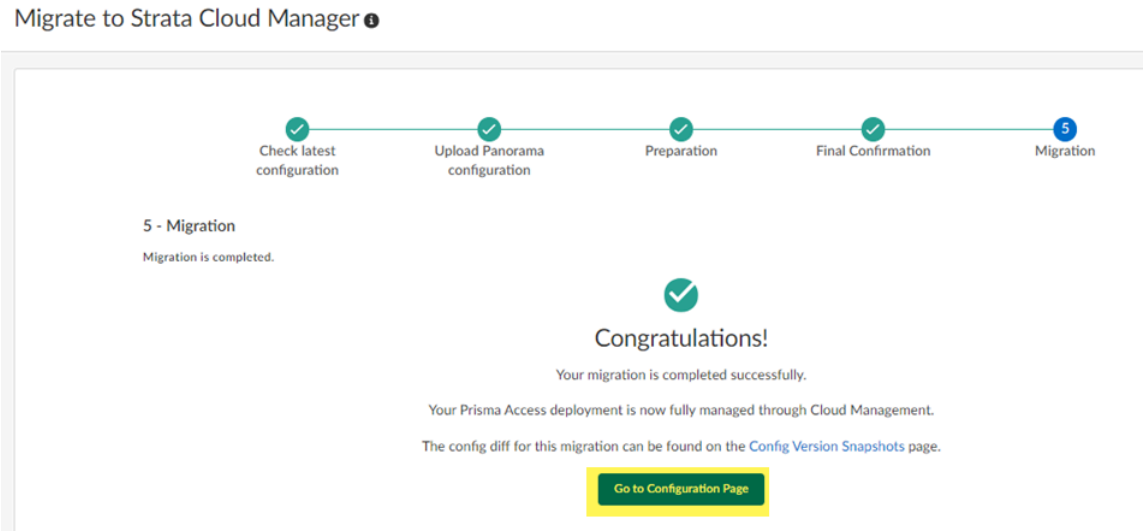
您也可以单击 **Acknowledge**（确认）以确认您的更改（但不强制要求）。

单击 **Complete Migration**（完成迁移）后，您将无法返回到 **Panorama** 托管部署，并且您的部署将永久使用 **Strata Cloud Manager** 来进行管理。

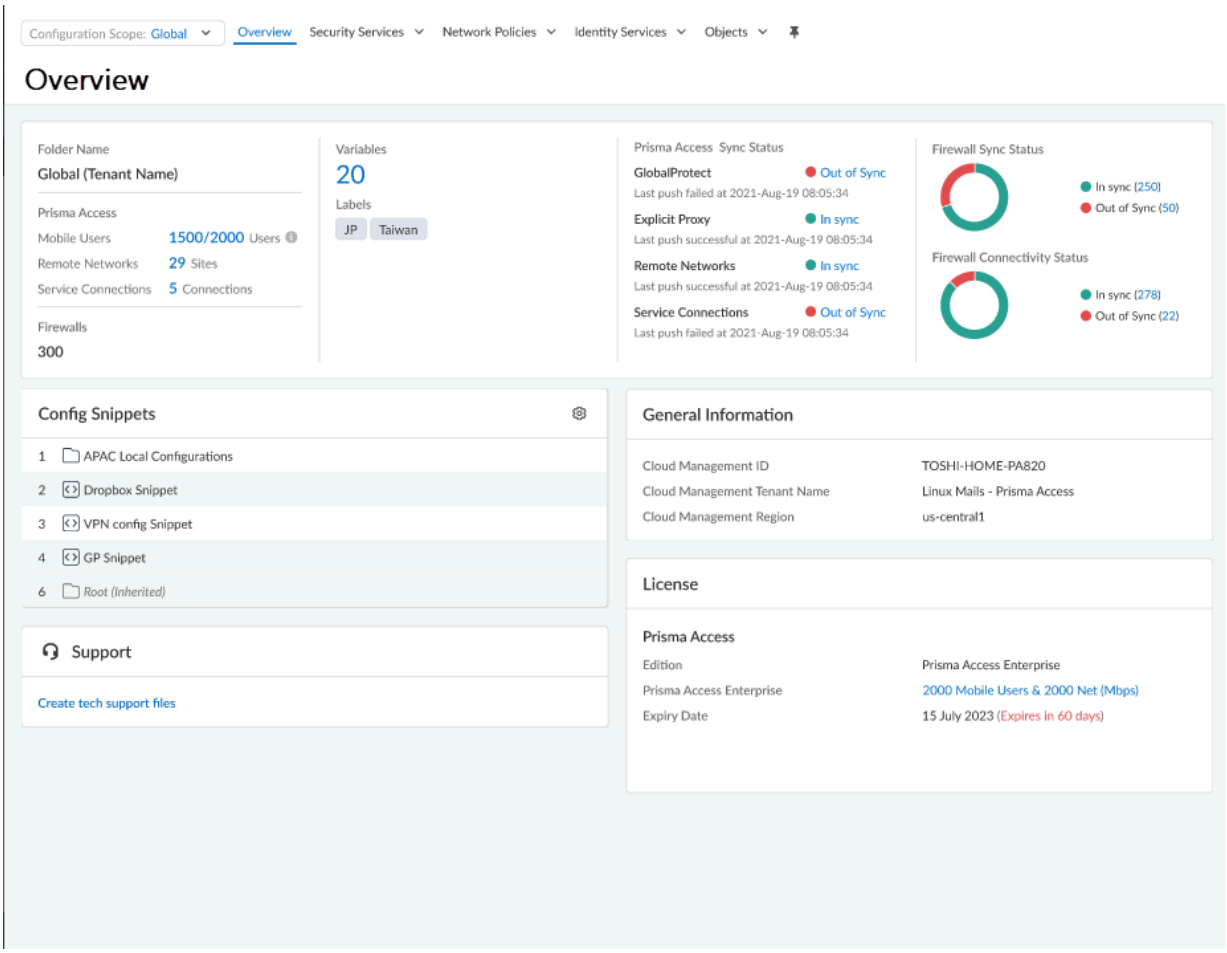


 ©2025 Palo Alto Networks, Inc.

STEP 13 | （可选）单击 **Go to Configuration Page**（转到配置页）以查看迁移的配置。



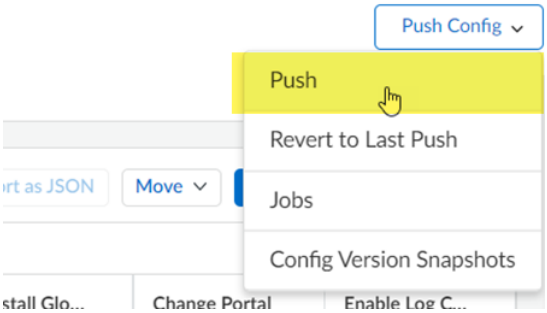
此时将显示迁移的部署。



 ©2025 Palo Alto Networks, Inc.

STEP 14 | 单击 **Push Config**（推送配置） > **Push**（推送）以应用您已迁移的配置更改。

此推送操作可确保迁移已成功完成，并且 Prisma Access 已将所有更改应用于迁移的配置。



STEP 15 | 记下推送操作期间收到的任何消息，如果发现任何问题，请根据需要对配置进行更改。

©2025 Palo Alto Networks, Inc.

Prisma Access 版本和升级

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

Prisma Access 发行和更新使您能够保持最新状态并确保用户安全。部分更新由 Palo Alto Networks 管理，例如 Prisma Access 基础设施更新，您将提前收到通知，以便您可以制定周全计划。其他更新由您负责，您必须尽早安排指定版本的内容更新、软件更新和插件版本（根据需要）。

通过访问 https：//sase.status.paloaltonetworks.com/ 网站，您可以检索所有云服务（包括 *Prisma Access* 和 *Strata Logging Service*）的状态以及每个服务正常运行时间的历史记录。您还可以在该网站注册以接收电子邮件或短信通知。这样，当有基础设施更新计划时，您会提前收到通知；更新发生时，您会收到实时通知；而且当 *Palo Alto Networks* 创建、更新或解决某个事件时，您也会得到相应通知。

Prisma Access 版本类型

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

Prisma Access 有升级，涉及主要版本和基础架构维护，其中包括为您的远程网络和移动用户提供最佳安全性的新功能和优化。

以下列表定义了发布类型，以及我们为每个发布提供的预先通知。为了确保您收到所有发布的通知，请在 https://sase.status.paloaltonetworks.com/ 网站上为 Prisma Access 注册电子邮件或短信通知，并在 Strata Cloud Manager 中注册提醒。

- 主要版本 — 主要版本通常包含重要的新功能和优化，并且此类更新会通过 Palo Alto Networks 设置的计划维护窗口进行推送。Palo Alto Networks 通过 sase.status.paloaltonetworks.com 以电子邮件通知形式向客户告知此类计划维护活动。

  通知 — Palo Alto Networks 提供以下主要版本的通知：

部署类型	通知期限
生产部署	Palo Alto Networks 会在主要版本发布前 21 天发出通知。
VPN 部署	Palo Alto Networks 会在主要版本发布前 7 天发出通知。

  除了计划的主要版本升级外，*Palo Alto Networks* 可能还需要进行紧急计划升级，这些升级遵循不同的时间表。

  实验室租户不属于 Prisma Access 服务水平协议 (SLA)，强烈建议客户仅将租户用于预生产测试和资格鉴定目的。

- 基础架构维护 — 包括增量功能和优化。在某些情况下，Palo Alto Networks 可能会将修补程序与基础架构维护结合在一起。

  通知 — Palo Alto Networks 提供以下通知：

部署类型	通知期限
生产部署	Palo Alto Networks 在基础设施维护前 10 天发出通知。

©2025 Palo Alto Networks, Inc.

部署类型	通知期限
VPN 部署	Palo Alto Networks 在基础设施维护前 7 天发出通知。

除了计划的主要版本升级外，*Palo Alto Networks* 可能还需要进行紧急计划升级，这些升级遵循不同的时间表。

- 云服务插件版本（仅限 **Panorama** 管理的部署）— 如果 Prisma Access 需要新插件，可以在版本正式发布 (GA) 日期通过 Palo Alto Networks 客户支持门户 (CSP) 和 Panorama 下载。

  Prisma Access 可能会强制所有租户升级到特定的云服务插件版本，以保持向后兼容性和支持的软件版本。此类强制活动将提供 **14** 天的预先通知（通过 sase.status.paloaltonetworks.com 页面）来规划插件的升级。该服务强烈建议您在最新插件可供下载时立即升级。

紧急计划升级

Palo Alto Networks 偶尔需要执行紧急数据平面或基础架构升级，其中包括修补程序或紧急错误修复（例如，针对零日威胁或插件更改的修复）。Palo Alto Networks 将尽力在紧急计划升级前 48 小时通知您；但是，您有时可能会收到时间更短的紧急计划升级通知。

©2025 Palo Alto Networks, Inc.

Prisma Access 升级类型

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

Palo Alto Networks 升级其基于云的基础设施，无需您进行任何干预。某些升级需要您执行某项操作，例如安装新插件。

以下列表包括不同类型的 Prisma Access 升级：

- 基础架构升级 — Palo Alto Networks 升级了 Prisma Access 基础架构，也称为 Prisma Access 控制平面，其中包括底层服务后端、编排和监控基础架构。

  您预计每年将收到 4 至 6 次基础设施升级。
- 数据平面升级 — Palo Alto Networks 升级了 Prisma Access 数据平面，可对您的网络和用户流量进行流量检查并实施安全策略。

  您使用该应用程序注册数据平面升级电子邮件警报通知并指明您的升级首选项。
- **Prisma Access 计划维护** — Prisma Access 每两周预留一次时间来执行与基础设施的修补程序和紧急错误修复相关的维护。
- （仅限 Panorama 托管部署）云服务插件升级 — 当有新插件版本可用时，您的网络管理员需要升级管理 Prisma Access 的 Panorama 设备上的云服务插件。
- （仅限 Panorama 托管部署） **Panorama** 软件版本升级 — 可能需要 升级您的 Panorama 软件以确保继续兼容 Prisma Access。

下表显示了每个版本中包含的内容，包括我们提供的维护窗口以及对 Prisma Access 服务的任何影响。

升级类型	维护时段	影响
基础架构升级	2-8 小时	对网络流量没有影响；但是您无法在维护时段内执行提交。 Palo Alto Networks 将升级安排在当地时间进行，以尽量减少对业务功能的干扰。
数据平面升级	72 小时	Palo Alto Networks 使用此窗口为所有客户升级数据平面。您可以在此窗口期间进行配置更改和提交。我们的目标是尽量减少对网络流量的影响，但在某些情况下可能会出现短暂的中断。如需更多信息，请参

©2025 Palo Alto Networks, Inc.

升级类型	维护时段	影响
		阅 Prisma Access 数据平面升级。 使用该应用程序注册数据平面升级电子邮件警报通知并指明您的升级首选项，包括升级的首选时间窗口。
云服务插件升级（仅限 Panorama 管理部署）	当插件可用时，您可以安装它。	Prisma Access 可能要求您将所有租户升级到特定插件版本以保持向后兼容性和支持的软件版本。 在插件升级期间，您无法在 Panorama 中进行配置更改和提交。
Panorama 软件版本升级（仅限 Panorama 管理部署）	您可以在管理 Prisma Access 的 Panorama 上计划和执行升级。	当 Prisma Access 在主要版本发布后升级基础架构和数据平面时，升级可能与早期版本的 Panorama 不兼容。由于 Prisma Access 和云服务插件经常发布新版本，Panorama 的软件兼容性（终止支持）日期比 Panorama 版本的软件终止支持日期要短，并且仅适用于与 Prisma Access 兼容的 Panorama 版本。有关详细信息，包括 Panorama 与 Prisma Access 配合使用时的支持终止日期，请参阅 Palo Alto Networks 兼容性矩阵中的 Prisma Access 和 Panorama 版本兼容性。

©2025 Palo Alto Networks, Inc.

Prisma Access 的软件和内容更新频率

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

- Strata Cloud Manager
- Panorama

Prisma Access (Managed by Strata Cloud Manager) 的软件和内容更新频率

下表描述了 Prisma Access 如何更新其基础架构组件，包括内容和软件更新。此表还指示 Prisma Access 是否会自动更新软件。如有任何更新并非自动进行，您可以了解如何应用这些基础架构更新。

您还可以从中心查看所有云服务的状态。

组件	更新时间表	注释
GlobalProtect 应用程序	• **GlobalProtect** 应用程序主要版本（例如 **x.0** 或 **4.*x***）—Prisma Access 会在 *x.0.1* 版本正式发布后 7-10 天内，使用最新的主要版本更新应用程序。 例如，假设应用程序版本为 4.0，Prisma Access 会在 4.0.1 版本正式发布后 7-10 天内更新应用程序。 • **GlobalProtect** 应用程序次要版本（例如 **4.1.*x***）—Prisma Access 会在该版本正式发布后 7-10 天内，使用最新的次要版本更新应用程序。	通过云端控制可供升级的应用程序版本。
Prisma Access 基础架构中的 PAN-OS 软件升级 — 已计划	当发布 Prisma Access 的新版本时，Palo Alto Networks® 会升级 PAN-OS 基础架构。Palo Alto Networks® 会在计划升级前三周通知您。	注册后即可通过电子邮件或短信通知在中心接收基础架构升级信息。
应用程序和威胁更新	每天，阈值为 24 小时。 Palo Alto Networks® 会在每个月的第三个星期二发布新建 App-ID。计划在 24 小时阈	

©2025 Palo Alto Networks, Inc.

组件	更新时间表	注释
	值内审核并整合这些新建 App-ID。使用新建 App-ID 筛选器可最大限度地减少这种可能的流量影响。 新建 App-ID 特性可让您查看网络上的新应用程序，并显示有关新分类的应用程序活动的详细信息。您所掌握的内容将有助于您做出有关如何更新您的安全策略以实施最新分类的 App-ID 的正确决策。	
防病毒保护	每小时，整点过后 10 分钟	Prisma Access 始终与最新的防病毒软件版本保持同步。
WildFire	实时	Prisma Access 始终与最新的 WildFire 版本保持同步。
GlobalProtect 数据文件	每小时	Prisma Access 始终与最新的 GlobalProtect 数据文件版本保持同步。
无客户端 VPN 应用程序签名	每小时	Prisma Access 始终与最新的无客户端 VPN 应用程序签名版本保持同步。

Prisma Access (Managed by Panorama) 的软件和内容更新频率

下表向您介绍软件和内容更新，以便您获取最新的应用程序和威胁签名，并利用 Palo Alto Networks 提供的威胁防护功能。如果 **Cloud Controlled?**（是否通过云端控制？）列的属性为 **No**（否），则您可以执行所需的操作来更新组件。

组件	更新时间表	是否通过云端控制？（是/否）	注释
升级 Panorama 软件以兼容 Prisma Access	对于 Prisma Access 主要版本，您可能需要针对以下用例升级 Panorama 版本： • 需要升级 — 有时，您需要升级 Panorama 上的软件版本，以保持	否	请参阅 Panorama 软件版本与 Prisma Access 兼容性的支持终止 (EoS) 日期，了解 Panorama 版本将于何时不兼容 Prisma Access。请参阅 Prisma Access 与 Panorama 版本的兼容性，了解当

©2025 Palo Alto Networks, Inc.

组件	更新时间表	是否通过云端控制？（是/否）	注释
	与 Prisma Access 的兼容性。 • 维护时段 — 您的组织需要安排维护时段来升级 Panorama 软件版本。 • 影响 — 您必须升级 Panorama 版本才能使用新版本的插件。 • 通知 — Palo Alto Networks 将在计划的主要版本升级前 100 天向您发送通知。 • 可选升级 — 在其他情况下，您可能需要升级 Panorama 软件版本才能使用 Prisma Access 在主要版本中支持的新功能。 • 维护时段 — 您的组织需要安排维护时段来升级 Panorama 软件版本。 • 影响 — 您必须升级 Panorama 才能使用 Prisma Access 支持的新功能。 • 通知 — Palo Alto Networks 将在计划的主要版本升级（如 Prisma Access 版本类型 中所定义）前 21 天通知您任何		前支持的可用于 Prisma Access 的 Panorama 版本。要将 Panorama 升级到新版本，请参阅安装 Panorama 的内容和软件更新。

©2025 Palo Alto Networks, Inc.

组件	更新时间表	是否通过云端控制？（是/否）	注释
	Panorama 要求。		
云服务插件版本	插件发布后可用。	否	您需要执行任务来升级插件。有关 Prisma Access 何时更新其插件版本的详细信息，请参阅 Prisma Access 版本类型。请参阅升级云服务插件，以升级 Panorama 设备中的插件。
GlobalProtect 应用程序	• **GlobalProtect** 应用程序主要版本（例如 **x.0** 或 **5.*x***）—Prisma Access 会在 *x*.0.1 版本正式发布后 7-10 天内，使用最新的主要版本更新门户上的代理。 例如，假设代理版本为 5.1，Prisma Access 会在 5.1.1 版本发布后 7-10 天内更新门户上的代理。 • **GlobalProtect** 应用程序次要版本（例如 **5.1.*x***）—Prisma Access 会在该版本正式发布后 7-10 天内，通过最新的基础架构维护更新门户上的代理。	是	通过云端控制可供升级的应用程序版本；但是，您可以在应用程序的多个不同的托管版本之间进行选择，并可以控制如何以及何时向最终用户推出 GlobalProtect 应用程序更新。有关详细信息，请参阅GlobalProtect 应用程序升级。 如果您的 Prisma Access 部署需要 GlobalProtect 应用程序的修补程序，请向 Palo Alto Networks 技术支持部门提交支持案例以寻求帮助。
应用程序和威胁更新	每天，阈值为 24 小时。 Palo Alto Networks 会在每个月的第三个星期二发布新建 App-ID。计划在 24 小时	是	

©2025 Palo Alto Networks, Inc.

组件	更新时间表	是否通过云端控制？（是/否）	注释
	阈值内审核并整合这些新建 App-ID。 新建 App-ID 特性可让您查看网络上的新应用程序，并显示有关新分类的应用程序活动的详细信息。您所掌握的内容将有助于您做出有关如何更新您的安全策略以实施最新分类的 App-ID 的正确决策。		
防病毒保护	每小时，整点过后 10 分钟	是	Prisma Access 始终与最新的防病毒软件版本保持同步。
WildFire	实时	是	一旦 WildFire 公共云能够生成新发现的恶意软件的 WildFire 签名，Prisma Access 就会检索这些签名。
GlobalProtect 数据文件	每小时	是	Prisma Access 始终与最新的 GlobalProtect 数据文件版本保持同步。
无客户端 VPN 应用程序签名	每小时	是	Prisma Access 始终与最新的无客户端 VPN 应用程序签名版本保持同步。

©2025 Palo Alto Networks, Inc.

Prisma Access 数据平面升级

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证

Prisma Access (Managed by Strata Cloud Manager) 自动执行数据平面升级，无需任何干预。

Prisma Access 在该服务上执行数据平面升级，以便提供新的安全特性和功能，帮助保护组织的最终用户、业务资产和数字化转型。当新版本的 Prisma Access 需要数据平面升级时，您需要了解升级过程的工作原理，并在升级之前具备所需的前提条件。

您可以期望您的数据飞机每年升级一到两次。某些版本除了提供所需的数据平面升级之外，可能还提供可选的数据平面升级，以支持需要它的 Prisma Access 功能。

- 数据平面升级概述
- 数据平面升级示例

数据平面升级概述

Prisma Access 在两个周末日期分两个阶段升级数据平面，并使用 Strata Cloud Manager 随时通知您升级情况。在高级别上，在升级过程中执行以下步骤。

- 来自 Strata Cloud Manager 的电子邮件通知将在预定数据平面升级开始日期之前 21 天到达。此电子邮件通知为阶段 1 提供数据平面升级开始日期。

  您可能会看到 *Strata Cloud Manager* 填充 *21* 天通知之前的日期，但在收到 *21* 天通知之前，此日期可能不是最终日期。
- 在电子邮件中，系统会要求您选择并提交要首先升级的位置以及通过 Strata Cloud Manager 升级的首选时间窗口。

  您可以多次更改并提交给定租户的第一个升级地点和时间窗口。服务将为升级选择在计划开始日期前七天发生的最后一次提交。升级开始日期后 7 天内，您无法进行任何更改。

  如果进行更改，可能需要最多 30 分钟才能在 Insights 上的“升级仪表板”中显示所做的更改。Prisma Access 处理并完成更改后，将通过电子邮件提醒通知您。

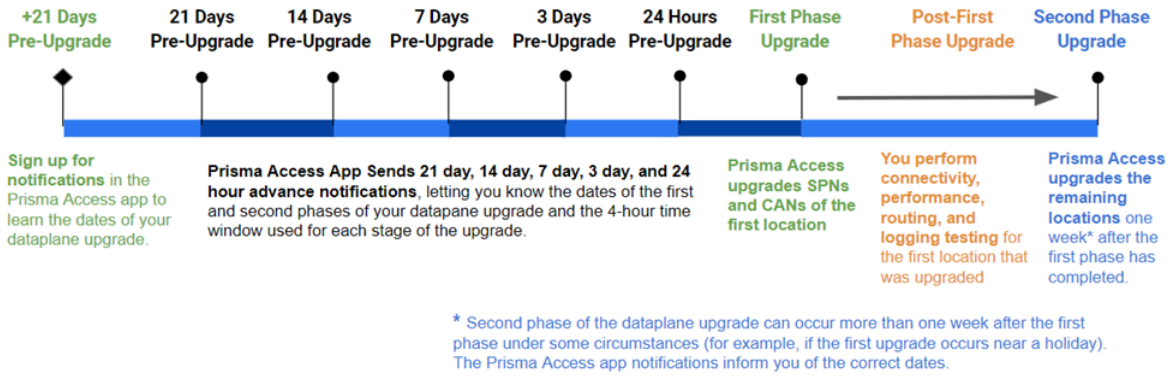
  *Palo Alto Networks*强烈建议您选择能够反映整个部署的位置。例如，如果您有移动用户、服务连接和远程网络部署，请选择具有所有部署类型的一个或多个位置。
- Prisma Access 将在为所选位置选定的一个或多个本地时间窗口内执行升级的第 1 阶段。
- 如果所选升级位置具有“移动用户—GlobalProtect”、“移动用户—显式代理”、服务连接或远程网络的任意组合，则每个部署的数据平面都将升级到所需的数据平面版本，如本节后面所述。
- 在第一个位置完成升级后，您将收到一封通过 Strata Cloud Manager 发送的电子邮件通知。Palo Alto Networks 建议您监视服务，了解数据平面升级后立即出现的任何新问题。

©2025 Palo Alto Networks, Inc.

- 万一您发现新问题，必须向 Palo Alto Networks 技术支持团队报告。

  该技术支持团队将调查问题并采取纠正措施，可能还包括回滚到以前的数据平面版本。这一决定将通过技术支持案例传达给您。
- 如果没有新问题或新问题与升级无关，Prisma Access 将在下一个周末继续进行数据平面升级。
- 其余地点的升级将在您为首次升级选择的同一时间窗口内进行(当地时间)。
- 数据平面升级完成后，您将通过电子邮件警报收到通知。
- 如果在数据平面升级后需要进行插件升级，Palo Alto Networks 建议您在数据平面升级完成后升级插件。

下图显示了升级使用的时间线，包括数据平面升级需要执行的任务（以绿色显示）以及 Prisma Access 执行的步骤。



以下部分提供有关数据平面升级过程的更多详细信息。

在注册通知后，Prisma Access 会通知您升级过程将使用的两个周末日期，并在升级第一阶段发生前 21 天、14 天、7 天、3 天和 24 小时发送这些通知。升级过程在两个阶段会出现：

- 第一阶段使用您提供的时间窗口升级您在第一个周末选择的地点，并在升级完成后通过电子邮件通知您。如果您没有先选择要升级的位置，或者没有选择时间窗口，Prisma Access 会为您做出选择。

  Palo Alto Networks 会在您通过 *Strata Cloud Manager* 选择的四个小时窗口内尝试升级位置。但是，在此窗口内完成所需的升级是尽力而为，*Palo Alto Networks* 不能保证在此期间升级该地点。如果在升级过程中出现任何问题，*Palo Alto Networks* 将在原定四小时窗口后 *24* 小时尝试升级。

  出于此原因，您应该安排一个 *72* 小时的更改请求窗口，从周五当地时间晚上 *8* 点开始，到周一当地时间晚上 *8* 点结束，用于数据平面升级的两个周末中的每一个周末。升级完成后，您将收到一封电子邮件。

  Prisma Access 在升级的第 1 阶段对部署进行以下更改。

部署类型	什么是升级
移动用户 — GlobalProtect 部署	Prisma Access 升级：

©2025 Palo Alto Networks, Inc.

部署类型	什么是升级
	• GlobalProtect 网关，也称为移动用户安全处理节点 *(MU-SPN)*，用于指定一个或多个位置。 • 与该区域关联的 GlobalProtect 门户。
移动用户 — 显式代理部署	Prisma Access 升级显式代理节点的显式代理位置或您指定的位置。
远程网络部署	Prisma Access 升级备份 (HA) 远程网络，也称为远程网络安全处理节点 *(RN-SPN)*，然后使备份远程网络成为您指定位置的活动节点。备份远程网络连接要到下个周末才会升级，届时所有位置的活动节点和备份节点都将升级。 如果所选位置有多个 RN-SPN，则所有主要节点都将升级到新的数据平面版本。
服务连接	Prisma Access 升级备份 (HA) 服务连接，也称为服务连接企业访问节点 (SC-CAN)，然后使备份服务连接成为您指定位置的活动节点。备份服务连接要到下个周末才会升级，届时所有位置的活动节点和备份节点都将升级。 如果所选位置有多个 SC-CAN，则所有备份节点都将升级到新的数据平面版本。
ZTNA 连接器	ZTNA 连接器不会升级；您可以根据需要升级 ZTNA 连接器。

在第一次和第二次升级之间，监视第一次升级的位置，并执行连接、性能、路由和日志记录测试，以确保这些位置升级成功。如果您在升级后遇到影响服务的故障，请向 Palo Alto Networks 技术支持部门开立支持案例以获得帮助。Palo Alto Networks 将尝试在 24 小时内将数据平面回滚到以前的数据平面版本，从而解决问题。

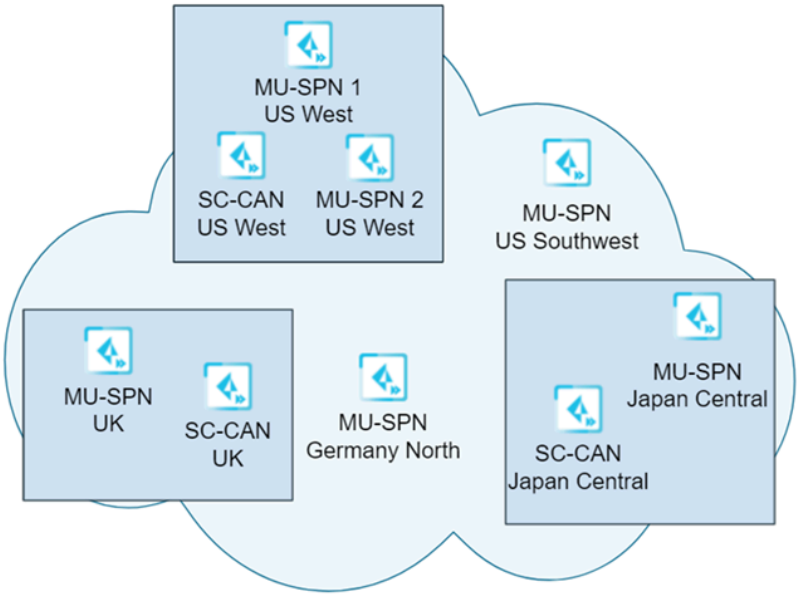
- 在 Prisma Access 升级第一个地点七天后，Prisma Access 将使用您为第一阶段选择的同一时间窗口升级您的其余地点（第 2 阶段升级），并在升级完成后通过电子邮件通知您。

升级窗口可以更长。例如，如果阶段 *2* 发生在美国的国庆节期间，则升级的第二阶段发生在第一阶段之后的 *14* 天，而不是 *7* 天。您收到的 *Strata Cloud Manager* 通知会显示即将进行的数据平面升级的具体时间表。

数据平面升级示例

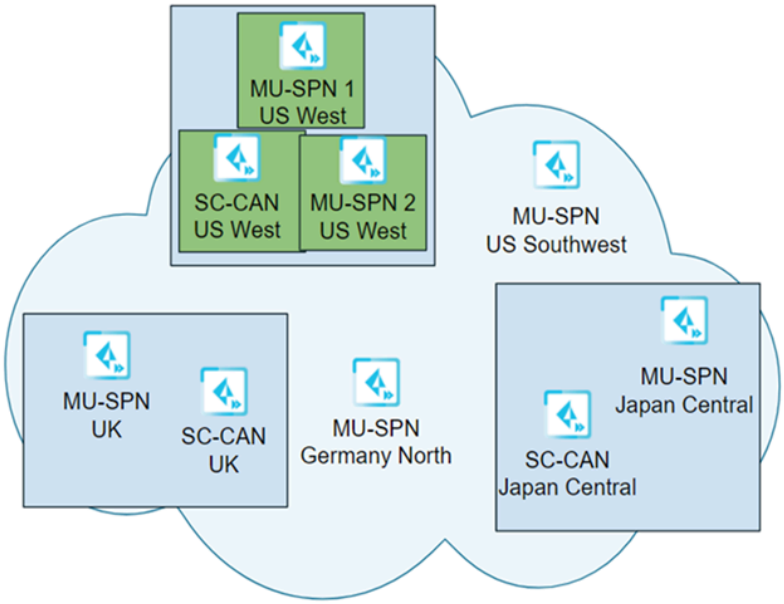
以下示例显示了具有五个网关 (MU-SPN) 和三个 SC-CAN 的移动用户部署的示例数据平面升级过程。美国西部位置有两个 MU-SPN 作为自动缩放事件的结果（在大量移动用户登录该位置后添加了额外的 MU-SPN）。

©2025 Palo Alto Networks, Inc.



在本例中，您选择了单个位置（美国西部）首先进行升级，并请求在周六上午 8:00 至中午 12:00 之间提供四个小时的升级窗口进行升级。

在第一个升级周末（阶段 1），美国西部位置的 SC-CAN 和 MU-SPN 的升级发生在上午 8:00 到晚上 12:00 之间。太平洋时间星期六。



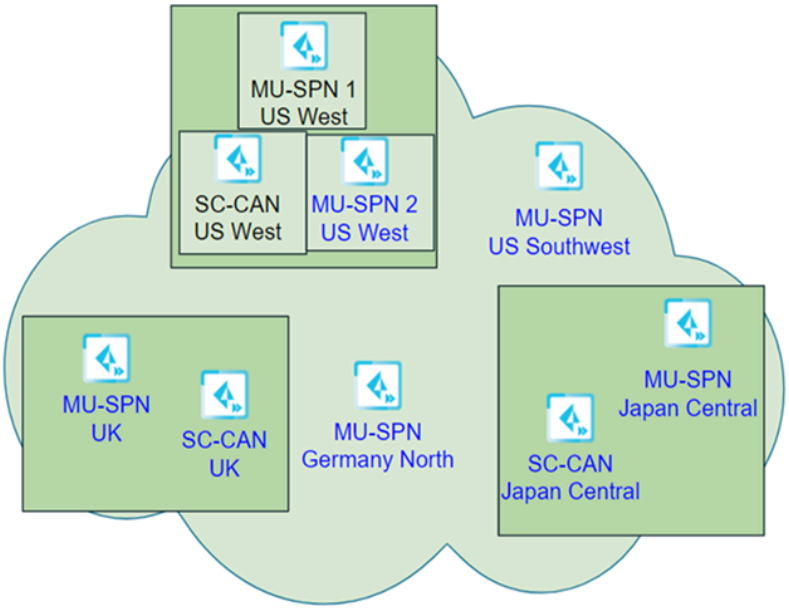
在第一个位置升级七天后，Palo Alto Networks 使用与第一阶段升级相同的四个小时时间窗口（星期六上午 8:00 至中午 12:00）升级其余组件（第二阶段）。

在本例中，Prisma Access 在升级数据平面时使用以下时区信息：

- 日本中部 MU-SPN 和 SC-CAN 使用日本当地时间进行升级。
- 英国 MU-SPN 和 SC-CAN 使用英国当地时间进行升级。

©2025 Palo Alto Networks, Inc.

- 美国西南 MU-SPN 升级使用太平洋时间。



©2025 Palo Alto Networks, Inc.

获取升级提醒和更新

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证

要了解您的数据平面升级的升级计划并选择您的升级偏好，您必须使用 Strata Cloud Manager 订阅 Prisma Access 通知。Strata Cloud Manager 使用电子邮件提醒您有关升级发生的两个周末日期；您选择要首先升级的位置或位置，以及用于升级的四小时时间窗口。

升级开始后，您还可以按照以下步骤所述使用 Strata Cloud Manager 监控升级状态。

STEP 1 | 从 Strata Cloud Manager 注册接收警报通知。

STEP 2 | 检查您的通知以了解即将进行的数据平面升级；然后，使用以下方法之一选择您的升级偏好。

- 选择 **Workflows**（工作流） > **Software Upgrades**（软件升级） > **Prisma Access** > **Upgrade Preferences**（升级首选项）。

  升级仪表板显示。

- 登录 Strata Cloud Manager，查看页面顶部的横幅以获取您计划的升级，并选择 **Click here**（点击这里）。
- 检查您的电子邮件以获取有关您计划升级的通知，并单击电子邮件中的超链接。
- 选择 **Workflows**（工作流） > **Software Upgrades**（软件升级） > **Prisma Access** > **Upgrade Preferences**（升级首选项）。

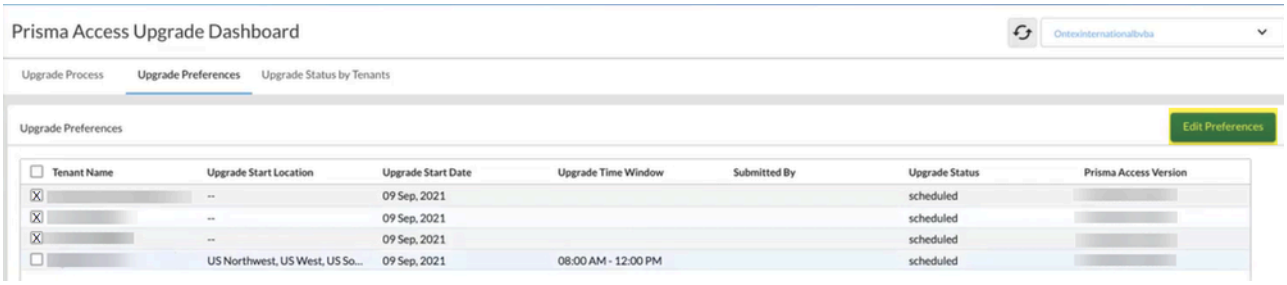
STEP 3 | （可选）阅读 **Upgrade Process**（升级过程）以了解升级过程的工作原理。

©2025 Palo Alto Networks, Inc.

STEP 4 | 选择 **Upgrade Preferences**（升级首选项）。

如果您有多租户部署，则所有租户将在此区域显示。如果您已经为您的部署选择了升级偏好，这些选择将在此处显示。

1. 选择要设置升级偏好的租户，然后选择 **Edit Preferences**（编辑首选项）。



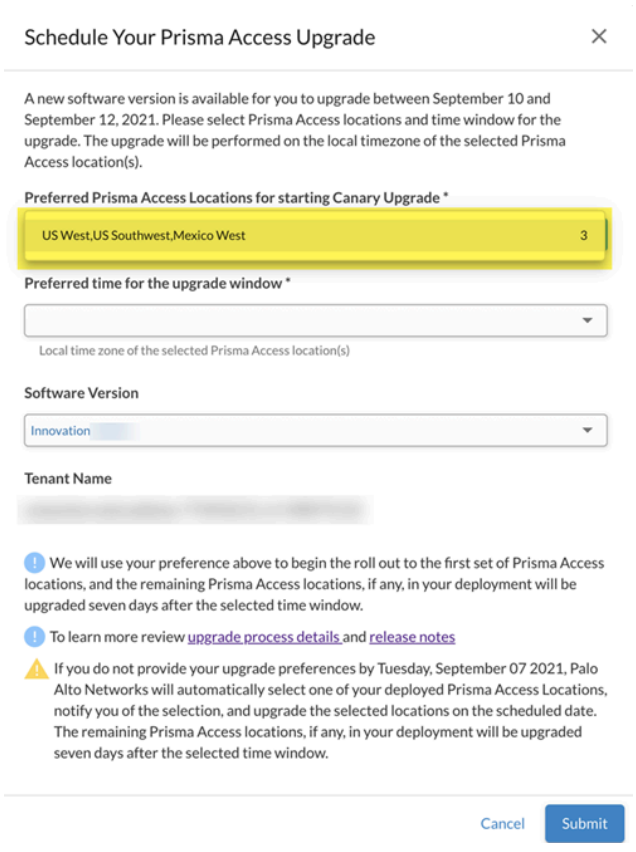
2. 选择您想要优先升级的 首选 **Prisma Access** 地点。

   *Palo Alto Networks*强烈建议您选择能够反映整个部署的位置。例如，如果您有移动用户、服务连接和远程网络部署，请选择具有所有部署类型的一个或多个位置。

   从下拉列表中选择。

   - Prisma Access 仅显示您已部署移动用户、远程网络、服务连接或其任意组合的位置。
   - 下拉列表中的组属于同一计算位置。

   Prisma Access 将通过电子邮件提醒您位置升级时的通知。



©2025 Palo Alto Networks, Inc.

在第一组 Prisma Access 位置成功升级后，Prisma Access 团队监控这些位置七天，然后升级所有剩余 Prisma Access 位置。选择一个单一位置或少数位置使您有机会在其余位置在一周后升级之前监控这些位置。

如果下拉列表中没有显示任何位置，您要么选择了没有共同部署位置的多个租户，要么您尚未为所选租户入驻任何位置。

3. 从可用选项列表中选择 **Preferred time for the upgrade window**（升级窗口的首选时间）。

   从以下升级时间窗口中选择。时间窗口是本地的，适用于正在升级的位置或多个位置，所有窗口均为四小时窗口。

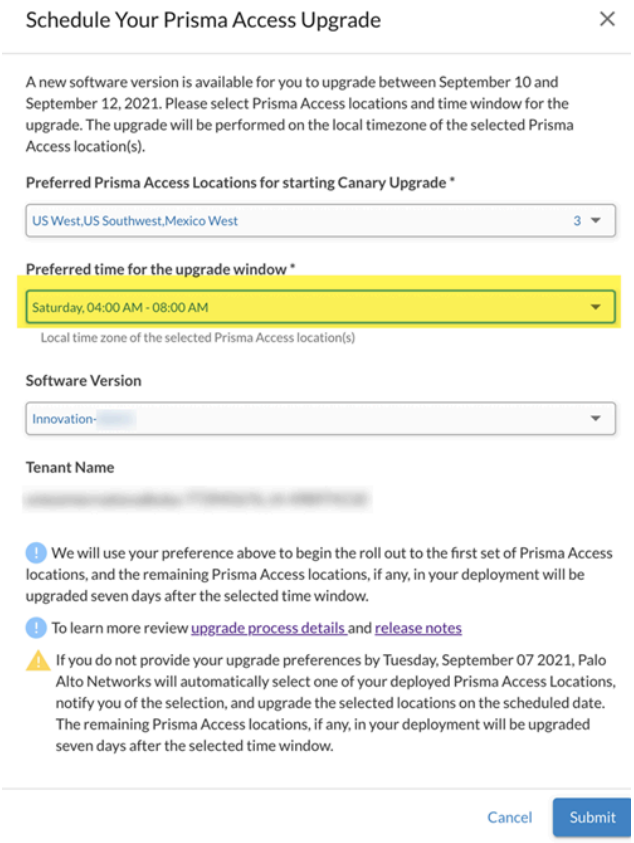
   - 星期五晚上 8:00 到午夜 12:00
   - 星期六凌晨 12:00（午夜）到凌晨 4:00
   - 星期六凌晨 4:00 到早晨 8:00
   - 星期六早晨 8:00 到中午 12:00
   - 星期六中午 12:00 到下午 4:00
   - 星期六下午 4:00 到晚上 8:00

   帕洛阿尔托网络根据您选择的 Prisma Access 位置或位置开始推出。服务将选择在计划开始日期前七天发生的最后一次提交进行升级。如果进行更改，可能需要最多 30 分钟才能

©2025 Palo Alto Networks, Inc.

在 Insights 上的“升级仪表板”中显示所做的更改。Prisma Access 处理并完成更改后，将通过电子邮件提醒通知您。

如果您在计划的升级窗口前七天内未提供升级偏好，*Palo Alto Networks* 将自动选择您已部署 *Prisma Access* 位置的第一组，通知您选择，并在计划日期升级所选位置。在您部署的剩余 *Prisma Access* 位置（如果有的话），将在选定的时间窗口后七天进行升级。



4. 选择您想要升级到的软件版本（如果有多个版本可用）。
5. **Commit**（提交）更改。

©2025 Palo Alto Networks, Inc.

STEP 5 | > > > > 在您的发布开始后，选择工作流软件升级Prisma Access按租户的升级状态，并查看按位置的升级状态。

此页面显示正在升级的每个位置的以下信息：

- 正在升级的租户的名称。
- 升级过程的开始和结束日期。
- 租户正在升级到的数据平面版本。
- 升级窗口的首选时间。
- 正在升级的初始位置。
- 剩余地点将升级的日期。

此外，表格显示了正在升级的位置、升级的开始日期和时间窗口，以及用于升级的时区。升级状态列为您提供以下信息：

升级状态	说明
已计划	数据平面升级已安排。
已启动	升级已开始。
正在进行	数据平面升级正在进行中。
重试	数据平面升级未成功完成，但 Prisma Access 仍然使用旧的数据平面版本正常运行。在周末维护窗口结束之前，Prisma Access 将重试升级。
成功	升级成功完成。

STEP 6 | 在第一组位置完成数据平面升级后，监控已升级的位置，并进行连接性、性能、路由和日志测试，以确保它们成功升级。

STEP 7 | 当第二组位置计划进行升级时，请监控这些位置并通过选择 工作流软件升级 租户升级状态 来检查它们的状态。 > > **Prisma Access** >

在数据平面升级完成后，Prisma Access 会向您发送电子邮件通知。

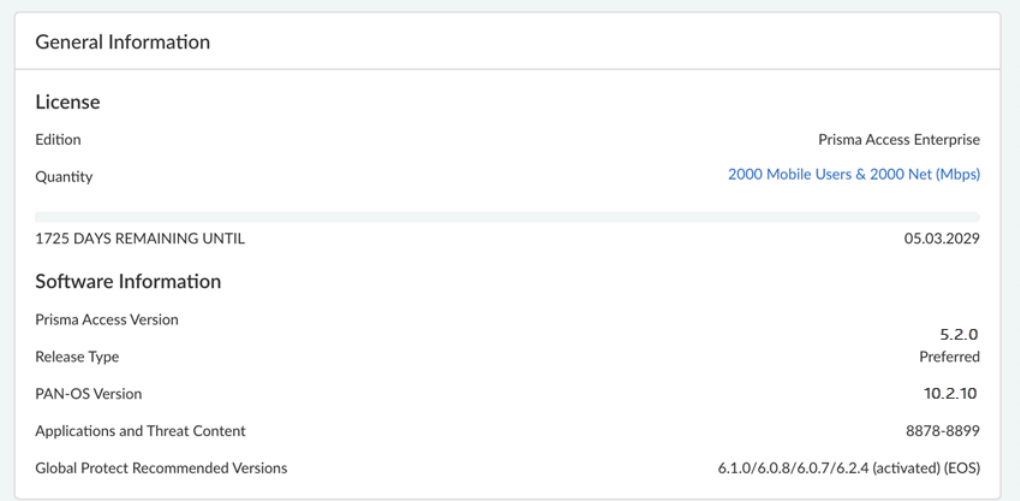
©2025 Palo Alto Networks, Inc.

查看 Prisma Access 软件版本

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

Prisma Access (Managed by Strata Cloud Manager)

> > **Prisma Access** > > 您可以在管理配置NGFW和概述一般信息中找到软件和内容版本信息。选择 **Prisma Access** 配置范围。



“一般信息”页为您提供以下信息：

面积图	说明
租户 **ID**	允许您共享联系信息（公司名称、联系人姓名、电子邮件和电话号码），以便就Palo Alto Networks服务升级事宜与您联系。 租户的 ID。
租户名称	租户的名称。
区域	房客的区域。
Prisma Access 版本	Prisma Access 的当前版本。

©2025 Palo Alto Networks, Inc.

面积图	说明
PAN-OS 版本	数据平面正在运行的PAN-OS版本。数据平面是 Prisma Access 基础设施的组成部分，可对网络和用户流量进行流量检查和策略实施。
版本类型	您正在运行的版本类型（首选或创新）。 创新版本需要比首选版本更高的PAN-OS数据平面。
应用程序和威胁内容	您正在运行的应用程序和威胁内容更新版本。

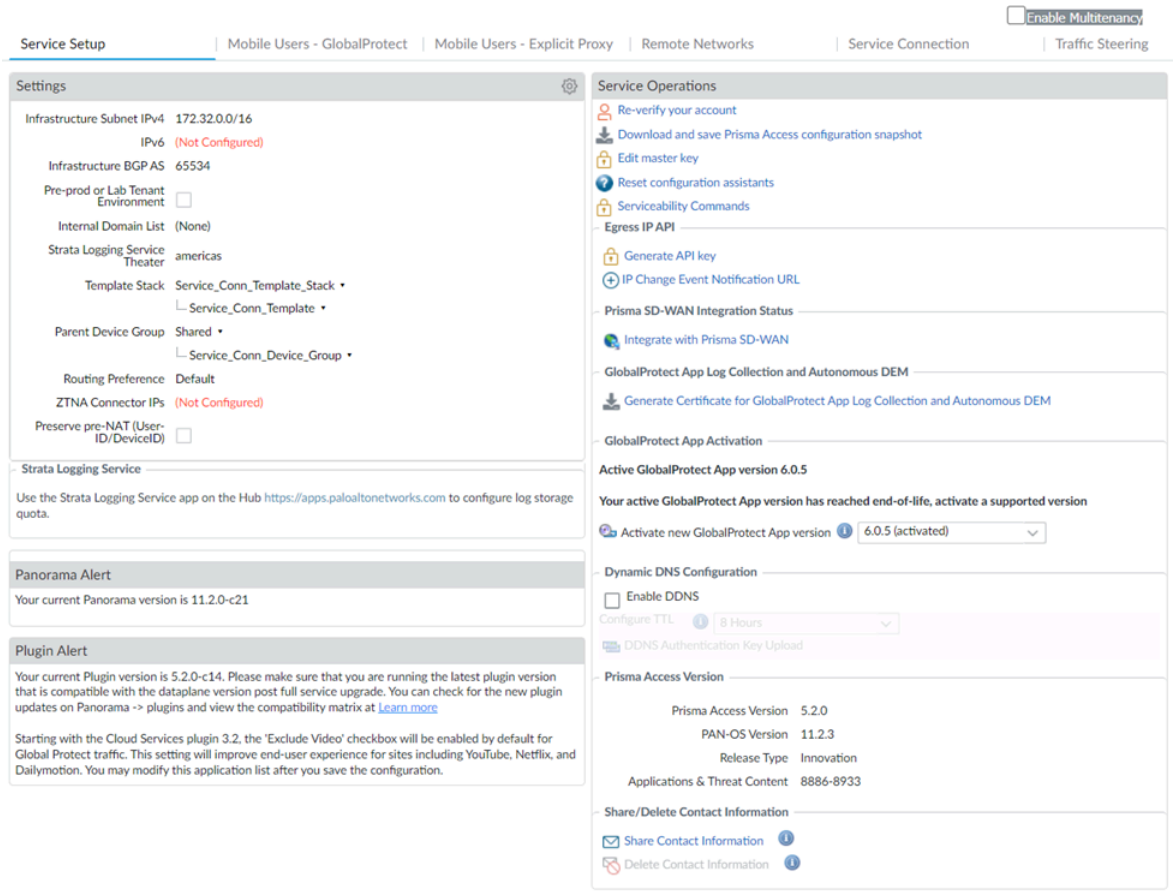
Prisma Access (Managed by Panorama)

Prisma Access 包含由您管理的组件（如 Panorama 和云服务插件）、Prisma Access 管理的组件（如数据平面版本）以及 Prisma Access 管理但您可以控制其版本的组件（托管在 Prisma Access 门户上的 GlobalProtect 版本）组成。 > > > 服务设置页面（Panorama Cloud Services配置服务设置）在单个页面中显示这些组件的状态。此页面还包含通知，向您显示当前运行的 Panorama 版本和插件版本何时将停止支持 (EoS) 与 Prisma Access 一起使用。Palo Alto网络会提前通知您EoS日期，以便您的组织有足够的时间来计划升级。

所有日期均为协调世界时（*UTC*）。

“服务设置”页提供以下信息：

©2025 Palo Alto Networks, Inc.



面积图	说明
Panorama警报	显示正在运行的当前Panorama版本。Prisma Access升级要求区域为您提供有关Panorama版本的信息，包括当前兼容的Panorama版本达到其支持终止（EoS）日期的日期。使用此信息在EoS日期之前规划您的Panorama升级。
插件警报	显示当前安装在管理 Prisma Access 的 Panorama 上的云服务插件。**Upgrade requirements**（升级要求）区域为您提供了下一个插件版本发布的日期、升级到下一个插件的截止日期以及您无法使用早期插件版本进行更改和提交的日期。使用此信息规划下一次云服务插件升级。
Prisma SD-WAN 集成状态	选择**Integrate with Prisma SD-WAN**（与 **Prisma SD-WAN** 集成）以激活 CloudBlade 瘦客户端，该瘦客户端允许 Prisma SD-WAN 和 Prisma Access 之间的功能。

©2025 Palo Alto Networks, Inc.

面积图	说明
GlobalProtect应用程序日志收集和自治**DEM**	如果您已启用 GlobalProtect 应用程序日志收集以进行故障排除，或要为您的移动用户启用自主数字体验管理 (ADEM)，请单击 **Generate Certificate for GlobalProtect App Log Collection and Autonomous DEM**（生成 **GlobalProtect** 应用程序日志收集和自主 **DEM** 的证书）以生成证书。此证书允许 GlobalProtect 应用程序使用 Strata Logging Service（收集日志）和自治 DEM 进行身份验证。Prisma Access > > > 生成证书时，还会将证书下载到要推送到移动终端的“共享”中Mobile_User_Template模板下的“Panorama设备证书管理证书”中的“设备证书”中的“设备证书”。
GlobalProtect 应用程序激活	显示移动用户可以从 Prisma Access 门户下载的 GlobalProtect 应用程序的当前运行（活动）版本，并显示您可以升级到的可用 GlobalProtect 应用程序版本。
动态 **DNS** 配置	显示您是否已启用动态DNS（DDNS）进行远程网络故障排除。
Prisma Access 版本	Prisma Access 的当前版本。
PAN-OS 版本	数据平面正在运行的PAN-OS版本。数据平面是 Prisma Access 基础设施的组成部分，可对网络和用户流量进行流量检查和策略实施。
版本类型	您正在运行的版本类型（首选或创新）。 创新版本需要比首选版本更高的PAN-OS数据平面。
应用程序和威胁内容	您正在运行的应用程序和威胁内容更新版本。
分享/删除联系信息	允许您共享联系信息（公司名称、联系人姓名、电子邮件和电话号码），以便就Palo Alto Networks服务升级事宜与您联系。 如果您以前输入过联系人信息，则可以删除在此区域中输入的信息。 请勿在联系人信息区域中使用以下任何特殊字符： • "（双引号） • '（撇号）

©2025 Palo Alto Networks, Inc.

面积图	说明
	• < （小于符号） • > （大于号） • & （与号）

©2025 Palo Alto Networks, Inc.

©2025 Palo Alto Networks, Inc.

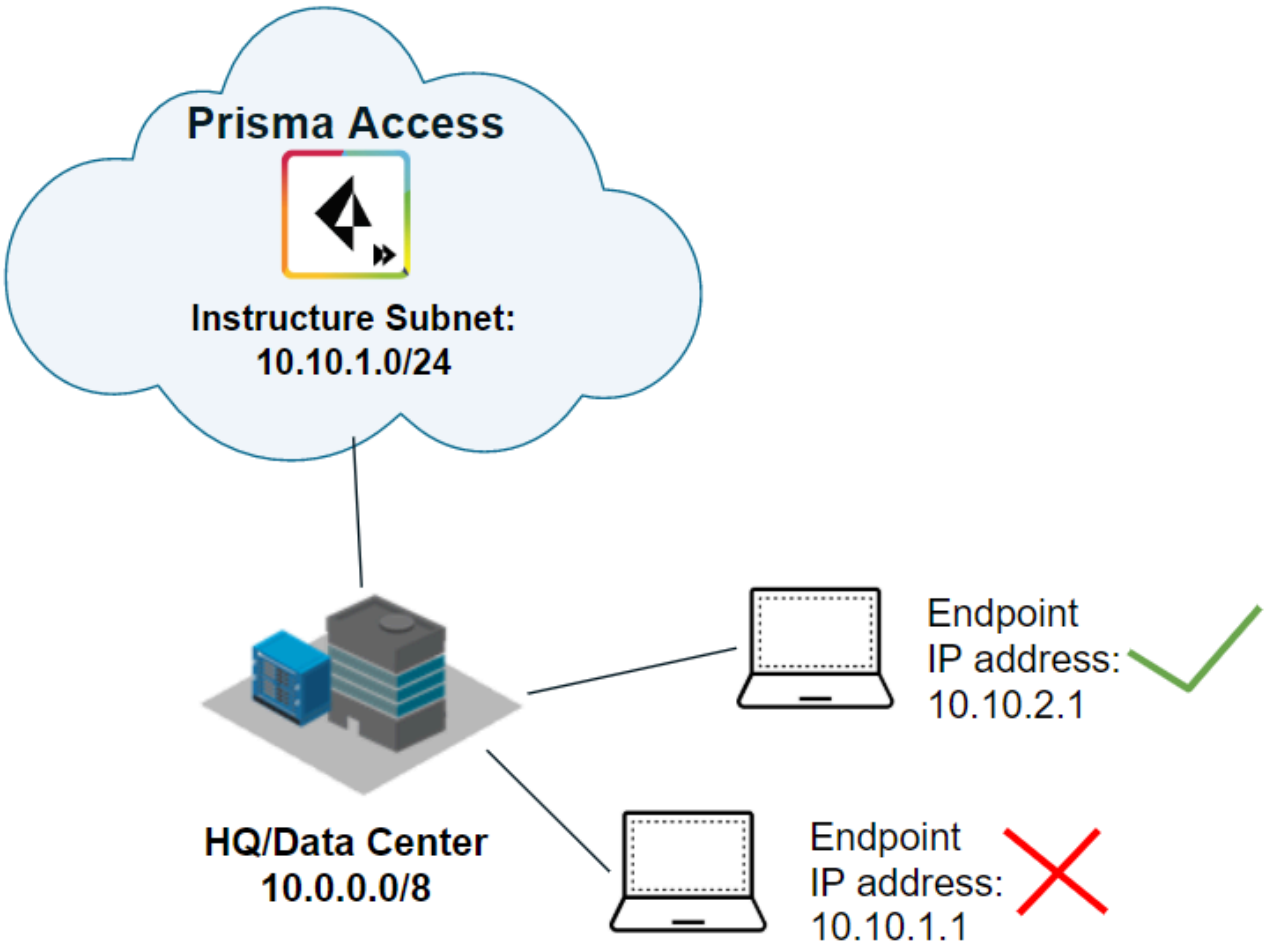
Prisma Access 设置

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证

添加基础设施子网时，请遵循以下建议和要求：

- 您可以从组织的 IP 地址池中的现有超网分配 Prisma Access 基础设施子网，但不要将基础结构子网中的任何 IP 地址分配给现有网络中的任何其他用途。

  以下示例显示了从现有超网 10.0.0.0/8 分配的 Prisma Access 基础设施子网 10.10.1.0/24。将 10.10.1.0/24 指定为基础设施子网后，您的组织无法使用该子网中的任何 IP 地址。例如，您可以将 10.10.2.1 分配给端点，但不允许使用 10.10.1.1，因为该 IP 地址是基础设施子网的一部分。



- 如果为基础设施子网创建新的子网，请使用不与内部使用的其他 IP 地址重叠的子网。
- （推荐）使用符合 RFC 1918 的子网。虽然支持使用不符合 RFC 1918 的（公共）IP 地址，但我们不建议这样做，因为它可能与互联网公共 IP 地址空间发生冲突。
- 请勿指定与以下 IP 地址和子网重叠的任何子网，因为 Prisma Access 保留这些 IP 地址和子网供其内部使用。
  - 169.254.0.0/16
  - 100.64.0.0/10
- 子网不能与计划用于为移动用户部署分配的地址池的 IP 地址池重叠。
- 因为服务基础结构可能非常大，所以您必须至少指定一个 /24 子网。

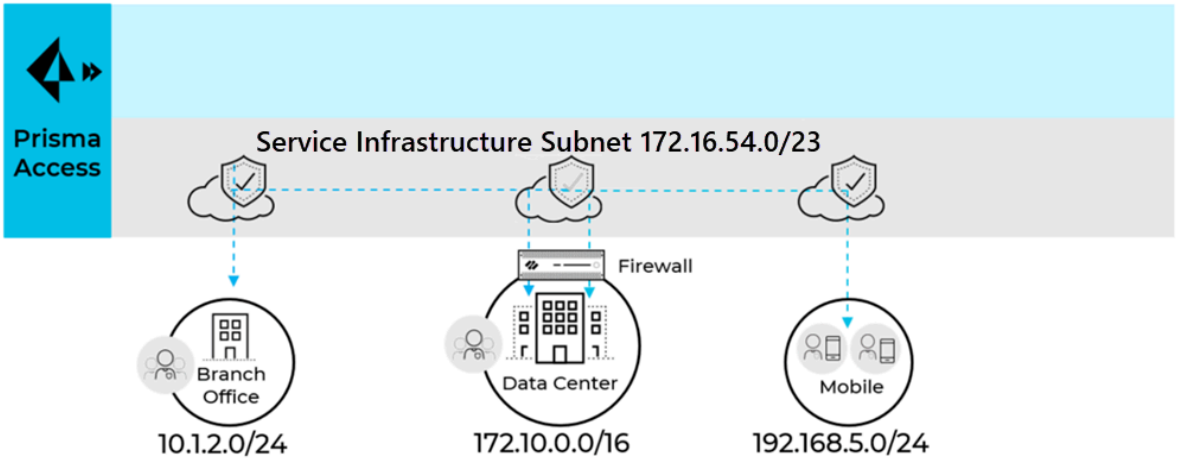
 ©2025 Palo Alto Networks, Inc.

设置 Prisma Access

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

在使用 Prisma Access 来保护远程网络和移动用户之前，请先配置基础架构子网。Prisma Access 使用此子网内的 IP 地址在您的远程网络位置、移动用户、总部和数据中心（如果适用）之间建立网络。Prisma Access 还使用服务连接从您的总部或数据中心访问内部资源。

该子网络将是您现有网络的扩展。因此，它不应与网络中任何现有 IP 子网重叠。以下示例显示了用于 Prisma Access 基础架构子网的 172.16.54.0/23 子网。



对于站点少于 50 个且移动用户少于 2500 人的小型网络，可以考虑 /24 子网。对于站点少于 100 个且移动用户少于 5000 人的中型网络，可以考虑 /23 子网。在大多数情况下，/23 子网就足够了。如果有超过 100 个站点或 5000 个移动用户，或者预计未来会增长，请联系 Palo Alto Networks 以评估是否需要更大的子网规模。

了解如何设置 Prisma Access。

- Strata Cloud Manager
- Panorama

设置 Prisma Access (Strata Cloud Manager)

以下工作流程为您提供了安装和配置 Prisma Access 的摘要步骤 。

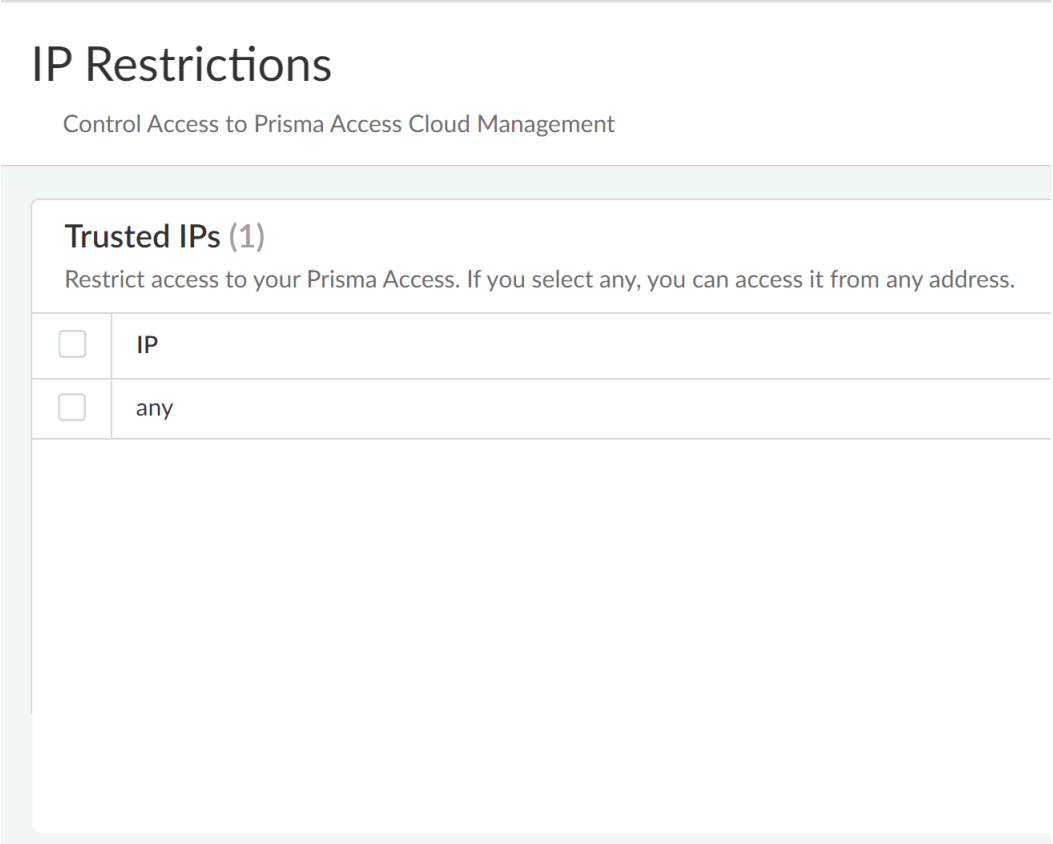
STEP 1 | 发射 Strata Cloud Manager 通过集线器。

1. 启动互联网浏览器并 登录 到 中心。
2. 启动 Strata Cloud Manager

©2025 Palo Alto Networks, Inc.

STEP 2 | 指定受信任的 IP 地址 Prisma Access (Managed by Strata Cloud Manager) 管理员。

只有从这些源 IP 地址登录（并且成功通过身份验证）的管理员才能访问 Prisma Access (Managed by Strata Cloud Manager)。IP 地址必须是公共地址。默认情况下，不强制执行任何受信任的地址（列表设置为“任何”）。首先，在左侧导航面板上找到 “设置”菜单，然后单击“**IP** 限制”。



STEP 3 | 确定您的许可要求；然后 激活并安装 Prisma Access 组件。

STEP 4 | 启用服务基础架构和服务连接，允许 Prisma Access 元素之间进行通信。

STEP 5 | 根据部署需要，使用 GlobalProtect 或 Explicit Proxy 保护移动用户的安全。

STEP 6 | 规划、创建和配置远程网络连接。

STEP 7 | （可选）将身份验证方法从本地身份验证更改为组织的身份验证方法。

STEP 8 | （可选） 转发日志Strata Logging Service 到外部 Syslog 接收器。

STEP 9 | （可选）检查状态 Prisma Access。

您可以检索所有云服务的状态，包括 Prisma Access 和 Strata Logging Service，并通过从 中心访问应用程序实例来记录服务正常运行时间的历史记录。

您还可以注册电子邮件或短信通知，以便在计划基础设施更新时、发生更新时以及 Palo Alto Networks® 创建、更新或解决事件时收到通知。要注册电子邮件更新，请转到 中心 主页的资源部分，然后选择 服务状态。然后，您可以 订阅 云服务的特定更新和事件。

©2025 Palo Alto Networks, Inc.

设置 Prisma Access (Panorama)

以下工作流程为您提供了安装和配置的摘要步骤 Prisma Access (Managed by Panorama) 使用权。

如果您要设置包含多个实例的部署 *Prisma Access* 在单个 *Panorama*（多租户）上，请参见 。大多数组织不需要创建和管理多个租户。

STEP 1 | 将以下 URL 和端口添加到与管理 Prisma Access 的 Panorama 设备一起使用的任何安全设备上的允许列表中。

此外，如果您的 Panorama 设备使用**Panorama** > **Setup**（设置） > **Service**（服务） > **Proxy Server**（代理服务器）），或者您使用 Prisma Access 的 SSL 转发代理，请务必将以下 URL 和端口添加到代理或代理服务器的允许列表中。

- api.gpcloudservice.com（用于 Prisma Access）
- api.paloaltonetworks.com（对于 Prisma Access）
- apitrusted.paloaltonetworks.com（对于 Prisma Access
- Strata Logging Service 所需的 FQDN 和端口

如果 *Panorama* 设备和互联网之间有 *Palo Alto Networks* 下一代防火墙，则必须在防火墙上添加安全策略规则，以允许 ***paloalto-logging-service*** 和 ***paloalto-shared-services****App-ID* 从 *Panorama* 设备访问互联网。这些应用程序允许 *SSL* 安全通信 *Prisma Access* 以及 *Strata Logging Service Panorama* 设备用于查询日志。如果 *Panorama* 设备位于传统第 *4* 层防火墙后面，则允许端口 *443* 和 *444* 从 *Panorama* 出站，以允许来自 *Panorama* 的此流量。请注意，打开第 *4* 层端口而不是使用 *Palo Alto Networks App-ID* 的安全性较低，因此不推荐。

STEP 2 | 将 Panorama 使用的端口 添加到网络中的允许列表中。

STEP 3 | 确定您的许可要求；然后 激活并安装 Prisma Access 组件。

STEP 4 | 将现有的 Panorama 配置导入 Prisma Access，或创建新的 模板 和 设备组 以开始配置 Prisma Access。

为了将配置（例如安全策略、身份验证策略、服务器配置文件、安全配置文件、地址对象和应用程序组）推送到 Prisma Access，您必须使用要推送到的配置设置创建新的模板和设备组

©2025 Palo Alto Networks, Inc.

Prisma Access或者通过将现有设备组和模板添加到模板堆栈和设备组层次结构中来利用它们 Prisma Access 当您使用该服务时创建。

Prisma Access 根据您购买的内容创建以下模板和设备组（例如，如果您没有购买显式代理许可证，您将看不到显式代理模板和设备组）：

- 模板：
  - 显式代理模板
  - 显式代理模板堆栈
  - 移动用户模板
  - 移动用户模板堆栈
  - 远程网络模板
  - 远程网络模板堆栈
  - 服务连接模板
  - 服务连接模板堆栈
- 设备组：
  - 显式代理设备组
  - **Mobile_User_Device_Group**
  - 远程网络设备组
  - 服务连接设备组

配置简化 Prisma Access 因为您不必配置任何基础设施设置，例如接口和路由协议。此配置是自动化的，并从 Panorama 推送到服务自动创建的模板和设备组中。您可以直接从插件配置服务所需的任何基础设施设置，例如创建到远程网络位置的支持 IPSec 设备的 IPSec VPN 隧道所需的设置。您可以选择将模板和设备组层次结构添加到配置中以简化服务设置。

为了简化服务设置，请在开始使用设置任务之前创建或导入所需的 模板 和 设备组Prisma Access。

创建模板和设备组时 Prisma Access，则无需为其分配托管设备。相反，您将把它们添加到模板堆栈和设备组层次结构中， Prisma Access 创建。不要添加由 Prisma Access 到任何其他模板堆栈或设备组。

STEP 5 | 使用以下方式注册电子邮件通知Strata Cloud Manager。

Prisma Access 使用此应用程序的通知为您提供有关该服务的通知，包括任何数据平面升级。

 ©2025 Palo Alto Networks, Inc.

STEP 6 | 更改 Panorama 和云服务插件的默认主密钥。

作为最佳安全做法，Palo Alto Networks 建议更改 Panorama 和 Cloud Services 插件中的主密钥，并且每月更改一次主密钥。

由于全景和 Prisma Access 主密钥不同步，Palo Alto Networks 建议您不要在 Panorama 中自动轮换主密钥，而无需在 Prisma Access。您可以使用 Panorama UI 或 API 命令来更改主密钥。

请务必跟踪您部署的主密钥，因为主密钥无法恢复。如主密钥到期，那么您必须输入当前的主密钥才能配置新的主密钥。如果在主密钥过期时您无法提供当前主密钥，则必须将 *Panorama* 设备重置为出厂默认设置。

1. 更改 Panorama 中的主密钥。
   1. 选择 全景 > 主密钥和诊断。

      不要指定 当前主密钥。
   2. 配置 **New Master Key**（新主密钥），并 **Confirm Master Key**（配置主密钥）。

      记下您配置的主密钥。
   3. 配置主密钥 Lifetime（生命周期）和 Time for Reminder（提醒时间）。
   4. 单击 **OK**（确定）。
2. 更改主密钥 Prisma Access 通过选择 **Panorama** > 云服务 > 配置 > 服务操作 > 编辑主密钥，然后输入您为 Panorama 输入的相同主密钥。

您还可以使用 API 命令更改主密钥。这需要两个步骤——一个是更改全景主密钥，另一个是更改 Prisma Access 主密钥。使用以下 API 命令来更改主密钥：

- Panorama：**XML API** > 操作命令 > 请求 > 主密钥
- Prisma Access：**XML API** > 操作命令 > 请求 > 插件 > **cloud_services** > **prisma-access** > **sync**

STEP 7 | 启用服务基础架构和服务连接，允许 Prisma Access 元素之间进行通信。

1. 计划启用服务基础架构和服务连接。
2. 启用服务基础架构。
3. 创建服务连接 以允许访问您的公司资源。

   即使您不需要访问公司资源，仍应创建服务连接以支持移动用户与远程网络之间的访问。

 ©2025 Palo Alto Networks, Inc.

STEP 8 | Prisma Access 移动用户部署 并根据您的部署需要使用 GlobalProtect 或 Explicit Proxy保护移动用户的安全。

要设置 GlobalProtect Prisma Access (Managed by Panorama)：

1. 通过在 Mobile_User_Template 中创建两个区域（例如，Mobile-Users 和 Internet）并 映射区域来配置移动用户的区域。您要将任何未连接 Prisma Access 的用户或总部/分支机构的服务区映射到“不可信”。

   在 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Mobile Users**（移动用户）下，将互联网映射到“不可信”，并将 “移动用户” 映射到“可信”。
2. 配置身份验证。

   我们建议第一步使用本地身份验证，以便验证是否已设置服务以及您的用户是否可以访问互联网。稍后可以切换为使用公司身份验证方法。
3. 为设备组配置安全策略。

   要创建允许流量流向互联网的安全策略，请选择 Mobile_User_Device_Group **Policies**（策略） > **Security**（安全） > **Pre Rules**（前导规则），并 > **Add**（添加）规则。例如：移动用户到互联网。
4. 提交并推送您的更改以开始使用该服务。
5. 选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Monitor**（监控） > **Mobile Users**（移动用户）以查看 **Status**（状态），并验证您是否可以 ping 门户 FQDN。
6. 验证 Prisma Access 通过 下载和安装 GlobalProtect 应用程序来保护移动用户的互联网流量，使用该应用程序以移动用户（本地用户）身份连接到门户，浏览互联网上的几个网站，并检查 Panorama 上的流量日志。

要使用显式代理保护移动用户的安全：

1. 阅读 显式代理配置准则。
2. 配置 SAML 身份验证。显式代理需要 SAML 身份验证。
3. 使用 Cloud Identity Engine设置组映射。
4. 完成显式代理配置。
5. 提交并推送更改。

STEP 9 | 规划、创建和配置远程网络连接。

1. 向 Prisma Access 添加一个或多个远程网络。

   您可以上线一个地点，然后使用批量导入功能添加其他地点。
2. 创建安全策略规则以允许流量从远程网络流向总部（例如：信任到信任）。
3. 验证服务连接、远程网络连接和移动用户之间的连接。

STEP 10 | 运行用于检索 Prisma Access IP 地址的 API 脚本 并 使用旧脚本检索移动用户 IP 地址。

您可以将那些地址添加到组织网络上的允许列表中，以限制对企业网络和应用程序的入站访问。

 ©2025 Palo Alto Networks, Inc.

STEP 11 | （可选）将身份验证方法从本地身份验证更改为组织的身份验证方法。

1. 创建符合您组织要求的身份验证配置文件（SAML、LDAP、RADIUS 等）。
2. 如果您的组织使用本地身份验证服务器（如 RADIUS 或 Active Directory），请添加 Prisma Access 用作内部请求的源 IP 地址（检索 Prisma Access 的 IP 地址）以允许网络中的列表，或允许整个基础设施子网的 IP 地址（Prisma Access 从该子网获取环回 IP 地址）。
3. 更新身份验证配置文件 Prisma Access 门户和网关使用这个新的身份验证配置文件。

STEP 12 | （可选） 转发日志Strata Logging Service 到外部 Syslog 接收器。

©2025 Palo Alto Networks, Inc.

配置 Prisma Access 服务基础架构

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证 ❑ 预生产或实验室租户所需的最低 Prisma Access 版本：3.0-Preferred

Prisma Access 使用此子网创建网络主干，以便在分支网络、移动用户和 Prisma Access 安全基础架构以及您计划通过服务连接连接到 Prisma Access 的总部和数据中心网络之间进行通信。

为了实现远程网络位置、移动用户以及您计划通过服务连接连接到 Prisma Access 的总部或数据中心之间的通信，请设置服务基础架构子网。Prisma Access 使用此子网创建网络主干，以便在分支网络、移动用户和 Prisma Access 安全基础架构以及您计划通过服务连接连接到 Prisma Access 的总部和数据中心网络之间进行通信。

- Strata Cloud Manager
- Panorama

配置 Prisma Access 服务基础设施 (Strata Cloud Manager)

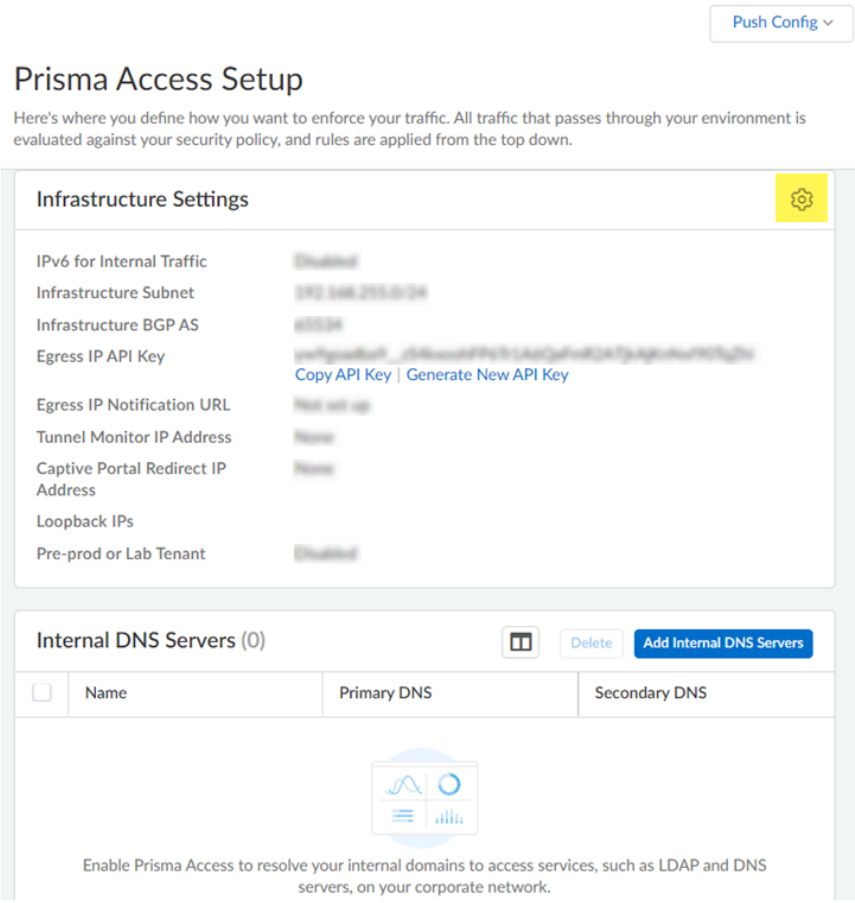
为 Prisma Access 添加基础设施子网时，请遵循以下建议和要求：

- ❑ 使用符合 RFC 1918 的子网。虽然支持使用不符合 RFC 1918 的（公共）IP 地址，但不建议这样做，因为它可能与互联网公共 IP 地址空间发生冲突。
- ❑ 请勿指定与 169.254.0.0/16 和 100.64.0.0/10 子网范围重叠的任何子网，因为 Prisma Access 保留这些 IP 地址和子网供其内部使用。
- ❑ 此子网是现有网络的扩展，因此不能与您在公司网络中使用的任何 IP 子网或您为适用于用户的 Prisma Access 或适用于网络的 Prisma Access 分配的 IP 地址池重叠。
- ❑ 由于服务基础设施需要大量 IP 地址，因此必须指定一个 /24 子网（例如，172.16.55.0/24）。
- ❑ 如果您对远程网络或服务连接使用动态路由，则还必须配置符合 RFC 6996 的 BGP 私有 AS 编号。

STEP 1 | 启动 Prisma Access。

 ©2025 Palo Alto Networks, Inc.

STEP 2 | 转至 **Workflows**（工作流） > **Prisma Access** 设置 > **Prisma Access** > 基础设施设置，然后单击齿轮来编辑设置。



STEP 3 | 在 **Infrastructure Subnet**（基础设施子网）中，输入 Prisma Access 可用于在远程网络位置、移动用户，以及总部或数据中心之间通信的基础设施子网。您计划通过服务连接将这些总部和数据中心连接到 Prisma Access。

使用符合 *RFC 1918* 的子网作为基础设施子网。虽然支持使用不符合 *RFC 1918* 的（公共）*IP* 地址，但不建议这样做，因为它可能与互联网公共 *IP* 地址空间发生冲突。

STEP 4 | （可选）如果您正在配置 IPv6，请选择 **IPv6 for Internal Traffic**（内部流量的 **IPv6**），然后选择 IPv6 子网。

STEP 5 | 输入要在 Prisma Access 基础设施中使用的基础设施 **BGP AS**。

如果您想启用动态路由，以便 Prisma Access 能够动态发现通往您远程网络、总部或数据中心位置资源的路由，您必须使用边界网关协议 (BGP)。基础设施 **BGP AS** 是标识 BGP 可用于发送流量的路由的自治系统 (AS) 编号。如果不提供 AS 编号，Prisma Access 使用默认 AS 编号 (65534)。

如果要指定自己的 AS 编号，则必须使用符合 RFC 6996 的私有 AS 编号。可接受的格式为 4 字节 AS 纯数字表示法 [64512-65534]、[4200000000-4294967294]，或者是AS 点分表示法 [0.64512-0.65534]、[64086.59904-65535.65534]。

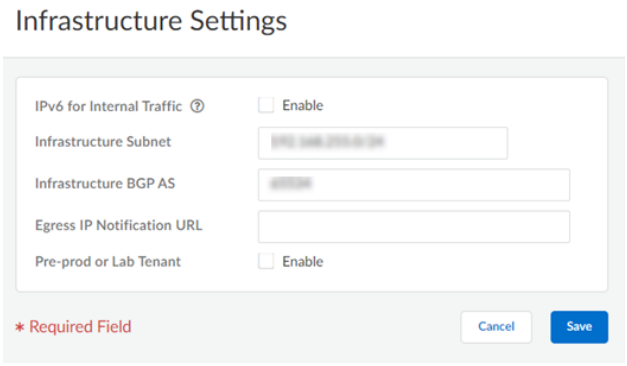
©2025 Palo Alto Networks, Inc.

STEP 6 | 如果您允许用户基于源 IP 地址访问应用程序，您需要获取来自 Prisma Access 的流量所使用的源 IP 地址列表，以便在应用程序访问策略中允许这些地址通过。

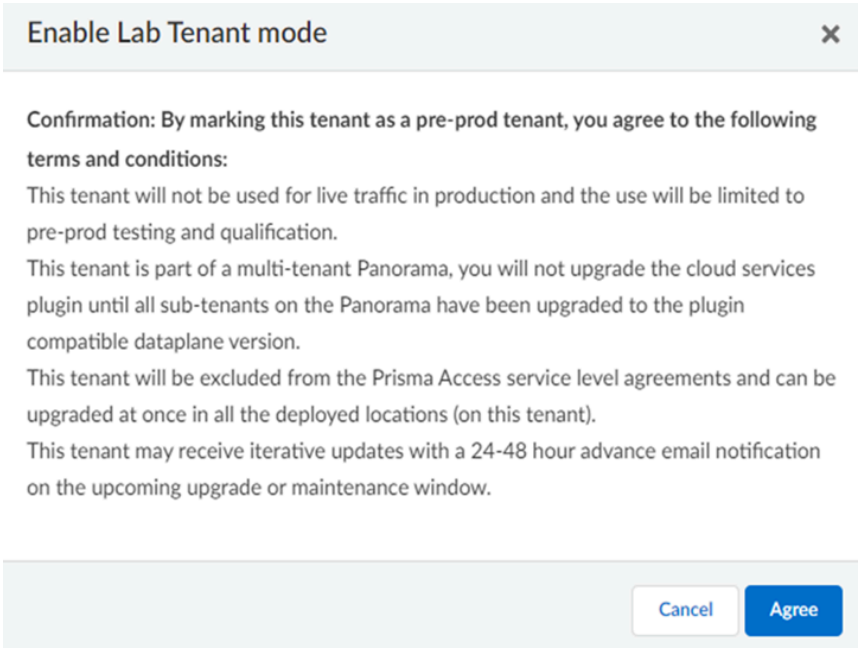
依次选择 **Copy**（复制）和 **Egress IP API Key**（出口 **IP API** 密钥）以启用 Prisma Access 出口 IP 地址 API。此外，由于 Prisma Access 用途会定期更改（例添加新位置时，Prisma Access 需要在现有位置扩展资源时或者基础设施升级时），您需要知道 IP 地址何时发生变化，以便您可以更新策略规则，或者通过定义 **Egress IP Notification URL**（出口 **IP** 通知 **URL**）来自动执行这些更新。有关更多详细信息，请参阅检索 Prisma Access 的 IP 地址。

STEP 7 | （可选）启用租户作为预生产或实验室租户。

1. 依此选择 **Enable**（启用）、**Pre-prod or Lab Tenant**（预生产租户或实验室租户）以作为预生产租户或实验室租户启用租户。



2. 选择 **Agree**（同意）以确认。



当您将租户启用为预生产或实验室租户时，您可以在升级其他生产租户之前单独为该租户安排升级。租户会在即将进行的升级前 24 到 48 小时收到通知。从预生产或实验室租户禁用租户时，该租户将被视为生产租户。

3. **Save**（保存）更改。

 ©2025 Palo Alto Networks, Inc.

STEP 8 | 要使 Prisma Access 能够解析内部域，请选择 **Add Internal DNS Servers**（添加内部 **DNS** 服务器）。

如果您计划配置服务连接以便能够访问公司网络中的资源，并且还需要 Prisma Access 来解析您的内部域，您必须定义内部域列表。对内部域列表中的域的 DNS 查询将发送到您的本地 DNS 服务器，以确保资源可供 Prisma Access 远程网络用户和移动用户使用。

1. 输入 Prisma Access 用于解析内部域名的 **Primary DNS**（主 **DNS**）服务器和 **Secondary DNS**（辅助 **DNS**）服务器。
2. 依次选择 **Add**（添加）、**Domain Names**（域名），以添加您希望 Prisma Access 解析的域名。

   在域列表中的域前可以使用通配符 (*)，例如 *.acme.local 或 *.acme.com。

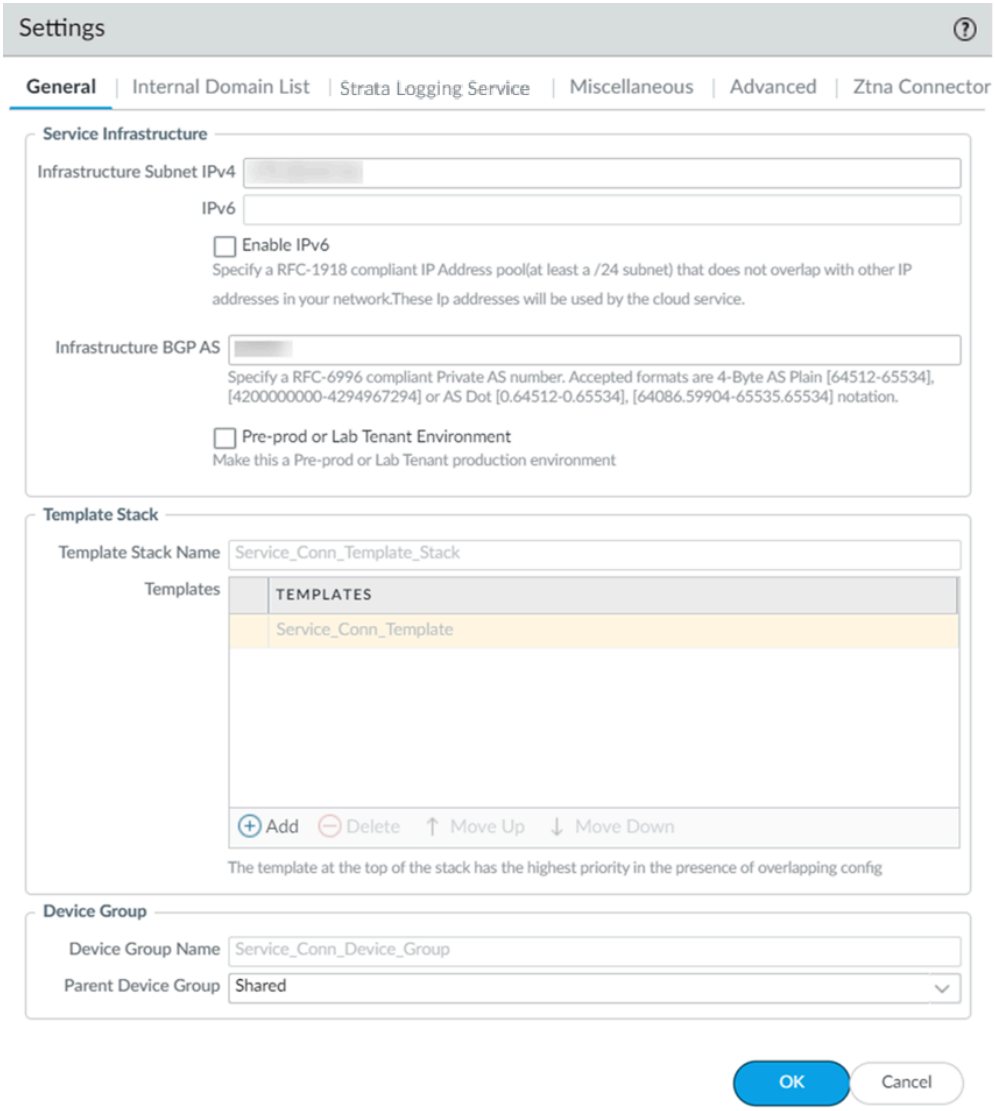
STEP 9 | 选择 **Push Config**（推送配置）以将服务基础设施设置保存到 Prisma Access。

配置 Prisma Access 服务基础设施 (Panorama)

在开始设置 Prisma Access 以保护远程网络和/或移动用户的安全之前，必须配置基础设施子网，Prisma Access 将使用该子网来创建网络主干，以便在服务连接、远程网络和移动用户之间进行通信，以及与您计划通过服务连接而连接到 Prisma Access 的企业网络进行通信。由于设置基础设施需要大量 IP 地址，因此您必须至少使用 /24 子网（例如 172.16.55.0/24）。确保遵循所有准则和要求。

©2025 Palo Alto Networks, Inc.

STEP 1 | 选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Service Setup**（服务设置），然后单击齿轮图标来编辑设置。



STEP 2 | 在 **General**（常规）选项卡上，指定符合要求的 **Infrastructure Subnet**（基础设施子网），例如 172.16.55.0/24。

STEP 3 | （可选）如果您正在配置 IPv6，请选择 **IPv6 for Internal Traffic**（内部流量的 **IPv6**），然后选择 IPv6 子网。

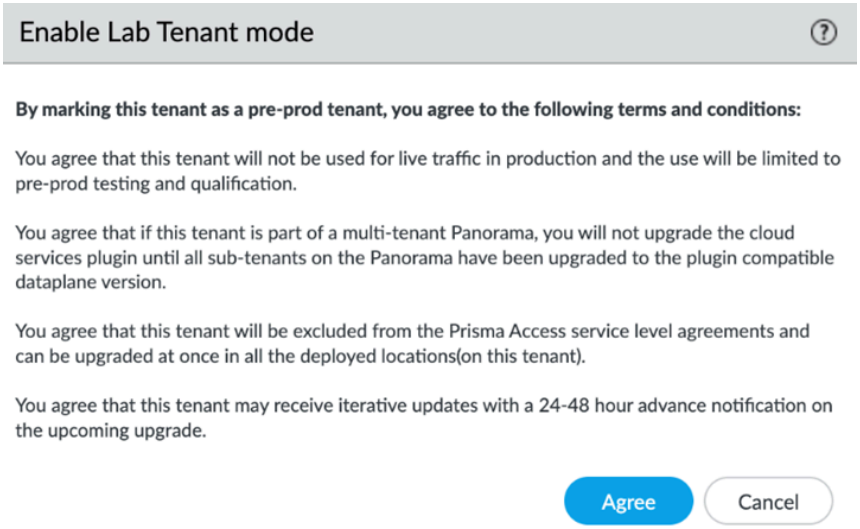
STEP 4 | （可选）如果要启用 Prisma Access 以使用 BGP 动态发现远程网络和总部/数据中心位置上资源的路由，请输入要在 Prisma Access 基础设施中使用的 **Infrastructure BGP AS**（基础设施 **BGP AS**）。

如果您不提供 AS 编号，则将使用默认 AS 编号 65534。

 ©2025 Palo Alto Networks, Inc.

STEP 5 | （可选）启用租户作为预生产或实验室租户环境。

当您将租户启用为预生产或实验室租户时，您可以在升级其他生产租户之前单独为该租户安排升级。租户会在即将进行的升级前 24 到 48 小时收到通知。



从预生产或实验室租户禁用租户时，该租户将被视为生产租户。

适用于 *Clean Pipe* 的 *Prisma Access* 不支持此功能。

©2025 Palo Alto Networks, Inc.

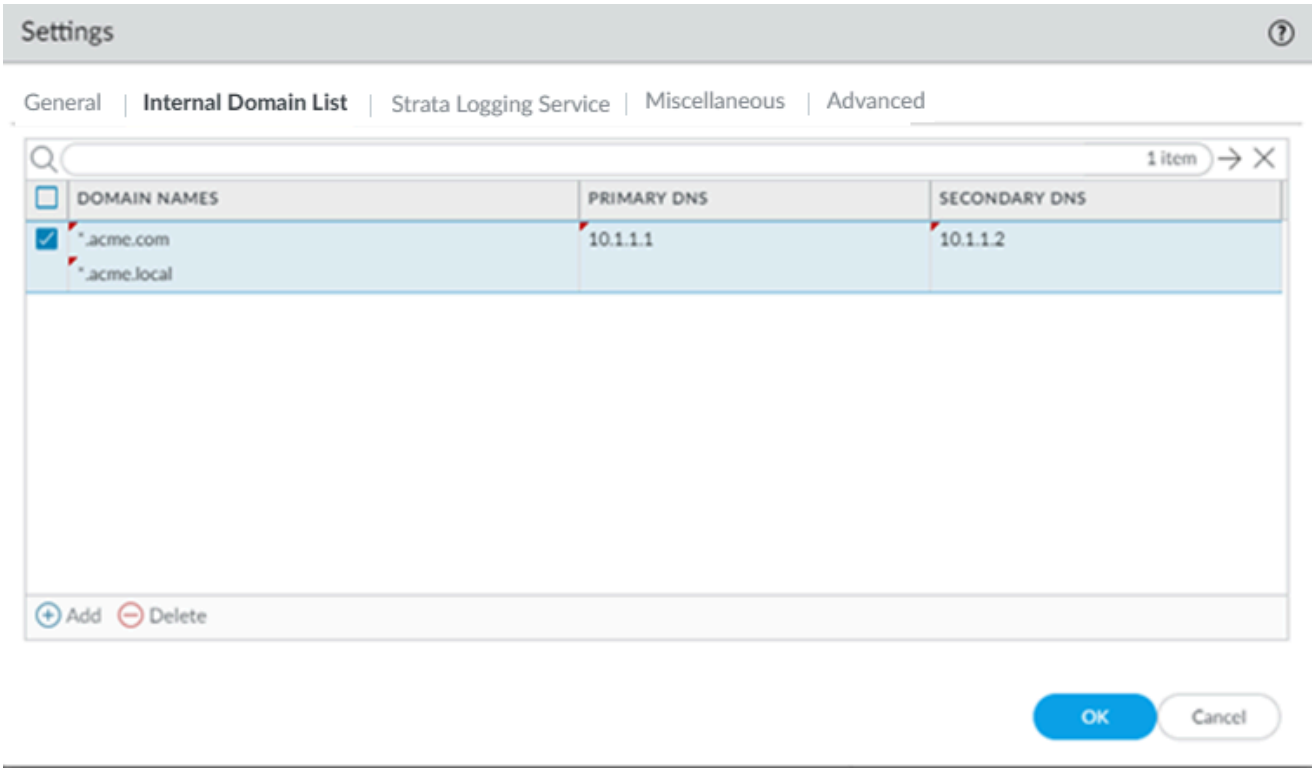
STEP 6 | （可选）启用 Prisma Access 以使用企业 DNS 服务器解析内部域。

如果您需要 Prisma Access 能够解析您的内部域以通过服务连接访问公司网络上的服务（如 LDAP 服务器），请使用此步骤。例如，如果您希望企业域的 DNS 查找仅限于企业 DNS 服务器，请在此处指定企业域和企业 DNS 服务器。

1. 选择 **Internal Domain List**（内部域列表）选项卡。
2. 选择 **Add**（添加）i添加您希望 Prisma Access 用于解析内部域名的 **Domain Names**（域名）、**Primary DNS**（主 **DNS**）和 **Secondary DNS**（辅助 **DNS**）服务器。

   在域列表中的域前可以使用通配符 (*)，例如 *.acme.local 或 *.acme.com。

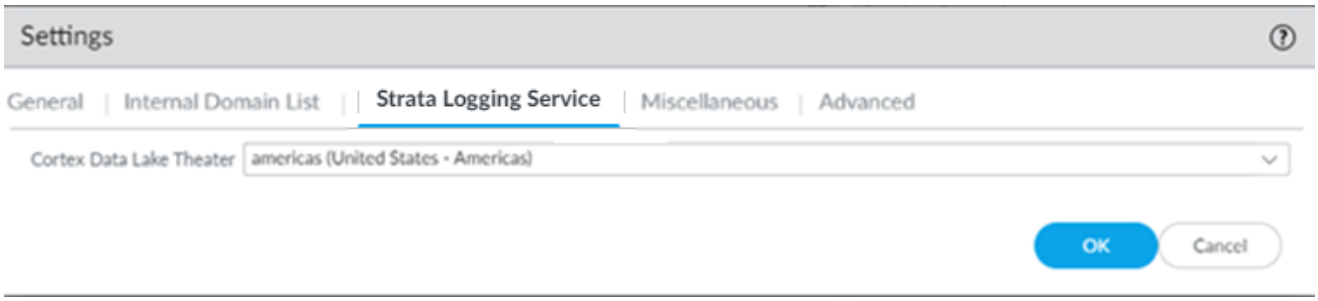
   请勿输入 *127.0.0.1* 地址，因为这可能会导致 *Prisma Access* 内部路由问题。



 ©2025 Palo Alto Networks, Inc.

STEP 7 | 启用 Strata Logging Service。

1. 选择 **Strata Logging Service** 选项卡。
2. 选择一个 **Strata Logging Service Theater**（**Strata Logging Service** 大区），然后单击 **OK**（确定）。



3. 配置您正在使用的设备组，以便通过一个日志转发配置文件将设置推送到 Prisma Access 设备，该配置文件会将所需的日志类型转发至 **Panorama/Strata Logging Service**。

   进行新安装后或者从 Prisma Access 模板堆栈中移除非 Prisma Access 模板时，云服务插件将自动添加以下日志设置（**Device**（设备） > **Log Settings**（日志设置））：

   - 系统日志 **(system-gpcs-default)**、User-ID 日志 **(userid-gpcs-default)**、HIP Match 日志 **(hipmatch-gpcs-default)** 和 GlobalProtect 日志 **(gp-prismaaccess-default)** 的日志设置已添加到 Mobile_User_Template。
   - 系统日志 **(system-gpcs-default)**、User-ID 日志 **(userid-gpcs-default)** 和 GlobalProtect 日志 **(gp-prismaaccess-default)** 的日志设置已添加到 Remote_Network_Template。
   - 系统日志（**system-gpcs-default**）和 GlobalProtect 日志（**gp-prismaaccess-default**）的日志设置已添加到 Service_Conn_Template。

   这些日志设置配置会自动将系统、User-ID、HIP 匹配和 GlobalProtect 日志转发至 Strata Logging Service。

   要应用日志设置更改，请执行以下步骤，然后提交并推送您的更改：

   - 要将日志设置应用于移动用户模板，请选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Mobile Users**（移动用户），单击齿轮图标以编辑设置，然后单击“OK（确定）”。
   - 要将日志设置应用于远程网络模板，请选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Remote Networks**（远程网络），单击齿轮图标来编辑设置，然后单击“OK（确定）”。
   - 要将日志设置应用于服务连接模板，请选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Service Setup**（服务设置），单击齿轮图标编辑设置，然后单击“OK（确定）”。

   为其他日志类型启用日志转发的方式取决于日志类型。对于基于策略匹配生成的日志，请使用日志转发配置文件。有关详细信息，请参阅 Strata Logging Service 入门指南。

©2025 Palo Alto Networks, Inc.

STEP 8 | （可选）配置 **Miscellaneous**（其他）设置。

1. （可选）通过选择 **Append the ending token to the URLs in the URL filtering configuration**（将结束标记附加到 **URL** 过滤配置中的 **URL**），将为外部动态列表 (EDL) 或自定义 URL 类别中的 URL 附加结束标记。

   如果您在 EDL 或自定义 URL 类别中使用 URL，但未在 URL 后附加正斜杠 (**/**)，则可能会允许比预期更多的 URL。例如，输入 **`example.com`** 作为匹配 URL（而不是 **`example.com/`**）也会匹配 example.com.website.info 或 example.com.br。

   通过选择 **Append the ending token to the URLs in the URL filtering configuration**（将结束标记附加到 **URL** 过滤配置中的 **URL**），Prisma Access 将为 EDL 或自定义 URL 类别中的 URL 设置结束标记，这样，如果您输入 **`example.com`**，Prisma Access 将其视为 example.com/ 并且仅匹配该 URL。

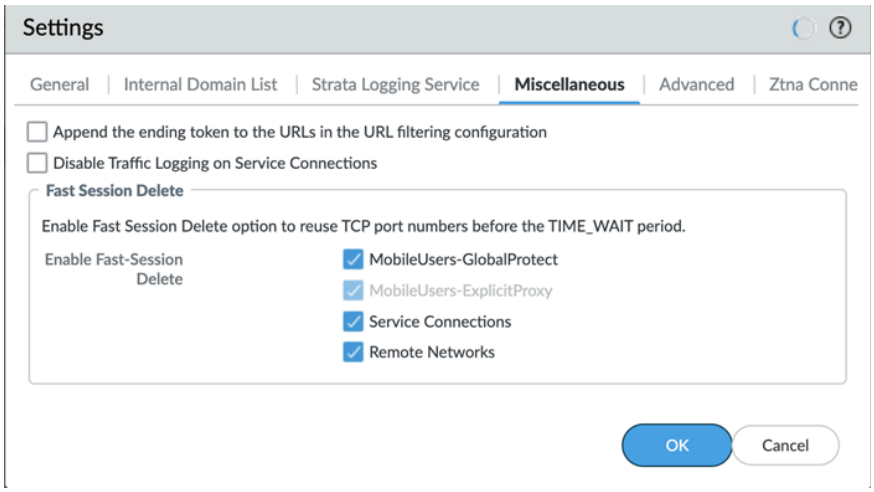
2. （可选）**Disable Traffic Logging on Service Connections**（禁用服务连接上的流量日志记录），以禁用 Prisma Access 部署的服务连接上的日志记录。

   如果服务连接记录的大多数流量是非对称流量，则可能需要禁用服务连接日志记录以减少 Strata Logging Service 日志记录存储空间的消耗。如果您的部署没有通过服务连接的非对称流量，则无需禁用日志记录。

3. （可选）要为远程网络、服务连接或“移动用户—GlobalProtect”部署启用“快速会话删除”，请选中 **Mobile Users—GlobalProtect**（移动用户—**GlobalProtect**）、**Service Connections**（服务连接）或 **Remote Networks**（远程网络）的复选框。

   快速会话删除功能使 Prisma Access 能够在 TCP TIME_WAIT 状态期结束前重复使用 TCP 端口号，该功能对于解密后可能存续时间较短的 SSL 会话尤为实用。

   对于“移动用户—显式代理”部署，快速会话删除是其功能的关键部分，无法禁用。



 ©2025 Palo Alto Networks, Inc.

STEP 9 | （可选）配置 **Advanced**（高级）设置（路由首选项、服务连接的对称网络路径选项和 HIP 重新分配）。

1. 指定与服务连接一起使用的 **Routing Preference**（路由首选项）。

   您可以指定网络首选项，以使用组织的网络或 Prisma Access 网络来处理服务连接流量。

   - **Default**（默认）—Prisma Access 在其内部网络中使用默认路由。
   - **Hot potato routing**（热土豆路由）—Prisma Access尽快将服务连接流量移交给组织的广域网。

   要更改 *Prisma Access* 服务连接路由方法，需要全面了解组织的拓扑和路由设备，以及了解 *Prisma Access* 路由的工作方式。我们建议您在更改默认路由方法之前仔细阅读服务连接流量的路由。

2. 配置用于服务连接的 **Backbone Routing**（骨干路由）。

   默认情况下，Prisma Access 骨干网络要求您建立对称网络路径，用于路由通过服务连接从数据中心或总部位置返回的流量。如果要将 ECMP 或其他负载均衡机制用于来自 CPE 的服务连接，则可以通过 Prisma Access 骨干网络启用非对称流。

   - 选择 **no-asymmetric-routing** 可要求流量通过服务连接主干时保持对称性。
   - 选择 **asymmetric-routing-only** 可允许 Prisma Access 流量在通过服务连接主干时不必对称。
   - 如果某个位置有多个服务连接，则可以通过选择 **asymmetric-routing-with-load-share**（默认设置），利用 Prisma Access 部署中的负载均衡。但是，负载均衡是尽最大努力实现的，如果其中一个服务连接中断，负载均衡将失败。

3. 使用 Prisma Access 重新分发 HIP 信息 使用服务连接重新分发来自移动用户和远程网络用户的 HIP 信息。

4. 在 Prisma Access GlobalProtect 部署中识别和隔离感染设备以使 Prisma Access 能够识别和隔离与 GlobalProtect 应用程序连接的感染设备。

5. 如果您希望 Prisma Access 在隧道关闭且没有备用隧道的情况下删除静态路由，请选择 **Withdraw Static Routes if Service Connection or Remote Network IPSec tunnel is down**（如果服务连接或远程网络 **IPsec** 隧道关闭，则撤回静态路由）

   Prisma Access 会在以下情况下删除路由：

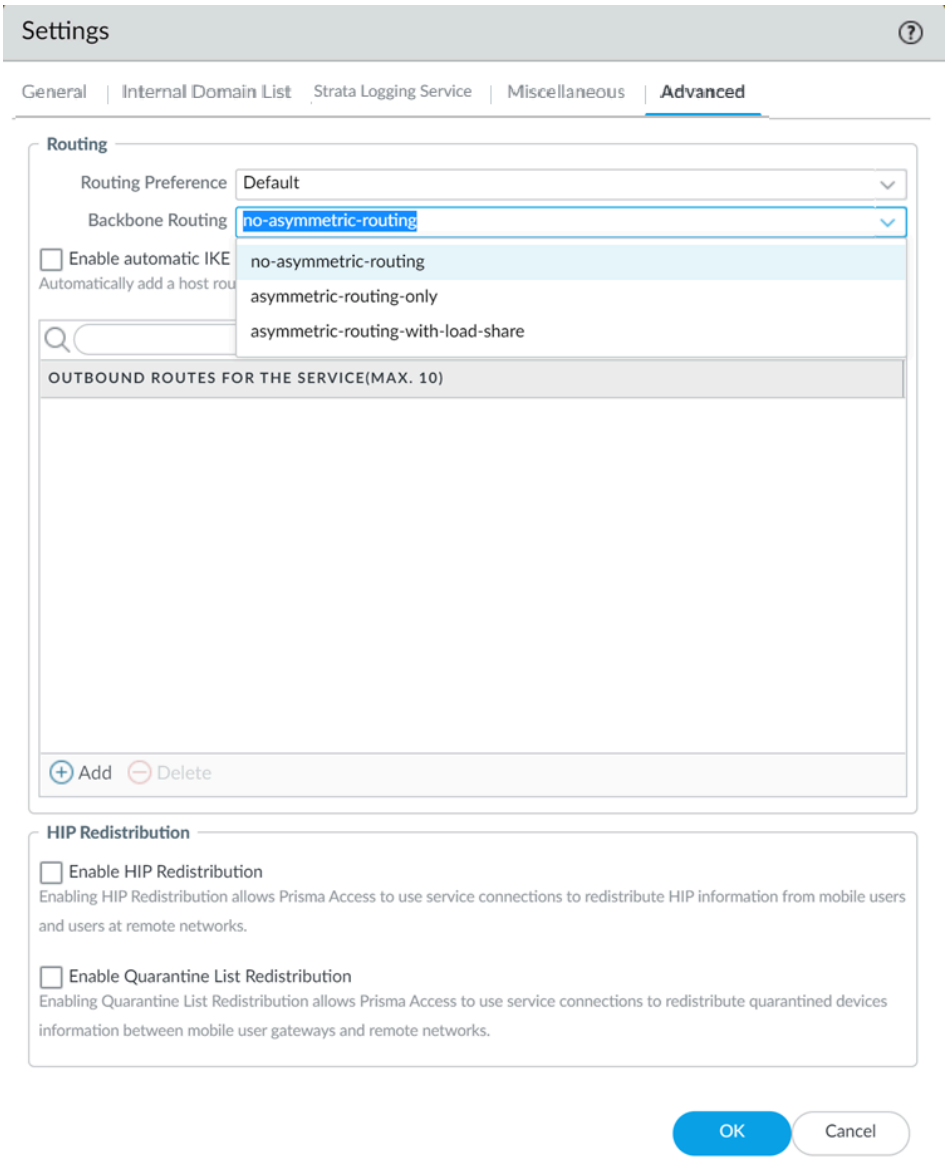
   - 主隧道关闭且没有辅助隧道。
   - 配置了主隧道和辅助隧道，但两条隧道均关闭。

   如果未启用隧道监控，则无法应用此更改。

6. （可选）如果您希望通过互联网将远程网络和服务连接 IPSec 隧道数据包路由到静态 IKE 网关，则选择 **Enable automatic IKE peer host routes for Remote Networks and Service Connections**（为远程网络和服务连接启用自动 **IKE** 对等主机路由）。

7. （可选）通过添加最多 10 个前缀来指定 **Outbound Routes for the Service (Max 10)**（该服务的出站路由（最大 **10** 个）），Prisma Access 会在所有服务连接和远程网络连接上为其添加静态路由。然后，Prisma Access 通过互联网将流量路由到这些前缀。

 ©2025 Palo Alto Networks, Inc.



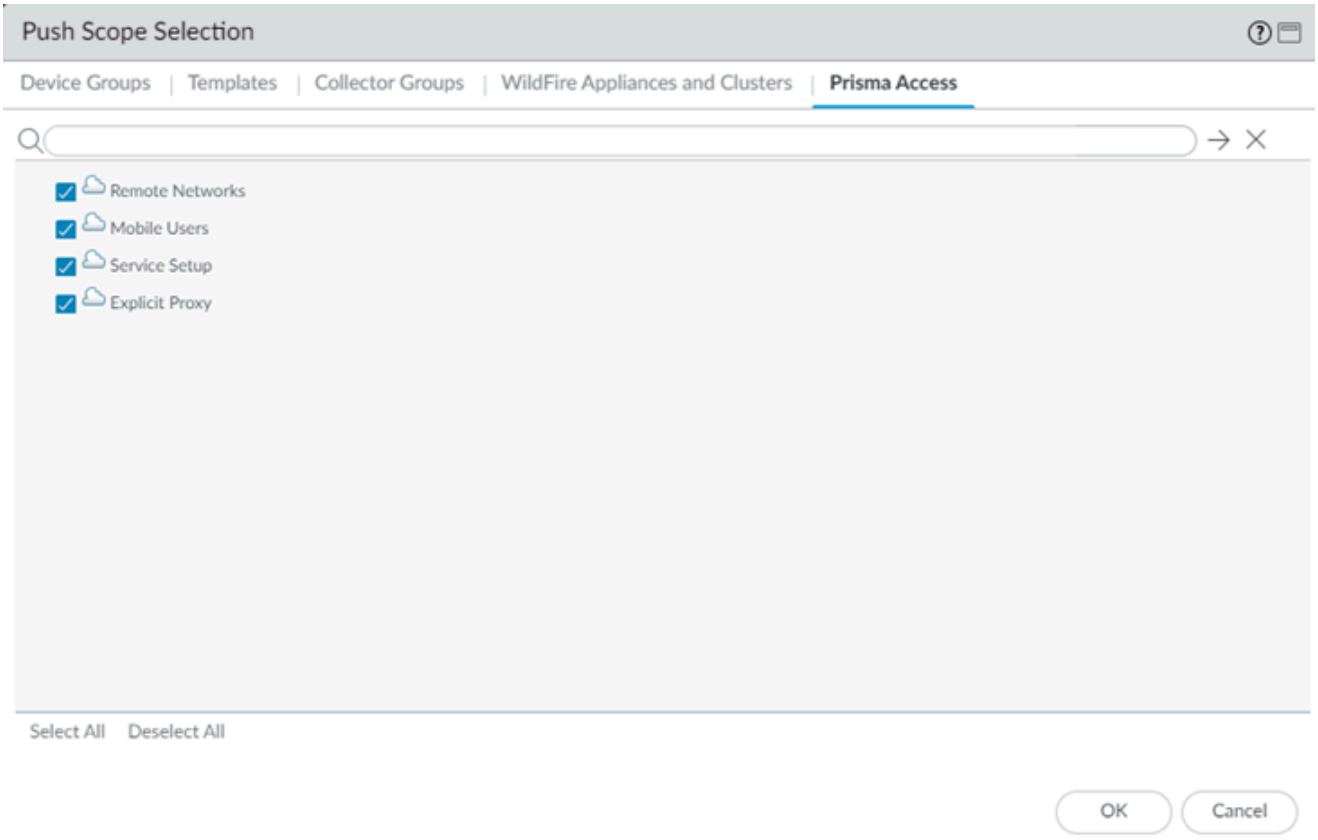
STEP 10 | 单击 **OK**（确定）以保存对“Service setup（服务设置）”的设定。

©2025 Palo Alto Networks, Inc.

STEP 11 | 将所有更改提交到 Panorama 并将配置更改推送到 Prisma Access。

1. 单击 **Commit**（提交） > **Commit to Panorama**（提交到 **Panorama**）。
2. 单击 **Commit**（提交） > **Push to Devices**（推送到设备），然后单击 **Edit Selections**（编辑选择）。
3. 在 **Prisma Access** 选项卡上，确保选择了 **Service setup**（服务设置），然后单击 **OK**（确定）。

   Prisma Access 应该会自动选择需要提交的组件。

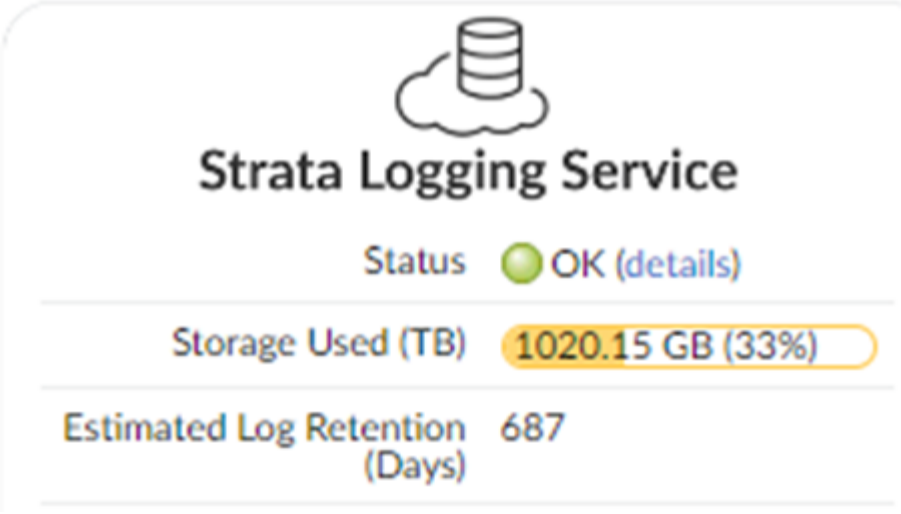


4. 单击 **Push**（推送）。

©2025 Palo Alto Networks, Inc.

STEP 12 | 验证 Prisma Access 已成功连接到 Strata Logging Service。

1. 选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Status**（状态） > **Strata Logging Service**，并验证状态为 **OK**（正常）。



如果状态为 **Error**（错误），请单击详细信息链接查看任何错误。

STEP 13 | 继续设置 Prisma Access：

- 创建服务连接以允许访问私有应用
- 配置适用于网络的 Prisma Access
- 配置适用于用户的 Prisma Access

 ©2025 Palo Alto Networks, Inc.

移动用户：IP 地址分配

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

在设置了 Prisma Access 的部署后，了解 IP 地址的变化情况将很有帮助，这样您就可以主动规划基础设施，检索 IP 地址，并相应地将所需的 IP 地址添加到允许列表中。IP 地址的变化可能是你所做更改的结果（例如，添加了另一个移动用户位置），也可能是 Prisma Access 自动执行的操作所导致的变化（例如，大量移动用户访问单个 Prisma Access 网关）。

首次为用户部署 Prisma Access 后，Prisma Access 将为每个门户和网关分配两个 公用 *IP* 地址和出口 *IP* 地址（如果适用）。这些 IP 地址是唯一的，不会共享，专用于您的 Prisma Access 部署，并且在 Prisma Access 订阅到期和宽限期结束之前，将一直分配给您的租户。

如果你有多租户设置，则 Prisma Access 为每个租户添加专用 IP 地址。

由于公共 IP 地址是 Prisma Access 在向基于互联网的目标发送请求时所使用的源 IP 地址，您可能需要知道这些具体的公共 IP 地址，并将它们添加到您网络中的允许列表中，以便为您的用户提供对诸如 SaaS 应用程序或可公开访问的合作伙伴应用程序等资源的访问权限。

如果发生以下事件，则可以将新的公共 IP 地址添加到租户：

- 大量移动用户访问同一位置中的某个位置。

  为满足为大量用户提供服务的容量需求，Prisma Access 可能会添加一个或多个网关，Prisma Access 添加一个或多个网关以容纳数量增加的用户，将一个或多个现有的公共 IP 地址分配给新网关，并向移动用户位置添加一组新的 IP 地址，以替换之前使用的 IP 地址。
- 可向部署中添加一个或多个位置。

  添加更多位置时，Prisma Access 会添加另一个网关，并为每个新添加的位置添加一组新的 IP 地址。

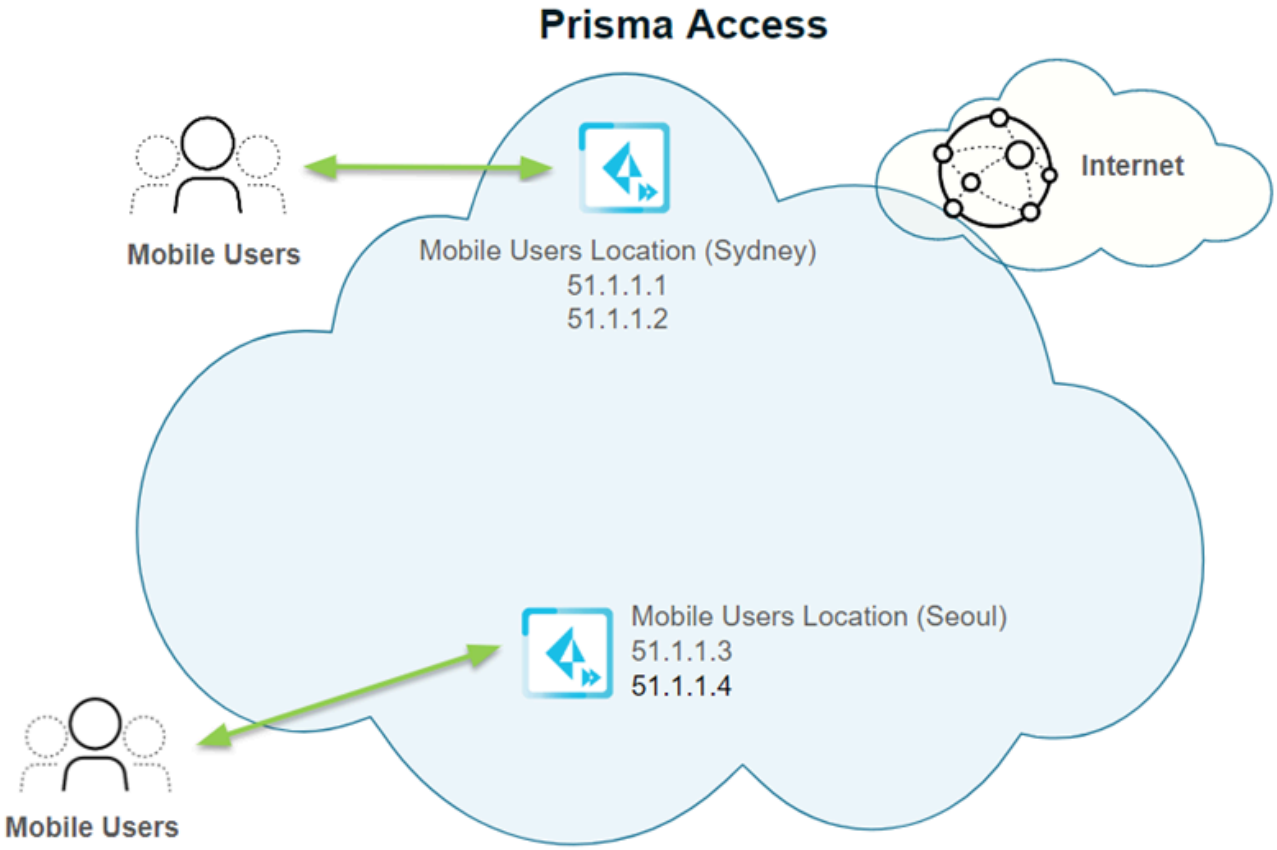
由于 Prisma Access 在缩放事件后和添加位置后会启用更多公用 IP 地址，因此您应添加 IP 更改事件通知 URL，或使用 API 检索移动用户地址，以获得有关 Prisma Access 基础设施中 IP 地址更改的通知。然后，您可以将任何已添加或更改的地址添加到允许列表中。

示例：公共 IP 地址扩展示例（移动用户）

以下示例说明 Prisma Access 在缩放事件期间或在您添加新位置时使用的移动用户公用 IP 地址分配过程。

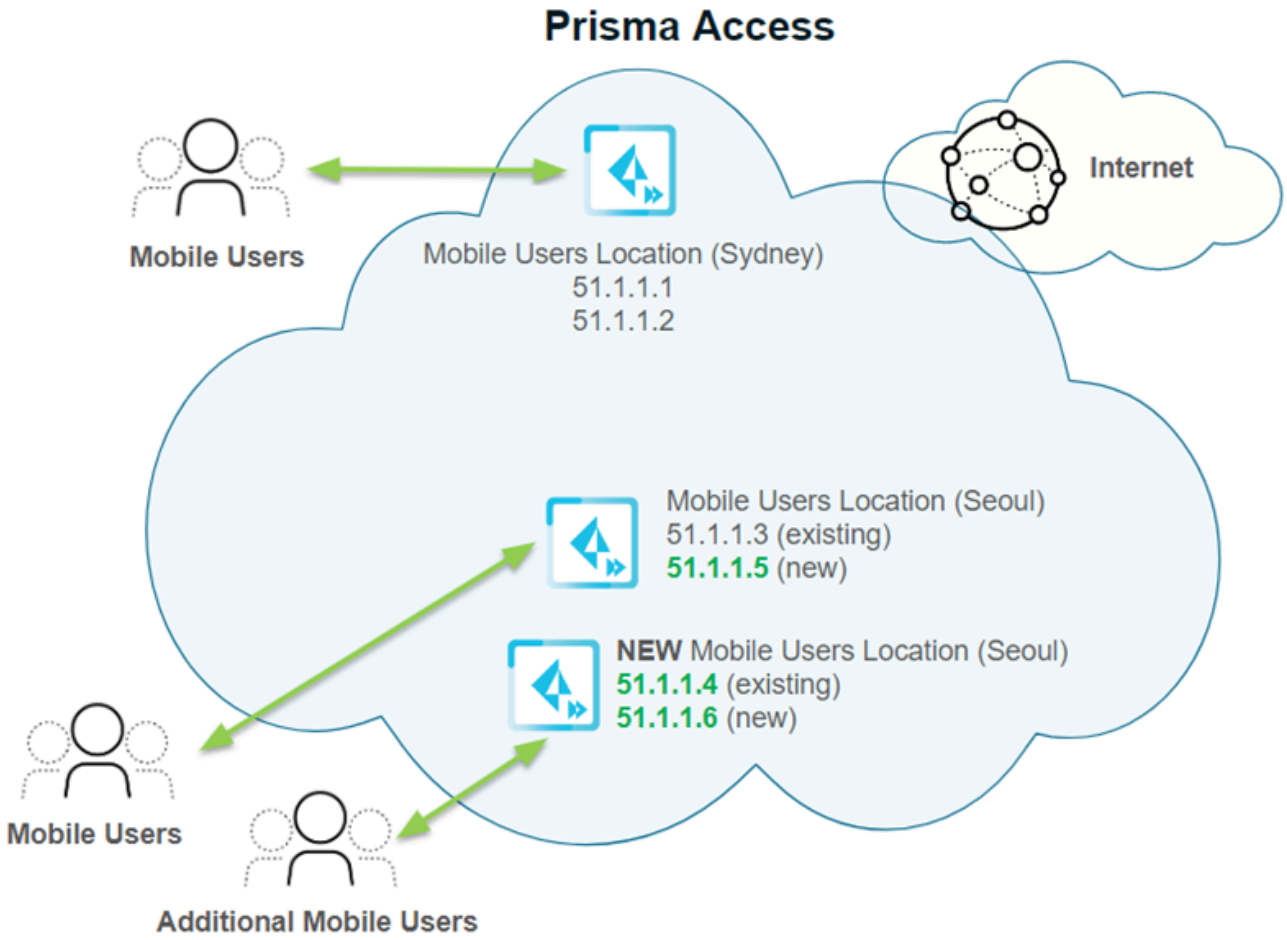
在下面的示例中，您为新的移动用户部署指定了亚太地区的两个地点：悉尼和首尔。每个位置都有两个网关 IP 地址。

 ©2025 Palo Alto Networks, Inc.



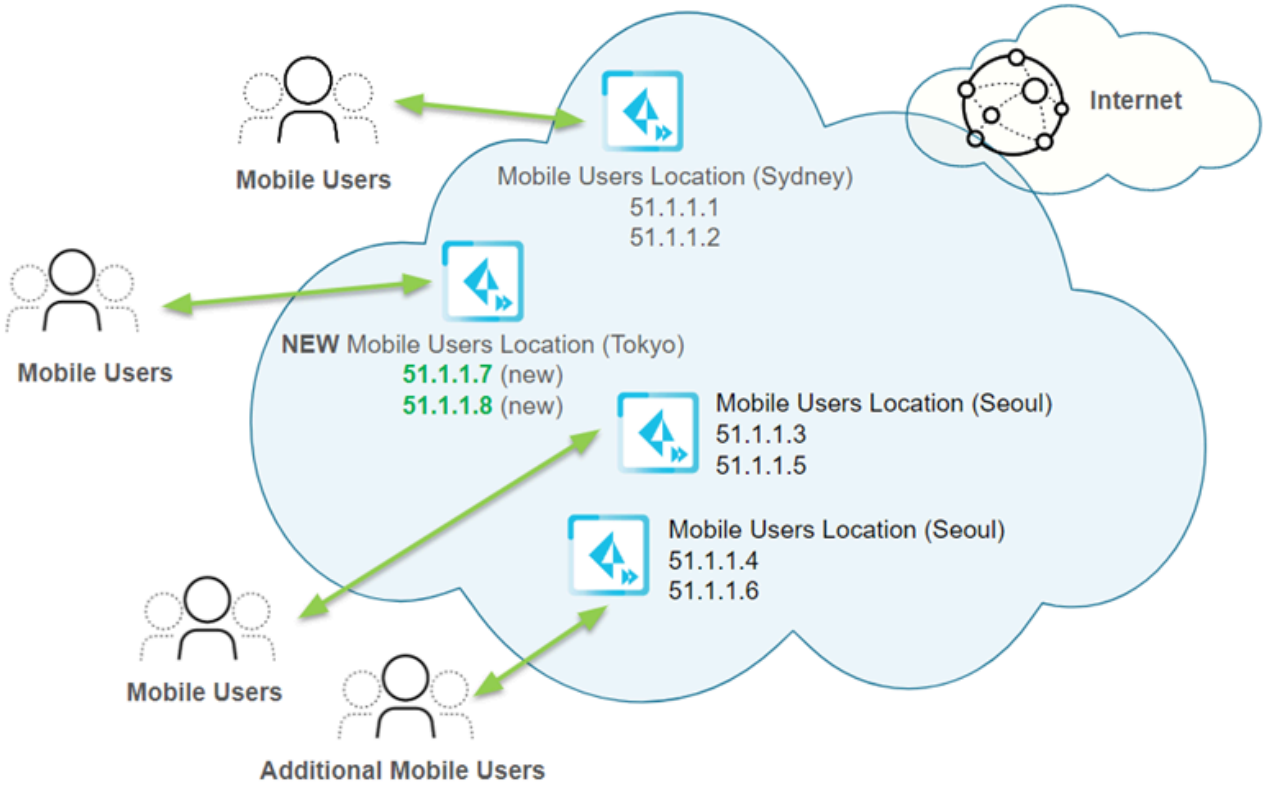
然后，大量用户登录到首尔这个地点。为了容纳这些额外的用户，Prisma Access 将为“首尔”地点添加了第二个网关，从第一个首尔网关 (51.1.1.4) 中获取一个网关地址，并将其分配给第二个首尔网关。然后添加另外两个 IP 地址（本示例中为 51.1.1.5 和 51.1.1.6），并将这两个 IP 地址添加到两个首尔网关中。

©2025 Palo Alto Networks, Inc.



然后您在亚太地区添加另一个位置“东京”。Prisma Access 将为新网关创建两个新的 IP 地址（51.1.1.7 和 51.1.1.8）。

 ©2025 Palo Alto Networks, Inc.



每次在您添加位置或发生扩展事件时，都应检索新出口和网关 IP 地址（由 Prisma Access 分配），并将其添加到网络中的允许列表中。Prisma Access 始终为每个位置中的所有活动网关保留两组 IP 地址。

回环 IP 地址分配（移动用户）

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证

回环地址是 Prisma Access 用于向内部源发出请求的 IP 地址，从基础结构子网分配。在基础设施或数据平面升级期间，移动用户的回环 IP 地址可能会更改。

在基础设施或数据平面升级期间，服务连接或远程网络连接的回环 *IP* 地址不会更改；只有移动用户的 *VoIP* 地址可能会更改。

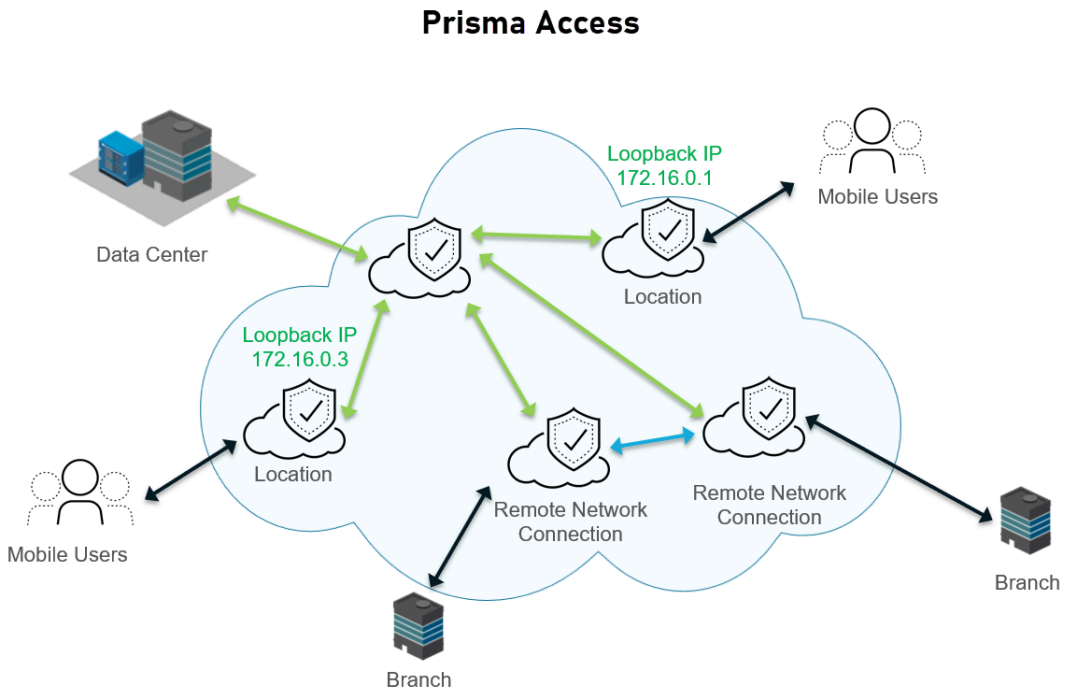
Prisma Access 从您在启用 Prisma Access 基础设施时指定的基础设施子网中分配回环 IP 地址。您可以将整个基础设施子网添加到允许列表中，并且在进行基础设施或数据平面升级期间，无需再为移动用户的回环 IP 地址变更进行规划。要查找基础设施子网，请选择

 ©2025 Palo Alto Networks, Inc.

- Prisma Access (Managed by Strata Cloud Manager)：**Workflows**（工作流） > **Prisma Access 设置** > **Prisma Access** > **Infrastructure Settings**（基础设施设置），然后查看 **Infrastructure Subnet**（基础设施子网）
- Prisma Access (Managed by Panorama)：**Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息） > **Service Infrastructure**（服务基础设施），然后查看 **Infrastructure Subnet**（基础设施子网）

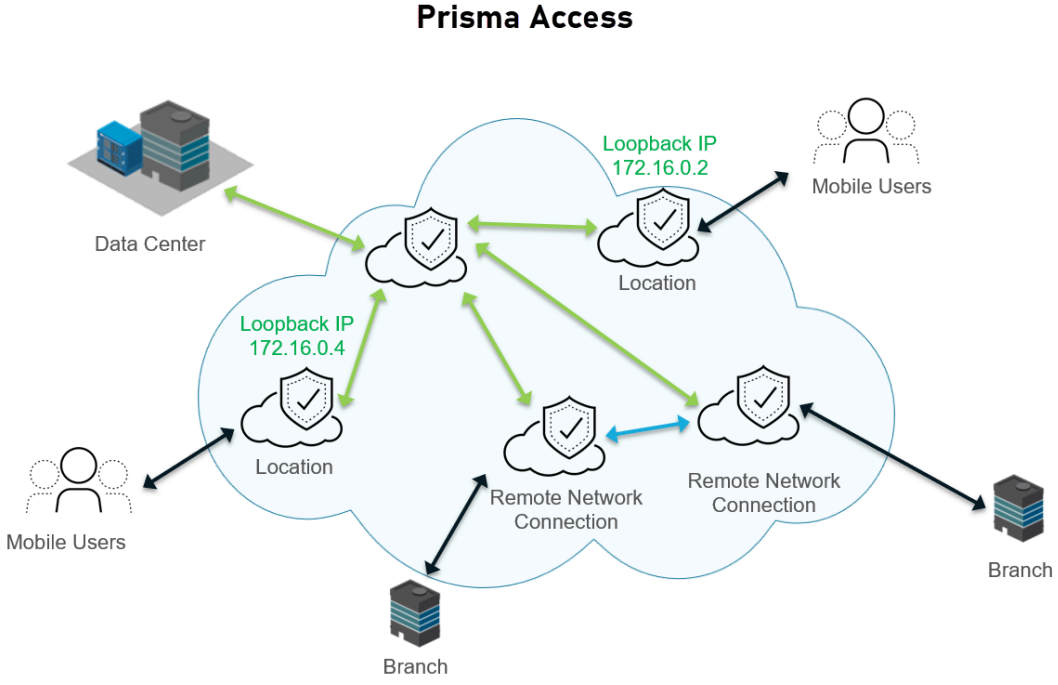
使用用来检索公共 IP 地址和回环 IP 地址的 API 来获取这些地址。

以下示例显示了基础设施子网为 172.16.0.0/16 的 Prisma Access 部署。Prisma Access 已为基础设施子网中的移动用户分配了回环 IP 地址 172.16.0.1 和 172.16.0.3。



在基础设施或数据平面升级后（例如，为云服务插件的新版本做准备），Prisma Access 会为基础设施子网中的移动用户分配两个不同的 IP 地址（172.16.0.1 更改为 172.16.0.2，172.16.0.3 更改为 172.16.0.4）。

©2025 Palo Alto Networks, Inc.

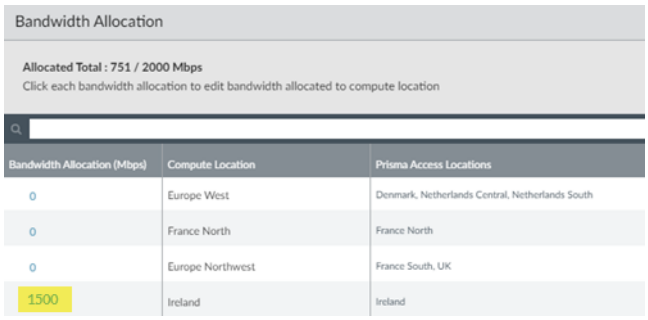


 ©2025 Palo Alto Networks, Inc.

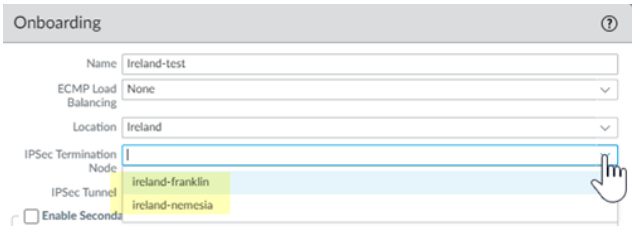
远程网络：IPSec 终止节点和服务 IP 地址

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	• Prisma Access 许可证

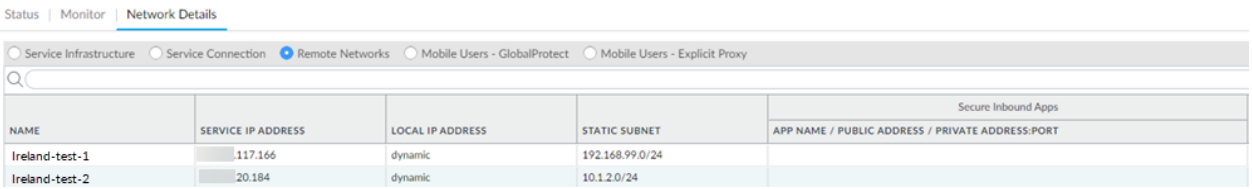
当您载入远程网络时，您将其与 *IPSec* 终止节点关联，每个 IPSec 终止节点都有一个与其关联的 **IP** 地址。您在为远程网络连接设置 IPSec 隧道时，将此地址用作 CPE 的对等 IP 地址。每个终端节点可以为您提供高达 1,000 Mbps 的带宽。将超过 1,000 Mbps 的带宽分配给计算地点为您提供了多个**Service IP Address**（服务 **IP** 地址）。



当您在爱尔兰的计算地点载入远程网络时，可以选择两个 IPSec 终止节点，因为总带宽超过 1,000 Mbps。



每个 IPSec 终止节点都有自己的 **Service IP Address**（服务 **IP** 地址），请参考 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息） > **Remote Networks**（远程网络）中显示的信息。



 ©2025 Palo Alto Networks, Inc.

远程网络：与带宽分配相关的 IP 地址变化

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证

如果您有旧版 Prisma Access，则本节适用按位置分配带宽的部署。任何新部署都按计算位置分配带宽；要了解 Prisma Access 如何分配这些 IP 地址，请参阅远程网络：IPSec 终止节点和服务 IP 地址。

远程网络连接的 IP 地址是唯一的、不共享的，并且专用于您的 Prisma Access 部署。Prisma Access 将其作为远程网络载入的一部分创建后，这些 IP 地址不会改变，并且 IP 地址在升级后仍然存在。但是，增加现有连接的带宽时要小心，因为如果增加带宽导致某个位置的带宽超过 500 Mbps，则远程网络的 IP 地址可能会发生变化。

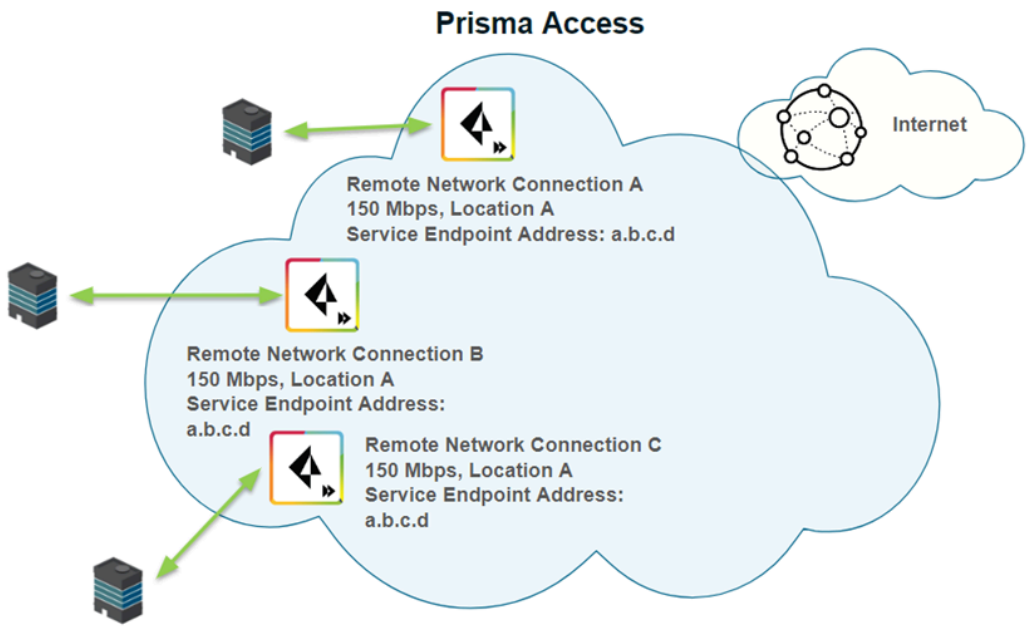
此外，如果 *Prisma Access* 创建新的 *Prisma Access* 计算位置，并决定将这个新的计算位置与您已经加入的位置一起使用，则传出 *IP* 地址可改变。

这些带宽指南仅在升级现有连接时适用。单个远程网络连接（即使是 1000 Mbps（预览版）连接）始终会接收单个 服务 IP 地址，无论其大小如何。

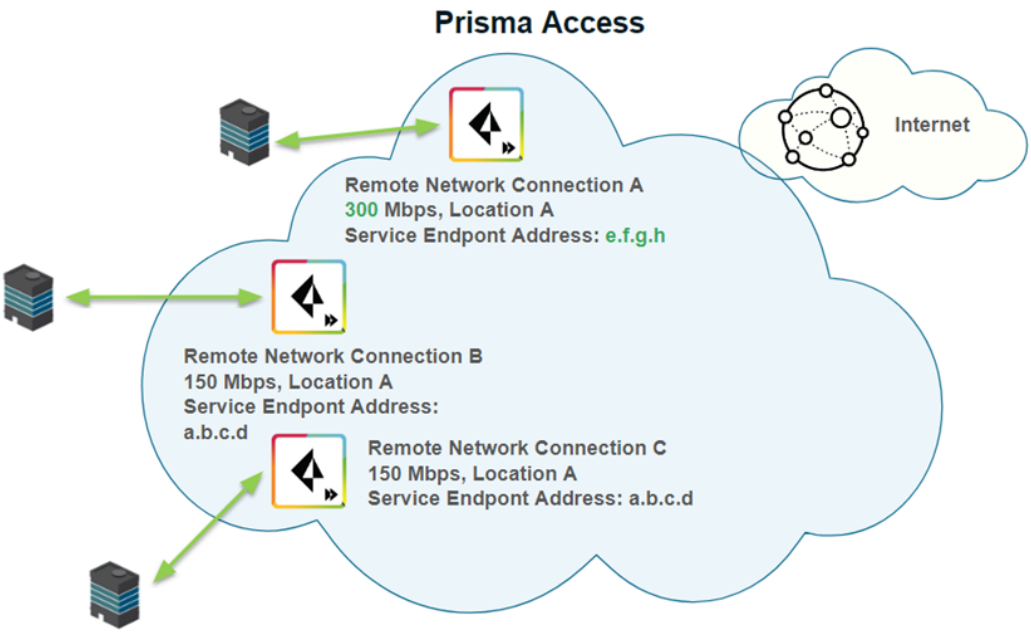
1000 Mbps 带宽选项处于预览模式。预览期间的吞吐量是尽力而为的，实际性能将根据流量组合而有所不同。

以下示例显示同一位置的三个远程网络连接，每个连接的带宽为 150 Mbps。由于总带宽为 500 Mbps，Prisma Access 为该位置的所有连接分配单个 IP 地址。

©2025 Palo Alto Networks, Inc.



以下示例显示远程网络连接 A 的带宽从 150 Mbps 增加到 300 Mbps。由于所有连接的总带宽现在已超过 500 Mbps，Prisma Access 为具有额外带宽的连接分配新的服务 IP 地址。其余服务 IP 地址保持不变。



相反，假设有四个远程网络的带宽为 100 Mbps，如果将其中一个远程网络的带宽增加到 100 Mbps，则该远程网络的服务 **IP** 地址不会改变，因为总带宽现在为 500 Mbps。

如果减少远程网络连接的带宽，则服务 ***IP*** 地址不会改变。

©2025 Palo Alto Networks, Inc.

要在 Panorama 中查找服务 IP 地址，请选择 **Panorama** > 云服务 > 状态 > 网络详细信息选项卡，然后单击远程网络单选按钮以显示远程网络的服务 **IP** 地址，或使用 API 脚本。

©2025 Palo Alto Networks, Inc.

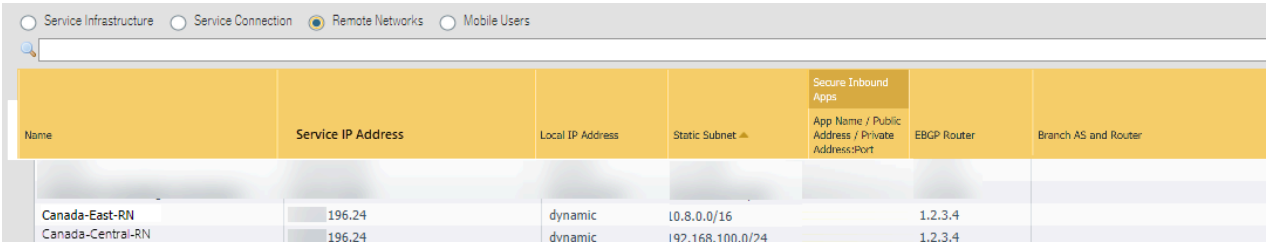
远程网络： IP 地址和传出 IP 地址分配

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	• Prisma Access 许可证

Prisma Access 在全球范围内拥有超过 100 个可用地点，以满足部署需求并提供本地化体验。两个位置可能映射到相同的地址，当您为远程网络连接设置 IPSec 隧道时，您将其用作对等 IP 地址。然而，这些位置可能会使用不同的传出 IP 地址，以确保用户获得该地区的正确默认语言。

服务连接不支持语言本地化，因为服务连接不支持访问互联网。*Prisma Access* 为每个服务连接仅分配一个服务 *IP* 地址，该 *IP* 地址在地理上注册到您在接入期间指定的位置对应的计算位置。

以下示例展示了在加拿大部署的两个远程网络位置的客户部署：加拿大中部和加拿大东部。Prisma Access 将相同的 **Service IP Address**（服务 **IP** 地址）分配给这两个位置。在配置远程网络隧道时，当您为远程网络连接创建 IPSec 隧道时，请使用此 IP地址 作为对等 IP 地址。



然而，加拿大东部使用的默认语言（法语）与加拿大中部（英语）不同。因此，Prisma Access 为其分配不同的传出 IP 地址。如果您运行用于传出 IP 地址的 API 脚本，您将收到这两个位置的两个不同 IP 地址。

©2025 Palo Alto Networks, Inc.

检索 Prisma Access 的 IP 地址

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

如果您手动将 Prisma Access 基础架构的 IP 地址添加到网络的允许列表中，或者如果您使用自动化脚本来强制实施基于 IP 的限制，以便限制对企业应用程序的入站访问，那么您应该了解这些地址的作用，为什么需要允许它们，以及您为检索它们而执行的任务。

在您完成 Prisma Access 配置之前，Prisma Access 不会提供这些 IP 地址。部署完成后，您可以使用 API 脚本检索这些 IP 地址。API 脚本使用您从 Prisma Access 用户界面上获取的 API 密钥和您创建的 .txt 文件（用于指定要检索的地址）。

虽然在完成 Prisma Access 配置之前，您不会执行这些任务，但提前了解这些概念很有用，因为这样您就能理解部署完成后该做什么。

- Strata Cloud Manager
- Panorama

检索 Prisma Access IP 地址 (Strata Cloud Manager)

Prisma Access 基础设施 IP 地址

下表列出了 Prisma Access 每种部署类型的用途，以及运行 API 脚本检索 IP 地址时使用的关键字，以及是否需要将它们添加到允许列表中。

部署类型	IP 地址类型	说明
移动用户	Prisma Access 网关 (**gp_gateway**)	检索网关 IP 地址。将网关和门户 IP 地址添加到移动用户部署的允许列表中。 移动用户连接到 Prisma Access 网关，以便访问您已提供访问权限的内部或互联网资源，例如 SaaS 或公共应用程序。
	Prisma Access 门户 (**gp_portal**)	检索门户 IP 地址。将网关和门户 IP 地址添加到移动用户部署的允许列表中。 移动用户登录 Prisma Access 门户来接收初始配置和网关位置。
	环回 IP 地址	此地址是 Prisma Access 为向内部源发出的请求使用的源 IP 地址，并从基础设施分配。将环回 IP 地址添加到网络中的允许

 ©2025 Palo Alto Networks, Inc.

部署类型	IP 地址类型	说明
		列表中，以便 Prisma Access 访问内部资源，如 RADIUS 或 Active Directory 身份验证服务器。 Palo Alto Networks 建议您允许网络中整个基础设施子网的所有 IP 地址，因为移动用户的环回地址可能会发生变化。
移动用户 — 显式代理	身份验证缓存服务 (ACS)	Prisma Access 存储显式代理用户的身份验证状态的服务的地址。 此地址仅用于移动用户（显式代理）部署。
	网络负载均衡器	Prisma Access 用于显式代理网络负载均衡器的地址。 此地址仅用于移动用户（显式代理）部署。
远程网络	远程网络 IP 地址 (**remote_network**)	包括 Prisma Access 为 Prisma Access 远程网络连接分配的 **Service IP Addresses**（服务 **IP** 地址），以及 Prisma Access 用于确保远程网络用户获得适合其所在地区的正确默认语言的 传出 IP 地址。将这些地址添加到网络的允许列表中，以便 Prisma Access 访问互联网资源。
	环回 IP 地址	这是 Prisma Access 用于向内部源发出请求的源 IP 地址，由基础设施子网分配。将环回 IP 地址添加到允许列表中，以便 Prisma Access 访问内部资源，如 RADIUS 或 Active Directory 身份验证服务器。

运行用于检索 IP 地址的 API 脚本

按照以下步骤检索 Prisma Access 在其基础设施中使用的 IP 地址。

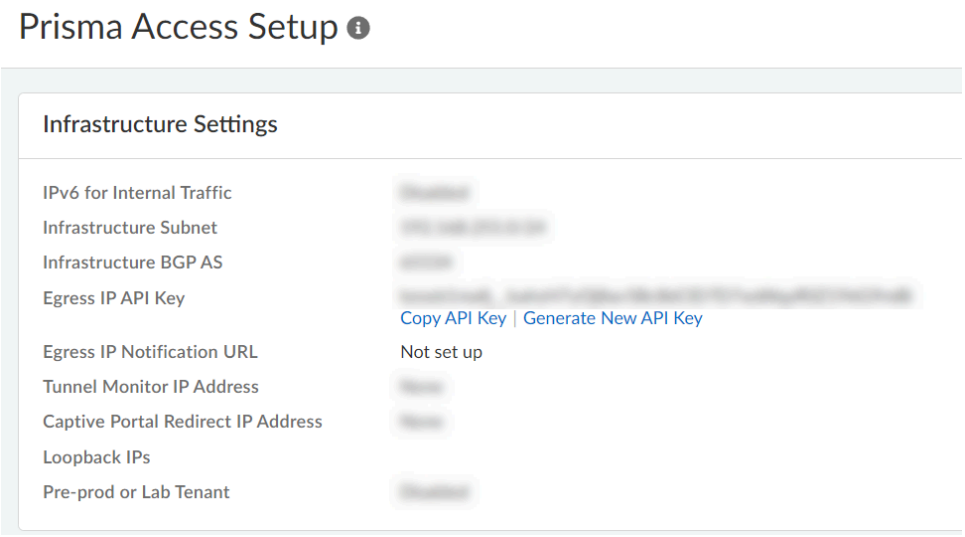
此命令不检索环回地址；要检索环回 *IP* 地址，请使用旧版 API 命令。

©2025 Palo Alto Networks, Inc.

STEP 1 | 获取 API 密钥。

您需要此密钥对 Prisma Access 进行身份验证，并使用 API 命令检索 IP 地址列表。

1. 转到 Prisma Access (Managed by Strata Cloud Manager)然后选择 **Workflows**（工作流）> **Prisma Access** 设置 > **Prisma Access** > **Infrastructure Settings**（基础架构设置）。
2. 选择 **Generate New API Key**（生成新的 **API** 密钥）。



如果您已经生成 API 密钥，则会显示当前密钥。如果您尚未生成密钥或想要替换现有密钥以满足密钥轮换的审计或合规性检查，请单击 **Generate New API Key**（生成新的 **API** 密钥）以获取新密钥。

STEP 2 | 创建一个.txt 文件并将 API 命令选项添加到文件中。

使用 API 的命令分为两步。首先，创建一个 .txt 文件，指定要检索的 IP 地址的参数，然后将该文件保存在可从运行命令的位置访问的文件夹中。然后，运行 API 并在命令中指定创建的 .txt 文件的名称和位置。

在 .txt 文件中指定以下关键字和参数。本主题中的示例使用文件名 **options.txt**，但您可以指定任何文件名，只要在命令中引用它即可。

参数	可能的选择（关键词）	注释
serviceType	**all** **remote_network** **gp_gateway** **gp_portal** **swg_proxy** **rbi**	**all** — 检索您需要添加到所有服务类型（远程网络、移动用户（网关和门户）以及清洁管道，适用于您的部署）的允许列表中的 IP 地址。 **remote_network** — 检索您需要添加到远程网络部署允许列表中的 IP 地址。 **gp_gateway** — 检索您需要添加到移动用户部署允许列表中的网关 IP 地址。 **gp_portal** — 检索您需要添加到移动用户部署允许列表中的门户 IP 地址。

 ©2025 Palo Alto Networks, Inc.

参数	可能的选择（关键词）	注释
		swg_proxy — 检索每个已部署的显式代理位置、身份验证缓存服务 (ACS) 和网络负载均衡器的传出 IP 地址。 **rbi** — 检索您需要添加到远程浏览器隔离 (RBI) 部署的允许列表中，以便连接到 SaaS 应用程序的传出 IP 地址。
addrType	**all** 活动 **service_ip** **auth_cache_service** **network_load_balancer**	**all** 或 **active** — 检索您需要添加到允许列表的所有 IP 地址。 此 API 不会检索环回 IP 地址。要检索环回 IP 地址，请使用旧版 API 命令。 **service_ip** — 检索 **Service IP Address**（服务 IP 地址），当您为远程网络连接设置 IPSec 隧道时，将其用作对等 IP 地址。 **auth_cache_service** — 检索显式代理 ACS 的 IP 地址（仅适用于移动用户 - 显式代理部署）。 **network_load_balancer** — 检索显式代理网络负载均衡器的 IP 地址（仅适用于移动用户 - 显式代理部署）。
actionType	**pre_allocate**	仅限移动用户部署 — **pre_allocate** 的 **actionType** 允许您检索适用于移动用户部署的 Prisma Access 网关和门户的 IP 地址或子网。将其与 **gp_gateway** 的 **serviceType** 一起使用，以便检索预分配的网关 IP 地址，并与 **gp_portal** 的 **serviceType** 一起使用，以便检索预分配的网关 IP 地址。 通过检索预先分配的 IP 地址，您可以在加入移动用户位置之前将网关和门户 IP 地址添加到组织的允许列表中，这样，移动用户就可以在您加入位置后立即访问外部 SaaS 应用程序。
location	**all** **deployed**	**all** — 从所有位置检索 IP 地址。对于移动用户部署，此关键字将检索您在载入期间添加的位置和未添加的位置的 IP 地址。 **deployed** — 检索您在移动用户载入期间添加的所有位置的 IP 地址。 此关键字仅适用于移动用户部署。Prisma Access 在配置期间关联每个移动用户位置的 IP 地址，即使您在移动用户载入期间没有选

©2025 Palo Alto Networks, Inc.

参数	可能的选择（关键词）	注释
		择该位置。如果您指定 **all**，API 命令将检索所有移动用户位置的 IP 地址，包括您未为部署选择的位置。如果您指定 **deploy**，则 API 命令将仅检索您在载入期间选择的位置的 IP 地址。

按照以下格式指定 .txt 文件中的选项：

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

STEP 3 | 输入以下命令来检索 IP 地址：

- 要使用 Prisma Access 2.1 中引入的较新 API，请输入以下命令：

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

截至 *2023* 年 *5* 月，一些云管理部署使用 *https://api.prod6.datapath.prismaaccess.com/getPrismaAccessIP/v2*（请注意，*URL* 中是 *prod6*，而不是 *prod*）。

- 要使用旧版 API，请输入以下命令。此命令使用将于 2022 年 5 月弃用的旧版 API 端点：

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

其中 *option.txt* 是您在上一步中创建的 .txt 文件，而 *Current-API-Key* 是 Prisma Access API 密钥。

例如，给定一个 .txt 文件名 **option.txt** 和一个 API 密钥 **12345abcde**，使用以下 API 命令检索所有位置的公共 IP 地址：

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

API 命令可以返回大量信息。为了使输出更具可读性，如果您安装了 *Python*，则可以在 *cURL* 命令末尾添加 `| python -m json.tool`。

API 命令返回以下格式的地址：

```
{ "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": "success"
```

其中：

- **address_details** 显示每个位置的地址详细信息。
  - **serviceType** 显示 IP 地址的类型（远程网络 (**remote_network**)、Prisma Access 网关 (**gp_gateway**)，Prisma Access 门户（**gp_portal**）、清洁管道（**clean_pipe**） 或远程浏览器隔离（**rbi**）。
  - **addressType** 指定使用 `addrType` 关键字指定的地址类型（如果您为移动用户位置预分配 IP 地址，则为 活动或预分配）。
  - 地址显示您需要添加到允许列表中的 IP 地址。

    如果 API 返回多个 IP 地址，Prisma Access 汇总地址字段中的 IP 地址。
- 地址列出了您需要添加到允许列表中的位置的所有 IP 地址。
- 区域是Prisma Access与 IP 地址相关联的位置。
- **zone_subnet** 是移动用户网关和门户的子网。如果您为移动用户位置预先分配 IP 地址，Prisma Access 也会提供此子网。

如果 .txt 文件中的选项有任何问题，API 将返回类似以下内容的错误：

```
 {"status": "error","result":"Invalid json format in the request.
trace_id: xxxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx "}
```

STEP 4 | 使用您检索到的 IP 地址更新本地服务器或 SaaS 应用程序策略规则上的允许列表。

API 命令示例

在 API 命令的 .txt 文件中输入关键字和参数时，请使用以下示例。要更改命令的输出，请更改 .txt 文件中的选项；命令本身不会改变。

检索这些 IP 地址	在 .txt 文件中指定这些参数	注释
移动用户 IP 地址		
所有移动用户 IP 地址	`{ "serviceType": "gp_gateway", "addrType": "all", "location": "all" }`	*addrType* 为 *all* 意味着 Prisma Access 检索所有移动用户网关 IP 地址。 *location* 为 *all*，表示 Prisma Access 会检索所有可用位置的 IP 地址，包括您尚未加入的位置。Prisma Access 会保留未加入位置的 IP 地址，以便您可以在加入位置之前将这些 IP 地址添加到允许列表中。

©2025 Palo Alto Networks, Inc.

检索这些 IP 地址	在 .txt 文件中指定这些参数	注释
已加入的移动用户位置的 IP 地址	`{ "serviceType": "gp_gateway", "addrType": "all", "location": "deployed" }`	*location* 类型为 *deployed* 意味着 Prisma Access 仅检索您在移动用户入职期间选择的位置的 IP 地址。
已注册移动用户位置的所有活动 IP 地址	`{ "serviceType": "gp_gateway", "addrType": "active", "location": "deployed" }`	*addrType* 为 *active* 意味着 Prisma Access 仅检索您加入的位置的 IP 地址。
远程网络 **IP** 地址		
检索所有远程网络 IP 地址	`{ "serviceType": "remote_network", "addrType": "all", "location": "all" }`	此命令检索您已加入的远程网络的公共和传出 IP 地址。请勿使用 *deployed* 的 *location*。您可以使用 *active* 的 *addrType*，但该命令检索的地址与指定 *addrType* 为 *all* 时相同。
显式代理 **IP** 地址		
检索已部署位置的 ACS IP 地址	`{ "serviceType": "swg_proxy", "location": "deployed", "addrType": "auth_cache_service" }`	此命令检索您的显式代理部署的 ACS IP 地址。输入 *all* 的 *addrType* 将检索所有地址类型（ACS 和网络负载均衡器 IP 地址）。
远程浏览器隔离 **IP** 地址		
检索已部署位置的远程浏览器隔离 (RBI) IP 地址	`{ "serviceType": "rbi", "location": "all", "addrType": "all" }`	此命令检索每个已部署 RBI 位置的传出 IP 地址。您可以将这些 IP 地址添加到允许列表中，以连接到 SaaS 应用程序。

用于检索 IP 和环回地址的传统脚本

下表显示了与 Prisma Access并提供有关适合您的部署类型的 API 的信息和建议。

这些传统命令检索两种类型的 IP 地址：*public IP* 和 *egress IP* 地址。我们为您提供了两种不同的旧式 API 命令，以便您可以检索需要添加到允许列表中的所有 IP 地址。

- *public IP address* 是 Prisma Access 用于向基于互联网的来源发出的请求。将公共 IP 地址添加到网络中的允许列表，以提供 Prisma Access 到互联网资源，如 SaaS 应用程序或可公开访问的合作伙伴应用程序。

  移动用户、远程网络和清洁管道部署使用公共 IP 地址。

 ©2025 Palo Alto Networks, Inc.

- *egress IP address* 是指 Prisma Access 用于到互联网的出站流量，并且您还必须将这些地址添加到允许列表中，以允许 Prisma Access 访问互联网资源。

  除其他目的外，Prisma Access 使用出口 IP 地址，以便用户能够以他们期望的语言接收网页 Prisma Access 地点。所有位置都有公共 IP 地址；但是，并非所有位置都有传出 IP 地址。以下位置不使用传出 IP 地址：

  - 巴林
  - 比利时
  - 法国北部
  - 法国南部
  - 中国香港
  - 爱尔兰
  - 韩国
  - 中国台湾
  - 英国

  移动用户、远程网络和清洁管道部署使用传出 IP 地址。

移动用户部署中使用的命令	
命令名称	注释
get_egress_ip_all=yes 命令 `curl -k -H header-api-key:`当前 *API* 密钥`"https://api.gpcloudservice.com/getAddrList/latest?get_egress_ip_all=yes`	此命令检索您添加到允许列表的所有 IP 地址，以便 Prisma Access 到互联网资源，如 SaaS 应用程序或可公开访问的合作伙伴应用程序。此命令有以下限制： • 此命令可以检索大量地址（超过 200 个）。如果您的企业无法将此数量的 IP 地址添加到允许列表，您可以使用 *gpcs_gp_gw* 和 *gpcs_gp_portal* 关键字仅检索您当前正在使用的 IP 地址；但是，每次添加位置时都必须重新运行这些命令。此外，如果发生扩展事件，您将需要将新的 IP 地址添加到允许列表中。 • Prisma Access 没有列出与这些 IP 地址关联的位置；因此，我们建议您将此命令返回的所有 IP 地址添加到允许列表中。 • 此命令不会给您环回地址。
gpcs_gp_gw 和 **gpcs_gp_portal** 关键字 `curl -k -H header-api-key:`*Current-API-Key*`"https://api.gpcloudservice.com/getAddrList/latest?fwType=gpcs_gp_gw |`	如果您的部署限制可以添加到允许列表的 IP 地址数量，请使用此命令。将此命令返回的所有 IP 地址添加到网络中的允许列表。您还可以使用此命令检索环回 IP 地址。

 ©2025 Palo Alto Networks, Inc.

移动用户部署中使用的命令	
命令名称	注释
gpcs_gp_portal&addrType=public_ip | egress_ip_list | loopback_ip"	

远程网络部署中使用的命令	
命令名称	注释
gpcs_remote_network 关键字 `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"`	使用此命令查找需要添加到远程网络部署允许列表中的 IP 地址。 您还可以使用此命令查找远程网络部署的传出 IP 地址；在某些情况下，传出和 IP 地址可能不同。

清洁管道部署中使用的命令	
命令名称	注释
gpcs_clean_pipe 关键字 `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"`	使用此命令查找需要添加到清洁管道部署允许列表中的 IP 地址。

检索移动用户部署的公共和传出 **IP** 地址

该旧脚本已被较新的 API 脚本取代。Palo Alto Networks 建议您使用较新的脚本来检索除环回地址之外的所有 IP 地址。

如果您要将公共 IP 地址添加到允许列表以允许移动用户访问 SaaS 或公共应用程序， Prisma Access 为每个网关和门户 IP 地址提供两个 IP 地址，以便在扩展或其他事件期间可以使用一个 IP 地址。您可以在使用这组 IP 地址之前将其添加到允许列表中，以防止在扩展事件期间移动用户访问 SaaS 或公共应用程序时出现任何问题。

通过完成以下任务来检索这些新地址：

 ©2025 Palo Alto Networks, Inc.

STEP 1 | 通过选择 **Workflows**（工作流） > **Prisma Access** 设置 > **Prisma Access** > **Infrastructure Settings**（基础架构设置） > **Generate New API Key**（生成新的 **API** 密钥）来获取 API 密钥。

您需要此密钥来验证 Prisma Access 并使用下面列出的 cURL 命令检索 IP 地址列表。只有 Panorama 管理员或超级用户可以生成或访问此 API 密钥。

STEP 2 | 输入以下命令来检索移动用户公共 IP 地址：

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

其中 *Current-API-Key* 是 Prisma Access API 密钥。

例如，给定 API 密钥 **12345abcde**，使用以下 API 命令检索所有位置的公共 IP 地址：

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

检索公共、环回和传出 **IP** 地址

要检索公共、环回和传出 IP 地址，请完成以下步骤。

STEP 1 | 检索 Prisma Access 的公共 IP 地址、环回 IP 地址或两者。

手动或在自动化脚本中使用 API 密钥和 API 端点 URL：

```
header-api-key：当前 API 密钥 “https://api.gpcloudservice.com/
getAddrList/latest?fwType=$fwType&addrType=$addrType”
```

其中您需要将当前 API 密钥替换为您的 API 密钥，并使用以下一个或两个关键字和参数：

关键字	描述
fwType 关键字	
gpcs_gp_gw	检索 Prisma Access 网关 IP 地址（用于移动用户部署）。
gpcs_gp_portal	检索 Prisma Access 门户 IP 地址（用于移动用户部署）。
gpcs_remote_network	检索 Prisma Access 远程网络 IP 地址（用于远程网络部署）。
gpcs_clean_pipe	检索 Prisma Access 清理管道 IP 地址。addrType
关键字	
公共 **IP**	检索 Prisma Access 对基于互联网的源发出的请求所使用的源 IP 地址。

 ©2025 Palo Alto Networks, Inc.

关键字	描述
	对于移动用户位置，Prisma Access 按位置列出 IP 地址。对于远程网络，Prisma Access 按远程网络名称列出 IP 地址。
传出 **IP** 列表	检索 IP 地址 Prisma Access 使用公共 IP 地址来向互联网传输额外的出站流量。 对于移动用户位置，Prisma Access 按位置列出 IP 地址。对于远程网络，Prisma Access 按远程网络名称列出 IP 地址。
回环 **IP**	检索 Prisma Access 对内部源（例如 RADIUS 或 Active Directory 服务器）发出的请求所使用的源 IP 地址，并从基础设施子网分配。

如果你不指定关键字， Prisma Access 检索所有 IP 地址。

例如，您可以尝试以下 cURL 命令来手动检索所有远程网络的公共 IP 地址列表：

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

或者使用一个简单的 python 脚本来检索所有 IP 地址的列表，例如：

```
 #!/usr/bin/python import subprocess import json api_key =
 '1234y9ydxb__0UmxetVTbC8XTyFMaoT4RBZBKBjfX419YVufeFG7' # Replace
 with your key api_end_point = 'https://api.gpcloudservice.com/
getAddrList/latest' # This call retrieves IP addresses
 for all your Prisma Access firewalls args = ['curl', '-
k', '-H', 'header-api-key:' + api_key, 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 | 使用您检索到的 IP 地址更新本地服务器或 SaaS 应用程序策略规则上的允许列表。

为移动用户位置预分配 IP 地址

Prisma Access 对于移动用户（GlobalProtect 部署）使用网关和门户 IP 地址，对于移动用户（显式代理部署）使用身份验证缓存服务 (ACS) 和网络负载均衡器 IP 地址。移动用户 - GlobalProtect IP 地址称为 *egress IP addresses*。如果您需要在加入位置之前预先分配移动用户 IP 地址（例如，如果您的组织需要将移动用户的 IP 地址添加到 GlobalProtect 部署的允许列表中，以允许移动用户访问外部 SaaS 应用程序），您可以运行 API 脚本 来 Prisma Access 在您加入之前，请提前为某个位置预先分配这些 IP 地址。然后，您可以在加入该位置之前将该位置的传出 IP 地址添加到组织的允许列表中。

 ©2025 Palo Alto Networks, Inc.

API 响应还包括请求位置的传出 IP 地址的公共 IP 池子网。您添加的任何位置的传出 IP 地址都是此子网的一部分。将子网添加到允许列表可供将来添加位置，而无需进一步修改允许列表。

除非您使用 API 脚本请求，否则 Prisma Access 不会预先分配您的 IP 地址和子网。运行预分配脚本后，它们的有效期为 90 天。这些 IP 地址和子网是唯一的，不共享，并且专用于您的 Prisma Access 有效期内部署。您必须在有效期结束之前登记您的位置，否则您将丢失地址；要随时查找有效期，请运行 API 脚本。

Palo Alto Networks 建议您仅为稍后想要加入的位置预先分配 *IP* 地址。

要预分配 IP 地址，请完成以下任务。

STEP 1 | 检索 Prisma AccessAPI 密钥。

STEP 2 | 通过创建 .txt 文件并在创建的 .txt 文件中指定以下选项来预先分配移动用户传出 IP 地址。

在 .txt 文件中输入以下文本：

- 移动用户 — **GlobalProtect** 部署：

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

- 移动用户—显式代理部署：

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

location 是您想要预先分配 IP 地址的 Prisma Access 位置。

最多输入 12 个位置。当 Prisma Access 检索预先分配的 IP 地址时，输入超过 12 个位置可能会导致超时错误。

STEP 3 | 输入此 CURL 命令。

 ©2025 Palo Alto Networks, Inc.

STEP 4 | 通过重新打开 .txt 文件、删除现有信息并编辑它来检索您请求的 IP 地址和子网，包括其有效期。

- 移动用户 — **GlobalProtect** 部署：
  - 要请求 Prisma Access 来检索所有预分配的 IP 地址，请在 .txt 文件中输入以下文本。

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

  - 要请求 Prisma Access 检索所有预先分配的 IP 地址 Prisma Access 给定位置的网关，在 .txt 文件中输入相同的信息，但在 .txt 文件中将 “`all`” 替换为 “`gp_gateway`””。
  - 要请求 Prisma Access 检索为指定位置的 Prisma Access 门户预分配的所有 IP 地址，请在 .txt 文件中输入相同的信息，但在 .txt 文件中用 “`gp_portal`” 替换 “`all`”。
- 移动用户—显式代理部署：

  要请求 Prisma Access 预分配您需要添加到显式代理部署允许列表中的所有 IP 地址，请在 .txt 文件中输入以下文本。

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

Palo Alto Networks 建议输入 `all`，以便您可以检索所有必需的预分配传出 IP 地址以添加到您的允许列表中。

对于“移动用户 - *GlobalProtect*”部署，*API* 命令可以返回大量信息。为了使输出更具可读性，如果您安装了 *Python*，则可以在 *cURL* 命令末尾添加 `| python -m json.tool`。

STEP 5 | 重新输入此 CURL 命令以检索预分配的地址。

Prisma Access 返回以下格式的信息：

```
    "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-
allocated", "validity_period_remaining" :"90 days" } , },
```

其中变量代表以下 API 命令输出：

变量	说明
prisma-access-zone1	Prisma Access 已检索预分配 IP 地址的位置。
ip-address1 和 *ip-address2*	Prisma Access 已为指定位置预先分配的传出 IP 地址。

 ©2025 Palo Alto Networks, Inc.

变量	说明
	Prisma Access 为每个位置检索两个 IP 地址；您必须将这两个 IP 地址都添加到允许列表中。
subnet-and-mask1 和 *subnet-and-mask2*	Prisma Access 已为您部署中的传出 IP 地址预先分配并保留的子网。
service-type	预分配的传出 IP 地址的类型（Prisma Access 门户为 `gp_portal`，Prisma Access 网关为 `gp_gateway`）。
validity-period	预分配 IP 地址有效的剩余时间（以天为单位）。 在 IP 地址有效期结束之前登记您的移动用户位置。如果预分配的 IP 地址过期，您可以重新运行 API 脚本来检索另一组预分配的 IP 地址。

如果您尝试为满足以下条件之一的位置预分配 IP 地址，则可能会收到错误：

- 您已载入该位置。
- 您载入后，又删除了该位置。

  在这种情况下，在 .txt 文件中输入以下文本以检索该位置的移动用户 - GlobalProtect IP 地址：

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

- 您已达到许可证允许的最大移动用户位置数，并且无法再添加任何位置。
- 您输入的位置名称不正确。
- 您输入了除 **gp_gateway** 之外的 **serviceType**。
- 您输入了除 **pre_allocate** 之外的 **actionType**。

设置 Prisma Access IP 地址更改通知

要获得远程网络的公共 IP 地址更改以及服务连接、远程网络连接和移动用户的环回 IP 地址更改的通知，您可以指定一个可在发生更改时提醒您的 URL。Prisma Access 使用 HTTP POST 请求发送通知。此 POST 请求包含以下 JSON 格式的通知数据：

```
{"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"}
```

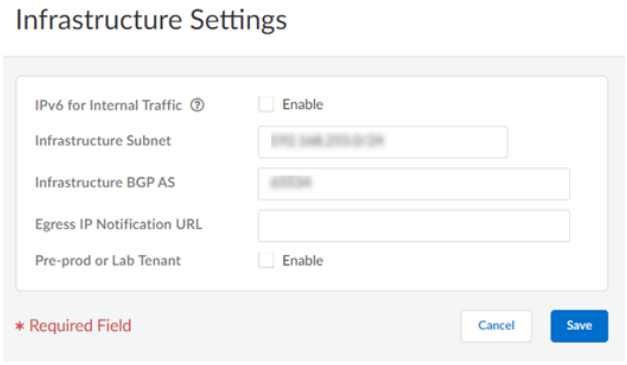
收到通知时，您必须遵循两步流程。首先，您必须手动或以编程方式检索 IP 或环回地址。然后，您必须更新组织相应允许列表中的 IP 地址，以确保用户不会遇到任何服务中断。

Prisma Access 会在新 *IP* 地址生效前几秒钟发送此通知。我们建议您使用自动化脚本来检索新 *IP* 地址并将其添加到网络中的允许列表中。

要添加 IP 通知 URL，请完成以下任务。

STEP 1 | 转到 **Workflows**（工作流） > **Prisma Access** 设置 > **Prisma Access** > **Infrastructure Settings**（基础架构设置）。

STEP 2 | 添加 **Egress IP Notification URL**（传出 **IP** 通知 **URL**），以便您在 Prisma Access 基础设施中收到 IP 地址更改通知。



您可以为正在监听更改通知的 HTTP 或 HTTPS Web 服务指定 IP 地址或 FQDN。Prisma Access 使用公共 IP 地址从互联网发送这些通知。

您无需推送配置即可使通知 URL 生效。

检索 Prisma Access IP 地址 (Panorama)

如果您手动将 Prisma Access 基础架构的 IP 地址添加到网络的允许列表中，或者如果您使用自动化脚本来强制实施基于 IP 的限制，以便限制对企业应用程序的入站访问，那么您应该了解这些地址的作用，为什么需要允许它们，以及您为检索它们而执行的任务。

Prisma Access 在您完成 Prisma Access 配置之后才会提供这些 IP 地址。部署完成后，您可以使用 API 脚本检索这些 IP 地址。API 脚本使用您从 Prisma Access 用户界面获取的 API 密钥和您创建的 .txt 文件，其中指定了您想要检索的地址。

 ©2025 Palo Alto Networks, Inc.

如果您有“移动用户 — *GlobalProtect*”部署，则可以使用 *Prisma Access* 用户界面（而不是此 *API*）来管理公共 *IP* 地址分配，并确认这些 *IP* 地址已添加到您的允许列表中，然后 *Prisma Access* 才能释放这些 *IP* 地址。这样，*Prisma Access* 就只会配置允许列表中的 *IP* 地址。

下表列出了 Prisma Access 用于每种部署类型的 IP 地址的列表，以及运行 API 脚本检索 IP 地址时使用的关键字，并描述是否应将它们添加到组织的允许列表中。

部署类型	IP 地址类型	说明
移动用户 — **GlobalProtect**	Prisma Access 网关 (**gp_gateway**)	网关 IP 地址。您必须将网关和门户 IP 地址都添加到移动用户部署的允许列表中。 移动用户连接到 Prisma Access 网关，以便访问您已提供访问权限的内部或互联网资源，例如 SaaS 或公共应用程序。 对于移动用户，在初始部署期间 Prisma Access 为您部署的每个位置分配两个 IP 地址。
	Prisma Access 门户 (**gp_portal**)	门户 IP 地址。您必须将网关和门户 IP 地址都添加到移动用户部署的允许列表中。 移动用户登录 Prisma Access 门户来接收初始配置和网关位置。
	环回 IP 地址	Prisma Access 为向内部来源发出的请求使用的源 IP 地址，从 配置 Prisma Access 服务基础设施 (Panorama) 进行分配。将环回 IP 地址添加到网络中的允许列表中，以便 Prisma Access 访问内部资源，如 RADIUS 或 Active Directory 身份验证服务器。 Palo Alto Networks 建议您允许网络中整个基础设施子网的所有 IP 地址，因为环回 IP 地址可能会发生变化。要查找基础设施子网，请选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network**

©2025 Palo Alto Networks, Inc.

部署类型	IP 地址类型	说明
		Details（网络详细信息） > **Service Infrastructure**（服务基础架构）。该子网显示在 **Infrastructure Subnet**（基础设施子）区域中。 要检索环回 IP 地址，请使用旧版 API 脚本。
移动用户 — 显式代理	身份验证缓存服务 (ACS)	Prisma Access 存储显式代理用户的身份验证状态的服务的地址。 此地址仅用于移动用户的显式代理。
	网络负载均衡器	Prisma Access 用于显式代理网络负载均衡器的地址。 此地址仅用于移动用户的显式代理。
远程网络	远程网络 IP 地址 (**remote_network**)	分配给 Prisma Access 远程网络连接的 **Service IP Addresses**（服务 **IP** 地址）Prisma Access，以及 Prisma Access 用于确保远程网络用户获得适合其所在地区的正确默认语言的 远程网络：IP 地址和传出 IP 地址分配。将这些地址添加到网络的允许列表中，以便 Prisma Access 访问互联网资源。
	环回 IP 地址	Prisma Access 为向内部来源发出的请求使用的源 IP 地址，从 配置 Prisma Access 服务基础设施 (Panorama) 进行分配。将环回 IP 地址添加到允许列表中，以便 Prisma Access 访问内部资源，如 RADIUS 或 Active Directory 身份验证服务器。要检索环回 IP 地址，请使用旧版 API 脚本。

©2025 Palo Alto Networks, Inc.

部署类型	IP 地址类型	说明
清洁管道	清洁管道 IP 地址 (**clean_pipe**)	将这些 IP 地址添加到允许列表中，以允许 Clean Pipe 服务访问互联网资源。
	环回 IP 地址	Prisma Access 为向内部来源发出的请求使用的源 IP 地址，从 配置 Prisma Access 服务基础设施 (Panorama) 进行分配。将环回 IP 地址添加到允许列表中，以便 Prisma Access 访问内部资源，如 RADIUS 或 Active Directory 身份验证服务器。要检索环回 IP 地址，请使用旧版 API 脚本。

运行用于检索 Prisma Access IP 地址的 API 脚本

Prisma Access 提供了一个 API 脚本，您可以使用它来检索其在其基础设施中使用的公共和私有 IP 地址。如果您需要将公共 IP 地址添加到组织网络中的允许列表中，请按照以下步骤通过 API 脚本检索这些 IP 地址。

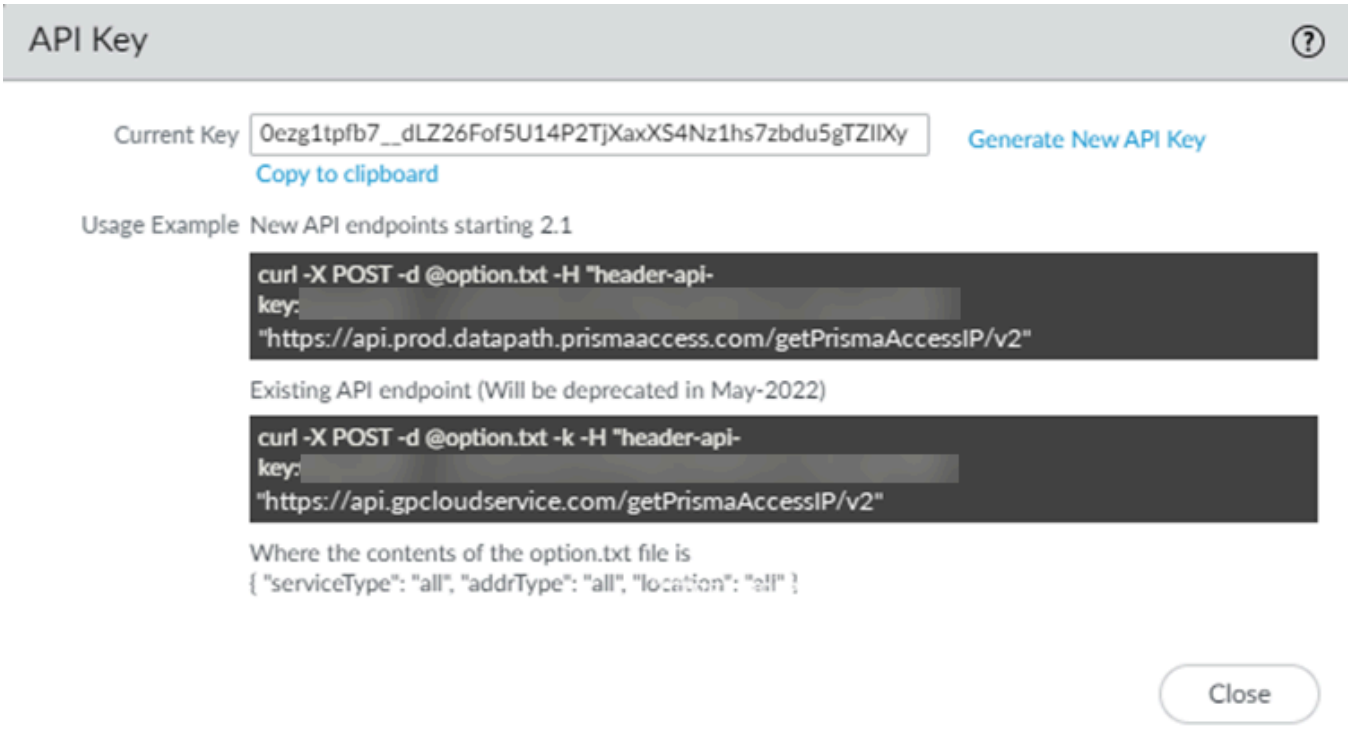
此命令不检索环回地址；要检索环回 *IP* 地址，请使用旧版 API。

 ©2025 Palo Alto Networks, Inc.

STEP 1 | 获取 API 密钥。

您需要此密钥对 Prisma Access 进行身份验证，并使用 API 命令检索 IP 地址列表。只有 Panorama 管理员或超级用户可以生成或访问此 API 密钥。

1. 选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Service Setup**（服务设置）。
2. 选择 **Generate API Key**（生成 **API** 密钥对）。



如果您已经生成 API 密钥，则会显示 **Current Key**（当前密钥）。如果您尚未生成密钥或想要替换现有密钥以满足密钥轮换的审计或合规性检查，请单击 **Generate New API Key**（生成新的 **API** 密钥）来获取新密钥。

STEP 2 | 创建一个.txt 文件并将 API 命令选项添加到文件中。

使用 API 的命令分为两步。首先，创建一个 .txt 文件，指定要检索的 IP 地址的参数，然后将该文件保存在可从运行命令的位置访问的文件夹中。然后，运行 API 并在命令中指定创建的 .txt 文件的名称和位置。

在 .txt 文件中指定以下关键字和参数。有关示例，请参阅 检索 Prisma Access IP 地址的 API 示例。本文档中的示例使用文件名 **options.txt**，但您可以指定任何文件名，只要在命令中引用它即可。

参数	可能的选择（关键字）	注释
serviceType	**all** **remote_network** **gp_gateway**	**all** — 检索您需要添加到所有服务类型（远程网络、移动用户（网关和门户）以及清洁管道，适用于您的部署）的允许列表中的 IP 地址。

©2025 Palo Alto Networks, Inc.

参数	可能的选择（关键字）	注释
	gp_portal **clean_pipe** **swg_proxy** **rbi**	**remote_network** — 检索您需要添加到远程网络部署允许列表中的 IP 地址。 **gp_gateway** — 检索您需要添加到移动用户部署允许列表中的“移动用户 — GlobalProtect” 网关 IP 地址。 **gp_portal** — 检索您需要添加到移动用户部署允许列表中的“移动用户 — GlobalProtect” 门户 IP 地址。 **clean_pipe** — 检索您需要添加到清洁管道部署允许列表中的 IP 地址。 **swg_proxy** — 检索每个已部署的显式代理位置、身份验证缓存服务 (ACS) 和网络负载均衡器的传出 IP 地址。 **rbi** — 检索您需要添加到远程浏览器隔离 (RBI) 部署的允许列表中，以便连接到 SaaS 应用程序的传出 IP 地址。
addrType	**all** 活动 **service_ip** **auth_cache_service** **network_load_balancer**	**all** 或 **active** — 检索您需要添加到允许列表的所有 IP 地址。 此 API 不会检索环回 IP 地址。要检索环回 IP 地址，请使用旧版 API。 **service_ip** — 检索 **Service IP Address**（服务 **IP** 地址），当您为远程网络连接设置 IPSec 隧道时，将其用作对等 IP 地址。 **auth_cache_service** — 检索显式代理 ACS 的 IP 地址（仅适用于显式代理部署）。 **network_load_balancer** — 检索显式代理网络负载均衡器的 IP 地址（仅适用于显式代理部署）。

©2025 Palo Alto Networks, Inc.

参数	可能的选择（关键字）	注释
actionType	**pre_allocate**	仅限移动用户部署 — **pre_allocate** 的 **actionType** 允许您检索适用于移动用户部署的 Prisma Access 网关和门户的 IP 地址或子网。将其与 **gp_gateway** 的 **serviceType** 一起使用，以便检索预分配的网关 IP 地址，并与 **gp_portal** 的 **serviceType** 一起使用，以便检索预分配的门户 IP 地址。 通过检索预先分配的 IP 地址，您可以在加入移动用户位置之前将网关和门户 IP 地址添加到组织的允许列表中，这样一来，移动用户就可以在您加入位置后立即访问外部 SaaS 应用程序。
location	**all** **deployed**	**all** — 从所有位置检索 IP 地址。对于移动用户部署，此关键字将检索您在载入期间添加的位置和未添加的位置的 IP 地址。 **deployed** — 检索您在移动用户载入期间添加的所有位置的 IP 地址。 此关键字仅适用于移动用户部署。Prisma Access 在配置期间将 IP 地址与每个移动用户位置关联，即使您在移动用户载入期间没有选择该位置。如果您指定 **all**，API 命令将检索所有移动用户位置的 IP 地址，包括您未选择用于部署的位置。如果您指定 **deploy**，则 API 命令将仅检索您在载入期间选择的位置的 IP 地址。

按照以下格式指定 .txt 文件中的选项：

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


©2025 Palo Alto Networks, Inc.

STEP 3 | 输入以下命令来检索 IP 地址：

- 要使用 Prisma Access 2.1 中引入的较新 API，请输入以下命令：

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

从 *2023* 年 *5* 月开始，一些 *Panorama* 管理部署使用 *https://api.prod6.datapath.prismaaccess.com/getPrismaAccessIP/v2*（请注意，*URL* 中是 *prod6*，而不是 *prod*）。

- 要使用旧版 API，请输入以下命令。此命令使用将于 2022 年 5 月弃用的旧版 API 端点：

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

其中 *option.txt* 是您在上一步中创建的 .txt 文件，而 *Current-API-Key* 是 Prisma Access API 密钥。

例如，给定一个 .txt 文件名 **option.txt** 和一个 API 密钥 **12345abcde**，使用以下 API 命令检索所有位置的公共 IP 地址：

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

*API*命令可以返回大量信息。为了使输出更具可读性，如果您安装了 *Python*，则可以在 *cURL* 命令末尾添加 `| python -m json.tool`。

API 命令返回以下格式的地址：

```
{ "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": "success"
```

其中：

- **address_details** 显示每个位置的地址详细信息。
  - **serviceType** 显示 IP 地址的类型（远程网络 (**remote_network**)、Prisma Access 网关 (**gp_gateway**)，Prisma Access 门户（**gp_portal**）、清洁管道（**clean_pipe**） 或远程浏览器隔离（**rbi**）。
  - **addressType** 指定使用 `addrType` 关键字指定的地址类型（如果您为移动用户位置预分配 IP 地址，则为 活动或预分配）。
  - 地址显示您需要添加到允许列表中的 IP 地址。

    如果 API 返回多个 IP 地址，Prisma Access 汇总地址字段中的 IP 地址。
- 地址列出了您需要添加到允许列表中的位置的所有 IP 地址。
- 区域是Prisma Access与 IP 地址相关联的位置。
- **zone_subnet** 是移动用户网关和门户的子网。如果您为移动用户位置预先分配 IP 地址，Prisma Access 也会提供此子网。

如果 .txt 文件中的选项有任何问题，API 将返回类似以下内容的错误：

```
 {"status": "error","result":"Invalid json format in the request.
trace_id: xxxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx "}
```

STEP 4 | 使用您检索到的 IP 地址更新本地服务器或 SaaS 应用程序策略规则上的允许列表。

针对“移动用户—GlobalProtect”部署部署的 IP 优化

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager)	• Prisma Access 许可证 • Prisma Access 版本 5.0 或更高版本

IP 优化是一套体系结构增强功能，可减少部署中的 IP 地址总数，简化您的允许列表工作流，同时提高弹性并加快 Prisma Access 租户的接入速度。

- 针对“移动用户—**GlobalProtect** 部署”简化了公共 **IP** 地址允许列表管理–无论是添加一个 Prisma Access 位置，还是在现有 Prisma Access 位置体验扩展事件，都可能会导致新的 IP 地址被分配给移动用户安全处理节点 (MU-SPN)。最佳实践是检索新的出口和网关 IP 地址（由 Prisma Access 分配），然后添加到网络中的允许列表，以避免 SaaS 应用程序或企业防火墙中断。这可能会导致您需要管理大量 IP 地址的情况。IP 优化减少了您必须管理的 IP 地址数量。
- 更快接入 **Prisma Access** 租户–如果没有 IP 优化，您需要为 Prisma Access 和您的专用网络中的每台设备分配唯一的专用 IP 地址，这需要您从有限的企业可路由 IP 地址空间中分配较大的 IP 块。IP 优化允许 Prisma Access 默认从共享地址空间分配地址，并对私有应用程序流量进行 NAT。

 ©2025 Palo Alto Networks, Inc.

IP 优化仅适用于新的 Prisma Access GlobalProtect 部署。现有的 GlobalProtect 部署不符合条件，您从现有多租户部署创建的新租户也不符合条件。此外，如果您将 GlobalProtect 部署从使用本地网关和门户迁移到 Prisma Access，则在启用此功能之前，请确保所有用户运行的 GlobalProtect 应用程序版本为 6.1.4 及更高版本、6.2.3 及更高版本，或者 6.3.0 及更高版本。

请记下以下有关 IP 优化的额外要求：

- IP 优化需要 Prisma Access 5.0 或更高版本（对于移动用户优化），可以在第一次设置 GlobalProtect 时启用 IP 优化。
- 首次设置 GlobalProtect 时，系统会询问您是否要启用 Prisma Access IP 优化。
- IP 优化部署不支持使用 IPv6 访问公共（外部）应用程序；支持私有应用程序访问。要为您的新 Prisma Access 部署启用 IPv6，请联系您的 Palo Alto Networks 客户团队，他们将创建一个 TAC 案例来满足您的请求。
- 即使启用了 IP 优化，用于检索 Prisma Access IP 地址的 API 仍将照常工作。

©2025 Palo Alto Networks, Inc.

检索 Prisma Access IP 地址的 API 示例

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	• Prisma Access 许可证

在 .txt 文件中输入关键字和参数以供 API 命令检索基础架构 IP 地址时，请使用以下示例。要更改命令的输出，请更改 .txt 文件中的选项；命令本身不会更改。

检索这些 IP 地址	在 .txt 文件中指定这些参数	注释
移动用户 IP 地址		
所有移动用户 IP 地址	`{ "serviceType": "gp_gateway", "addrType": "all", "location": "all" }`	*addrType* 为 *all*，表示 Prisma Access 会检索所选设置 GlobalProtect 移动用户(Panorama) 位置的所有 IP 地址。 *location* 为 *all*，表示 Prisma Access 会检索所有可用位置的 IP 地址，包括您尚未加入的位置。Prisma Access 会保留未加入位置的 IP 地址，以便您可以在加入位置之前将这些 IP 地址添加到允许列表中。

已加入的移动用户位置的 IP 地址	`{ "serviceType": "gp_gateway", "addrType": "all", "location": "deployed" }`
	或
	`{ "serviceType": "gp_gateway", "addrType": "active", "location": "deployed" }`
		location 类型为 *deployed*，表示 Prisma Access 仅检索您已加入位置的 IP 地址。
		使用 *all* 或 *active* 的 *addrType* 检索这些网关 IP 地址。

远程网络 IP 地址		
检索所有远程网络 IP 地址	`{ "serviceType": "remote_network", "ad`	此命令检索您已加入的远程网络的公共和出口 IP 地址。请勿使用 *deployed* 的

©2025 Palo Alto Networks, Inc.

检索这些 **IP** 地址	在 **.txt** 文件中指定这些参数	注释
	`drType": "all", "loc ation": "all" }`	*location*。您可以使用 *active* 的 *addrType*，但该命令检索的地址与指定 *addrType* 为 *all* 时相同。
Clean Pipe IP 地址		
检索所有 Clean Pipe IP 地址	`{ "serviceType": " clean_pipe", "addrTy pe": "all", "locatio n": "all" }`	此命令检索您已加入的 Clean Pipe 的公共和出口 IP 地址。请勿使用 *deployed* 的 *location*。您可以使用 *active* 的 *addrType*，但该命令检索的地址与指定 *addrType* 为 *all* 时相同。
显式代理 **IP** 地址		
检索已部署位置的 ACS IP 地址	`{ "serviceType": "sw g_proxy", "location" : "all", "addrType": "all" }`	此命令检索每个已部署的显式代理位置、身份验证缓存服务 (ACS) 和网络负载均衡器（仅与显式代理部署相关）的出口 IP 地址。
远程浏览器隔离 **IP** 地址		
检索已部署位置的远程浏览器隔离 (RBI) IP 地址	`{ "serviceType": " rbi", "location": "a ll", "addrType": "al l" }`	此命令检索每个已部署 RBI 位置的出口 IP 地址。您可以将这些 IP 地址添加到允许列表中，以连接到 SaaS 应用程序。

©2025 Palo Alto Networks, Inc.

在 Prisma Access IP 地址更改时收到通知

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

要在远程网络的公共 IP 地址发生变更，以及服务连接、远程网络连接和移动用户的环回 IP 地址发生变更时收到通知，您可以指定一个URL，以便在发生变更时收到相关警报。Prisma Access 使用 HTTP POST 请求发送通知。此 POST 请求包含以下 JSON 格式的通知数据：

```
 {"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"}
```

收到通知时，您必须遵循两步流程。首先，您必须手动或编程来检索 IP 或环回地址。然后，您必须更新组织相应允许列表中的 IP 地址，以确保用户不会遇到任何服务中断。

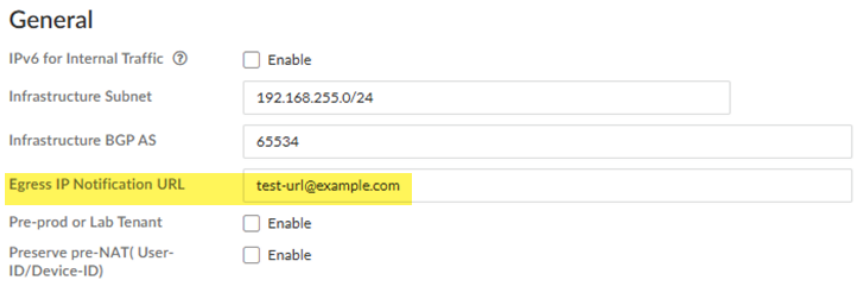
Prisma Access 会在新 *IP* 地址生效前几秒钟发送此通知。我们建议您使用自动化脚本来检索新 *IP* 地址并将其添加到网络中的允许列表中。

要添加 IP 地址通知 URL，请完成以下任务。

- 对于 Prisma Access (Managed by Strata Cloud Manager) 部署，转到 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Prisma Access** > **Infrastructure Settings**（基础设施设置），单击齿轮以编辑设置，添加 **Egress IP Notification URL**（出口 **IP** 通知 **URL**）（可

 ©2025 Palo Alto Networks, Inc.

以通过该 URL 收到有关 Prisma Access 基础设施中 IP 地址变化的通知），然后单击 **Save**（保存）以保存您的更改。



- 对于 Prisma Access (Managed by Panorama) 部署，请转到 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Service Setup**（服务设置），然后添加 **IP Change Event Notification URL**（**IP** 更改事件通知 **URL**）（可通过该 URL 收到有关 Prisma Access 基础设施中 IP 地址变化的通知），然后单击 **OK**（确定）。



您可以为监听更改通知的 HTTP 或 HTTPS Web 服务指定 IP 地址或 FQDN。Prisma Access 使用公共 IP 地址从互联网发送这些通知。

您无需提交更改，通知 URL 会自动生效。

©2025 Palo Alto Networks, Inc.

使用旧脚本检索 IP 地址

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	• Prisma Access 许可证

本节中描述的命令已被更新的 *API* 脚本取代 *Prisma Access 1.5*；但是，当您需要获取环回地址时，或者在脚本或其他自动化工具中使用它们的部署时，它们仍然受支持。

下表显示了与 Prisma Access并提供有关适合您的部署类型的 API 的信息和建议。

这些旧命令还会检索 公共 *IP* 和 *IP* 地址；不过，Palo Alto Networks 建议您使用较新的 API 脚本来检索这些命令，并且仅使用旧 API 来检索环回 IP 地址。

- 公有 *IP* 地址是 Prisma Access 用于向基于互联网的来源发出的请求。将公共 IP 地址添加到网络中的允许列表，以提供 Prisma Access 到互联网资源，如 SaaS 应用程序或可公开访问的合作伙伴应用程序。

  移动用户、远程网络和清洁管道部署使用公共 IP 地址。

- 传出 *IP* 地址 是指 Prisma Access 用于到互联网的出站流量，并且您还必须将这些地址添加到允许列表中，以允许 Prisma Access 访问互联网资源。

  除其他目的外，Prisma Access 使用传出 IP 地址，以便用户能够以他们期望的语言从 Prisma Access 地点接收网页。所有位置都有公共 IP 地址；但是，并非所有位置都有出口 IP 地址。以下位置不使用出口 IP 地址：

  - 在 Prisma Access 1.4 发布之前添加的任何位置。
  - 巴林
  - 比利时
  - 法国北部
  - 法国南部
  - 中国香港
  - 爱尔兰
  - 韩国
  - 中国台湾
  - 英国

  移动用户、远程网络和清洁管道部署使用出口 IP 地址。

移动用户部署中使用的命令	
命令名称	注释
get_egress_ip_all=yes 命令	此命令检索您添加到允许列表的所有 IP 地址，以便 Prisma Access 访问互联网资源，如 SaaS

©2025 Palo Alto Networks, Inc.

移动用户部署中使用的命令	
命令名称	注释
`curl -H header-api-key:Current-API-Key"https://api.prod.datapath.prismaaccess.com/getAddrList/latest?get_egress_ip_all=yes`	应用程序或可公开访问的合作伙伴应用程序。此命令有以下限制： • 此命令可以检索大量地址（超过 200 个）。如果您的企业无法将此数量的 IP 地址添加到允许列表，您可以使用 *gpcs_gp_gw* 和 *gpcs_gp_portal* 关键字仅检索您当前正在使用的 IP 地址；但是，每次添加位置时都必须重新运行这些命令。此外，如果发生扩展事件，您将需要将新的 IP 地址添加到允许列表中。 • Prisma Access 没有列出与这些 IP 地址关联的位置；因此，我们建议您将此命令返回的所有 IP 地址添加到允许列表中。 • 此命令不会给您环回地址。
gpcs_gp_gw 和 **gpcs_gp_portal** 关键字 `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"`	如果您的部署限制可以添加到允许列表的 IP 地址数量，请使用此命令。您必须将此命令返回的所有 IP 地址添加到网络中的允许列表中。您还可以使用此命令检索环回 IP 地址。

远程网络部署中使用的命令	
命令名称	注释
gpcs_remote_network 关键字 `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"`	使用此命令查找需要添加到远程网络部署允许列表中的 IP 地址。 您还可以使用此命令查找远程网络部署的传出 IP 地址；在某些情况下，传出和 IP 地址可能不同。

©2025 Palo Alto Networks, Inc.

清洁管道部署中使用的命令	
命令名称	注释
gpcs_clean_pipe 关键字 `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"`	使用此命令查找需要添加到清洁管道部署允许列表中的 IP 地址。

检索移动用户 IP 地址

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

从 *Prisma Access 1.5* 开始，此旧版脚本已被新的 *API* 脚本取代*Palo Alto Networks* 建议您使用脚本来检索除环回地址之外的所有 *IP* 地址。

如果您要添加公有 IP 地址以允许列表，以允许移动用户访问 SaaS 或公有应用程序，Prisma Access 为每个网关和门户 IP 地址提供两个 IP 地址，以便在扩展或其他事件期间可以使用一个 IP 地址。您可以在使用这组 IP 地址之前将其添加到 allow 名单中。为移动用户能够在扩展事件期间访问 SaaS 或公共应用程序防止任何问题。

通过完成以下任务来检索这些新地址：

STEP 1 | 通过选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Service Setup**（服务设置）来通过选择 API 密钥；然后，选择 **Generate API Key**（生成 **API** 密钥）。

您需要此密钥来对 Prisma Access 进行身份验证，并使用下面列出的 curl 命令检索 IP 地址列表。只有 Panorama 管理员或超级用户可以生成或访问此 API 密钥。

 ©2025 Palo Alto Networks, Inc.

STEP 2 | 输入以下命令来检索移动用户公共 IP 地址：

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

其中 *Current-API-Key* 是 Prisma Access API 密钥。

例如，给定 API 密钥 **12345abcde**，使用以下 API 命令检索所有位置的公共 IP 地址：

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

Prisma Access 每使用一组公有 IP 地址，则分配另一组 IP 地址。如果您认为 Prisma Access 已使用添加的公有 IP 地址集（例如，如果大量移动用户访问了单个位置），您可以再次运行此 API 命令以查找新的公有 IP 地址集。升级后，所有 IP 地址都将保留。

检索公共、环回和传出 IP 地址

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	• Prisma Access 许可证

从 *Prisma Access 1.5* 开始，此旧脚本已被新版脚本取代。*Palo Alto Networks* 建议您使用较新的脚本来检索除环回地址之外的所有 *IP* 地址。

要检索公共、环回和传出 IP 地址，请完成以下步骤。

STEP 1 | 获取 API 密钥并添加 **IP Change Event Notification URL**（**IP** 更改事件通知 **URL**），这样您就可以在 Prisma Access 基础设施中收到 IP 地址更改的通知。

有关详细信息，请参阅在 Prisma Access IP 地址更改时收到通知。

STEP 2 | 检索 Prisma Access 的公共 IP 地址、环回 IP 地址或两者。

手动或在自动化脚本中使用 API 密钥和 API 端点 URL：

```
header-api-key：当前 API 密钥 "https://
api.prod.datapath.prismaaccess.com/getAddrList/latest?
fwType=$fwType&addrType=$addrType“,
```

其中您需要将当前 API 密钥替换为您的 API 密钥，并使用以下一个或两个关键字和参数：

关键字	描述
fwType 关键字	

 ©2025 Palo Alto Networks, Inc.

关键字	描述
gpcs_gp_gw	检索 Prisma Access 网关 IP 地址（用于移动用户部署）。
gpcs_gp_portal	检索 Prisma Access 门户 IP 地址（用于移动用户部署）。
gpcs_remote_network	检索 Prisma Access 远程网络 IP 地址（用于远程网络部署）。
gpcs_clean_pipe	检索 Prisma Access 清理管道 IP 地址。addrType
关键字	
公共 **IP**	检索 Prisma Access 对基于互联网的源发出的请求所使用的源 IP 地址。 对于移动用户位置， Prisma Access 按位置列出 IP 地址。对于远程网络，Prisma Access 按远程网络名称列出 IP 地址。
传出 **IP** 列表	检索 IP 地址 Prisma Access 使用公共 IP 地址来向互联网传输额外的出站流量。 对于移动用户位置， Prisma Access 按位置列出 IP 地址。对于远程网络，Prisma Access 按远程网络名称列出 IP 地址。
回环 **IP**	检索 Prisma Access 对内部源（例如， RADIUS 或 Active Directory 服务器）发出的请求所使用的源 IP 地址， 并从基础设施子网分配。

如果你不指定关键字， Prisma Access 会检索所有 IP 地址。

例如， 您可以尝试以下 Curl 命令来手动检索所有远程网络的公共 IP 地址列表：

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

或者使用一个简单的 python 脚本来检索所有 IP 地址的列表， 例如：

```
  #!/usr/bin/python import subprocess import json api_key
 = '1234y9ydxb__0UmxetVTbC8XTyFMaoT4RBZBKBjfX419YVufeFG7'
 # Replace with your key api_end_point = 'https://
api.prod.datapath.prismaaccess.com/getAddrList/latest' # This call
```

 ©2025 Palo Alto Networks, Inc.

```
retrieves IP addresses for all your Prisma Access firewalls args =
['curl', '-k', '-H', 'header-api-key:' + api_key, 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)
```

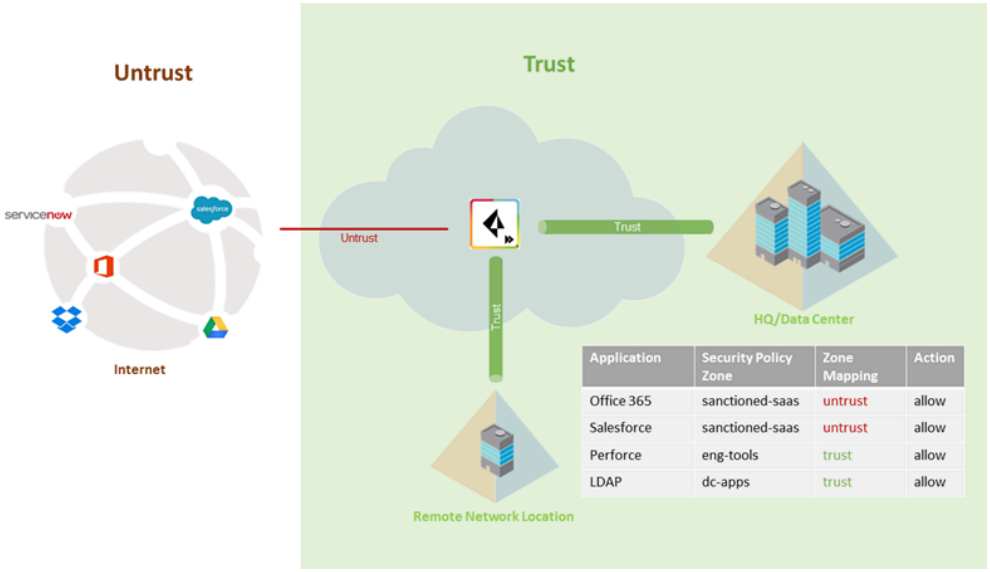
STEP 3 | 使用您检索到的 IP 地址更新本地服务器或 SaaS 应用程序策略规则上的允许列表。

 ©2025 Palo Alto Networks, Inc.

Prisma Access 区域

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

在防火墙上，区域与接口相关联。但在 Prisma Access 中，将自动设置网络基础设施。这意味着您无需再担心配置接口以及将它们与您创建的区域进行关联这些复杂问题。但为了实现一致的安全策略实施，您必须创建区域映射，以便 Prisma Access 将知道是否将区域与内部（信任）接口或外部（不信任）接口关联。这将确保您的安全策略规则正确执行。默认情况下，您推送到 Prisma Access 的所有区域都被设置为不信任。您应该将与互联网流量相关的任何区域（包括您认可的 SaaS 应用程序）设置为不信任。但对于所有允许访问内部网络或数据中心内的应用程序的区域，都必须将它们映射到信任。请注意下面的示例，所有经批准的 SaaS 应用程序（在本例中为 Office 365 和 Salesforce）都被划分到经批准的 SaaS 区域，以便对这些应用程序的使用实现可见性和策略执行。要使 Prisma Access 能够将批准的 SaaS 区域与面向外部的接口相关联，必须将此区域映射到不受信任。类似地，eng-tools 和 dc-apps 区域提供对公司办公室内应用程序的访问，因此您必须将它们指定为受信任区域。



Prisma Access 支持三个区域（信任、不信任和无客户端 VPN），并通过为您设置它们来简化策略创建。

服务区	说明
可信	包含公司网络内所有受信任和已登录的 IP 地址、服务连接或移动用户的区域。

©2025 Palo Alto Networks, Inc.

服务区	说明
不可信	公司网络之外的所有不受信任的 IP 地址、服务连接或移动用户。默认情况下，任何不受信任的 IP 地址或移动用户在本质上都是不可信的。
无客户端 VPN	对使用 HTML、HTML5 和 JavaScript 技术的常见企业Web 应用程序进行安全的远程访问。用户无需安装客户端软件，即可从启用 SSL 的 Web 浏览器进行安全访问。如果您需要合作伙伴或承包商能够访问应用程序，且安全启用非托管资产（包括个人设备），则这非常有用。 无客户端 *VPN* 的区域默认映射到信任区域；此设置无法更改。

显示 **inter-fw** 区域的 Prisma Access 日志是用于 Prisma Access 基础设施内通信的日志。

创建区域时，请勿使用以下任何区域名称，因为这些名称是用于内部区域的名称：

- trust
- untrust
- inter-fw
- 用于远程网络的任何名称（远程网络名称在 Strata Logging Service 日志中用作源区域）

显示 *inter-fw* 区域的 *Prisma Access* 日志是用于 *Prisma Access* 基础设施内通信的日志。

 ©2025 Palo Alto Networks, Inc.

Prisma Access 的 DNS

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

Prisma Access 允许您指定 DNS 服务器来解析组织内部域和外部域。这样做是为了提供对公司网络上服务（如 LDAP 和 DNS 服务器）的访问权限，特别是在您计划设置服务连接以提供对 HQ 或数据中心中此类资源的访问权限时。Prisma Access 支持针对移动用户的 DNS 解析 - Global Protect 和远程网络部署。对内部域列表中的域的 DNS 查询将发送到您的本地 DNS 服务器，以确保资源可供 Prisma Access 远程网络用户和移动用户使用。

例如，如果您希望企业域的 DNS 查找仅限于企业 DNS 服务器，请在此处指定企业域和企业 DNS 服务器。要确保端点使用 **DNS** 代理 **IP** 地址，必须将其配置为通过 **Workflow**（工作流）> **Prisma Access Setup**（**Prisma Access** 设置）> **Prisma Access** > **Prisma Access DNS Proxy IP Address**（**Prisma Access DNS** 代理 **IP** 地址）中显示的 IP 地址解析 DNS。

- Strata Cloud Manager
- Panorama

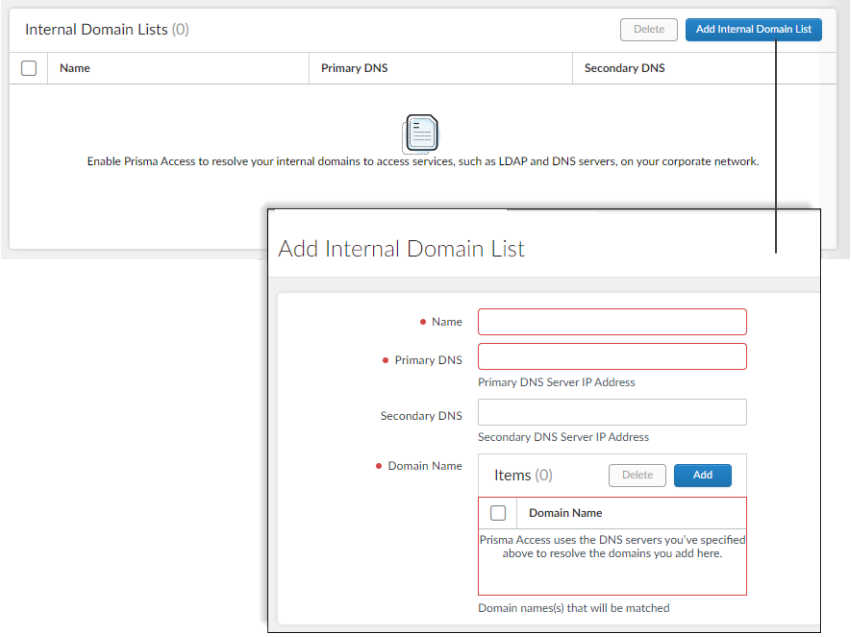
Prisma Access (Strata Cloud Manager) 的 DNS

下面介绍了如何设置 Prisma Access 以解析内部域，以及如何为移动用户部署和远程网络站点自定义 DNS 设置（以解析内部域和公共域）。

 ©2025 Palo Alto Networks, Inc.

设置适用于所有流量的内部域列表。

1. 选择 **Workflows**（工作流） > **Prisma AccessSetup**（设置） > **Prisma Access**，然后选择 **Add Internal DNS Servers**（添加内部**DNS**服务器）。



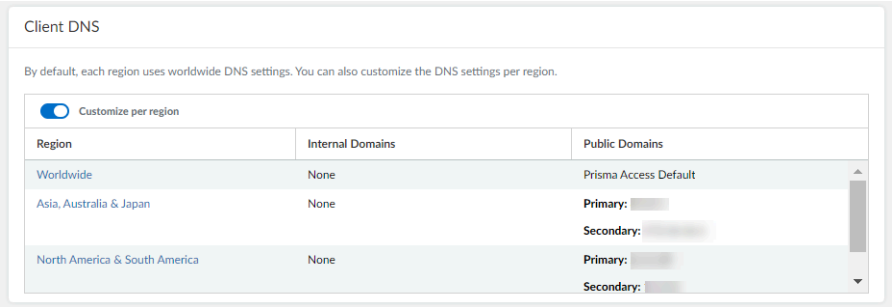
2. 输入 Prisma Access 用于解析内部域名的主 DNS 服务器和辅助 DNS 服务器。
3. 添加内部域名以发送到这些 DNS 服务器进行解析。

   在域列表中的域前可以使用通配符 (*)，例如 *.acme.local 或 *.acme.com。

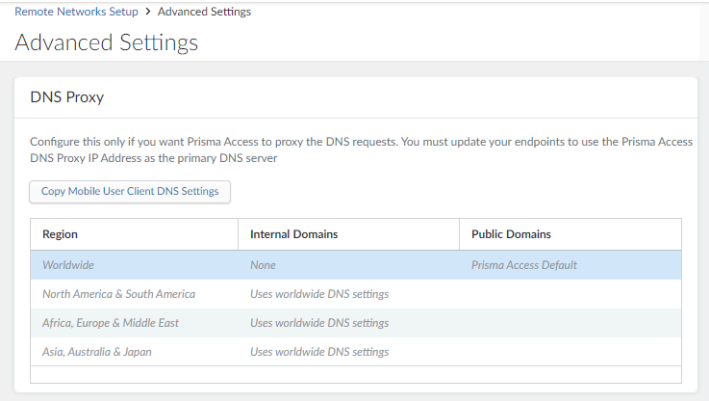
 ©2025 Palo Alto Networks, Inc.

添加内部域列表，这些域仅适用于特定移动用户部署或远程网络站点。

1. 配置 DNS 设置：
   - 移动用户 — 转到 **Workflows**（工作流） > **Prisma AccessSetup**（设置） > **GlobalProtect** > **Infrastructure Settings**（基础设施设置），然后找到 **Client DNS**（客户端 **DNS**）。



   - 远程网络 — 转到 **Workflows**（工作流） > **Prisma AccessSetup**（设置） > **Remote Networks**（远程网络） > **Advanced Settings**（高级设置），然后找到 **DNS Proxy**（**DNS** 代理）。



2. 使用默认值“Worldwide”（Prisma Access 的默认 DNS 服务器）或根据地区自定义设置。在任何情况下，选择要调整的区域并自定义该区域的 DNS 设置。
3. 选中 **use these DNS settings to resolve internal domains**（使用这些 **DNS** 设置来解析内部域）选项，也可以选择 **Use the internal DNS Server for resolving public domains too**（也使用内部 **DNS** 服务器解析公共域）。如果不选择此选项，Prisma Access 将使用其云默认 DNS 服务器来解析公共域的请求。
4. 允许从移动用户 IP 地址池中的所有地址到 DNS 服务器的流量。

   Prisma Access 中的 DNS 代理会将请求发送到您指定的 DNS 服务器。DNS 请求中的源地址是您分配给区域的 IP 池中的第一个 IP 地址。为确保您的 DNS 请求能够到达服务器，需要确保允许移动用户 IP 地址池中的所有地址向您的 DNS 服务器发送流量。

Prisma Access (Panorama) 的 DNS

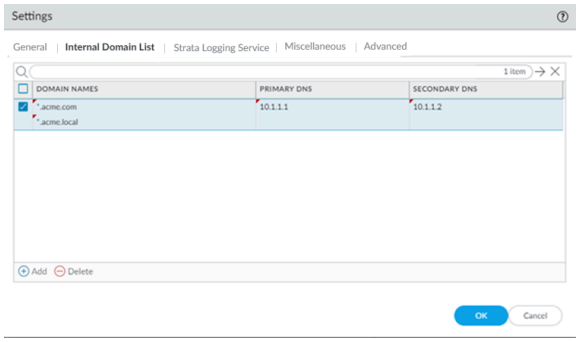
设置 Prisma Access 以解析内部域。

 ©2025 Palo Alto Networks, Inc.

设置适用于所有流量的内部域列表。

1. 选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Service Setup**（服务设置），然后单击齿轮图标来编辑“Settings（设置）”。
2. 选择 **Internal Domain List**（内部域列表）选项卡。
3. 添加您希望 Prisma Access 用于解析内部域名的域名、主 DNS 和辅助 DNS 服务器。

   在域列表中的域前可以使用通配符 (*)，例如 *.acme.local 或 *.acme.com。

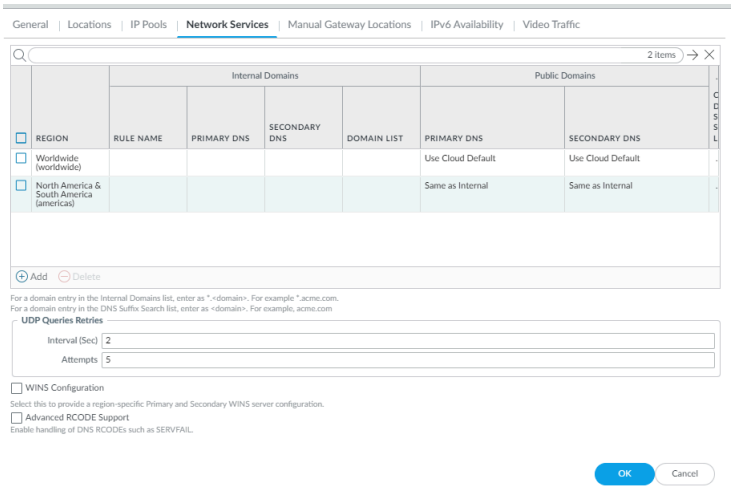


 ©2025 Palo Alto Networks, Inc.

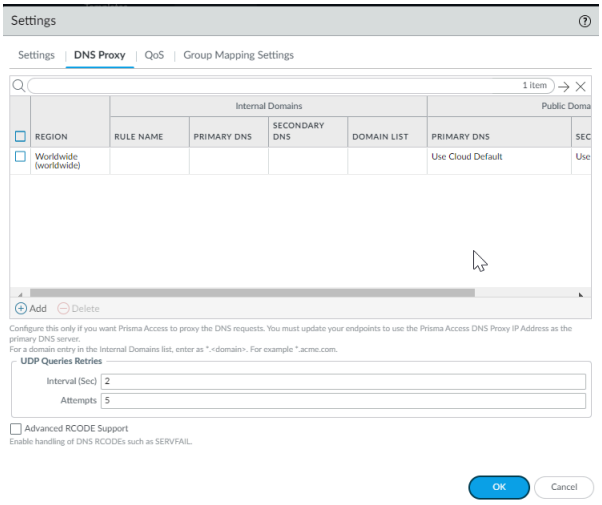
添加内部域列表，这些域仅适用于特定移动用户部署或远程网络站点。

1. 配置 DNS 设置：

   - 移动用户 — 转至 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > 移动用户 - **GlobalProtect**（**Mobile Users - GlobalProtect**），选择外部网关，然后单击 **Network Services**（网络服务）。



   - 远程网络 — 转到 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Remote Networks**（远程网络） > **Settings**（设置） > **DNS Proxy**（**DNS** 代理）。



2. 使用默认值“Worldwide”（Prisma Access 的默认 DNS 服务器）或根据地区自定义设置。在任何情况下，选择要调整的区域并自定义该区域的 DNS 设置。
3. 添加一条或多条规则来配置内部域的 DNS 设置。

   - 输入规则的唯一规则名称。
   - 如果您希望内部 DNS 服务器仅解析您指定的域，请在“Domain Lists（域列表）”中输入要解析的域。在域前面指定一个星号；例如 *.acme.com。最多可以指定 1024 个域条目。

     Prisma Access 具有预定义规则，可使用云默认服务器解析 *.amazonaws.com 域。如果希望内部 DNS 服务器解析更具体的 *.amazonaws.com 域（例

 ©2025 Palo Alto Networks, Inc.

如，*.s3.amazonaws.com），请在域列表中输入 URL。Prisma Access 在列表中按从长到短，从上到下的顺序评估域名。

- 如果您具有可以访问内部域的自定义 DNS 服务器，请指定主 DNS 服务器和辅助 DNS 服务器的 IP 地址，或选择“Use Cloud Default（使用云默认设置）”以使用 Prisma Access 的默认 DNS 服务器。

4. 指定 **Public Domains**（公共域）的 DNS 设置。
   - **Use Cloud Default**（使用云默认值） — 使用默认的 Prisma Access DNS 服务器。
   - **Same as Internal Domains**（与内部域相同） — 使用您用于解析内部域的同一服务器。选择此选项时，用于解析公共域的 DNS 服务器与 **Internal Domains**（内部域）部分中第一条规则配置的服务器相同。
   - **Custom DNS server**（自定义 **DNS** 服务器） — 如果您有可以访问公共（外部）域的 DNS 服务器，请在该字段中输入主 DNS 服务器地址。
5. （可选）您可以选择“Add a DNS Suffix（添加 DNS 后缀）”来添加客户端 DNS 后缀列表，以指定在用户输入了客户端无法解析的不合格主机名时应该在本地使用的后缀（例如 acme.local）。根据《Prisma Access 管理员指南（Panorama 托管）》的说明，不要在域名后缀（例如 acme.com）前输入通配符 (*)。可以添加多个后缀。
6. 允许从移动用户 IP 地址池中的所有地址到 DNS 服务器的流量。

   Prisma Access 中的 DNS 代理会将请求发送到您指定的 DNS 服务器。DNS 请求中的源地址是您分配给区域的 IP 池中的第一个 IP 地址。为确保您的 DNS 请求能够到达服务器，需要确保允许移动用户 IP 地址池中的所有地址向您的 DNS 服务器发送流量。

 ©2025 Palo Alto Networks, Inc.

Prisma Access 的高可用性

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	• Prisma Access 许可证

在高可用性 (HA) 配置中部署 Panorama 设备可以在系统或网络发生故障的情况下提供冗余，并确保您与 Prisma Access 的连接不会中断。在 HA 配置中，一个 Panorama 对端设备是活动-主要，另一个是被动-辅助。如果发生故障转移，辅助对端设备将变为活动状态并接管管理 Prisma Access 的角色。

为简化高可用性（HA）设置，请在购买 Prisma Access 和 Strata Logging Service 授权码及组件之后，且在激活并安装 Panorama Managed Prisma Access 之前，对高可用性模式下的 Panorama 设备进行配置。同时，要将计划安装云服务插件的主 Panorama 设备的序列号与授权码进行关联。但是，您也可以使用此过程来配置已安装该插件的现有 Panorama 设备。

无论您是刚刚开始使用一对新的 Panorama 设备，还是已经设置了独立的 Panorama 设备并完成了许可和安装过程，请确保在启用 HA 之前检查先决条件：

- 您必须在 客户支持门户 (CSP) 中，将 Panorama 对端设备 HA 注册到同一客户帐户。
- Panorama 对端设备必须具有相同的外形规格（相同型号的硬件设备或相同的虚拟设备）、相同的操作系统版本，并且必须具备相同的许可证组合。Prisma Access 和 Strata Logging Service 需要高级支持许可证。
- 主 Panorama 设备的序列号与您的 Prisma Access 和 Strata Logging Service 授权码绑定。如果您已经在独立 Panorama 设备上安装并设置了插件，请确保使用该 Panorama 设备作为主要对端设备。如果需要将此独立对端设备指定为辅助 Panorama 设备，请联系 Palo Alto Networks 支持以获取有关将许可证转移到 Panorama 主要对端设备的帮助，然后再继续。

如果您为某一对 *Panorama* 禁用 *HA* 并恢复到单个 *Panorama* 管理 *Prisma Access* 的配置，则必须 重新验证您的帐户，以防止在检索 *Prisma Access* 组件状态时出现错误。

要在 HA 配置中设置 Panorama 设备，请完成以下步骤。

STEP 1 | 设置 Panorama 高可用性。

将 Panorama 主设备设置为 **Primary**（主要），将 Panorama 辅助设备设置为 **Secondary**（辅助），并确保 Panorama 主设备的序列号与您的 Prisma Access 和 Strata Logging Service 授权码绑定。

 ©2025 Palo Alto Networks, Inc.

STEP 2 | 确保主要（活动）和辅助（被动）Panorama 设备已同步，并且它们之间的 HA 链接状态为正常。

1. 访问 Panorama 主设备上的 **Dashboard**（指示盘），然后选择 **Widgets**（小部件） > **System**（系统） > **High Availability**（高可用性）以显示 HA 小部件。
2. **Sync to peer**（同步到对端设备），单击 **Yes**（是），然后等待 **Running Config**（运行配置）显示 **Synchronized**（已同步）。
3. 确保 **Local**（本地）对端设备的状态为 **active**（活动）。
4. 访问 Panorama 被动设备上的 **Dashboard**（指示盘），然后选择 **Widgets**（小部件） > **System**（系统） > **High Availability**（高可用性）以显示 HA 小部件。
5. 确认 **Running Config**（运行配置）显示 **Synchronized**（已同步）。
6. 确保 **Local**（本地）对端设备的状态为 **passive**（被动）。

STEP 3 | 在 Panorama 主设备上安装 Prisma Access 组件。

1. 登录 Panorama 主设备，然后选择 **Panorama** > **Licenses**（许可证）。
2. 单击 **Retrieve the license keys from license server**（从许可证服务器检索许可证密钥）。
3. 激活并安装 Panorama Managed Prisma Access，包括生成一次性密码 (OTP) 和验证您的帐户。

STEP 4 | 检查是否已启用 HA。

1. 在 Panorama 主设备上，访问 CLI 并输入以下操作命令：

   tail follow yes mp-log plugin_cloud_services.log

2. 在日志输出中找到以下文本，其中 *X* 是 Panorama 主设备的序列号，*Y* 是 Panorama 辅助设备的序列号：

```
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/
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. 登录 客户支持门户 (CSP)，然后选择 **Assets**（资产） > **Cloud Services**（云服务），以验证两个 Panorama 对端设备是否已绑定到您的 Prisma Access 和 Strata Logging Service 许可证。

 ©2025 Palo Alto Networks, Inc.

4. 检查 Panorama 主要和辅助设备的字段。

   授权码、型号名称、许可证说明和到期日期字段对于 Panorama 主要和辅助设备应该相同，因为 Palo Alto Networks 已将 Prisma Access 许可证自动关联到 Panorama 辅助设备。

STEP 5 | 登录到 Panorama 辅助设备并激活和安装 Panorama Managed Prisma Access。

登录客户支持门户 (CSP) 生成 OTP 时，请确保指定 Panorama 辅助设备的序列号。

STEP 6 | 在 Panorama 主要和辅助设备上提交您的更改。

1. 依次选择 **Commit**（提交） > **Commit and Push**（提交并推送）以提交并推送更改。
2. 单击 **OK**（确定）和 **Push**（推送）。

STEP 7 | 验证主要和辅助 Panorama 设备是否仍处于同步状态。

 ©2025 Palo Alto Networks, Inc.

预定义模板：接入服务连接或远程网络

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	• Prisma Access 许可证

Prisma Access 包括预定义 IPSec 模板，可用于常见第三方 IPSec 和 SD-WAN 设备。这些配置文件可加速并简化服务连接及远程网络连接的接入过程，此类连接均采用上述设备之一作为连接的终端。

共享一个通用模板还能让您利用共同共享的加密算法、预共享密钥以及对等标识符，接入多个相同类型的远程连接。

- 预定义模板：接入服务连接或远程网络
- 常见 SD-WAN 设备支持的 IKE 和 IPSec 加密配置文件

Prisma Access 为您提供了以下预定义模板，您可以使用这些模板在本地设备与 Prisma Access 之间设置 IPSec 隧道：

- IPSec 隧道（**Network**（网络） > **IPSec Tunnels**（**IPSec** 隧道）），在 Remote_Network_Template 和 Service_Conn_Template 下面。
- IKE 网关（**Network**（网络） > **Network Profiles**（网络配置文件） > **IKE Gateways**（**IKE** 网关）），在 Remote_Network_Template 和 Service_Conn_Template 下面。
- IPSec 加密配置文件（**Network**（网络） > **Network Profiles**（网络配置文件） > **IPSec Crypto**（**IPSec** 加密）），在 Remote_Network_Template 和 Service_Conn_Template 下面。
- IKE 加密配置文件（**Network**（网络） > **Network Profiles**（网络配置文件） > **IKE Crypto**（**IKE** 加密）），在 Remote_Network_Template 和 Service_Conn_Template 下面。

目前，以下供应商的模板可用：

除了以下模板外，我们还提供了一个通用模板，您可以将其用于此处未列出的任何本地设备。

- Cisco 设备：
  - Cisco 集成服务路由器 (ISR)
  - Cisco 自适应安全设备 (ASA)
- Citrix
- Prisma SD-WAN（前身为 CloudGenix）
- Riverbed
- Silver Peak

要使用 Prisma Access 提供的模板接入服务连接或远程网络连接，请完成以下任务。

 ©2025 Palo Alto Networks, Inc.

STEP 1 | 在 Panorama 中，执行配置，以便模板显示在 Panorama 中。

升级云服务插件时，新模板不会自动显示。升级后完成此步骤一次，使模板永久显示。新安装将此初始配置作为其首次设置的一部分执行，不需要此额外步骤。

如果您删除了这些模板，然后需要将其恢复，也可以完成此步骤。

- 针对服务连接，请依次选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Service Setup**（服务设置），单击 **Settings**（设置）区域的齿轮图标以打开 **Settings**（设置），最后单击 **OK**（确定）。
- 对于远程网络连接，请选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Remote Networks**（远程网络），单击**Settings**（设置）区域的齿轮图标以打开 **Settings**（设置）菜单，然后单击 **OK**（确定）。

STEP 2 | 选择 **Network**（网络），然后选择正确的 **Template**（模板）（如果您正在创建远程网络连接，则选择 **Remote_Network_Template**；如果您正在创建服务连接，则选择 **Service_Conn_Template**）。

STEP 3 | 确定用于终止服务连接或远程网络连接的设备类型，并查找用于该设备的模板。

如果您的 *SD-WAN* 或 *IPSec* 设备不在列表中，请使用通用配置文件。

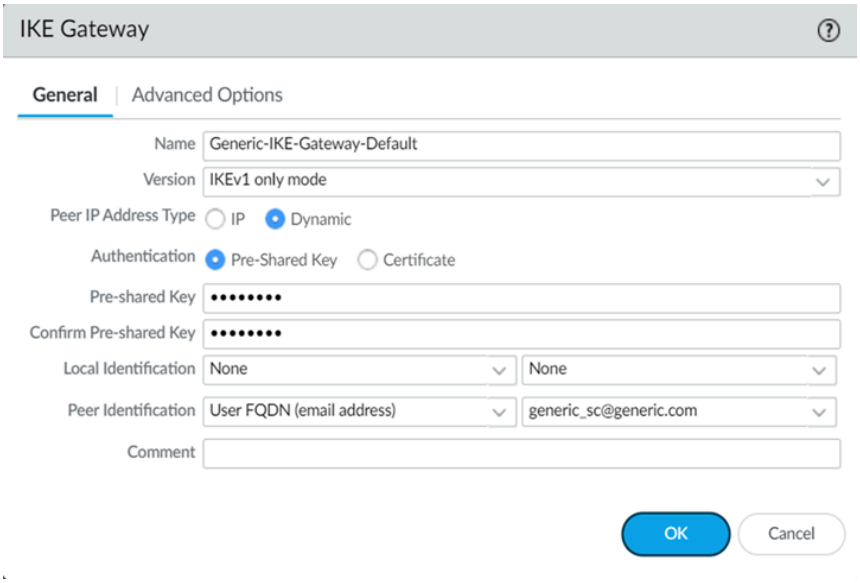
 ©2025 Palo Alto Networks, Inc.

STEP 4 | 选择 **Network**（网络） > **Network Profiles**（网络配置文件） > **IKE Gateways**（**IKE**网关），并对您的设备的 IKE 网关配置文件进行以下更改：

您可以在不更改的情况下使用 IPSec 加密配置文件和 IKE 加密配置文件；但是，您必须对 IKE 网关配置文件进行特定更改，以匹配网络设置。

- （可选）如果您知道将与 Prisma Access 设置 IPSec 隧道的本地设备的公网 IP 地址，请将 **Peer IP Address Type**（对等 **IP** 地址类型）指定为 **IP**，并输入 IPSec 隧道的 **Peer Address**（对等地址），以此来设置一个静态 IP 地址。
- 如果为 IPSec 通道使用预共享密钥，请指定 **Pre-shared Key**（预共享密钥）。
- 将 **Peer Identification**（对等标识）指定为 **IP Address**（**IP** 地址）或 **User FQDN**（用户 **FQDN**）。

  请确保您在配置用于终止 IPSec 隧道另一端的设备时与此处指定的设置相匹配。



STEP 5 | 在服务连接或远程网络连接上，指定与 IPSec 隧道另一端的设备相匹配的 **IPSec tunnel**（**IPSec** 隧道）配置。

©2025 Palo Alto Networks, Inc.

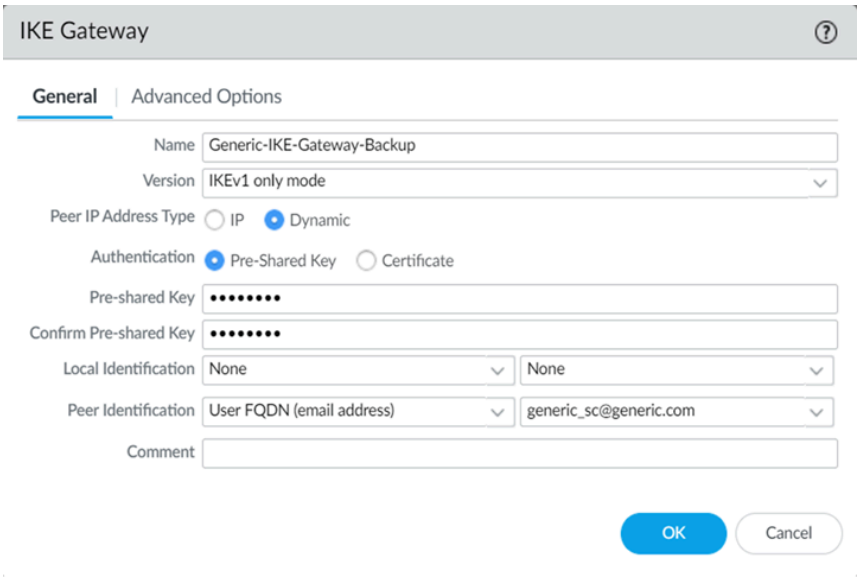
STEP 6 | （可选）如果需要为服务连接或远程连接添加备用通道（辅助 WAN），请执行以下附加配置步骤。

以下部署不支持配置辅助 WAN：

- 如果您的辅助 WAN 的主 IPSec 隧道设置为主动-主动模式。
- 如果您的客户端设备 (CPE) 的主 IPSec 隧道和辅助 IPSec 隧道设置为等价多路径 (ECMP) 配置。

1. 为备份通道创建新的 IKE 网关，从要创建副本的预定义模板中复制设置。

   以下示例为通用网络设备创建备份通道配置。

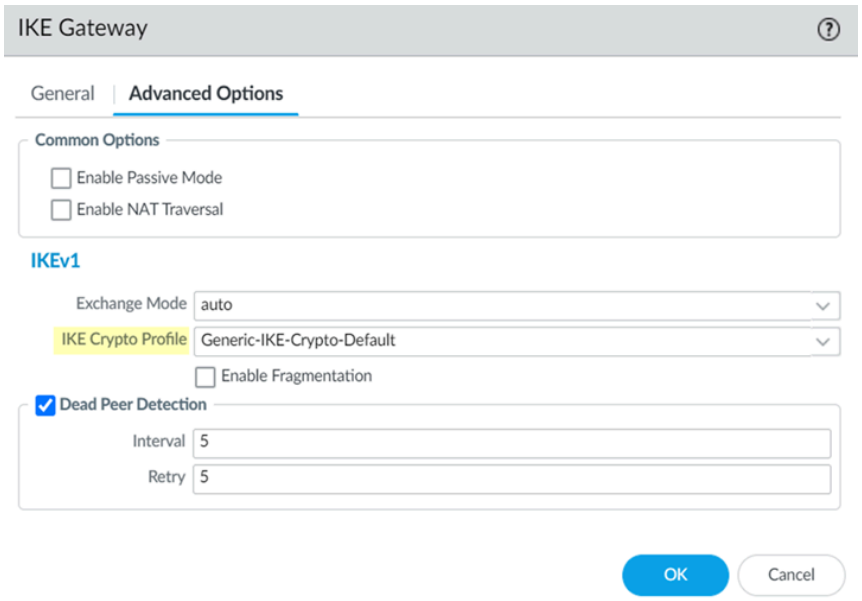


2. 在 **Advanced Options**（高级选项）下，指定您要使用的预定义模板的 **IKE Crypto Profile**（**IKE** 加密配置文件）。

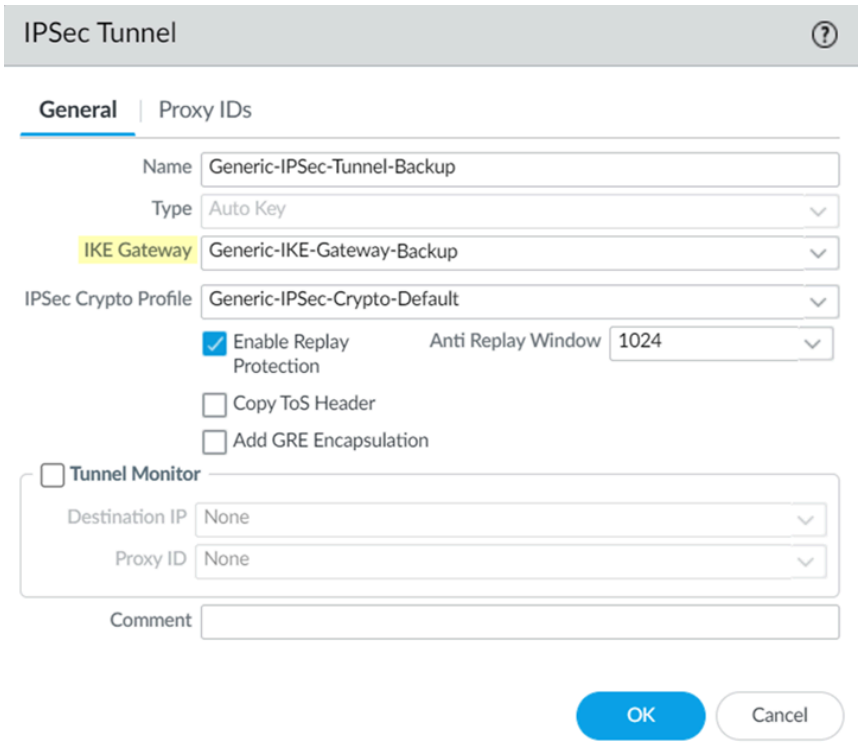
   Palo Alto Networks 建议您对 IPSec 隧道使用 GCM 密码而不是 CBC 密码。

   如果要接入 Prisma SD-WAN，请选择 **Enable Passive Mode**（启用被动模式）。

 ©2025 Palo Alto Networks, Inc.

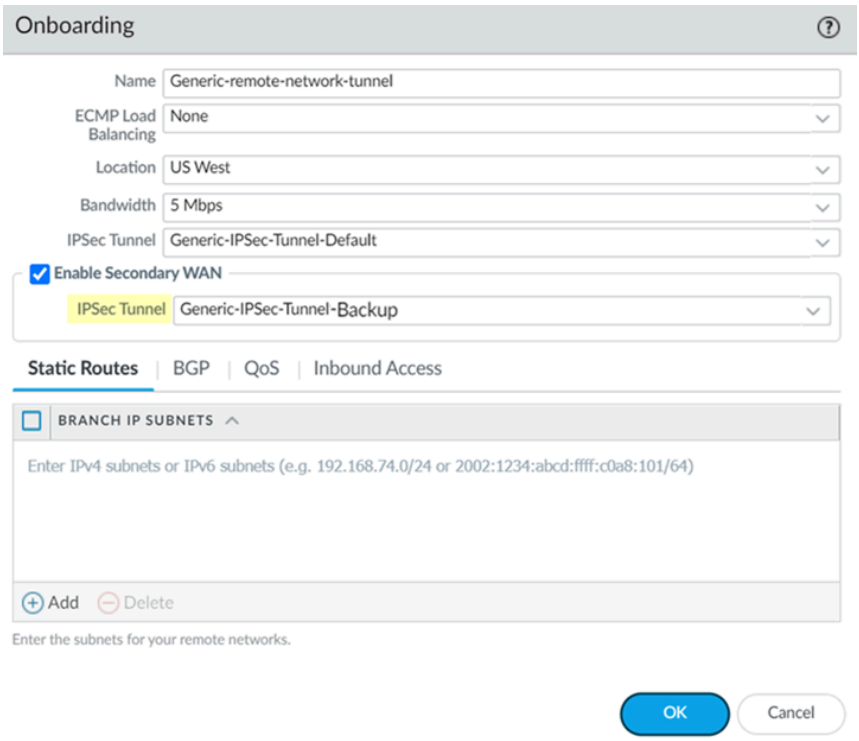


3. 创建新的 IPSec 隧道，指定您创建的新 IKE 网关，但从默认模板复制所有其他设置。



4. 接入服务连接或远程网络连接时，选择 **Enable Secondary WAN**（启用辅助 **WAN**）并指定为备份 WAN 创建的隧道。

 ©2025 Palo Alto Networks, Inc.



STEP 7 | 通过匹配加密算法、预共享密钥和对等体标识符，完成服务连接或远程网络连接的配置，这些操作需在用于终止 IPSec 隧道另一端的设备上进行。

STEP 8 | （可选）如果您需要接入多个使用相同类型网络设备的远程网络连接，请选择 **Export**（导出）以导出远程网络的配置，编辑设置，然后选择 **Import**（导入）以导入该配置。

常见 SD-WAN 设备支持的 IKE 和 IPSec 加密配置文件

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	☐ Prisma Access 许可证

本节介绍许多常见 SD-WAN 设备支持的加密配置文件。如果您正在配置 SD-WAN 设备，请使用这些配置文件作为指南，了解您可以在 Prisma Access 中为远程网络进行的配置。

- Aruba SD-WAN 支持 IKE 和 IPSec 加密配置文件
- Aryaka SD-WAN 支持 IKE 和 IPSec 加密配置文件
- Citrix SD-WAN 支持 IKE 和 IPSec 加密配置文件
- Prisma SD-WAN 设备支持 IKE 和 IPSec 加密配置文件
- Nuage Networks SD-WAN 支持 IKE 和 IPSec 加密配置文件
- Riverbed SteelConnect SD-WAN 支持 IKE 和 IPSec 加密配置文件

 ©2025 Palo Alto Networks, Inc.

- Silver Peak SD-WAN 支持 IKE 和 IPSec 加密配置文件
- Viptela SD-WAN 支持 IKE 和 IPSec 加密配置文件

 ©2025 Palo Alto Networks, Inc.

©2025 Palo Alto Networks, Inc.

Prisma Access 服务连接

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

服务连接（也称为企业访问节点（简称 CAN））允许移动用户和远程网络用户访问专用应用程序和资源，并允许移动用户和远程网络相互通信。

除服务连接外，Palo Alto Networks 还为您提供可用于访问私有应用程序的其他服务：

- ZTNA 连接器—零信任网络访问 (ZTNA) 连接器可让您简单安全地将 Prisma Access 连接到组织的私有应用程序。ZTNA 连接器允许移动用户和分支机构用户使用自动安全隧道访问您的私有应用程序。您还可以使用 Cloud Identity Engine 自动发现私有应用程序以使用 ZTNA 进行保护。
- Prisma Access Colo-Connect—借助 Colo-Connect，您可以使用 Prisma Access 通过可提供高带宽服务连接的云互连来保护私有应用程序。

Palo Alto Networks 建议始终在 Prisma Access 部署中创建服务连接。所有服务连接都具有以下特征：

- 服务连接允许访问总部或数据中心中的资源。

  例如，如果您的安全策略要求使用本地身份验证服务（如 Active Directory）进行用户身份验证，则需要启用 Prisma Access 以访问该服务所在的公司位置（并创建一个服务帐户，以便该服务能够使用这个帐户来访问该位置）。同样，如果您拥有远程网络和移动用户需要访问的公司资源，则必须启用 Prisma Access 才能访问相应的公司网络。

  如果您出于此原因创建服务连接，则应在实现服务连接之前对其进行规划。
- 服务连接允许远程网络和移动用户相互通信。

  即使您不需要访问总部或数据中心，也可能需要允许移动用户访问您的远程网络位置。在这种情况下，您可以使用占位符值创建服务连接。这是必要的，因为尽管所有远程网络连接都是完全网状互联的，但移动用户是通过中心辐射型网络中的服务连接连接到远程网络。因此，如果现有服务连接不在理想的地理位置，也可以使用占位符值创建服务连接。
- 服务连接不支持语言本地化，因为服务连接不支持到互联网的出口。在每个服务连接时，Prisma Access 仅分配一个服务 IP 地址，并且该 IP 地址会在地理位置上注册到计算地点，此计算地点对应于您在注册流程中指定的位置。

您收到的服务连接数量取决于您的 Prisma Access 许可证。

- 如果您拥有 ZTNA 或企业许可证，则服务连接的数量取决于您的许可证版本。如果您有本地版本，则最多可以配置两个服务连接；如果您有全球版本，则最多可以配置五个服务连接。
  - 通过 ZTNA 连接器，您可以将 Prisma Access 连接到组织的私有应用程序。ZTNA 连接器允许移动用户和分支机构用户使用自动安全隧道访问您的私有应用程序。有关详细信息，请参阅Prisma Access ZTNA 连接器。
- 如果您管理多个租户并拥有 ZTNA 或企业许可证，则每个租户的服务连接数量取决于您为每个租户分配的单位数量以及您拥有的许可证类型。
  - 如果您拥有全球许可证并为租户分配至少 1,000 个单元，则最多可以为该租户分配五个服务连接。
  - 如果您拥有全球许可证并为租户分配 200 到 999 个单元，则最多可以为该租户分配两个服务连接（与本地部署的连接数相同）。
  - 如果您拥有本地许可证，则无论分配的单元数量超过最小值 200，您最多可以为每个租户分配两个服务连接。

  对于全球和本地许可证，如果需要更多许可证，可以为服务连接购买额外许可证。有关高级部署中的服务连接，请参阅Prisma Access 服务连接高级部署。

在开始配置服务连接之前，请先查看需要收集哪些信息。

©2025 Palo Alto Networks, Inc.

规划服务连接。

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

创建服务连接以允许 Prisma Access 执行以下任务：

- 允许访问您的总部或数据中心的资源。

  如果您拥有远程网络和移动用户需要访问的公司资源，则必须启用 Prisma Access 才能访问相应的公司网络。
- 允许远程网络和移动用户之间相互通信。

  即使不需要 Prisma Access 用户连接到总部或数据中心，您也可能需要允许移动用户访问远程网络站点。此用例需要服务连接，因为尽管所有远程网络站点均已完全联网，但移动用户基础设施却并非如此。通过最低限度地配置服务连接，可建立移动用户访问分支网络所需的中心辐射型网络。

  为了提高网络效率，请在靠近远程网络或移动用户最常访问的网络的位置创建服务连接。

收集总部或数据中心信息

在开始配置服务连接之前，请为您希望 Prisma Access 能够连接的每个总部或数据中心收集以下信息。

如果您创建服务连接是为了仅允许移动用户访问远程网络位置，则无需收集此信息。

对于 **Prisma Access (Managed by Strata Cloud Manager)** 和 **Prisma Access (Managed by Panorama)** 服务连接：

- ❑ 公司站点上支持 IPSec 的防火墙、路由器或 SD-WAN 设备连接。
- ❑ 用于终止从 Prisma Access 到公司网络上支持 IPSec 的设备的主 VPN 隧道的 IPSec 设置。
- ❑ 用于终止从 Prisma Access 到公司网络上支持 IPSec 设备的辅助 VPN 隧道的 IPSec 设置。

  如果您拥有包含 IPSec 隧道、隧道监控和 IPSec 加密配置文件配置的现有模板，则可以将该模板添加到模板堆栈以简化 IPSec 隧道的创建过程。或者，您可以编辑自动创建的 Service_Conn_Template 并创建在创建返回公司站点的 IPSec 隧道时所需的 IPSec 配置。Prisma Access 还提供一组适用于常用网络设备的预定义 IPSec 模板，以及适用于预定义模板中未包含的任何设备的一个通用模板。
- ❑ 站点上的 IP 子网列表。
- ❑ Prisma Access 必须能够解析的内部域列表。

©2025 Palo Alto Networks, Inc.

- Prisma Access 可以向网络站点上的公司接入节点发送 ICMP ping 请求以进行 IPSec 隧道监控的 IP 地址。

  确保整个 Prisma Access 基础设施子网都可以通过 ICMP 访问此地址。
- 服务基础设施子网的网络可达性设置。

  确保可从总部或数据中心访问整个服务基础设施子网。Prisma Access 使用这些 IP 地址处理来自此子网的所有控制平面流量。

仅适用于 **Prisma Access Panorama** 服务连接：

只有在 ***Prisma Access (Managed by Panorama)*** 中计划服务连接时才需要此信息。

- 如果访问需要，则提供用于身份验证的服务帐户。
- 用于服务连接的路由类型（静态或动态 (BGP)）。

  要让 Prisma Access (Managed by Panorama) 将用户路由到所需资源，您必须提供到这些资源的路由。您可以通过以下一种或多种方法来执行此操作：
  - 为您希望用户能够访问的每个子网或特定资源定义静态路由。
  - 在服务连接位置和 Prisma Access 之间配置 BGP。
  - 使用这两种方法的组合

 ©2025 Palo Alto Networks, Inc.

配置 Prisma Access 中的服务连接

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

创建服务连接以允许 Prisma Access 执行以下任务：

- 允许访问您的总部或数据中心的资源。

  如果您拥有远程网络和移动用户需要访问的公司资源，则必须启用 Prisma Access 才能访问相应的公司网络。在开始配置服务连接之前，请为您希望 Prisma Access 能够连接的每个总部或数据中心收集以下信息。

  - 公司站点上支持 IPSec 的防火墙、路由器或 SD-WAN 设备连接。
  - 用于终止从 Prisma Access 到公司网络上支持 IPSec 的设备的主 VPN 隧道的 IPSec 设置。
  - 用于终止从 Prisma Access 到公司网络上支持 IPSec 设备的辅助 VPN 隧道的 IPSec 设置。

    如果您拥有包含 IPSec 隧道、隧道监控和 IPSec 加密配置文件配置的现有模板，则可以将该模板添加到模板堆栈以简化 IPSec 隧道的创建过程。或者，您可以编辑自动创建的 Service_Conn_Template 并创建在创建返回公司站点的 IPSec 隧道时所需的 IPSec 配置。Prisma Access 还提供一组适用于常用网络设备的预定义 IPSec 模板，以及适用于预定义模板中未包含的任何设备的一个通用模板。
  - 站点上的 IP 子网列表。
  - Prisma Access 必须能够解析的内部域列表。
  - Prisma Access 可以向网络站点上的公司接入节点发送 ICMP ping 请求以进行 IPSec 隧道监控的 IP 地址。

    确保整个 Prisma Access 基础架构子网都可以通过 ICMP 访问此地址。
  - 服务基础架构子网的网络可达性设置。

    确保可从总部或数据中心访问整个服务基础架构子网。Prisma Access 使用这些 IP 地址处理来自此子网的所有控制平面流量。
  - （仅适用于 Prisma Access (Managed by Panorama)）如果访问需要，则提供用于身份验证的服务帐户。
  - （仅适用于 Prisma Access (Managed by Panorama)）用于服务连接的路由类型（静态或动态 (BGP)）。
  - （仅适用于 Prisma Access (Managed by Panorama)）为了将用户路由到所需资源，您必须提供到这些资源的路由。您可以通过以下一种或多种方法来执行此操作：
    - 为您希望用户能够访问的每个子网或特定资源定义静态路由。
    - 在服务连接位置和 Prisma Access 之间配置 BGP。
    - 使用这两种方法的组合

©2025 Palo Alto Networks, Inc.

- 允许远程网络和移动用户之间相互通信。

  即使不需要 Prisma Access 用户连接到总部或数据中心，您也可能需要允许移动用户访问远程网络站点。此用例需要服务连接，因为尽管所有远程网络站点均已完全联网，但移动用户基础架构却并非如此。通过最低限度地配置服务连接，可建立移动用户访问分支网络所需的中心辐射型网络。

  为了提高网络效率，请在靠近远程网络或移动用户最常访问的网络的位置创建服务连接。

- Strata Cloud Manager
- Panorama

配置 Prisma Access 中的服务连接 (Strata Cloud Manager)

要为 Prisma Access (Managed by Strata Cloud Manager) 配置服务连接以允许访问私有应用程序或内部公司资源，请完成以下步骤。

STEP 1 | 选择 **Workflows**（工作流） > **Prisma Access** 设置 > **Service Connections**（服务连接），然后选择 **Add Service Connection**（添加服务连接）。

STEP 2 | 为服务连接指定描述性 **Name**（名称）。

STEP 3 | 选择您的总部或数据中心所在的 **Prisma Access** 地点。

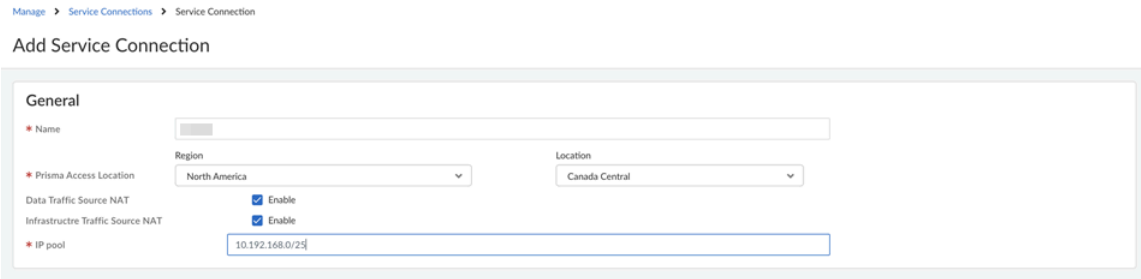
©2025 Palo Alto Networks, Inc.

STEP 4 | （可选）为移动用户—GlobalProtect IP 池地址、基础架构子网中的 IP 地址（或两者）启用源 NAT。

您可以在一个或多个服务连接中指定一个子网，这些服务连接用于对 Prisma Access GlobalProtect 移动用户与数据中心的私有应用程序和资源之间的流量执行 NAT。

- 数据流量源 **NAT** — 对移动用户 IP 地址池地址执行 NAT，以确保不会向数据中心通告这些地址，并且仅会在数据中心内通告和路由您在服务连接中指定的子网。
- 基础设施流量源 **NAT** — 对基础设施子网中的地址执行 NAT，以确保不会向数据中心通告这些地址，并且仅会在数据中心内通告和路由您在服务连接中指定的子网。
- **User-ID** — 选中后，Prisma Access 使用此服务连接重新分发标识。

  User-ID 重新分发管理 — 有时，在规模特别大的 *Prisma Access* 部署中，需要重新分发 *User-ID* 以进行精细控制。*User-ID* 重新分发管理允许您通过删除 ***User ID***（用户 ***ID***）列中的复选标记来手动禁用某些服务连接的默认标识重新分发行为，然后选择要用于标识重新分发的特定服务连接。对于大多数配置，无需执行此操作。请联系 *Palo Alto Networks* 支持部门以激活此功能。
- 源 **NAT** 池 — 指定用于在移动用户 IP 地址池、基础设施子网（或两者）上执行 NAT 的 IP 地址池。
  - 使用专用 IP (RFC 1918) 子网或路由域中可路由的合适子网。
  - 确保子网不与移动用户—GlobalProtect IP 地址池、基础设施子网或用于此租户的任何其他源 NAT 地址重叠。
  - 输入介于 /25 和 /32 之间的子网。



STEP 5 | 选择 **IPSec Tunnel**（**IPsec** 隧道）。如果尚未设置主 IPSec 隧道或辅助 IPSec 隧道，请选择 **Set Up**（设置），然后按照以下步骤操作。

1. 为隧道指定一个描述性 **Name**（名称）。
2. 选择 IPSec 设备的 **Branch Device Type**（分支设备类型）以及您用于与 Prisma Access 建立隧道的总部或数据中心。
3. 对于 **Branch Device IP Address**（分支设备 **IP** 地址），选择使用标识隧道端点的静态 **IP** 地址或 **Dynamic**（动态）IP 地址。

   如果将 **Branch Device IP Address**（分支设备 **IP** 地址）设置为 **Dynamic**（动态），则还必须添加总部或数据中心的 IKE ID（**IKE Local Identification**（**IKE** 本地标识））或添加

 ©2025 Palo Alto Networks, Inc.

Prisma Access 的 IKE ID（**IKE Peer Identification**（**IKE** 对等体标识）），以使 IPSec 对等体能够进行身份验证。

由于在服务连接完全部署之前，您没有用于 Prisma Access IKE ID 的值（**IKE Peer Identification**（**IKE** 对等体标识）），因此通常希望设置总部或数据中心的 IKE ID（**IKE Local Identification**（**IKE** 本地标识）），而不是设置 Prisma Access IKE ID。

STEP 6 | 打开 **Tunnel Monitoring**（隧道监控）。

输入总部或数据中心网络上的隧道监控 **Destination IP**（目标 **IP**）地址，以便 Prisma Access 确定隧道是否已打开，如果您的分支 IPSec 设备使用基于策略的 VPN，请输入关联的 **Proxy ID**（代理 **ID**）。

您输入的隧道监控 IP 地址将自动添加到分支子网列表中。

STEP 7 | **Save**（保存）隧道设置。

STEP 8 | 要添加或调整路由和服务质量设置，请转到 **Workflows**（工作流） > **Prisma Access** 设置 > **Service Connections**（服务连接），然后选择 **Add Service Connection**（添加服务连接）。**Set Up**（设置）或 **Edit**（编辑）**Routing**（路由）或 **QoS** 设置。

STEP 9 | 配置静态路由。

1. 如果使用静态路由来路由往返于总部或数据中心的流量，请选择 **Add**（添加）以添加要在分支机构保护的 IP 子网或 IP 地址。

   如果对总部或数据中心网络上的 IP 子网进行任何更改，则必须手动更新静态路由。

STEP 10 | 配置动态路由。

1. 如果使用动态路由来通告总部或数据中心子网，请选择 **Enable BGP for Dynamic Routing**（为动态路由启用 **BGP**）。
2. （可选）选择 **MRAI Timer**（**MRAI** 计时器）值。

   BGP 路由提供一个计时器，您可以使用它来定制网络中的 BGP 路由收敛，称为最小路由通告间隔 *(MRAI)*。MRAI 用于对每个目标的更新进行速率限制，BGP 路由器至少需等待所配置的 MRAI 时间，然后才能发送前缀相同的通告。数字越小，收敛时间就越快，但能在网络中创建的通告也越多。数字越大，可发送的通告数量就越少，但也会使路由收敛速度变慢。由您来决定在网络中输入的具体数字，以便在更快的路由收敛和更少的通告数量之间取得最佳平衡。

   将 MRAI 范围配置为 1 到 600 秒，默认值为 30 秒。
3. 要减少通过 BGP 向客户终端设备 (CPE) 通告的移动用户 IP 子网的数量，请选择 **Summarize Mobile User Routes before advertising**（在通告之前汇总移动用户路由），以指定 Prisma Access 在通告之前汇总子网。

   默认情况下，Prisma Access 以 /24 子网的形式通告移动用户的 IP 地址池；如果将它们汇总起来，Prisma Access 会根据您指定的子网来通告该池。例如，Prisma Access 使用 /20 子网通告公共用户移动 IP 池 10.8.0.0/20，而不是在通告之前将池划分为 10.8.1.0/24、10.8.2.0/24、10.8.3.0/24 等子网。汇总这些通告可以减少 CPE 路由表中存储的路由数量。例如，您可以将 IP 池汇总与可接受有限数量路由的云 VPN 网关（虚拟专用网关 (VGW) 或传输网关 (TGW)）结合使用。

 ©2025 Palo Alto Networks, Inc.

4. （可选）要让 Prisma Access 使用 eBGP 为远程网络发起默认路由通告，请选择 **Advertise the Default Route**（通告默认路由）。确保您的网络没有由 BGP 通告的其他默认路由，否则可能会在网络中引入路由问题。
5. （可选）如果您配置了辅助广域网，并且需要更改辅助（备份）BGP 对等体的对等体地址，请选择 **Use different BGP Peer for Secondary Tunnel**（使用不同的 **BGP** 对等体作为辅助隧道），然后输入唯一的对等体，或者输入辅助广域网的本地 IP 地址。
6. 要将服务连接中的团体添加到客户终端设备 (CPE) 的 eBGP 对等体中的出站前缀，请将 **Add no-export community**（添加无导出团体） 设置为 **Enabled Out**（启用出站）。默认情况下 **Disabled**（禁用）此功能。

   请勿选择 **Enabled In**（启用入站） 或 **Enabled Both**（启用两者），因为这些选项不受支持。
7. （自选）选择 **Do Not Export Routes**（不导出路由），以防止 Prisma Access 将路由转发到总部或数据中心。

   默认情况下，Prisma Access 通告所有 BGP 路由信息，包括本地路由以及它从其他服务连接、远程网络和移动用户子网收到的所有前缀。选中此复选框可防止 Prisma Access 发送任何 BGP 通告，但仍使用其收到的 BGP 信息从其他 BGP 邻居学习路由。

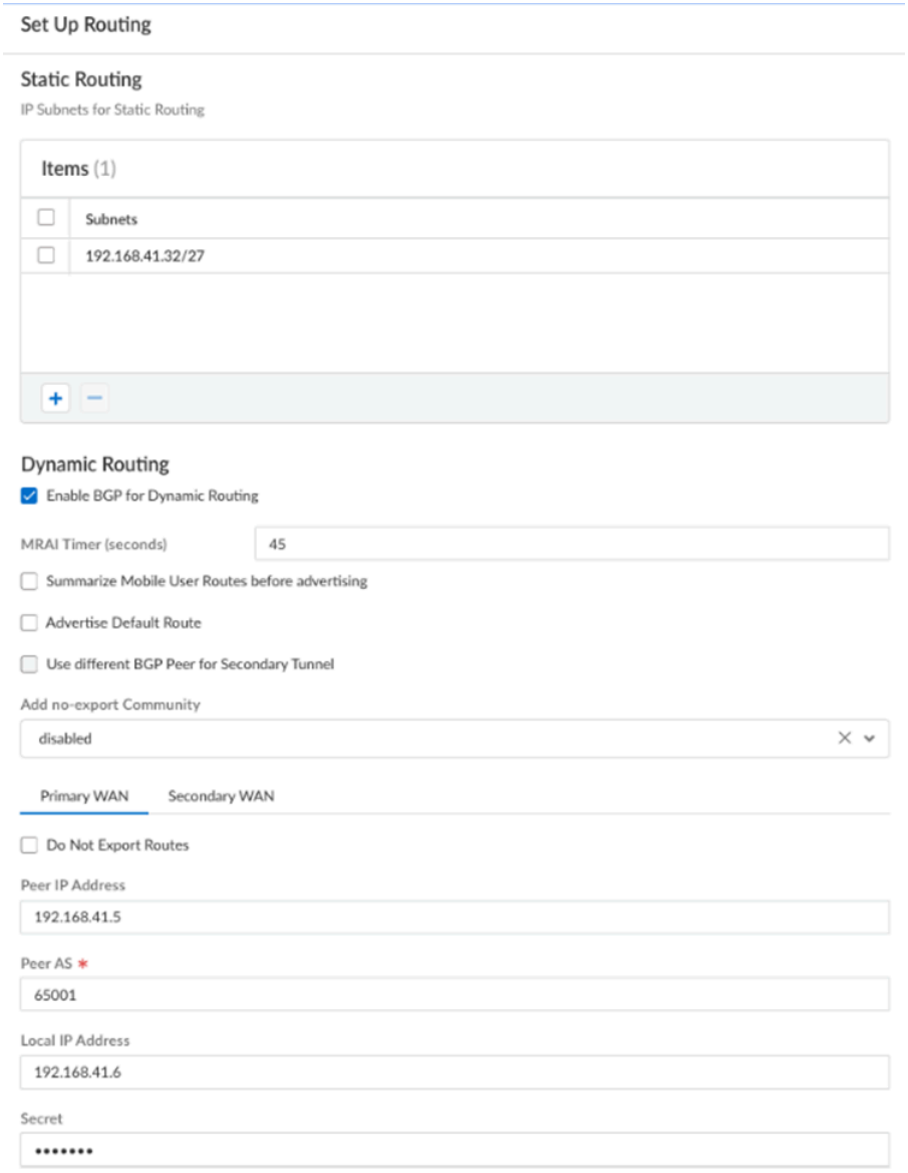
   如果您选择此选项，*Prisma Access* 不会发送 *BGP* 通告，因此您必须在本地设备上配置静态路由以建立返回 *Prisma Access* 的路由。
8. 输入分配给总部或数据中心网络上的 eBGP 路由器作为路由器 ID 的 **Peer IP Address**（对等体 **IP** 地址）。
9. 输入 **Peer AS**（对等 **AS**），即您网络的自治系统 (AS)。

   使用符合 RFC 6996 标准的 BGP 私有 AS 编号。
10. 输入 Prisma Access 用作 BGP 的本地 IP 地址的 **Local IP Address**（本地 **IP** 地址）。

    仅当总部或数据中心设备需要本地地址才能成功建立 BGP 对等互连时，才需要本地地址。确保指定的地址不会与基础设施子网或远程网络中的子网中的 IP 地址产生冲突或重叠。
11. 输入用于对 BGP 对等体通信进行身份验证的 **Secret**（机密）密码。

©2025 Palo Alto Networks, Inc.

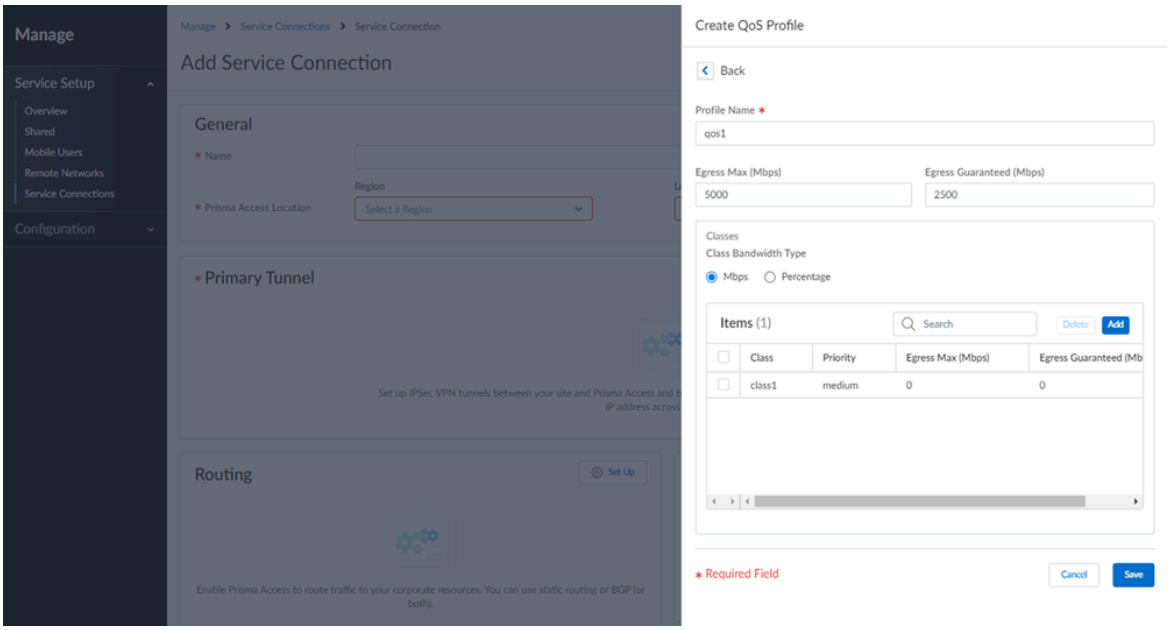
12. 选择 **Confirm Secret**（确认机密）。



 ©2025 Palo Alto Networks, Inc.

STEP 11 | （可选）配置 QoS。

首先，添加 QoS 配置文件以定义 QoS 类，将根据 QoS 类调整总部或数据中心与 Prisma Access 之间的流量。然后，创建 QoS 策略规则并将配置文件添加到该规则，以对匹配的总部或数据中心流量实施 QoS。



1. 输入 **QoS Profile**（**QoS** 配置文件）的名称。
2. 选择 **Create New**（新建）。
3. 将离开总部或数据中心服务连接的流量的最大吞吐量（以 Mbps 为单位）设置为 **Egress Max**（出口最大）。

   您可以指定一个值，不超过总部或数据中心的最大许可带宽。
4. 将保证带宽设置为 **Egress Guaranteed**（出口保证）（以 Mbps 为单位）。

   任何超过出口保证值的流量都会得到尽可能地处理，但是并不保证效果。任何保证但未使用的带宽仍可供所有流量使用。
5. 定义每个 QoS **Class**（类）并将其附加到策略规则。

   QoS 类确定与 QoS 策略规则匹配的流量的优先级和带宽。单个 QoS 配置文件中最多包含 8 个可定义的 QoS 类。除非另行配置，否则会为与 QoS 类不匹配的流量分配类 4。
6. 配置 QoS 类的**Priority**（优先级）。

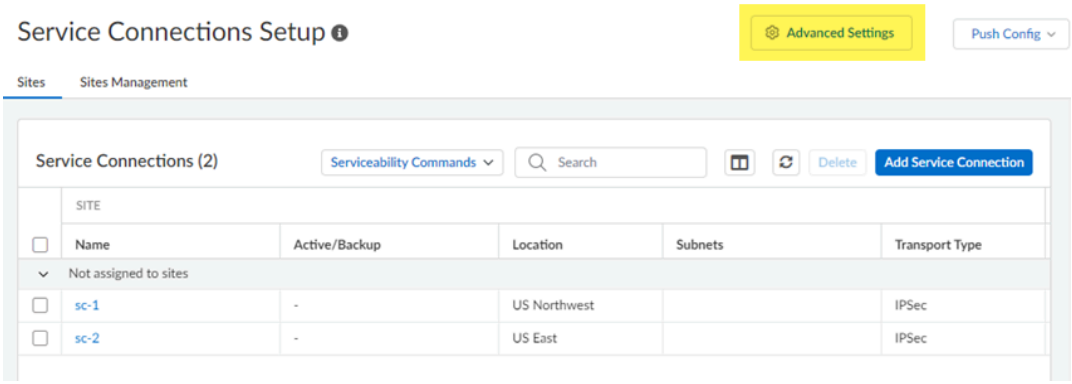
   优先级包括实时、高、中或低。
7. 配置 **Egress Max**（出口最大）值。

   QoS 类的出口最大值或多个 QoS 类的组合出口最大值不得超过 QoS 配置文件的出口最大值。
8. 配置 **Egress Guaranteed**（出口保证）值。

   分配给 QoS 类的保证带宽并非为该类保留的带宽；未使用的带宽仍可供所有流量使用。超过出口保证值的任何类的流量都会得到尽可能地处理，但是并不保证效果。

©2025 Palo Alto Networks, Inc.

STEP 12 | 为您的服务连接配置 **Advanced Settings**（高级设置）。



1. 指定用于服务连接的 **BGP Routing Preferences**（**BGP** 路由首选项）。

   您可以指定网络首选项，以使用组织的网络或 Prisma Access 网络来处理服务连接流量。

   - **Default**（默认）— Prisma Access 在其内部网络中使用默认路由。
   - **Hot potato routing**（热土豆路由）— Prisma Access 尽快将服务连接流量移交给组织的广域网。

   要更改 *Prisma Access* 服务连接路由方法，需要全面了解组织的拓扑和路由设备，以及了解 *Prisma Access* 路由的工作方式。我们建议您在更改默认路由方法之前仔细阅读服务连接流量的路由。

2. 如果您希望 Prisma Access 在隧道关闭且没有备用隧道的情况下删除静态路由，请选择 **Withdraw Static Routes if Service Connection or Remote Network IPSec tunnel is down**（如果服务连接或远程网络 **IPsec** 隧道关闭，则撤回静态路由）

   Prisma Access 会在以下情况下删除路由：

   - 主隧道关闭且没有辅助隧道。
   - 配置了主隧道和辅助隧道，但两条隧道均关闭。

   如果未启用隧道监控，则无法应用此更改。

3. 配置用于服务连接的 **Backbone Routing**（骨干路由）。

   默认情况下，Prisma Access 骨干网络要求您建立对称网络路径，用于路由通过服务连接从数据中心或总部位置返回的流量。如果要将 ECMP 或其他负载均衡机制用于来自 CPE 的服务连接，则可以通过 Prisma Access 骨干网络启用非对称流。

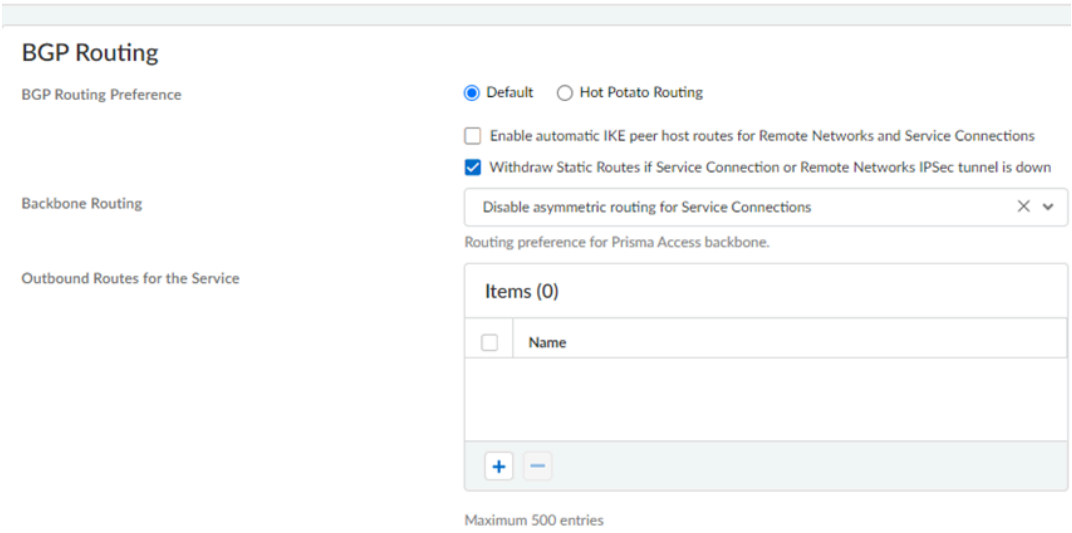
   - 选择 **Disable asymmetric routing for Service Connections**（禁用服务连接的非对称路由），以在服务连接骨干网络上使用对称流。
   - 选择 **Allow asymmetric routing for Service Connections**（允许服务连接的非对称路由），以允许 Prisma Access 在服务连接骨干网络上使用非对称流。
   - 如果某个位置有多个服务连接，则可以通过选择 **Allow asymmetric routing and load sharing across Service Connections**（允许服务连接之间的非对称路由和负载共享）（默认设置），利用 Prisma Access 部署中的负载均衡。但是，负载均衡是尽最大努力实现的，如果其中一个服务连接中断，负载均衡将失败。

     当您选择 **Allow asymmetric routing and load sharing across Service Connections**（允许服务连接之间的非对称路由和负载共享）时，Prisma Access 会在 GlobalProtect 门

 ©2025 Palo Alto Networks, Inc.

户和网关与服务连接之间实现网络冗余。此功能在移动用户数据平面与不同计算地点的服务连接之间提供冗余网络路径。实现冗余后，用户将能够更灵活地访问数据中心或总部位置的服务连接背后的资源。由于移动用户需要服务连接才能从远程网络访问资源，因此用户在访问远程网络位置中的资源时也具有更高的弹性。

4. （可选）通过添加最多 500 个前缀来指定 **Outbound Routes for the Service**（该服务的出站路由），Prisma Access 会在所有服务连接和远程网络连接上为其添加静态路由。然后，Prisma Access 通过互联网将流量路由到这些前缀。



更多 IKE 选项

根据您选择的 IPSec 设备类型，Prisma Access 会为 HQ/DC 的设备与 Prisma Access 之间的 IKE 第 1 阶段密钥交换过程提供一组建议的密码和密钥有效期。您可以使用建议的设置，也可以根据环境需要自定义设置。

为您的 IPSec 设备和 Prisma Access 选择用于 IKE 协商的 **IKE Protocol Version**（**IKE** 协议版本）。

如果选择 **IKEv1 Only Mode**（仅限 **IKEv1** 模式），Prisma Access 只能使用 IKEv1 协议进行协商。如果选择 **IKEv2 Only Mode**（仅限 **IKEv2** 模式），Prisma Access 只能使用 IKEv2 协议进行协商。如果选择 **IKEv2 Preferred Mode**（**IKEv2** 首选模式），则仅当您的 IPSec 设备也支持 IKEv2 时，Prisma Access 才会使用 IKEv2 协议。如果您的 IPSec 设备不支持 IKEv2，Prisma Access 将恢复使用 IKEv1 协议。

©2025 Palo Alto Networks, Inc.

添加 **IKEv1 Crypto Profile**（**IKEv1** 加密配置文件）以自定义 IKE 加密设置，这些设置定义用于 IKE 阶段 1 中密钥交换过程的加密和身份验证算法。

Prisma Access 根据用于建立此隧道的 **Branch Device Type**（分支设备类型）自动使用默认 IKE 加密配置文件。

- **Encryption**（加密） — 指定 IKE SA 协商中使用的加密算法。

  Prisma Access 支持以下加密算法：3des（168 位）、aes-128-cbc（128 位）、aes-192-cbc（192 位）、aes-256-cbc（256 位）和 DES（56 位）。还可以选择 Null（不加密）。
- 身份验证 — 指定 IKE SA 协商中使用的身份验证算法。

  Prisma Access 支持以下身份验证算法：sha1（160 位）、sha256（256 位）、sha384（384 位）、sha512（512 位）和 md5（128 位）。还可以选择 Null（无身份验证）。
- **DH Group**（**DH** 组） — 指定用于在 IKE SA 协商中为 IKE 生成对称密钥的 Diffie-Hellman (DH) 组。Diffie-Hellman 算法使用一方的私钥和另一方的公钥创建共享机密，即两个 VPN 隧道对等设备共享的加密密钥。

  Prisma Access 支持以下 DH 组：组 1（768 位）、组 2（1,024 位 — 默认）、组 5（1,536 位）、组 14（2,048 位）、组 19（256 位椭圆曲线组）、组 20（384 位椭圆曲线组）。要获得最强的安全性，请选择数字最高的组。
- **Lifetime**（有效期） — 指定 IKE 阶段 1 密钥有效的单位和时间长度（默认值为 8 小时）。对于 IKEv1，在密钥有效期到期之前，不会主动重新生成安全关联 (SA) 的密钥。IKEv1 阶段 1 重新生成密钥仅在 SA 过期时触发。对于 IKEv2，必须在密钥有效期到期之前重新生成 SA 密钥。如果 SA 在到期时未重新生成密钥，则 SA 必须开始新的第 1 阶段密钥。
- **IKEv2 Authentication Multiple**（**IKEv2** 身份验证倍数） — 指定密钥有效期的乘数值（范围为 0-50；默认为 0）以确定身份验证计数。身份验证计数是安全处理节点在必须开始重新进行 IKEv2 身份验证之前可以执行 IKEv2 IKE SA 重新生成密钥操作的次数。默认值 0 会禁用重新验证身份功能。

启用 **IKE Passive Mode**（**IKE** 被动模式），以便 Prisma Access 仅响应 IKE 连接，而不启动它们。

默认情况下，**IKE NAT Traversal**（**IKE NAT** 遍历）处于打开状态。

这意味着在 IKE 和 UDP 协议中使用 UDP 封装，使它们能够传递 IPSec VPN 隧道端点之间的网络地址转换 (NAT) 设备。

更多 IPSec 选项

根据您选择的 IPSec 设备类型，Prisma Access 提供一组建议的 IPsec 协议和密钥有效期设置，以在 IKE 第 2 阶段保护 IPSec 设备与 Prisma Access 之间的 IPSec 隧道内的数据，从而实现安全关联 (SA)。您可以使用建议的设置，也可以根据环境需要自定义设置。

 ©2025 Palo Alto Networks, Inc.

自定义 **IPSec Crypto Profile**（**IPsec** 加密配置文件），以定义在 IKE 第 2 阶段自动密钥 IKE 自动为 IKE SA 生成密钥时，如何保护隧道内的数据。

Prisma Access 会根据 **Branch Device Type**（分支设备类型）供应商自动配置默认 IPsec 加密配置文件。您可以使用默认配置文件或创建自定义配置文件。

- **IPsec** 协议 — 保护通过 VPN 隧道传输的数据。封装式安全措施负载 **(ESP)** 协议会加密数据、对源进行身份验证并验证数据完整性。身份验证标头 **(AH)** 协议对源进行身份验证并验证数据的完整性。

  如果使用 **ESP** 作为 IPsec 协议，还要指定 IPsec SA 协商中使用的 **Encryption**（加密）算法。

  Prisma Access 支持以下加密算法：aes-256-gcm（256 位）、aes-256-cbc（256 位）、aes-192-cbc（192 位）、aes-128-gcm（128 位）、aes-128-cbc （128 位）、3des（168 位）和 DES（56 位）。还可以选择 Null（不加密）。

Authentication（身份验证）— 指定 IPsec SA 协商中使用的身份验证算法。

Prisma Access 支持以下身份验证算法：sha1（160 位）、sha256（256 位）、sha384（384 位）、sha512（512 位）和 md5（128 位）。如果将 IPSec 协议设置为 ESP，您还可以选择无（不进行身份验证）。

DH Group（**DH** 组）— 在 IPsec 安全关联 (SA) 协商中为 IKE 指定 Diffie-Hellman (DH) 组。

Prisma Access 支持以下 DH 组：组 1（768 位）、组 2（1,024 位 — 默认）、组 5（1,536 位）、组 14（2,048 位）、组 19（256 位椭圆曲线组）、组 20（384 位椭圆曲线组）。要获得最强的安全性，请选择数字最高的组。如果您不想续订 Prisma Access 在 IKE 第 1 阶段创建的密钥，请选择 **no-pfs**（没有完美的向前保密）。如果选择此选项，Prisma Access 将重复使用当前密钥进行 IPsec SA 协商。

Lifetime（有效期）— 指定协商密钥有效的单位和时间长度（默认为 1 小时）。

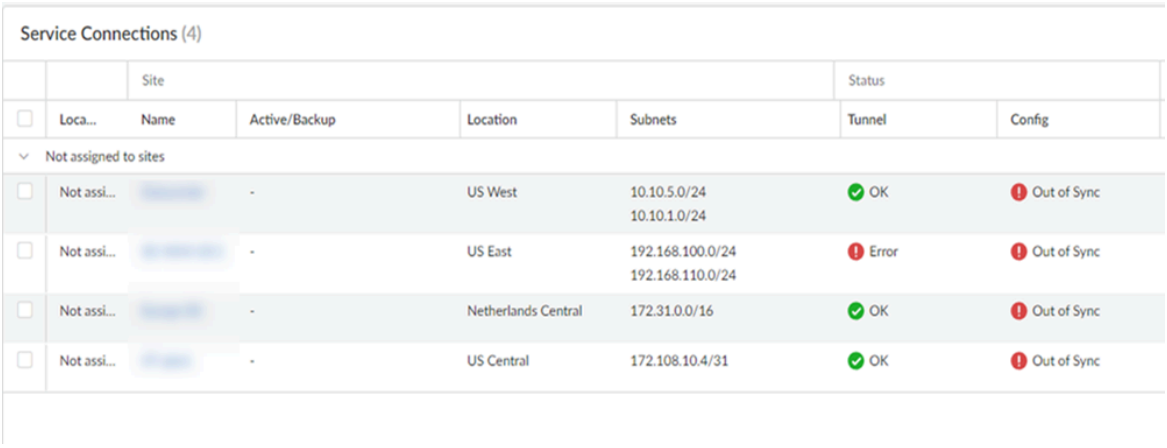
Lifesize（数据量） — 指定密钥可用于加密的数据单位和数量。

验证服务连接状态

要验证服务连接是否已成功设置，请选择 **Workflows**（工作流） > **Prisma Access** 设置 > **Service Connections**（服务连接），检查 **Status**（状态）是否显示 **OK**（正常）。

如果状态并非显示 **OK**（正常），请将鼠标悬停在状态图标上以查看任何错误。

©2025 Palo Alto Networks, Inc.



在 **Sites**（站点）区域中，您可以查看所有已加入的服务连接，以及它们的状态和其他详细信息。

站点

- **Name**（名称）— 服务连接的名称。
- **Active/Backup**（活跃/备用）— 服务连接的活跃和备用位置。
- **Subnets**（子网）— 向服务连接分配的基础设施子网。

状态

- **Tunnel**（隧道）— Prisma Access 与服务连接之间的连接的运行状态。
- **Config**（配置）— 您上次推送到服务的配置的状态。如果本地配置和云端配置匹配，则配置状态为 **In sync**（同步）。如果您在本地进行了更改，但尚未将配置推送到云端，则显示状态 **Out of sync**（不同步）。将鼠标悬停在状态指示器上，以获取更多详细信息。提交配置并将其推送到 Prisma Access 后，配置状态更改为 **In sync**（同步）。

Prisma Access

- **Location**（位置）— 部署服务连接的位置。
- **Service IP**（服务 **IP**）— 服务连接的 IP 地址。
- **EBGP Router**（**EBGP** 路由器）— 服务连接中 EBGP 路由器的 IP 地址。

链接

- **BGP IPv4** — 服务连接中 BGP IPv4 路由的状态。
- **BGP IPv6** — 服务连接中 BGP IPv6 路由的状态。
- **IPSec Tunnel**（**IPSec** 隧道）— 服务连接的 IPSec 隧道。您建立的第一个 IPSec 隧道将用作 **(Primary)**（主）隧道。如果建立了第二个 IPSec 隧道，则该隧道为 **(Secondary)**（辅助）隧道。
- **Peer IP Address**（对等体 **IP** 地址）— 服务连接的网关 IP 地址。

配置 Prisma Access 中的服务连接 (Panorama)

要为 Prisma Access Panorama 配置服务连接以允许访问私有应用程序或内部公司资源，请完成以下步骤。

©2025 Palo Alto Networks, Inc.

不要使用 *CLI* 载入和配置服务连接。如果您需要使用 *CLI* 实现载入服务连接，请与 *Palo Alto Networks* 团队联系。

STEP 1 | 选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Service Connection**（服务连接）。

STEP 2 | 将新的服务连接 **Add**（添加）到公司网络站点之一。

STEP 3 | 为公司站点指定 **Name**（名称）。

STEP 4 | 选择离站点所在位置最近的 **Location**（位置）。

请参阅本节以获取 Prisma Access 地点列表。

标有两个星号的位置是 **Local Zones**（本地服务区）。这些位置将计算、存储、数据库和基础架构服务置于人口密集和工业中心附近；然而，它们也存在一些局限性。要添加本地服务区，请联系您的 Palo Alto Networks 代表。

STEP 5 | 选择或添加新的 **IPSec Tunnel**（**IPSec** 隧道）配置，以访问公司位置的防火墙、路由器或 SD-WAN 设备：

- 如果您使用的是现有 **IPSec Tunnel**（**IPSec** 隧道）配置，请从下拉菜单中选择它。请注意，您为每个服务连接创建的隧道会将 Prisma Access 连接到每个公司位置支持 IPSec 的设

 ©2025 Palo Alto Networks, Inc.

备。IKE 网关配置中的对等地址对于每个隧道都必须是唯一的。但是，您可以重用其他一些常见的配置元素，例如加密配置文件。

您选择的 *IPSec* 隧道必须仅使用自动密钥交换和 *IPv4*。此外，请确保 *IPSec* 隧道、*IKE* 网关和加密配置文件名称不超过 *31* 个字符。

- 要创建新的 IPSec 隧道配置：

  单击 **New IPSec Tunnel**（新建 **IPSec** 隧道），为其指定 **Name**（名称），然后配置 IKE 网关、IPSec 加密配置文件和隧道监控设置。

- 如果 HQ 或数据中心位置的支持 IPSec 的设备使用基于策略的 VPN：

  在 **Proxy IDs**（代理 **ID**）选项卡上，**Add**（添加）与本地 IPSec 设备上配置的设置匹配的代理 ID，以确保 Prisma Access 可以成功建立与本地设备的 IPSec 隧道。

- 要检测重放攻击并使其无效：

  保持 **Enable Replay Protection**（启用重放保护）选中状态。

- 要保留原始 ToS 信息：

  选择 **Copy ToS Header**（复制 **ToS** 标头），将封装数据包的内部 IP 标头中的服务类型 (ToS) 标头复制到其外部 IP 标头中。

- 要为服务连接启用隧道监控：

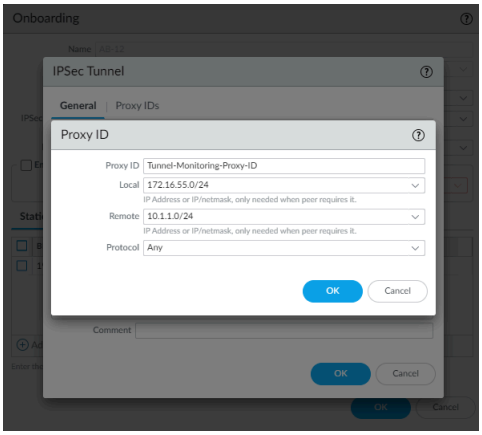
  选择 **Tunnel Monitor**（隧道监控）：

  - 输入 **Destination**（目标）IP 地址。

    在 HQ 或数据中心站点指定一个 IP 地址，Prisma Access 可以将 IPSec 隧道监控的 ICMP ping 请求发送到该地址。请确保整个 Prisma Access 基础架构子网都可以通过 ICMP 访问此地址。

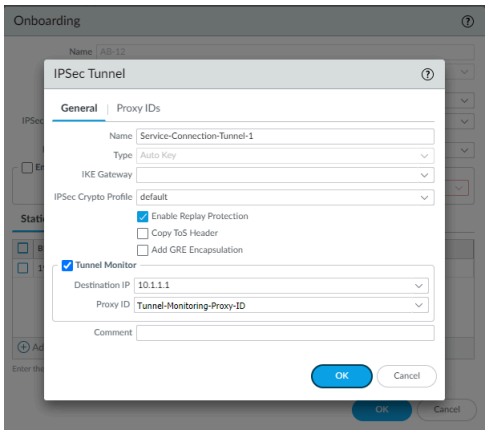
  - 如果对使用多个代理 ID 的对等设备使用隧道监控，请指定一个 **Proxy ID**（代理 **ID**）或添加一个 **New Proxy ID**（新代理 **ID**），以允许从基础架构子网访问 HQ 或数据中心站点。

    下图显示了一个代理 ID，其中服务基础架构子网（本示例中为 172.16.55.0/24）作为 **Local**（本地）IP 子网，HQ 或数据中心的子网（本示例中为 10.1.1.0/24）作为 **Remote**（远程）子网。



下图显示了您创建的代理 ID，该代理 ID 通过在 **Proxy ID**（代理 **ID**）字段中指定而应用于隧道监视器配置。

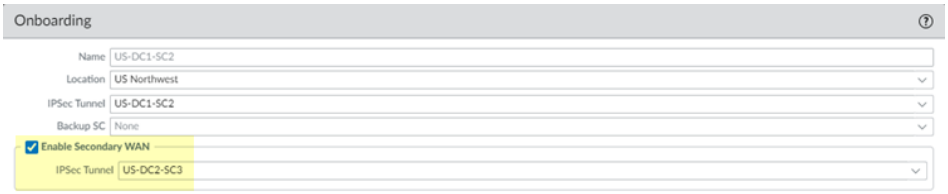
 ©2025 Palo Alto Networks, Inc.



您必须在 *CPE* 上配置一个到隧道监视器 *IP* 地址的静态路由，以使隧道监视正常工作。要查找用于从数据中心或 *HQ* 网络到 *Prisma Access* 的隧道监控的目标 *IP* 地址，请选择 ***Panorama*** > ***Cloud Services***（云服务）> ***Status***（状态）> ***Network Details***（网络详细信息），然后单击 ***Service Infrastructure***（服务基础架构）单选按钮，找到 ***Tunnel Monitor IP Address***（隧道监控 *IP* 地址）。

STEP 6 | 仅 BGP 和“热土豆”路由部署 — 选择一个服务连接作为首选备份（**Backup SC**（备份 **SC**））。

您可以选择已添加的任何服务连接。Prisma Access 使用您选择的 **Backup SC**（备份 **SC**）作为发生链路故障时的首选服务连接。选择备份服务连接后，可以防止在加入了两个以上的服务连接的情况下出现非对称路由问题。仅在热土豆路由模式下提供此选项。



STEP 7 | 如果在此位置有辅助 WAN 链路，请选择 **Enable Secondary WAN**（启用辅助 **WAN**），然后选择或配置 **IPSec Tunnel**（**IPSec** 隧道），方法与设置主IPSec 隧道相同。

如果主 WAN 链路中断，Prisma Access 会检测到中断，并通过辅助 WAN 链路建立到总部或数据中心位置的隧道。如果主 WAN 链路变为活动状态，则该链路将切换回主链路。

在以下部署中，不支持配置辅助 WAN：

- 如果辅助 WAN 的主 IPSec 隧道设置为主动/主动模式。
- 如果客户终端设备 (CPE) 的主 IPSec 隧道和辅助 IPSec 隧道设置为等价多路径 (ECMP) 配置。

如果您使用静态路由，隧道故障转移时间从检测时间算起不超过 15 秒，具体取决于您的 WAN 提供商。

如果您配置了 BGP 路由并启用了隧道监视，则确定安全参数索引 (SPI) 失败的最短默认保持时间是使用隧道监视器，当它检测到连续 15 秒的隧道失败时，将删除指向对等设备的所有路由。通过这种方式，隧道监控器确定 BGP 路由的行为。如果未配置隧道监控，保持计时器将确定在删除路由之前隧道关闭的时间。Prisma Access 使用 RFC 4271 定义的默认 BGP HoldTime

 ©2025 Palo Alto Networks, Inc.

值 90 秒，这是 Prisma Access 删除非活动 SPI 的路由之前的最长等待时间。如果对等 BGP 设备的配置保持时间较短，BGP 保持计时器将使用较低的值。

成功安装辅助隧道后，辅助路由将优先使用，直到主隧道恢复。如果主路由和辅助路由都已启动，则主路由优先。

如果您使用不同的 *BGP* 对等设备进行辅助（备份）连接，*Prisma Access* 不会接受 *CPE* 通告的 *Multi-Exit Discriminator (MED)* 属性。如果您在远程网络连接或服务连接上使用多个 *BGP* 对等设备，则此警告适用。

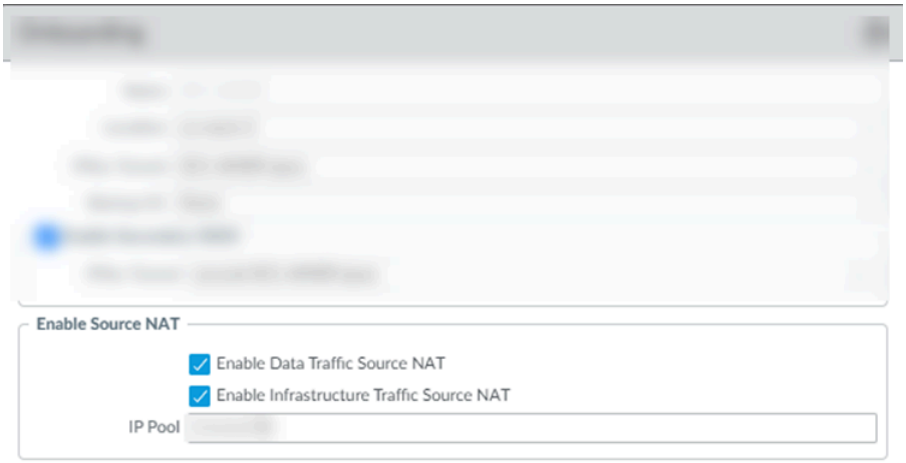
STEP 8 | （可选）为移动用户—GlobalProtect IP 池地址、基础架构子网中的 IP 地址（或两者）启用源 NAT。

您可以在一个或多个服务连接中指定一个子网，这些服务连接用于对 Prisma Access GlobalProtect 移动用户与数据中心的私有应用程序和资源之间的流量执行 NAT。

- 启用数据流量源 **NAT** — 对移动用户 IP 地址池地址执行 NAT，以确保不会向数据中心通告这些地址，并且仅会在数据中心内通告和路由您在服务连接中指定的子网。
- 启用基础架构流量源 **NAT** — 对基础架构子网中的地址执行 NAT，以确保不会向数据中心通告这些地址，并且仅会在数据中心内通告和路由您在服务连接中指定的子网。
- **User-ID** — 选中后，Prisma Access 使用此服务连接重新分发标识。

  User-ID 重新分发管理 — 有时，在规模特别大的 *Prisma Access* 部署中，需要重新分发 *User-ID* 以进行精细控制。*User-ID* 重新分发管理允许您通过删除 ***User ID***（用户 ***ID***）列中的复选标记来手动禁用某些服务连接的默认标识重新分发行为，然后选择要用于标识重新分发的特定服务连接。对于大多数配置，无需执行此操作。请联系 *Palo Alto Networks* 支持部门以激活此功能。
- **IP 池** — 指定用于在移动用户 IP 地址池、基础架构子网（或两者）上执行 NAT 的 IP 地址池。

  使用专用 IP (RFC 1918) 子网或路由域中可路由的合适子网，并且与移动用户—GlobalProtect IP 地址池或基础架构子网不重叠。输入介于 /25 和 /32 之间的子网。



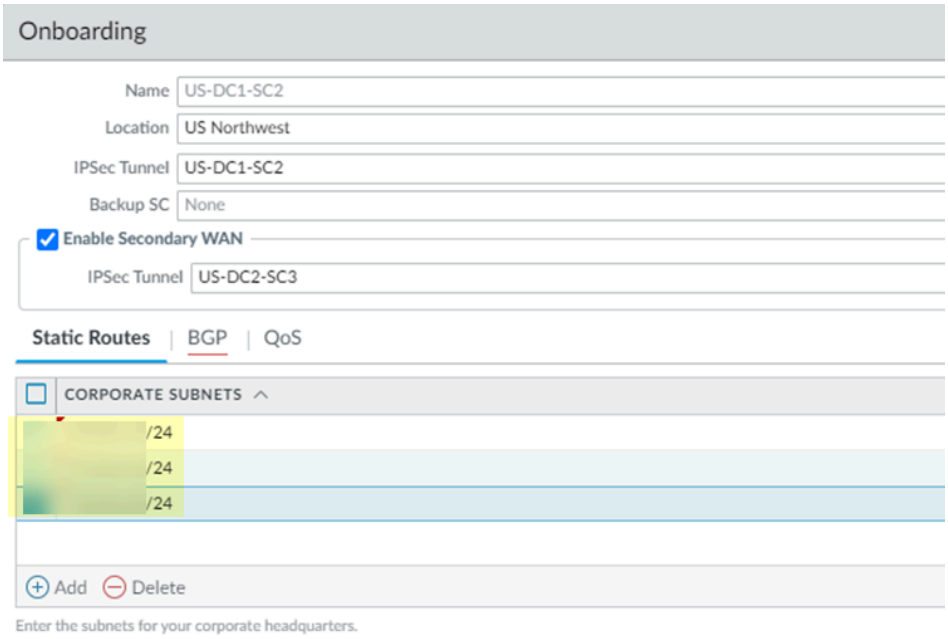
 ©2025 Palo Alto Networks, Inc.

STEP 9 | 启用到用户需要访问的公司站点的子网或单个 IP 地址的路由。

Prisma Access 使用此信息将请求路由到适当的站点。每个站点的网络不能相互重叠，也不能与您为服务基础架构或 Prisma Access for Users IP 池指定的 IP 地址池重叠。您可以配置 **Static Routes**（静态路由）、**BGP** 或两者的组合。

要配置 **Static Routes**（静态路由）：

1. 在 **Static Routes**（静态路由）选项卡上，单击 **Add**（添加）并输入子网地址（例如，172.168.10.0/24）或资源的单个 IP 地址，例如远程用户需要访问的 DNS 服务器（例如，10.32.5.1/32）。
2. 对 Prisma Access 在此位置需要访问的所有子网或 IP 地址重复此操作。



要配置 **BGP**：

1. 在 **BGP** 选项卡上，选择 **Enable**（启用）。

   启用 BGP 后，Prisma Access 会将外部 BGP (eBGP) 的生存时间 (TTL) 值设置为 8，以适应 Prisma Access 基础架构和终止 eBGP 连接的客户终端设备 (CPE) 之间可能发生的任何额外跳数。

   Prisma Access 不接受服务连接或远程网络连接的 *BGP* 默认路由通告。

2. （可选）可以选择下列选项：

   - 要将公司接入节点（服务连接）的**no-export**（无导出）团体添加到客户终端设备 (CPE) 的 eBGP 对等体中的出站前缀，请将 **Add no-export community**（添加无导出团体）设置为 **Enabled Out**（启用出站）。默认情况下 **Disabled**（禁用）此功能。

     请勿在热土豆路由模式下使用此功能。

 ©2025 Palo Alto Networks, Inc.

- 要防止 Prisma Access BGP 对等体将路由转发到组织的网络中，选择 **Don't Advertise Prisma Access Routes**（请勿通告 **Prisma Access** 路由）。

  默认情况下，Prisma Access 通告所有 BGP 路由信息，包括本地路由以及从其他服务连接、远程网络和移动用户子网收到的所有前缀。选中此复选框可防止 Prisma Access 发送任何 BGP 通告，但仍使用其收到的 BGP 信息从其他 BGP 邻居学习路由。

  如果您选择此选项，*Prisma Access* 不会发送 *BGP* 通告，因此您必须在本地设备上配置静态路由以建立返回 *Prisma Access* 的路由。
- 要减少通过 BGP 向客户终端设备 (CPE) 通告的移动用户 IP 子网的数量，请选择 **Summarize Mobile User Routes before advertising**在通告之前汇总移动用户路由），以指定 Prisma Access 在通告之前汇总子网。

  默认情况下，Prisma Access 以 /24 子网的形式通告移动用户的 IP 地址池；如果将它们汇总起来，Prisma Access 会根据您指定的子网来通告该池。例如，Prisma Access 使用 /20 子网通告公共用户移动 IP 池 10.8.0.0/20，而不是在通告之前将池划分为 10.8.1.0/24、10.8.2.0/24、10.8.3.0/24 等子网。汇总这些通告可以减少 CPE 路由表中存储的路由数量。例如，您可以将 IP 池汇总与可接受有限数量路由的云 VPN 网关（虚拟专用网关 (VGW) 或传输网关 (TGW)）结合使用。

  如果您启用了热土豆路由并启用路由汇总，则 *Prisma Access* 将不再添加 *AS-PATH*，这可能会导致非对称路由。在使用热土豆路由启用路由汇总之前，请确保从数据中心或总部位置返回的流量具有保证的对称返回。

3. （可选）选择 **MRAI** 计时器值。

   GP 路由提供一个计时器，您可以使用它来定制网络中的 BGP 路由收敛，称为最小路由通告间隔 *(MRAI)*。MRAI 用于对每个目标的更新进行速率限制，BGP 路由器至少需等待所配置的 MRAI 时间，然后才能发送前缀相同的通告。数字越小，收敛时间就越快，但能在网络中创建的通告也越多。数字越大，可发送的通告数量就越少，但也会使路由收敛速度变慢。由您

 ©2025 Palo Alto Networks, Inc.

来决定在网络中输入的具体数字，以便在更快的路由收敛和更少的通告数量之间取得最佳平衡。

将 MRAI 范围配置为 1 到 600 秒，默认值为 30 秒。

4. 输入为您要配置此服务连接的数据中心/HQ 网络上的 eBGP 路由器的路由器 ID 分配的 IP 地址作为 **Peer Address**（对等体地址）。
5. 输入 **Peer AS**（对等 **AS**），即数据中心/HQ 中的防火墙、虚拟路由器或 BGP 路由器所属的自治系统 (AS)。
6. （可选）输入 Prisma Access 用作 BGP 的本地 IP 地址的地址。

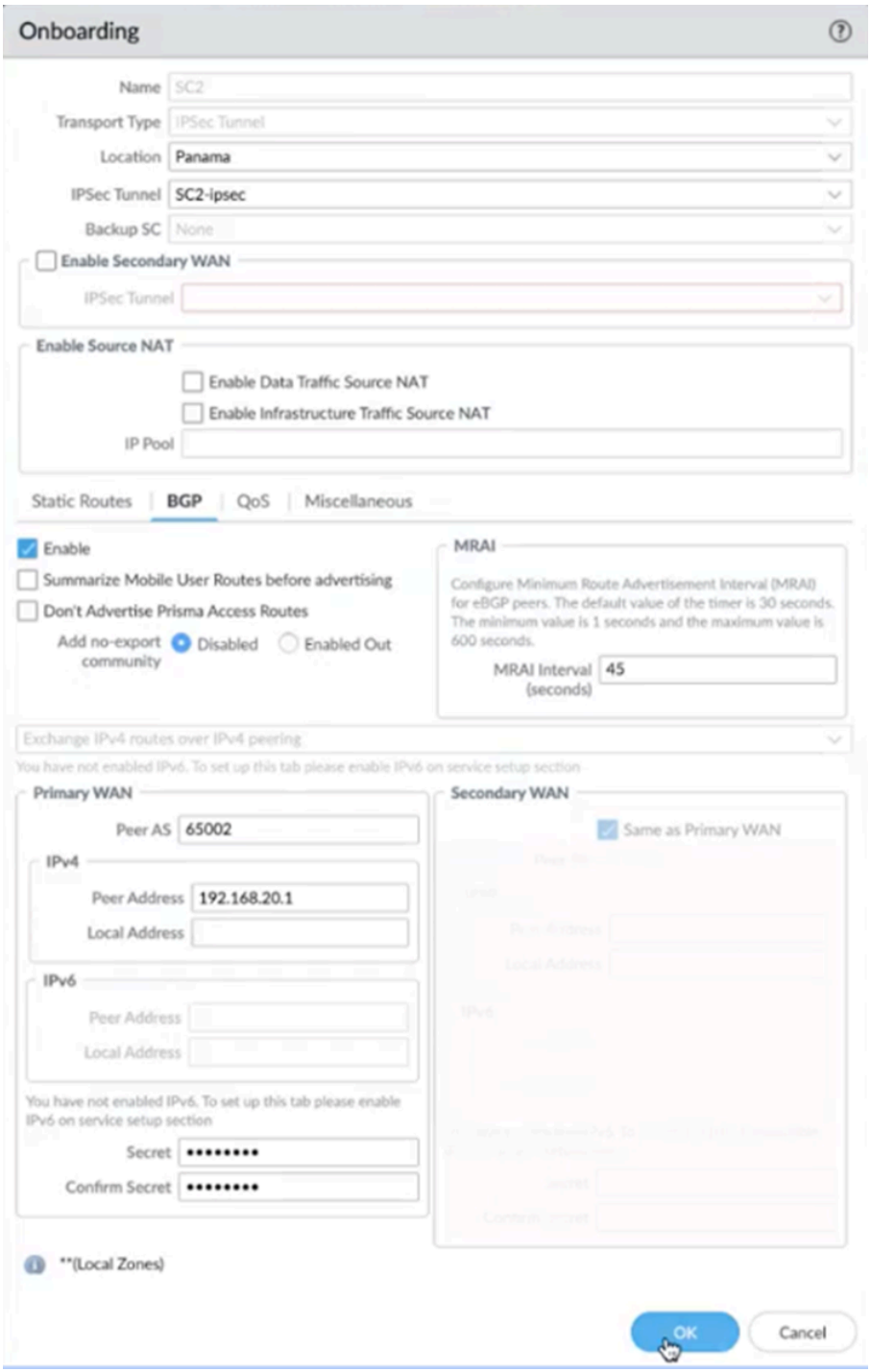
   当连接另一端的设备（例如 Amazon Web Service (AWS) 虚拟专用网关）需要特定的本地 IP 地址才能成功建立 BGP 对等连接时，指定 **Local Address**（本地地址）很有用。确保指定的地址不会与基础架构子网或服务连接中的子网中的 IP 地址产生冲突或重叠。

   您必须在 *CPE* 上配置到 *BGP* ***Local Address***（本地地址）的静态路由。

   如果将 IPV6 支持用于服务连接，则可以配置 **IPv6** 地址以及 **IPv4** 地址。您还需要在 Prisma Access 基础架构中全局启用 IPv6 网络，然后才能使用 IPv6 寻址。
7. （可选）输入并确认 **Secret**（机密）密码，以验证 BGP 对等体通信。

©2025 Palo Alto Networks, Inc.



STEP 10 | （可选）如果您配置了 **Secondary WAN**（辅助广域网），并且需要更改辅助（备份）BGP 对等体的 **Peer Address**（对等体地址）或 **Local Address**（本地地址），请取消选择 **Same as**

 ©2025 Palo Alto Networks, Inc.

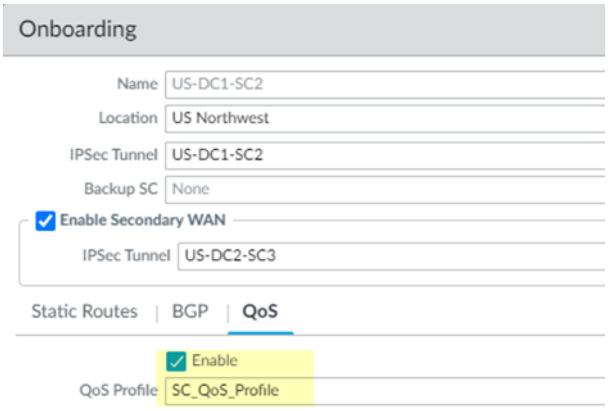
Primary WAN（与主广域网相同），然后输入唯一的对等体，或者输入辅助广域网的本地 IP 地址。

在某些部署中（例如，当使用 BGP 与 AWS VPN 网关对等时），主广域网和辅助广域网的 BGP 对等体可能有所不同。在这些情况下，您可以选择为辅助广域网设置不同的 BGP 对等体。

对于具有辅助广域网的 *BGP* 部署，*Prisma Access* 将主隧道和辅助隧道都设置为 ***UP*** 状态，但遵循网络流量的正常 *BGP* 主动备份行为。*Prisma Access* 将主隧道设置为活动状态，并仅通过该隧道发送和接收流量；如果主隧道发生故障，*Prisma Access* 将使用 *BGP* 规则检测故障，将辅助隧道设置为活动状态，并且仅使用辅助隧道发送和接收流量。

STEP 11 | （可选）为服务连接启用 **Quality of Service**（服务质量），并指定 QoS 配置文件或添加 **New QoS Profile**（新建 **QoS** 配置文件）。

您可以创建 QoS 配置文件来实现远程网络和服务连接的 QoS 流量整形，并将这些配置文件应用于使用 PAN-OS 安全策略标记的流量、使用本地设备标记的流量或带有 PAN-OS 标记和本地标记的流量。有关详细信息，请参阅远程网络的 QoS。

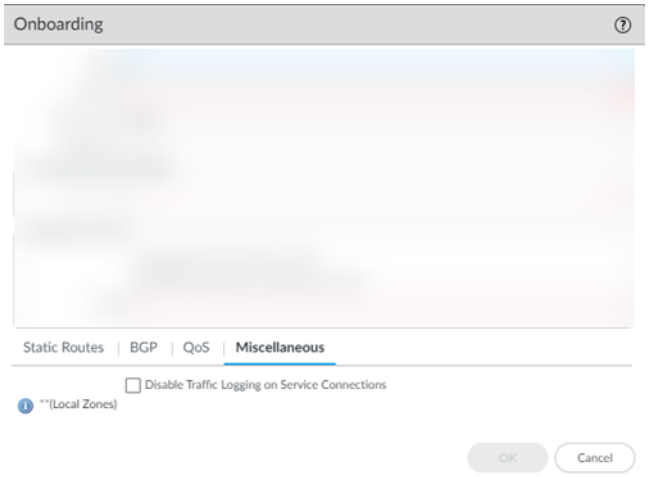


 ©2025 Palo Alto Networks, Inc.

STEP 12 | （可选）配置 **Miscellaneous**（其他）设置。

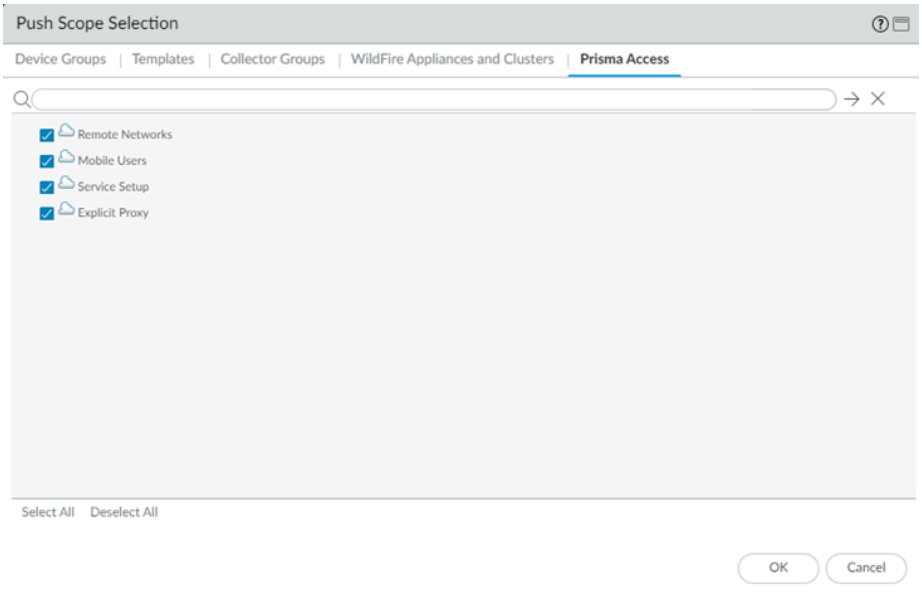
1. （可选）**Disable Traffic Logging on Service Connections**（禁用服务连接上的流量日志记录），以禁用 Prisma Access 部署的服务连接上的日志记录。

   如果服务连接记录的大多数流量是非对称流量，则可能需要禁用服务连接日志记录以减少 Strata Logging Service 日志记录存储空间的消耗。如果您的部署没有通过服务连接的非对称流量，则无需禁用日志记录。



STEP 13 | 将更改提交到 Panorama 并将配置更改推送到 Prisma Access。

1. 单击 **Commit**（提交） > **Commit and Push**（提交并推送）。
2. **Edit Selections**（编辑选择），在 **Prisma Access** 选项卡中，确保在 **Push Scope**（推送范围）中选择 **Service Setup**（服务设置），然后单击 **OK**（确定）。



3. 单击 **Commit and Push**（提交并推送）。

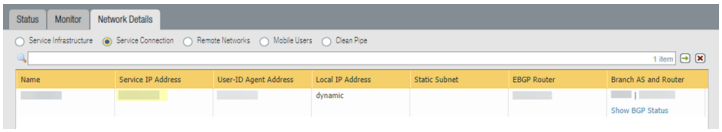
STEP 14 | 通过重复步骤 2 到步骤 11 来添加更多服务连接。

©2025 Palo Alto Networks, Inc.

STEP 15 | 配置从公司网络上支持 IPSec 的设备返回 Prisma Access 的 IPSec 隧道。

1. 要确定 Prisma Access 内的隧道的 IP 地址，请选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息），单击 **Service Connection**（服务连接）单选按钮，并记下该站点的 **Service IP Address**（服务 **IP** 地址）。

   Service IP Address（服务 **IP** 地址）是您在创建从支持 IPSec 的设备返回服务连接的隧道时需要连接的面向公众的地址。

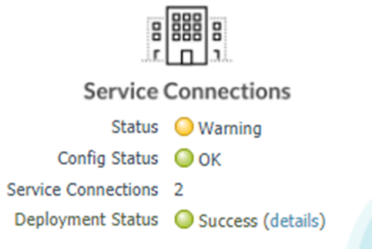
2. 在公司位置支持 IPSec 的设备上，配置连接到 Prisma Access 内的 **Service IP Address**（服务 **IP** 地址）的 IPSec 隧道，并在该设备上提交更改，以便建立隧道。

验证服务连接状态

要验证服务连接是否已成功设置，请选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Status**（状态），检查状态是否显示 **OK**（正常）。

如果您使用占位符值创建了服务连接以便在移动用户和远程网络用户之间进行通信，则无需验证服务连接状态。

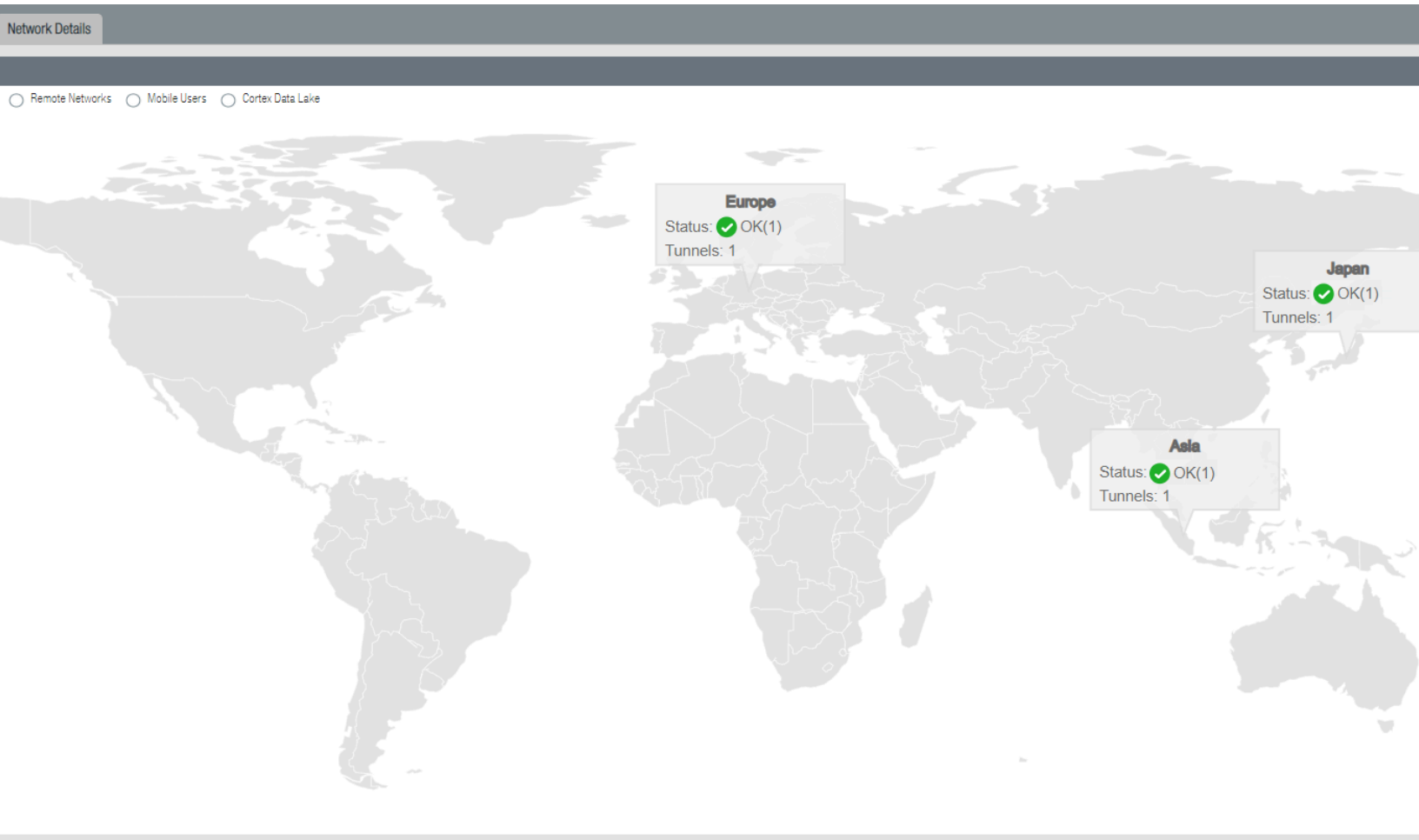
在 **Deployment Status**（部署状态）区域中，您可以在载入和部署作业完成前查看其进度，以及查看有关已完成作业的状态的更多信息。



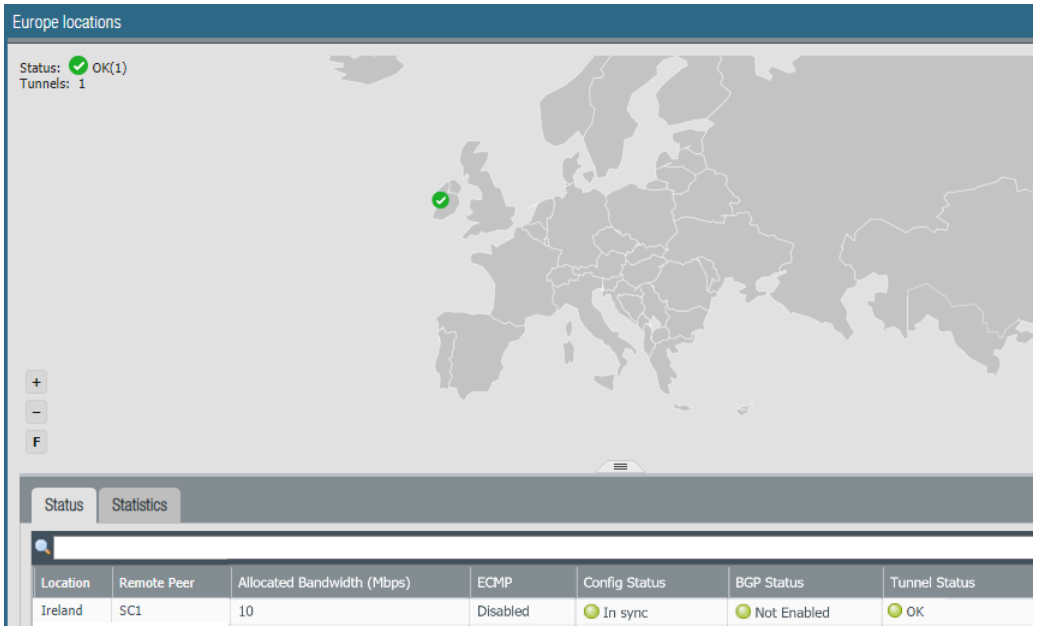
如果状态并非显示 **OK**（正常），请将鼠标悬停在状态图标上以查看任何错误。

要查看服务连接的图形表示以及状态详细信息，请在 **Monitor**（监控）选项卡上选择 **Service Connection**（服务连接）。

©2025 Palo Alto Networks, Inc.



选择一个区域以获取该区域的更多详细信息。



单击地图下方的选项卡，以查看有关服务连接的更多信息。

 ©2025 Palo Alto Networks, Inc.

Status（状态）选项卡：

- **Location**（位置）— 部署服务连接的位置。
- **Remote Peer**（远程对等体）— 此服务基础架构设置 IPSec 隧道的公司位置。
- **Allocated Bandwidth**（分配的带宽）— 分配的服务连接数量乘以 300 Mbps。

  此数字不反映可用的服务连接带宽。

  虽然每个服务连接提供约 *1 Gbps* 的吞吐量，但实际吞吐量取决于多个因素，包括：

  - 流量组合（例如，帧大小）
  - 服务连接与总部位置或数据中心之间的延迟和数据包丢失
  - 服务提供商性能限制
  - 客户终端设备性能限制
  - 其他客户数据中心流量
- **ECMP** — 如果您为此服务连接配置了等价多路径 (ECMP)。由于 ECMP 不用于服务连接，因此此状态为 **Disabled**（禁用）。
- **Config Status**（配置状态）— 您上次推送到服务的配置的状态。如果本地配置和云端配置匹配，则配置状态为 **In sync**（同步）。如果您在本地进行了更改，但尚未将配置推送到云端，则显示状态 **Out of sync**（不同步）。将鼠标悬停在状态指示器上，以获取更多详细信息。提交配置并将其推送到 Prisma Access 后，配置状态更改为 **In sync**（同步）。
- **BGP Status**（**BGP** 状态）— 显示公司/总部位置的防火墙或路由器与建立服务连接的 Prisma Access 之间的 BGP 状态的相关信息。虽然您可能会暂时看到状态经历各种 BGP 状态（**Idle**（空闲）、**Active**（活跃）、**Open sendOpen** 消息发送）、**Open pend**（**Open** 消息待处理）、**Open confirm**（**Open** 消息确认），但最常见的情况是，BGP 状态显示：
  - **Connect**（连接）— 数据中心/总部的路由器正在尝试与 Prisma Access 建立 BGP 对等体关系。
  - **Established**（已建立）— BGP 对等体关系已建立。

  如果 BGP 连接处于错误状态，此字段还会显示：
  - 警告 — 超过八分钟没有 BGP 状态更新。这可能表示防火墙中断。
  - **Error**（错误）— BGP 状态未知。
- **Tunnel Status**（隧道状态）— Prisma Access 与服务连接之间的连接的运行状态。

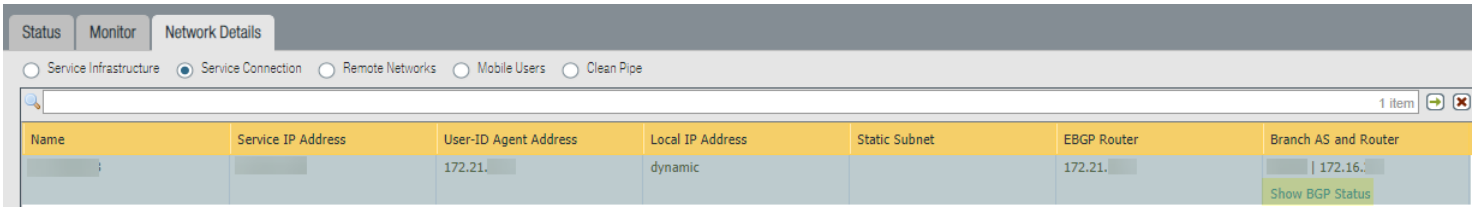
Statistics（统计信息）选项卡：

- **Location**（位置）— 部署服务连接的位置。
- **Remote Peer**（远程对等体）— 服务连接设置 IPSec 隧道的公司位置。
- **Ingress Bandwidth (Mbps)**（入口带宽 **(Mbps)**）— 从总部/数据中心位置流入 Prisma Access 的带宽。

 ©2025 Palo Alto Networks, Inc.

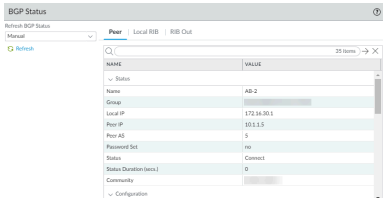
- **Ingress Peak Bandwidth (Mbps)**（入口峰值带宽 **(Mbps)**）— 从总部/数据中心位置流入云服务的峰值负载。
- **Egress Bandwidth (Mbps)**（出口带宽 **(Mbps)**）— 从 Prisma Access 流入总部/数据中心位置的带宽。
- **Egress Peak Bandwidth (Mbps)**（出口峰值带宽 **(Mbps)**）— 从 Prisma Access 流入总部/数据中心位置的峰值负载。
- **QoS** — 选择此按钮可显示图形图表，其中显示实时和历史 QoS 统计信息，包括每个类的丢包数。此图表仅显示启用了 QoS 的服务连接或远程网络连接。

如果配置了 BGP，则可以通过选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息） > **Service Connection**（服务连接） > **Show BGP Status**（显示 **BGP** 状态）来检查其状态。



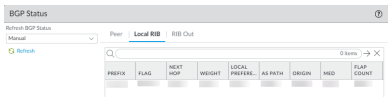
此时显示 BGP 状态对话框。此表为您提供以下信息：

- **Peer**（对等体）— BGP 对等体的路由信息，包括状态、路由总数、配置以及运行时统计信息和计数器。在 **bgpAfiIpv4-unicast Counters**（**bgpAfiIpv4-unicast** 计数器）的 **Incoming Total**（传入总数）和 **Outgoing Total**（传出总数）字段中显示路由总数。



- **Local RIB**（本地 **RIB**）— Prisma Access 本地使用的 BGP 路由。Prisma Access 从 BGP RIB-In 表中选择此信息，该表存储相邻网络设备发送的信息，应用本地 BGP 导入策略和路由决策，并将本地 RIB 信息存储在路由信息库 (RIB) 中。

  请注意，仅显示前 256 个条目。要查看其他条目，请在“筛选器”字段中输入子网或 IP 地址，然后单击“应用筛选器”以查看路由条目的子集（最多显示 256 个）。



- **RIB Out**（**RIB** 传出）— Prisma Access 通过 BGP 更新消息向其对等体通告的路由信息。

 ©2025 Palo Alto Networks, Inc.

使用服务连接实现移动用户和远程网络之间的访问

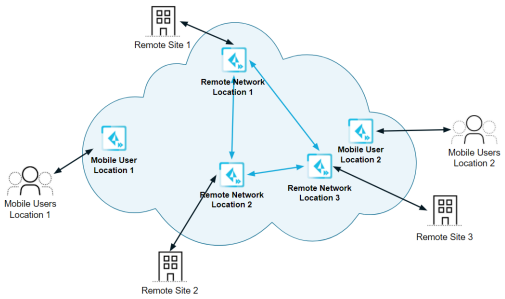
在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证，包括用于站点到站点和用户到站点访问的网络互连

要配置服务连接以连接移动用户和远程网络，请使用以下值 **Add**（添加）服务连接：

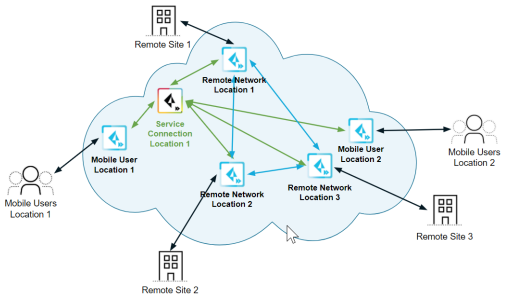
- 指定靠近您的移动用户的 **Region**（区域）。
- 使用占位符值 **Add**（添加）**IPSec** 隧道和 **IKE** 网关。
- 添加占位符公司子网。

  自从 Prisma Access 不通过此隧道路由任何流量，任何不与其他配置子网冲突或重叠的值都是有效的。

下面的例子展示了 Prisma Access 部署在不同地理区域和远程网络的移动用户。远程网络连接在网状网络中连接 Prisma Access 基础设施，但移动用户无法连接到远程网络。此外，不同地理区域的移动用户如果没有服务连接就无法互相连接。

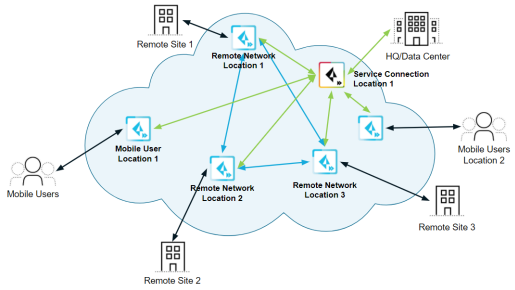


添加服务连接后，服务连接将以中心辐射型网络的形式连接移动用户和远程网络。

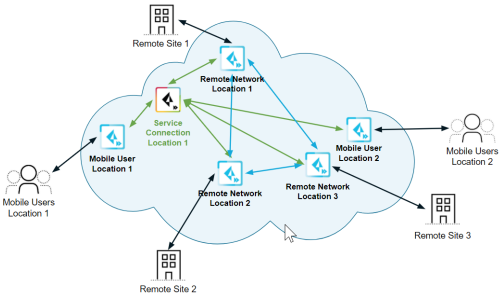


这种类型的服务连接很有用的另一种情况是当服务连接距离移动用户较远时。下图显示了此网络部署的一个示例。

©2025 Palo Alto Networks, Inc.



添加更靠近移动用户的第二个服务连接可以在移动用户和远程网络之间创建更高效的网络。



 ©2025 Palo Alto Networks, Inc.

服务连接的动态路由注意事项

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

工作原理 — 路由服务连接流量

Prisma Access 使用 BGP 进行动态路由，并使用 BGP 路径选择在路由表中安装路由。当 Prisma Access 使用服务连接将流量路由到您的总部或数据中心时，它使用能够有效引导流量的路由方法。Prisma Access 使用默认路由模型，该模型旨在适应大多数网络部署；但是，并非所有组织的网络都是一样的。为了适应更广泛的部署，Prisma Access 允许您选择另一种模式进行服务连接路由。以下各节介绍 Prisma Access 使用的 BGP 路由方法，以及在更改 Prisma Access 服务连接路由的默认方法之前，您需要考虑的组织网络因素。

要更改 *Prisma Access* 服务连接路由方法，需要彻底了解组织的拓扑和路由设备，同时了解本节所述的 *Prisma Access* 路由的工作原理。我们建议您在更改默认设置的路由方法之前仔细阅读本节。

Prisma Access 支持使用 BGP 进行静态路由和动态路由，以实现服务和远程网络连接；本节假设您使用 BGP 路由实现 Prisma Access 部署。当您选择 BGP 路由时，您组织的网络将从 Prisma Access 获取 BGP 信息。

服务连接的路由模式

您可以通过 Prisma Access 从以下路由模式中进行选择：

- 默认路由 — 这是 Prisma Access 使用的当前路由模型。

  如果您希望 Prisma Access 使用 BGP 最佳路径选择机制而不调整任何 BGP 属性，请使用此路由模式。在此模式下，Prisma Access 将遵从客户本地设备 (CPE) 发布的任何属性。
- 热土豆路由 — Prisma Access 以最快的速度将流量切换到您组织的网络。

  如果您希望组织的网络执行大多数路由决策，请使用此路由方法。

Prisma Access 默认路由

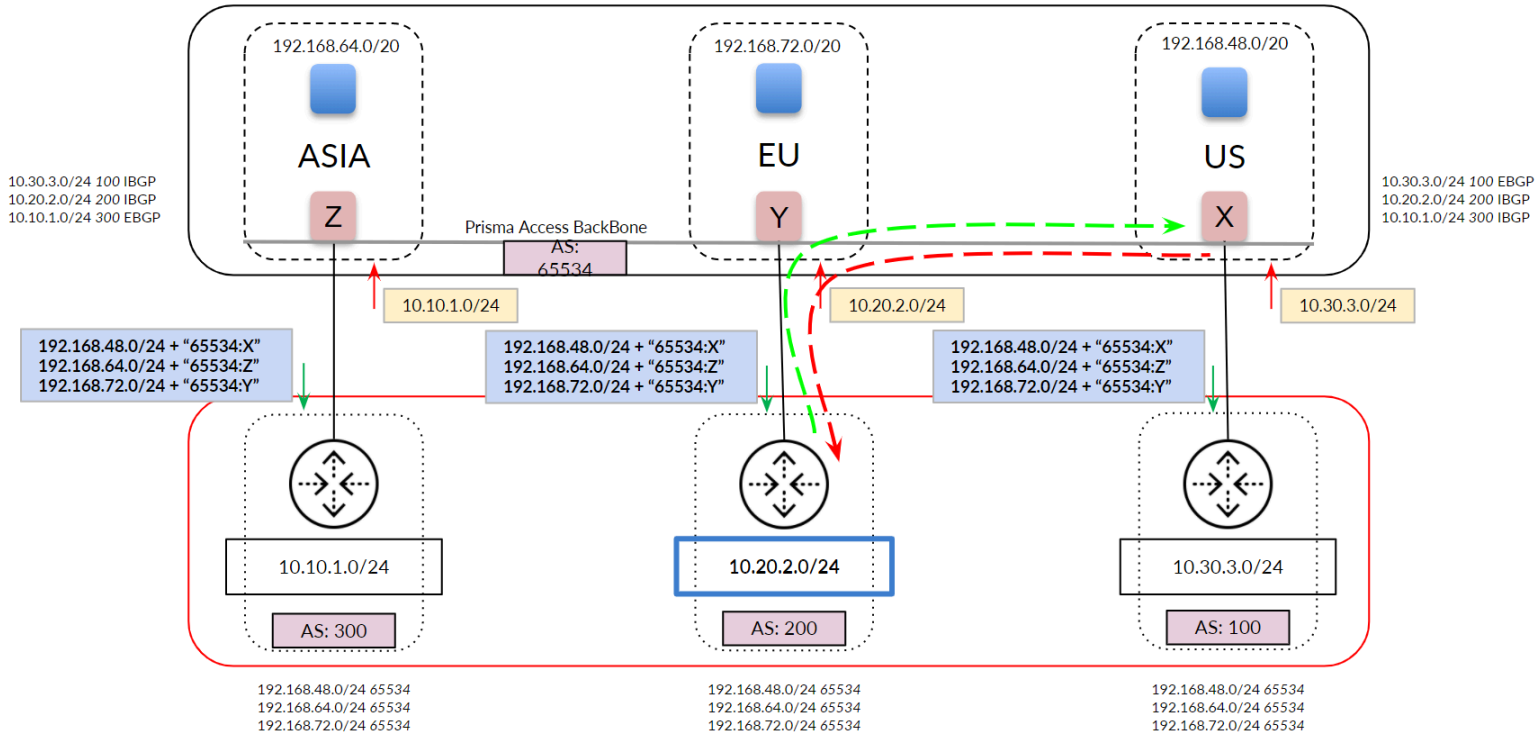
下图展示了在默认路由模式下，Prisma Access 对服务连接流量进行路由的一个示例。该组织的网络在三个数据中心有三个独立的网络，并且没有连接网络的主干网。在默认路由模式下，移动用户池在三个网络上平等地进行通告，如下图所示。

请注意，当 Prisma Access 在发布移动用户路由时，它会先发布这些路由；因此，它会以 /24 块的形式发布 /20 移动用户子网，因为前缀会被网关使用。

记下 Prisma Access 如何使用 BGP 路由通告：

 ©2025 Palo Alto Networks, Inc.

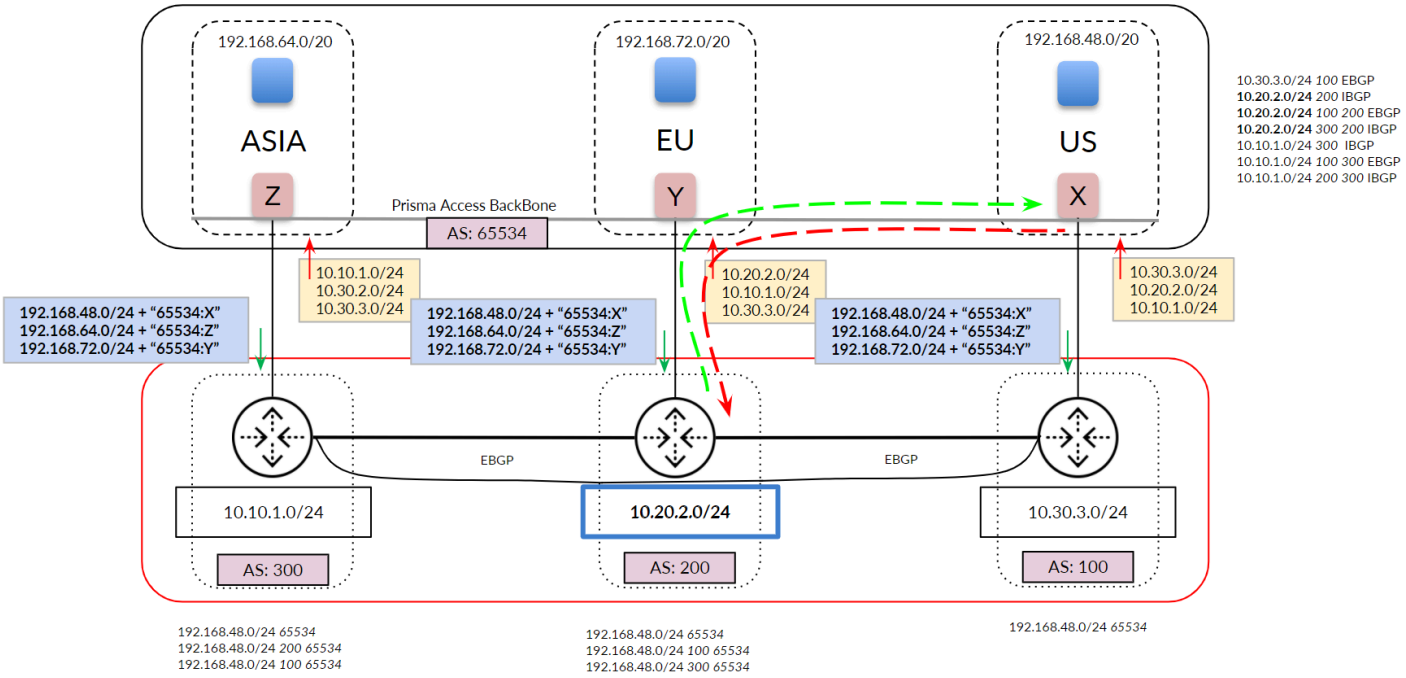
- Prisma Access 不调整移动用户通告路由的默认 BGP 属性（Prisma Access 将其 AS 编号添加到路由通告中）。
- Prisma Access 会发布其中的移动用户路由，并在通过服务连接公布的路由中添加 BGP 社区值。下图显示了具有三个服务连接和三个不同 IP 地址块的移动用户部署：`192.168.64.0/20` 用于亚洲、澳大利亚和日本地区，`192.168.72.0/20` 用于非洲、欧洲和中东地区，`192.168.48.0/20` 用于北美和南美地区。Prisma Access 将这些路由划分为 /24 块，并使用 Prisma Access 的 AS 编号 **65534** 通告这些路由，但还将 BGP 社区值附加到通告中（**Z** 代表亚洲、**Y** 代表欧盟、**X** 代表美国）。这些路线显示在图中间。通过这种方式，您可以区分网络中的服务连接，即使 Prisma Access 为它们分配相同的 AS 编号。



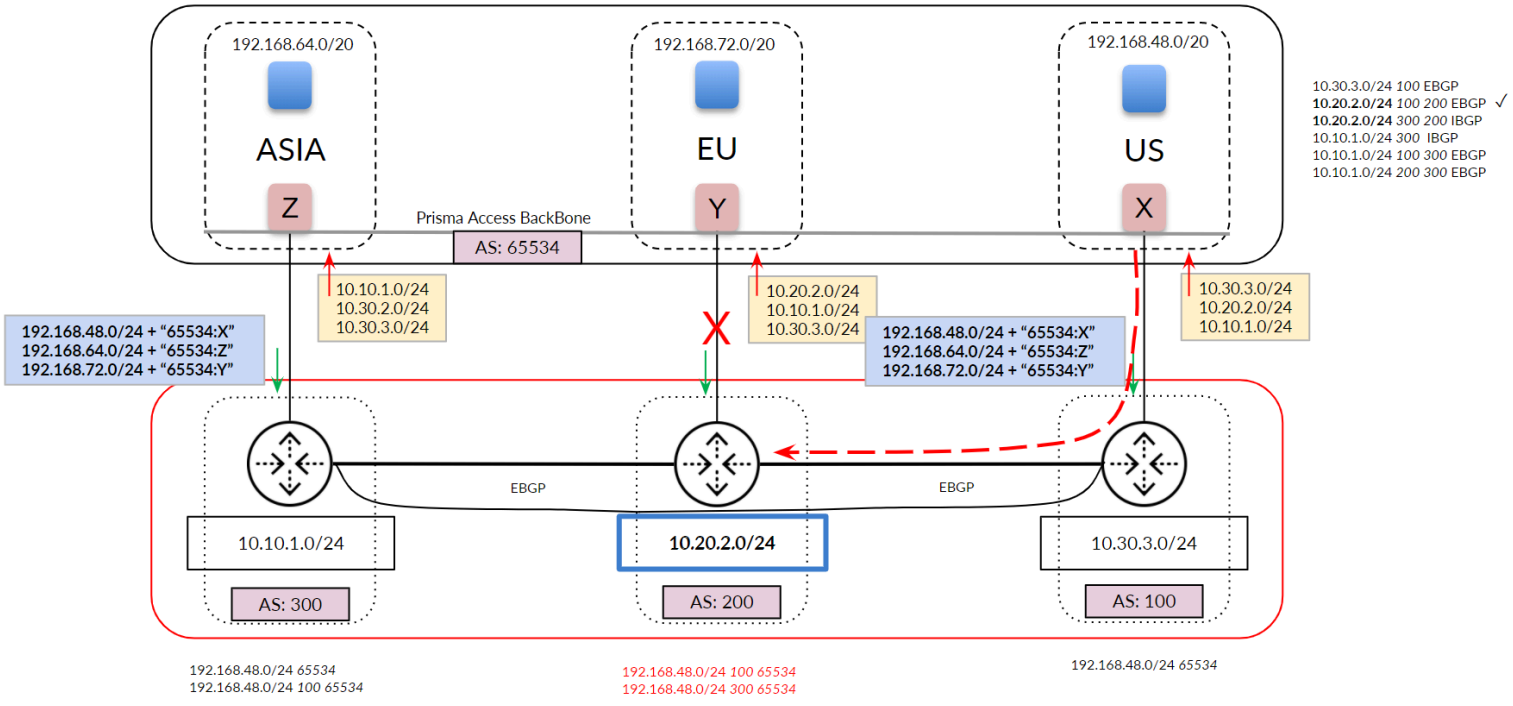
下图显示了具有全网状 eBGP 主干的更常见的网络。该图展示了 Prisma Access 从您所在组织的网络中学习到的路由信息（右上角）。请注意 Prisma Access 通过 Prisma Access 骨干网 (iBGP) 和您组织的骨干网 (eBGP) 学习到的额外路由。

对于北美和南美地区（图中为美国）的移动用户与贵组织的非洲、欧洲和中东地区（图中为欧盟）的数据中心之间的流量，Prisma Access 选择了通过欧盟服务连接的路径，因为它更倾向于 AS-PATH 更短的路由。

©2025 Palo Alto Networks, Inc.



在具有全网状 eBGP 骨干网的部署中，以下情况可能会出现不对称：由于客户数据中心的 ISP/CPE 故障，Prisma Access 无法访问特定数据中心。下图显示了当欧盟服务链路中断时可能发生的情况。您的网络检测到链路故障并为 AS 200 建立新的路由表。从美国服务连接到 AS 200 的流量会经过 AS 100，这是因为 AS 200 和 AS 100 之间骨干网络的 eBGP 路由优先于欧盟和美国服务连接之间的 iBGP 路由。然而，返程流量并不一定会采用相同路径，因为 CPE 可以选择任意一条路径（图中以红色显示）来返回流量。

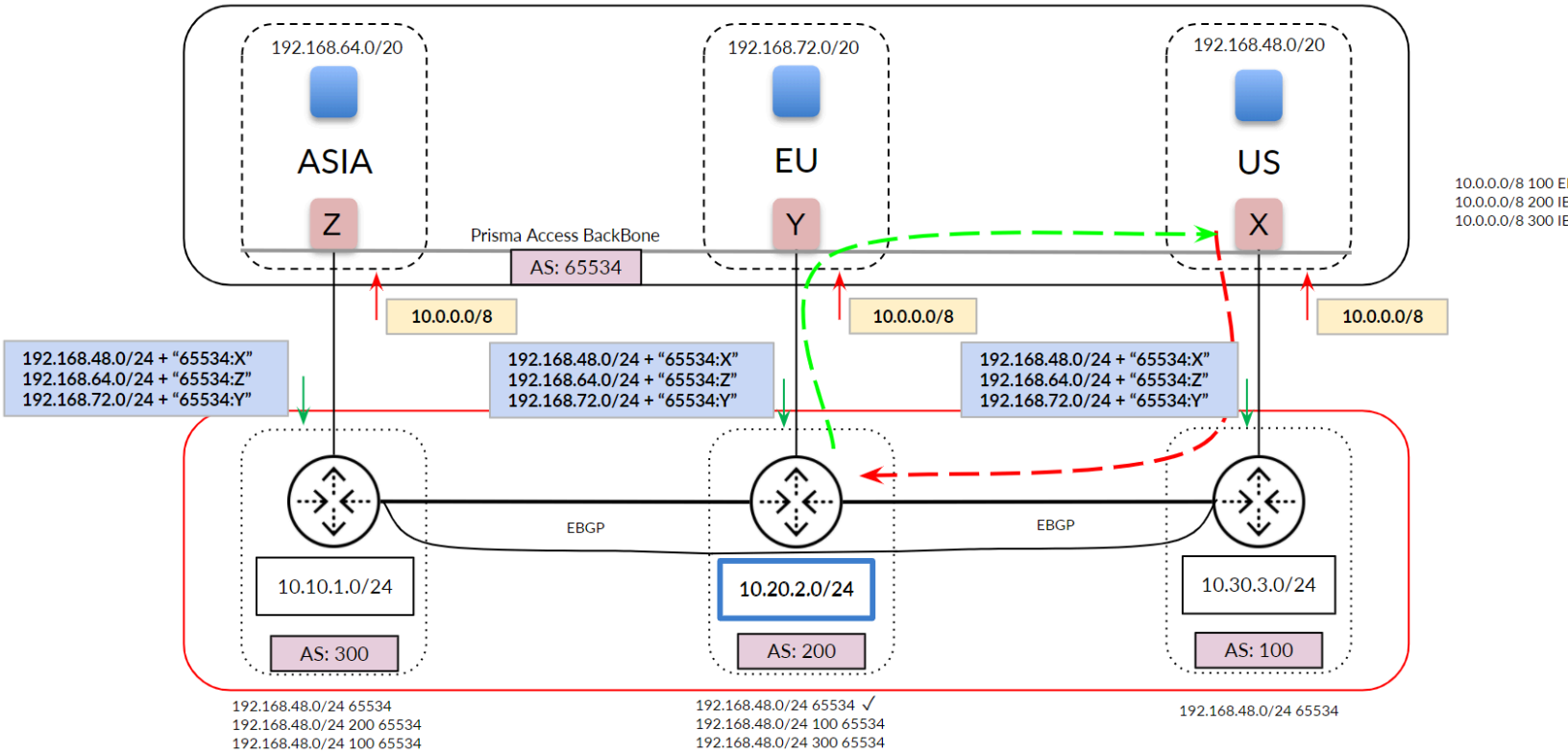


前面的示例展示了一个路由未进行聚合的网络（也就是说，在向 Prisma Access 发送 BGP 路由通告之前，您尚未进行路由汇总）。以下示例显示的网络中，网络在发送到 Prisma Access 之前汇

 ©2025 Palo Alto Networks, Inc.

总其到 10.0.0.0/8 的路由。如果选择默认路由，此配置可能会导致非对称路由问题，因为 Prisma Access 无法通过汇总路由确定正确的返回路径。

如果您的 *Prisma Access* 部署有远程网络，*Palo Alto Networks* 不建议在服务连接上使用路由汇总。服务连接上的路由汇总仅适用于移动用户部署。



如果您为移动用户使用路由聚合，我们强烈建议您启用热土豆路由，而不是默认路由，这样 Prisma Access 就会尽快将流量转交给您组织的网络。此外，我们建议您为每个服务连接选择一个如下节所述的 **Backup SC**（备份 **SC**），以实现确定的路由行为。

热土豆路由

当您选择 **Hot Potato Routing**（热土豆路由）时，Prisma Access 系统会尽快将绑定到服务连接/数据中心的流量从其内部网络流出。

采用热土豆路由时，Prisma Access 会在从网关发送的 BGP 前缀通告中添加自治系统路径 (AS-PATH) 的信息。当这些前缀从服务连接通告到组织的本地 CPE 时，会执行这种前置操作。Prisma Access 会对 AS-PATH 进行前置处理，以便您的 CPE 能正确区分主隧道和备用隧道的优先级。这样一来，如果主隧道出现故障，您的 CPE 就会选择备用隧道作为备份。

如果您为辅助（备份）BGP 对端设备指定了不同的 IP 地址，Prisma Access 会根据隧道类型添加更多前缀，如下表所示。

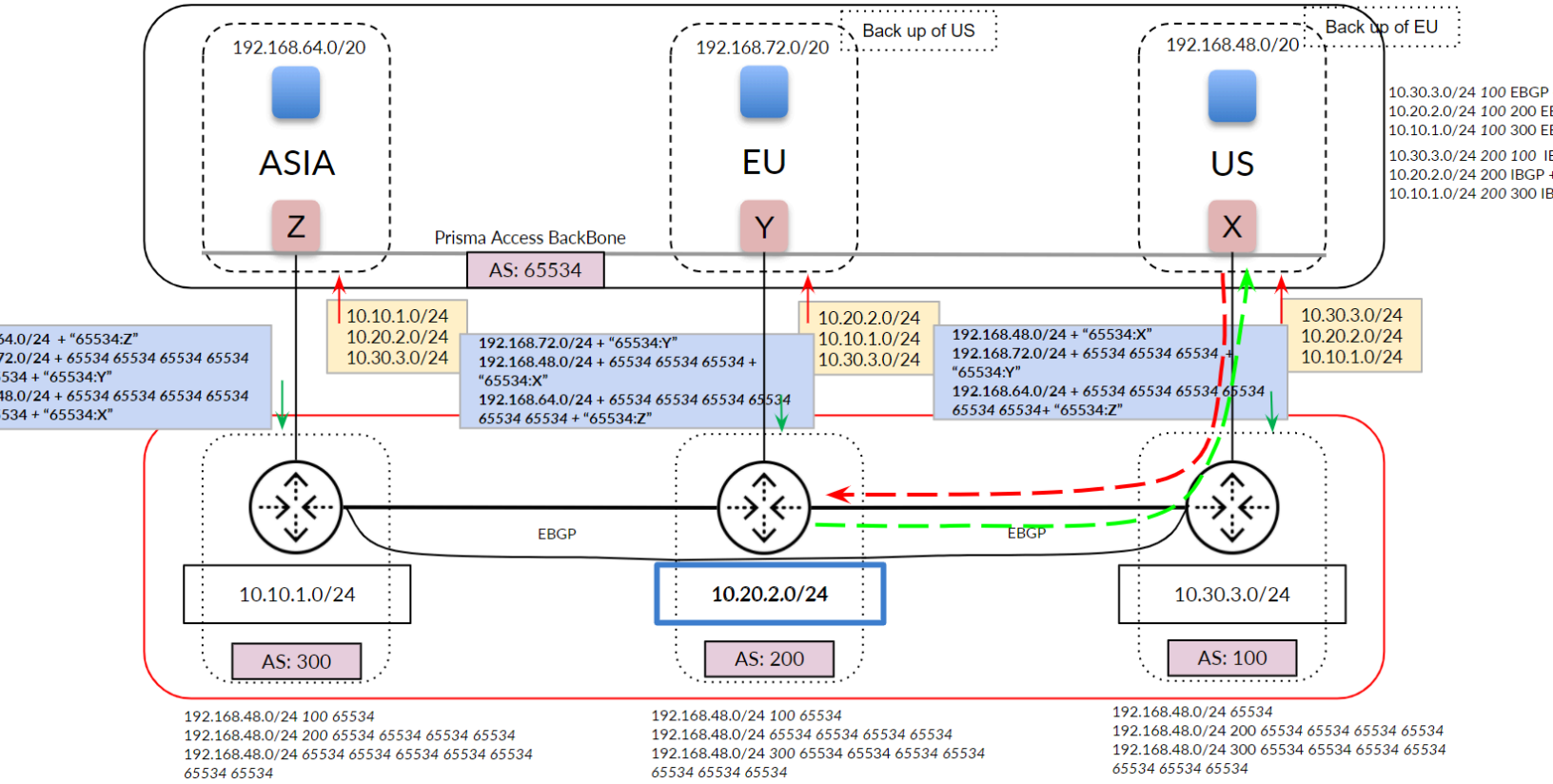
©2025 Palo Alto Networks, Inc.

前缀类型	服务连接隧道类型	**AS-PATH** 前置的次数	在 **CPE** 上看到的 **AS-PATH** 总数
来自主服务连接的网关前缀	具有相同 BGP 对端 IP 地址的主隧道或备用隧道	0	1
来自备份服务连接的网关前缀	具有相同 BGP 对端 IP 地址的主隧道或备用隧道	3	4
来自所有其他服务连接的网关前缀	具有相同 BGP 对端 IP 地址的主隧道或备用隧道	6	7
来自主服务连接的网关前缀	具有不同 BGP 对端 IP 地址的备用隧道	1	2
来自备份服务连接的网关前缀	具有不同 BGP 对端 IP 地址的备用隧道	4	5
来自所有其他服务连接的网关前缀	具有不同 BGP 对端 IP 地址的备用隧道	7	8

指定 **Backup Service Connection**（备份服务连接），以便 Prisma Access 在服务连接链路发生故障时，使用该服务连接作为备份。

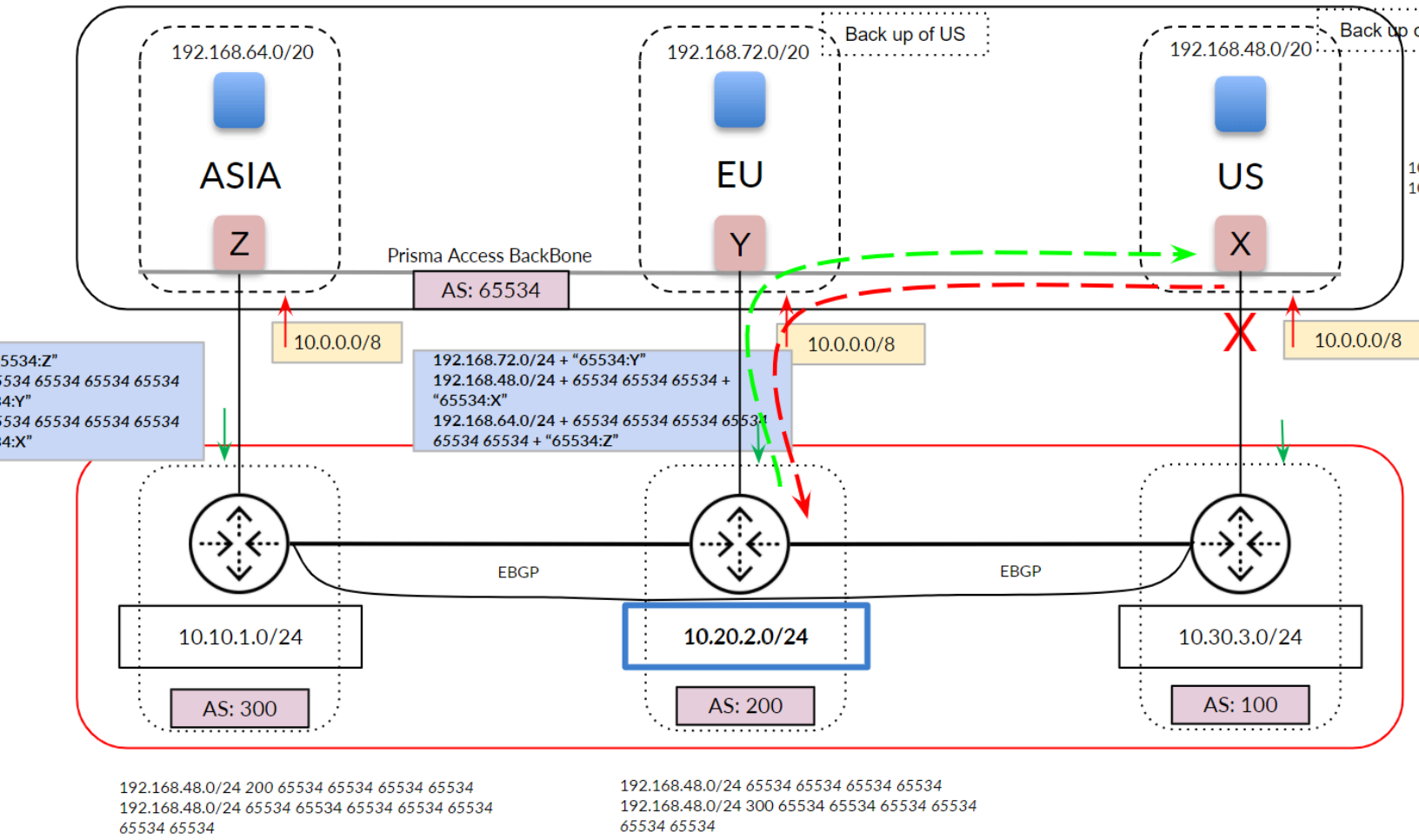
下图显示了美国服务连接和 AS 200 之间的流量热土豆路由配置，其中欧盟服务连接配置为美国连接的 **Backup Service Connection**（备份服务连接）。使用热土豆路由时，Prisma Access 会通过美国服务连接从最近的出口路径发送流量。回程流量会采用沿着 AS100 的相同路径，因为对于位于美国地区的移动用户群而言，这条路径的 AS-PATH 更短。Prisma Access 会根据隧道是主隧道还是备份隧道，或者既非主隧道也非备份隧道的情况，在其前缀通告中前置 AS-PATH。

©2025 Palo Alto Networks, Inc.



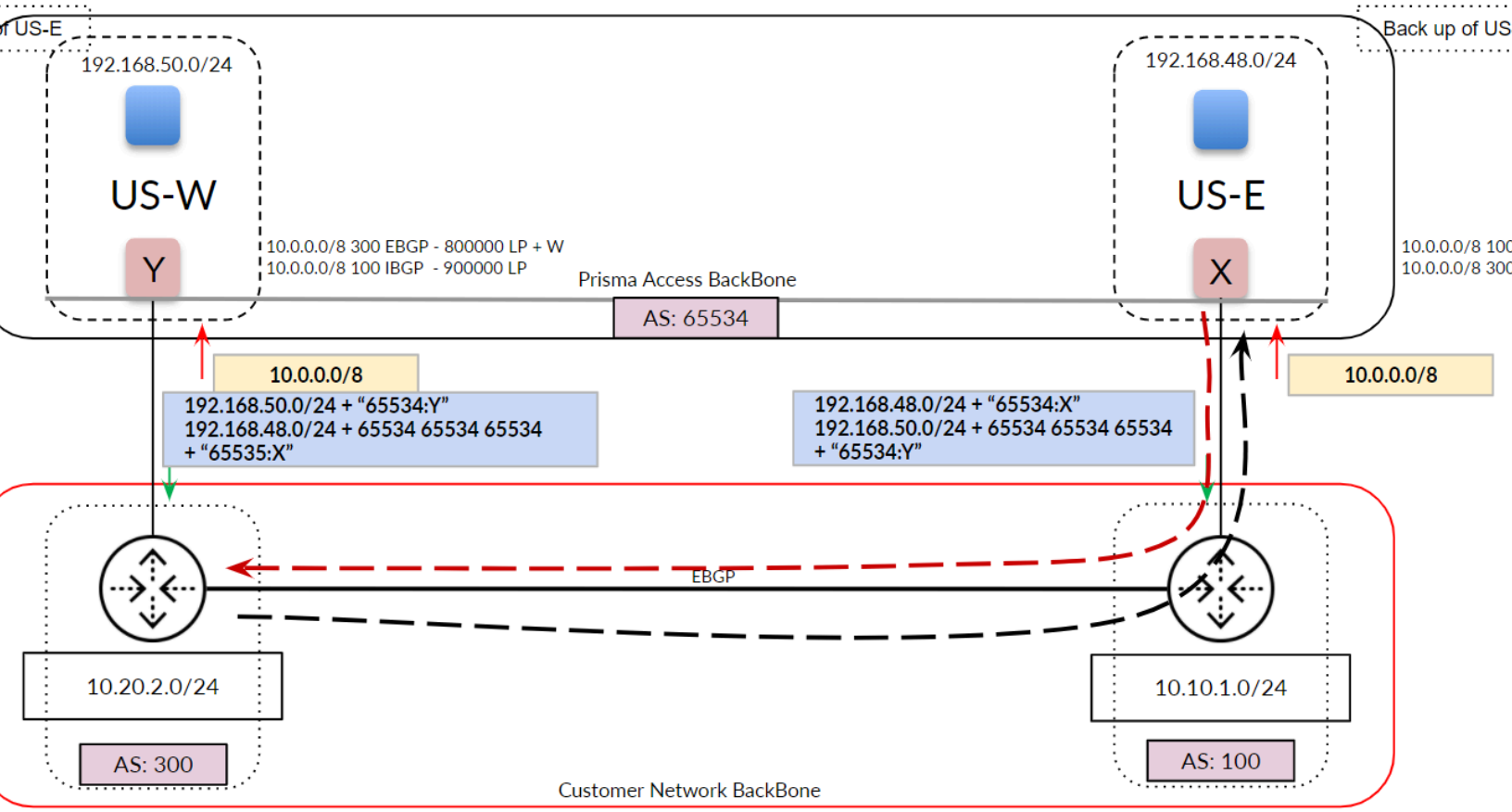
由于您已经设置了备份服务连接，因此，如果指向美国服务连接的链路中断，热土豆路由将使用通过欧盟服务连接的最短路径将流量发送出去。此路由方案也适用于使用路由聚合的网络。

©2025 Palo Alto Networks, Inc.



还可以将备份服务连接用于单个区域中的多个服务连接。下图显示了在北美地区使用两个服务连接的 Prisma Access 部署。在这种情况下，您为 US-W 服务连接指定 US-E 的 **Backup Service Connection**（备份服务连接），反之亦然，以确保对称路由。

©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.

Prisma Access ZTNA 连接器

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ ZTNA 连接器附加许可证 带附加许可证的基础许可证包括 8 个 ZTNA 连接器、100 个 FQDN 和 4 个 IP 子网功能。 带附加许可证的高级许可证包括 40 个 ZTNA 连接器、300 个 FQDN 和 1024 个 IP 子网功能。 带附加许可证的高级许可证包括 200 个 ZTNA 连接器、4000 个 FQDN 和 1024 个 IP 子网功能。 ❑ 如果您不购买 ZTNA 连接器附加许可证，Prisma Access 许可证将包括四个连接器、40 个 FQDN 和四个 IP 子网。此功能旨在让您在自己的环境中尝试 ZTNA 连接器。

凭借零信任网络访问 (ZTNA) 连接器，您可以简单安全地将 Prisma Access 连接到组织的私有应用程序。ZTNA 连接器允许移动用户和分支机构用户使用自动安全隧道访问您的私有应用程序。由于 ZTNA 连接器自动设置隧道，因此，您无需手动设置 IPSec 隧道和路由到数据中心或总部位置、公共云位置以及您的私有应用程序所在的合作伙伴网络。

您部署的 ZTNA 连接器虚拟机会自动连接到最近的 Prisma Access 位置，以确保最低延迟，并将每个连接器的访问带宽扩展到 2 Gbps，每个连接器组扩展到 8 Gbps。

Prisma Access 在默认情况下会拒绝所有访问，管理员必须明确允许通过基于我们获得专利的 User-ID、App-ID 和 Device-ID 创建的策略规则访问资源，帮助您减少攻击面和安全风险。一旦连接被允许，我们会持续验证该连接的可信度，持续检查安全威胁，并持续检查数据泄露。此外，使用 Prisma Access ZTNA 连接器时，您的应用程序的私有 IP 地址不会公开。

ZTNA 连接器组件

- 连接器 — 连接器是构建 Prisma Access 隧道的虚拟机。ZTNA 连接器实现了隧道管理自动化，无需指定 IPSec 和 IKE 设置。您要在虚拟机中载入连接器，这些连接器可以在云服务中载入（Amazon Web Services (AWS)、Google Cloud Platform (GCP)|Microsoft Azure），也可以在虚拟服务器 (VMware ESXi) 中载入，或者在基于内核的虚拟机 (KVM) 中载入。Palo Alto Networks 建议将虚拟机部署在与已载入 Prisma Access 的应用程序相同的子网中。您也可以提供不同的子网，只要连接器与应用程序之间有路由。

  在部署连接器虚拟机后，Prisma Access 可以管理虚拟机，包括提供升级虚拟机版本的选项。安装 ZTNA 连接器虚拟机后，它会发现最近的 Prisma Access 位置并启动到 Prisma Access 的安全 IPSec 隧道。
- 连接器组 — 连接器组是连接器和应用程序的逻辑分组。通过在连接器组中添加多个连接器，您为组内的应用程序提供了隧道冗余和增加的带宽。每个连接器组最多支持 4 个连接器。

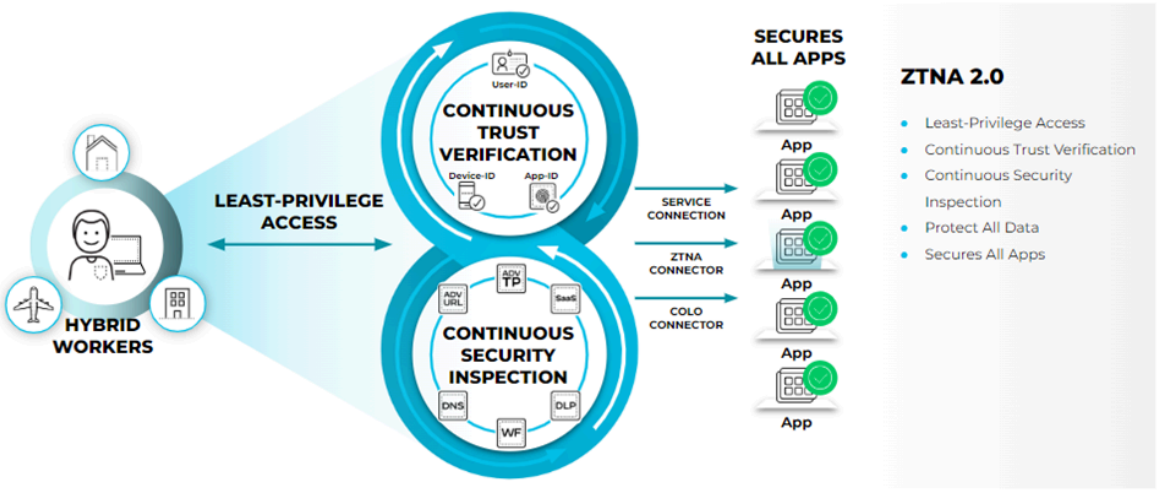
  如果您想通过不同的连接器提供对特定应用程序的访问，请将连接器放在单独的组中。
- 目标 — ZTNA 连接器载入 Prisma Access 的私有应用程序。使用 FQDN（**FQDN Targets**（**FQDN** 目标））、通配符（**Wildcard Targets**（通配符目标）），或应用所在的 IP 地址或子网，您可以定义要向其提供访问权限的特定应用程序。或者，通过从连接到 CIE 的 IdP 中提取应用程序，您可以让 ZTNA 连接器自动发现应用程序。

 ©2025 Palo Alto Networks, Inc.

ZTNA 连接器用例

在以下场景中使用 ZTNA 连接器：

- 连接到私有应用 — 使用 ZTNA 连接器处理连接到私有应用程序的所有从客户端发起的流量。



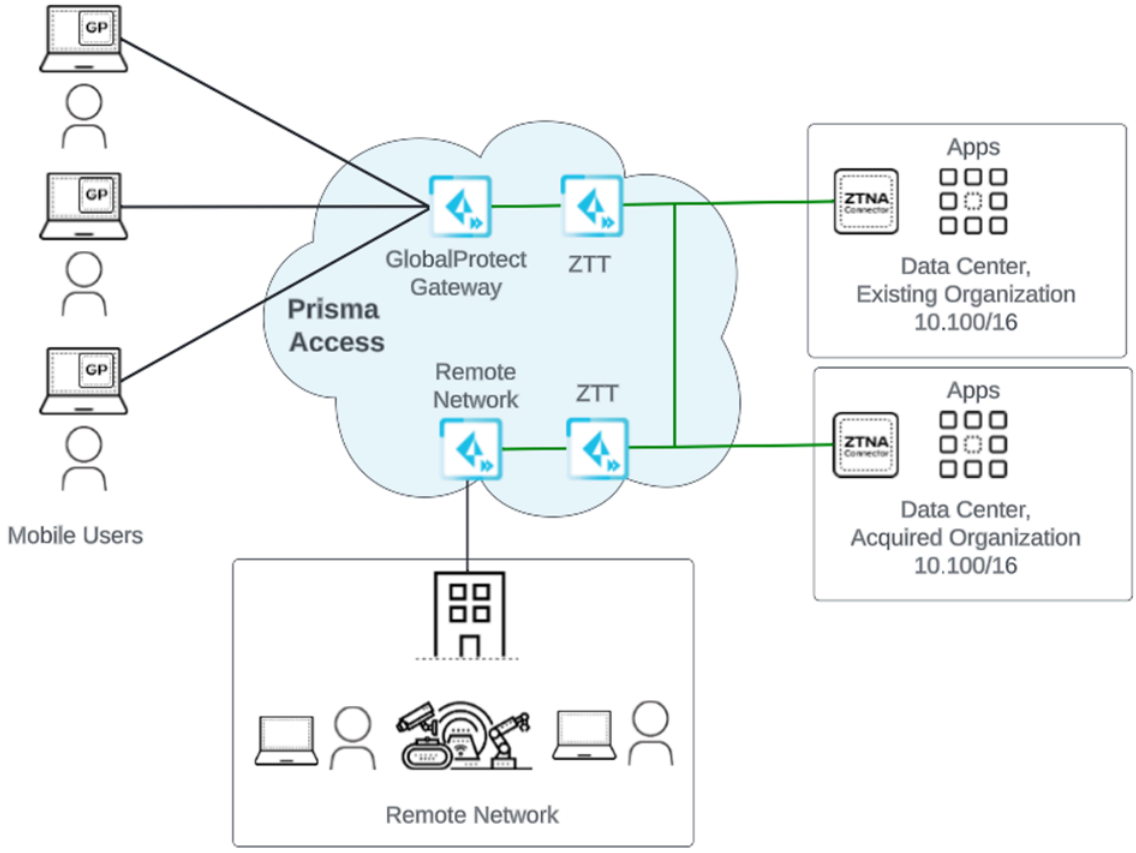
- 重叠的私有网络 — 如果您是大型企业的网络管理员，该企业已收购或并购另一组织，则两个网络可能使用重叠的地址范围（例如，RFC 1918 私有网络地址空间）。为了向您的用户提供对托管在重叠网络中的应用程序的访问，路由和 NAT 配置可能会变得很繁琐。ZTNA 连接器通过允许您使用 FQDN、FQDN 通配符和 IP 子网来连接到应用程序，简化了重叠网络中的应用程序访问，无需您配置 IP 路由。

  使用 ZTNA 连接器隧道终端 (ZTT)，ZTNA 连接器为您的用户提供了安全访问私有应用程序的能力。

  当您在计算区域激活 ZTNA 连接器时，ZTT 节点会自动载入。ZTNA 连接器自动与 ZTT 构成 IPSec 隧道。在删除一个区域内的所有连接器后，该区域内的 ZTT 节点仍将保持活跃 24 小时。

©2025 Palo Alto Networks, Inc.

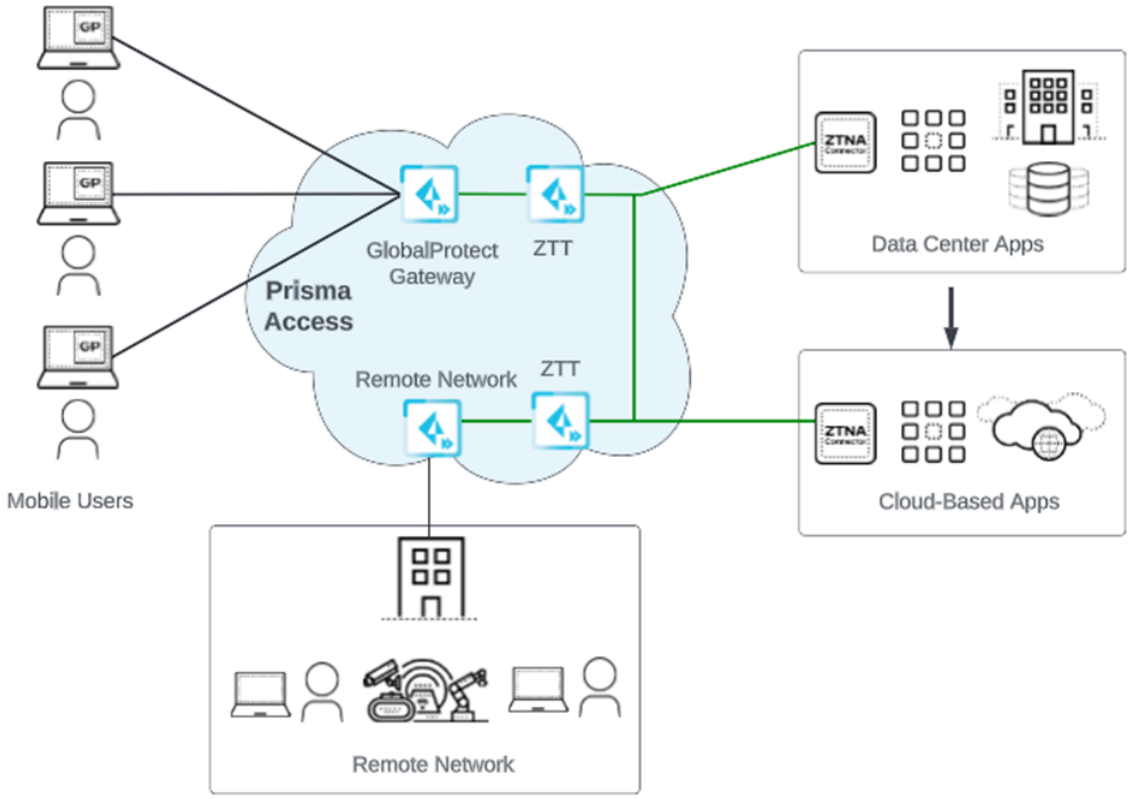
在同一区域内，如果在删除所有连接器后的 24 小时内部署了新的连接器，它将重用现有的 ZTT。如果在 24 小时后激活新的 ZTNA 连接器，则会创建新的 ZTT。



- 数据中心到云迁移 — 如果您的组织正在将本地应用程序迁移到云（无论是“直接迁移”(Lift and Shift) 现有的本地应用程序，还是开发云原生应用程序），您都可以在 AWS、GCP、Azure 或

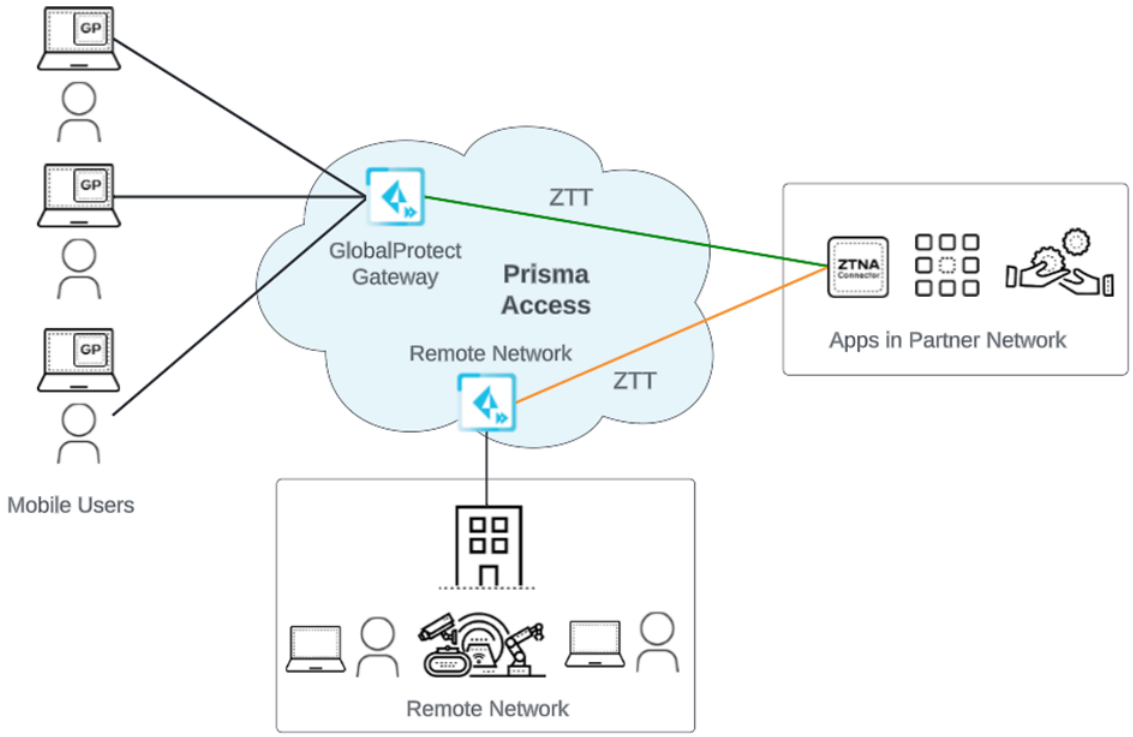
©2025 Palo Alto Networks, Inc.

其他云提供商的云 VPC 中托管应用程序。如果您有数百或数千个 VPC，ZTNA 连接器可以加速提供云交付应用访问的过程。



 ©2025 Palo Alto Networks, Inc.

- 在商业合作伙伴网络中访问应用程序 — 一些组织访问托管在商业合作伙伴网络中的应用程序。使用服务连接来连接这些应用程序需要手动路由和 NAT 配置。ZTNA 连接器允许您连接到这些应用程序，而无需执行手动 IP 路由配置。



 ©2025 Palo Alto Networks, Inc.

服务连接和 ZTNA 连接器的支持用例

ZTNA 连接器不是服务连接的替代方案。它可以与服务连接互补或共存，让您在保护私有应用程序时拥有灵活性。如果您已部署服务连接，则可以继续使用它们，除非您想要转移到不同的应用程序访问模型。下表显示了服务连接或 ZTNA 连接器的支持和不支持的用例。复选标记表示用例受支持；破折号 (—) 表示不受支持。

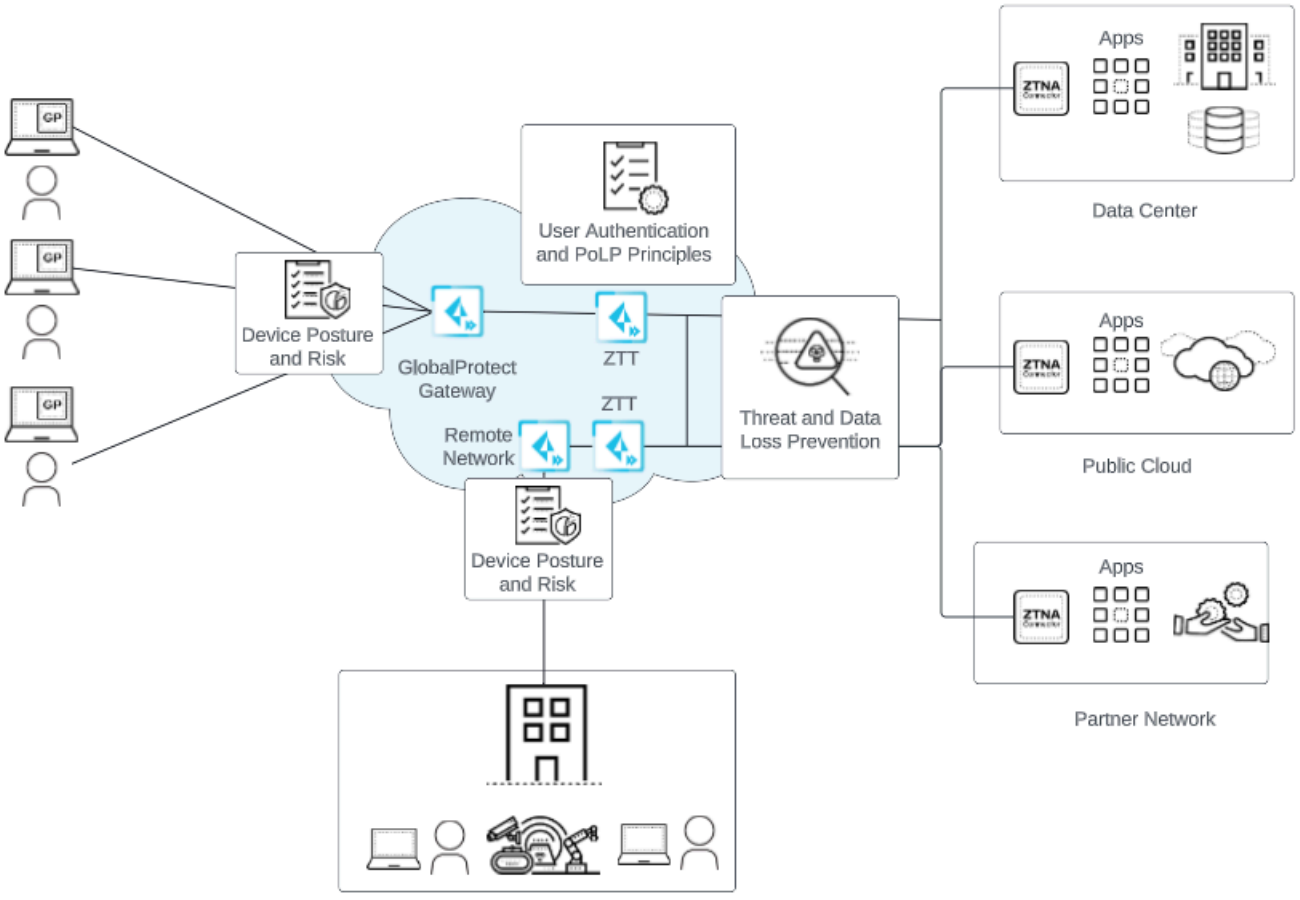
用例	ZTNA 连接器支持	服务连接支持
在重叠网络中访问应用程序	√	—
访问客户端发起的应用程序流量的所有端口和协议	√	√
自动建立到 Prisma Access 的隧道	√	—
自动发现 Prisma Access 的位置	√	—
自动扩展 Prisma Access 的位置以实现高达 10 Gbps 的吞吐量	√	—
使用 IP 地址和子网访问私有应用程序	√	√
服务器发起的流量（例如远程帮助台）接入到托管设备（GlobalProtect 移动用户或远程网络）。	—	√
需要唯一客户端 IP 地址的应用程序或服务	√	√
访问具有动态端口的应用程序（例如 FTP 主动模式或 VoIP）	—	√
应用了基于 User-ID 应用策略规则的混合部署，使用本地新一代防火墙	√	√

©2025 Palo Alto Networks, Inc.

ZTNA 连接器 2.0 原则

按照以下 ZTNA 连接器 2.0 原则，ZTNA 连接器可让您将私有应用程序连接到 Prisma Access：

- 设备状态和风险 — 在 Prisma Access 中使用基于 User-ID 的策略规则，您可以为用户和设备（包括移动用户和物联网设备）定义状态，以防未经授权访问私有应用程序。您还可以在 ZTNA 连接器与 Prisma Access 之间创建通用策略规则。
- 用户身份验证和最小权限访问 — 通过基于用户或组的用户身份验证和策略规则，您可以实施最小权限原则 (PoLP)，为用户提供所需应用程序的访问权限，同时阻止对不需要的应用程序的访问。
- 威胁和数据丢失防护 — Prisma Access 以及 ZTNA 连接器使用高级安全功能，如高级威胁防护、高级 URL 过滤、SaaS 安全、高级 WildFire 和企业 DLP，确保您的私有应用程序和应用数据的安全。



 ©2025 Palo Alto Networks, Inc.

ZTNA 连接器要求和指南.

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ ZTNA 连接器附加许可证 带附加许可证的基础许可证包括 8 个 ZTNA 连接器、100 个 FQDN 和 4 个 IP 子网功能。 带附加许可证的高级许可证包括 40 个 ZTNA 连接器、300 个 FQDN 和 1024 个 IP 子网功能。 带附加许可证的高级许可证包括 200 个 ZTNA 连接器、4000 个 FQDN 和 1024 个 IP 子网功能。 ❑ 如果您不购买 ZTNA 连接器附加许可证，Prisma Access 许可证将包括四个连接器、40 个 FQDN 和四个 IP 子网。此功能旨在让您在自己的环境中尝试 ZTNA 连接器。

在配置 ZTNA 连接器之前，请确保您了解连接器的要求和限制，以及部署时应遵循的准则。

支持的 Prisma Access 版本和要求

- Prisma Access 4.0 版本，并配备兼容的 SaaS 代理。

  将任何低于 4.0 的 Prisma Access 版本（包括任何 Innovation 版本）至少升级到 4.0 版本。

  如果您想要使用 FQDN 通配符或 IP 子网来访问应用程序，则至少需要 Prisma Access 5.0 版本。此外，Prisma Access 5.0 解锁了 Dump Overview、Packet Capture 和 Tech Support诊断工具的使用。
- 您必须将连接器版本升级到最低 6-2-2-ztna-connector-b1 才能使用 5.0 的功能。
- 为了 Prisma Access (Managed by Panorama)，升级云服务插件版本到最低 4.0 版本。升级到最新的云服务插件以解锁最新功能。

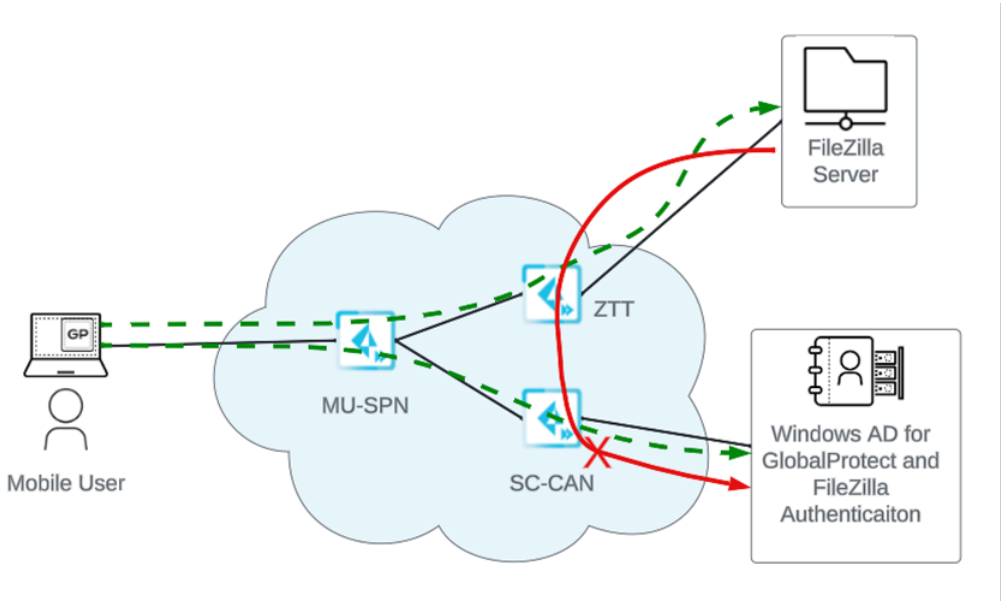
应用程序支持

ZTNA 连接器提供对您的所有私有应用程序流量的访问权限，但以下情况除外：

©2025 Palo Alto Networks, Inc.

- ZTNA 连接器不支持以下流量：
  - 来自数据中心的流量（例如 SCCM 或远程帮助台流量）。
  - User-ID 重新分发。
  - 执行端口跳跃的应用程序（例如 VoIP 或主动模式 FTP）。
  - 应用程序级网关 (ALG) 应用程序，例如主动模式 FTP 和 SIP。
  - 仅当您将数据中心域控制器和资源作为 IP 地址子网加入时，才支持应用程序的 Windows 集成身份验证（例如 NTLM 或 Kerberos）。支持 SAML、OAuth 和 LDAP。
  - 服务连接后的应用程序与 ZTNA 连接器后的应用程序之间的通信。

    例如，您在服务连接后托管 Windows Active Directory (AD) 服务器（因为 ZTNA 连接器后不支持 AD 服务器），并在 ZTNA 连接器后托管 FTP (Filezilla) 服务器。如果 FTP 服务器需要对 Windows AD 服务器进行身份验证，身份验证将失败，因为您无法使用 Prisma Access 作为服务连接公司访问节点 (SC-CAN) 和 ZTNA 连接器隧道终端 (ZTT) 之间的主干网络。



特性和功能限制

在设置和配置 ZTNA 连接器部署时，请记住以下限制：

- 在 ZTNA 对象名称中不要使用特殊字符，包括 < > !@#$%^& 以及中文、日文或韩语字符。
- 默认 Prisma Access 部署不支持以下功能；请联系您的 Palo Alto Networks 团队来激活它们：
  - 为具有 ZTNA 连接器 的 Prisma Access 基础设施 IP 地址使用 RFC 6598 地址

©2025 Palo Alto Networks, Inc.

- 连接器组指南 — 添加连接器组时，请遵循以下建议：
  - 单个连接器组中的所有应用程序都应使用相同的 DNS 服务器进行 DNS 解析。
  - 如果您从数据中心或总部位置访问应用程序，则连接器组中的所有应用程序都应来自同一数据中心或总部位置。
  - 不要在单个连接器组中添加两个或多个区域的连接器。连接器组中的所有连接器都应位于同一区域。
  - 从 Prisma Access 5.01 开始，您可以为每个 FQDN 目标或通配符目标指定最多 4 个连接器组（版本 5.0 及更低版本支持每个 FQDN 目标或通配符目标的一个连接器组）。确保在为每个 FQDN 目标或通配符目标分配连接器组时，不要将同一个应用程序分配给每个区域的超过 4 个连接器。

    例如，您已将同一个应用程序（FQDN 目标或通配符目标）分配给四个连接器组，每个组有一个连接器，并且所有连接器都位于同一区域中。这种配置是可以接受的，因为您没有在单个区域中为每个应用程序分配超过四个连接器。

    但是，如果将同一个应用程序（FQDN 目标或通配符目标）分配给三个连接器组，每个组有两个连接器，并且所有连接器都位于同一区域中，那么，这就是一种无效配置，因为您正在将六个连接器分配给单个区域中的同一个应用程序。
- 一些 ZTNA 连接器（例如，基于 AWS 的连接器或基于 Azure 的连接器）支持自动扩展，其中 AWS 或 Azure 监控连接器上的网络带宽利用率并自动调整容量以维持应用程序性能。当连接器上的网络带宽利用率下降时，AWS 或 Azure 会触发自动缩减。如果在 ZTNA 连接器中发生缩减，则由 ZTNA 连接器处理的标记为缩减的现有长寿命会话将提前终止。此行为不会影响缩减后发起的新流量会话。对于长期会话（例如 SSH 或 RDP），ZTNA 连接器会在缩减期间终止会话，您必须重新连接该会话。

扩缩和吞吐量注意事项

ZTNA 连接器支持以下最大值：

- 所有连接器组中的每个租户 4,096 个应用程序
- 每个租户 200 个连接器
- 每个连接器组 512 个应用程序
- 每个连接器组 4 个连接器
- 每个连接器 200,000 个并发会话

  每个连接器可支持 *200,000* 个并发连接。一个连接器组最多可包含 *4* 个连接器，每个连接器组最多可容纳 *800,000* 个并发连接。
- 26 个计算区域
- 每个连接器的吞吐量为 1 Gbps，每个 Prisma Access 计算位置的最大吞吐量为 10 Gbps

支持的应用程序托管环境

您可以在以下数据中心环境中部署 ZTNA 连接器虚拟机，并满足指定的最低要求：

 ©2025 Palo Alto Networks, Inc.

云提供商	实例大小	CPU 大小	内存大小	磁盘大小
Amazon AWS	每个区域 m5.xlarge	4 个 vCPU	16 GB	40 GB
Google Cloud Platform (GCP)	每个区域 n2-standard-4	4 个 vCPU	16 GB	40 GB
Microsoft Azure	每个区域的 Standard_D4_v3	4 个 vCPU	16 GB	40 GB
KVM	使用 qcow 镜像	4 个 vCPU	16 GB	40 GB
Hyper-V	使用 vhd 映像	4 个 vCPU	每个虚拟机 8 GB 内存	40 GB
VMware ESXi	使用 OVA 图像。在 vSphere 和 ESXi 主机上直接受支持	每个虚拟机 4 个 vCPU	每个虚拟机 8 GB 内存	40 GB 磁盘（厚配置）
对于 VMware ESXi，连接器虚拟机不支持 vMotion、虚拟机快照或迁移。 对于 KVM，连接器虚拟机不支持实时迁移和快照。				

您有责任托管虚拟机并确保它们可以连接到互联网。

AWS、GCP 和 Azure 都有 ZTNA 连接器，您可以在相应的市场上获取。您可以从 Palo Alto 客户支持门户下载 VMware ESXi Open Virtualization Application (OVA) 文件和 KVM qcow 文件。

网络要求

以下网络要求可实现 ZTNA 连接器和 Prisma Access 的连接：

- 启用 ZTNA 连接器后，Prisma Access 使用为远程网络和移动用户设置的 DNS 规则为 DNS 请求设置 DNS 代理 — GlobalProtect。
- UDP 有效负载大小（包括报头）在到 ZTNA 应用程序服务器的路径上不应超过 1,300 字节的 MTU 大小。Palo Alto Networks 建议将数据包保持在该 MTU 大小或以下。
- 允许 WAN 接口（端口 1）IP 地址的出站 UDP 端口 4500 和 UDP 500，以进行 IPSec 和 IKE 到 ZTNA 隧道终端 (ZTT) 的连接。如果要限制为单个 IP 地址启用出站 UDP 端口 500 和 4500 连接，请为 ZTNA 连接器的 **PA 服务 IP** 地址（在 **Workflows**（工作流） > **ZTNA Connector**（**ZTNA** 连接器） > **Connectors**（连接器））启用它。



 ©2025 Palo Alto Networks, Inc.

- 如果 ZTNA 连接器使用公共 IP 地址作为互联网接口，则必须允许 IP/50 封装安全有效负载 (ESP)。
- 允许从 WAN 接口（端口 1）IP 地址 HTTPS 连接到 ZTNA 连接器控制器的出站 TCP 端口 443。
- ZTNA 连接器自动配置 IPSec 隧道的 Prisma Access ZTT 端和 ZTNA 连接器端。IKE 和 ESP 的 DH 组/加密/哈希配置的算法为：ecp384/aes256/sha512。
- 不要终止 ZTNA 连接器创建并用于访问私有应用程序的 IPSec 隧道。
- （移动用户 - 仅限 GlobalProtect 部署）首次在 ZTNA 连接器中载入应用程序时，您必须刷新 GlobalProtect 应用程序，以便移动用户收到更新的 DNS 服务器配置。如果您从 ZTNA 连接器中删除了应用程序，则必须刷新 GlobalProtect 应用程序，以便移动用户可以接收更新的 DNS 服务器配置。
- 如果 ZTNA 连接器和私有应用程序之间存在防火墙，则防火墙必须允许从 ZTNA 连接器访问应用程序（也就是说，您必须允许私有应用程序访问应用服务器解析的 IP 地址、协议和端口）。

  此外，您还需要允许为应用程序目标运行状况探测配置的协议（TCP 或 ICMP）。连接器应用程序探测应用服务器，以便确定它是否可以提供对应用程序的访问权限，并且您可以将应用程序目标的探测类型 配置为 **tcp ping**、**icmp ping**或 **none**（无探测）。如果指定 **tcp ping**，则防火墙必须允许应用程序的 TCP 访问；如果指定 **icmp ping**，则防火墙必须允许应用程序的 ICMP 回显请求和答复。
- 在使用 ping 和 traceroute 诊断工具之前，请确保您的数据中心允许 ICMP。出于安全考虑，某些云环境不允许使用 ICMP；在这种情况下，这些工具不会显示任何活动。

  traceroute 诊断工具还使用随机 UDP 端口，因此，您必须允许所有 UDP 和 ICMP 错误回复，traceroute 工具才能正常运行。
- 确保您已在本地接口上配置 DNS 条目，以允许 ZTNA 连接器解析应用程序 FQDN，并且 ZTNA 连接器可以通过 UDP 端口 53（用于 DNS 解析的端口）访问 DNS 服务器。
- （ZTNA 连接器 5.0 及更高版本）确保您已在网络中配置安全规则，以允许 ZTNA 连接器对您的数据中心执行应用程序探测。ZTNA 连接器使用其数据中心接口 IP 地址作为探测应用服务器的应用程序的源 IP 地址。如果应用程序探测成功，则应用程序状态为 **Up**（启动），并且 ZTNA 连接器的用户会话具有与源 IP 地址相同的数据中心接口 IP 地址。如果应用程序探测不成功，则应用程序状态为 **Down**（关闭）；在这种情况下，您可以使用 ping 和 tcp ping 诊断工具来测试与应用程序的连接。
- 如果您在网络中使用 RFC 6598 共享地址，则必须指定 ZTNA 连接器可用于在以下位置之间进行路由的 IP 地址块：Prisma Access 和你的连接器之间，以及 Prisma Access 和您的私有应用程序之间。

 ©2025 Palo Alto Networks, Inc.

- 如果需要限制添加到组织允许列表中的 IP 地址和 FQDN 列表，请添加 允许 ZTNA 连接器使用的 IP 地址和 FQDN 中列出的项目。

  例如，如果您在美国设置 ZTNA 连接器，请将以下 URL 添加到组织的允许列表中：

  - 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 (for NTP)
  - 0.cloudgenix.pool.ntp.org (for NTP)
  - 1.cloudgenix.pool.ntp.org (for NTP)
  - 2.cloudgenix.pool.ntp.org (for NTP)
  - 3.cloudgenix.pool.ntp.org (for NTP)

  将先前 *FQDN* 的 *DNS* 解析限制为 *IPv4* 解析。*ZTNA* 连接器不支持使用 *IPv6* 建立与控制器 *FQDN* 的连接。

- 禁用控制器会话的 SSL 解密。

允许 ZTNA 连接器使用的 IP 地址和 FQDN

为了确保 ZTNA 连接器顺利运行，请将以下 URL 和 IP 地址添加到允许列表中。

服务名称	端口	方向	源接口 **Internet** 协议	目标地址和 **IP** 地址
ZTNA 连接器访问 Prisma Access	443	出站	ZTNA 连接器 WAN 端口	https://controller.cgnx.net ：52.8.93.87 地址：52.8.25.40 https://locator.cgnx.net 地址：13.56.217.238 地址：13.56.201.169 hood: 52.40.98.31 34.218.98.185 sugarloaf: 18.200.102.82 18.200.135.33 faber: 18.139.242.53

©2025 Palo Alto Networks, Inc.

服务名称	端口	方向	源接口 **Internet** 协议	目标地址和 **IP** 地址
				54.255.61.109 https://vmfg.cgnx.net ：52.53.122.104 地址：52.53.102.7 https:// controller.elcapitan.cgnx.net 地址：52.8.93.87 地址：52.8.25.40 https://vmfg.elcapitan.cgnx.net 地址：52.53.122.104 地址：52.53.102.7 https:// controller.hood.cgnx.net 地址：52.32.167.5 地址：54.70.168.33 https://vmfg.hood.cgnx.net 地址：50.112.136.184 地址：34.210.34.87 https:// controller.sugarloaf.cgnx.net 地址：108.128.176.192 地址：18.200.144.58 https://vmfg.sugarloaf.cgnx.net 地址：99.81.179.99 地址：99.80.52.255 https://sdwan-stats-hood- us.cgnx.net https://sdwan-stats-elcapitan- us.cgnx.net https://sdwan-stats-hood- jp.cgnx.net https://sdwan-stats-elcapitan- jp.cgnx.net https://sdwan-stats-hood- sg.cgnx.net

©2025 Palo Alto Networks, Inc.

服务名称	端口	方向	源接口 **Internet** 协议	目标地址和 **IP** 地址
				https://sdwan-stats-elcapitan-sg.cgnx.net https://sdwan-stats-hood-au.cgnx.net https://sdwan-stats-elcapitan-au.cgnx.net https://sdwan-stats-hood-in.cgnx.net https://sdwan-stats-elcapitan-in.cgnx.net https://sdwan-stats-hood-ca.cgnx.net https://sdwan-stats-elcapitan-ca.cgnx.net https://sdwan-stats-sugarloaf-eu.cgnx.net https://sdwan-stats-sugarloaf-de.cgnx.net https://sdwan-stats-sugarloaf-uk.cgnx.net https://controller.bowfell.cgnx.net ：13.41.243.90 地址：18.171.17.23 https://vmfg.bowfell.cgnx.net 地址：52.56.35.36 地址：52.56.224.242 https://controller.faber.cgnx.net 地址：52.74.47.220 地址：13.251.109.27 https://vmfg.faber.cgnx.net 地址：18.142.153.59 地址：52.74.58.219 h

©2025 Palo Alto Networks, Inc.

服务名称	端口	方向	源接口 Internet 协议	目标地址和 IP 地址
				ttps:// controller.townsend.cgnx.net ：13.55.31.41 地址：3.106.168.215 https:// vmfg.townsend.cgnx.net 地址：52.64.177.240 地址：13.55.164.51 https://sdwan-stats-faber-sg.cgnx.net https://sdwan-stats-bowfell-uk.cgnx.net https://sdwan-stats-townsend-au.cgnx.net
Ntp	123	出站	ZTNA 连接器 WAN 和 LAN 端口	time.nist.gov 0.cloudgenix.pool.ntp.org 1.cloudgenix.pool.ntp.org 2.cloudgenix.pool.ntp.org 3.cloudgenix.pool.ntp.org
DNS	53	出站	ZTNA 连接器 WAN 和 LAN 端口	客户或提供商 DNS 服务器

证书管理

为了确保安全通信会话中各方之间的信任，Prisma Access 使用数字证书。每个证书都包含用来加密明文或解密密文的加密密钥。此外，每个证书还包括用来对颁发者的身份进行验证的数字签名。颁发者必须在验证方的受信任的证书颁发机构 (CA) 列表内。或者，验证方确认颁发者没有撤销证书。Prisma Access 使用证书来保护解密和身份验证等功能，并保护连接到您的网络的所有客户端、服务器、用户和设备之间的通信。

对于加入 ZTNA 连接器的应用程序，请使用Prisma Access证书管理设置您的证书、添加证书颁发机构并定义证书检查。

©2025 Palo Alto Networks, Inc.

启用 ZTNA 连接器

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ ZTNA 连接器附加许可证 带附加许可证的基础许可证包括 8 个 ZTNA 连接器、100 个 FQDN 和 4 个 IP 子网功能。 带附加许可证的高级许可证包括 40 个 ZTNA 连接器、300 个 FQDN 和 1024 个 IP 子网功能。 带附加许可证的高级许可证包括 200 个 ZTNA 连接器、4000 个 FQDN 和 1024 个 IP 子网功能。 ❑ 如果您不购买 ZTNA 连接器附加许可证，Prisma Access 许可证将包括四个连接器、40 个 FQDN 和四个 IP 子网。此功能旨在让您在自己的环境中尝试 ZTNA 连接器。

必须先在 Prisma Access 中启用 ZTNA 连接器，然后才能设置。启用 ZTNA 连接器之前，请执行以下操作：

- 查看ZTNA 连接器要求和指南.。
- 识别您的应用程序 IP 和连接器 IP 地址块。您必须保留一个单独地址池，以便在 Prisma Access 内部使用，用于将流量路由到您将接入的连接器和私有应用程序。Prisma Access 会将您接入到 ZTNA 连接器的应用程序的 FQDN 解析为应用程序 IP 地址块中的 IP 地址。同样，Prisma Access 使用连接器 IP 地址块将远程网络或移动用户的流量路由到相应的 ZTNA 连接器。

  您应该为地址池保留至少一个 /16 子网。使用 RFC 1918 或 RFC 6598 地址。可在 ZTNA 连接器设置期间指定 RFC 1918 地址池而不是 RFC 6598；但在指定 RFC 1918 后，便无法将地址池类型更改回 RFC 6598。
- Strata Cloud Manager
- Panorama

启用 ZTNA 连接器 (Strata Cloud Manager)

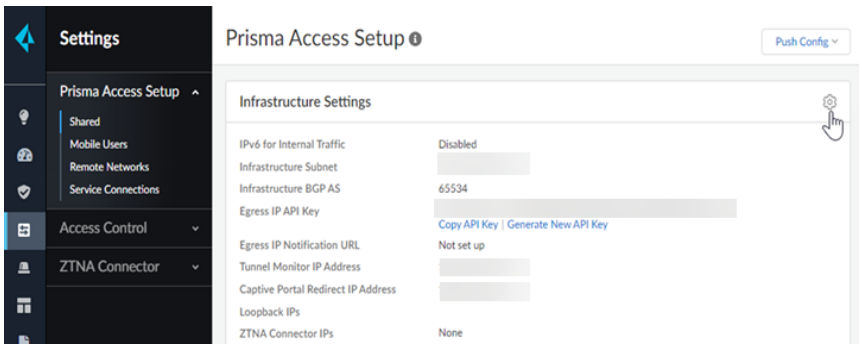
使用以下工作流程在云托管的 Prisma Access 中启用 ZTNA 连接器。

©2025 Palo Alto Networks, Inc.

STEP 1 | 配置 Prisma Access 内部使用的 IP 地址块，这些地址块用于将流量路由至 ZTNA 连接器和接入的私有应用程序。

必须为连接器和应用程序定义单独的 IP 地址块，并且这些地址块不能相互重叠，不能与 Prisma Access Infrastructure 子网重叠，也不能与 GlobalProtect IP 地址池重叠。

- 选择 **Workflows**（工作流） > **Prisma Access** 设置 > **Prisma Access** > **Infrastructure Settings**（基础设施设置）



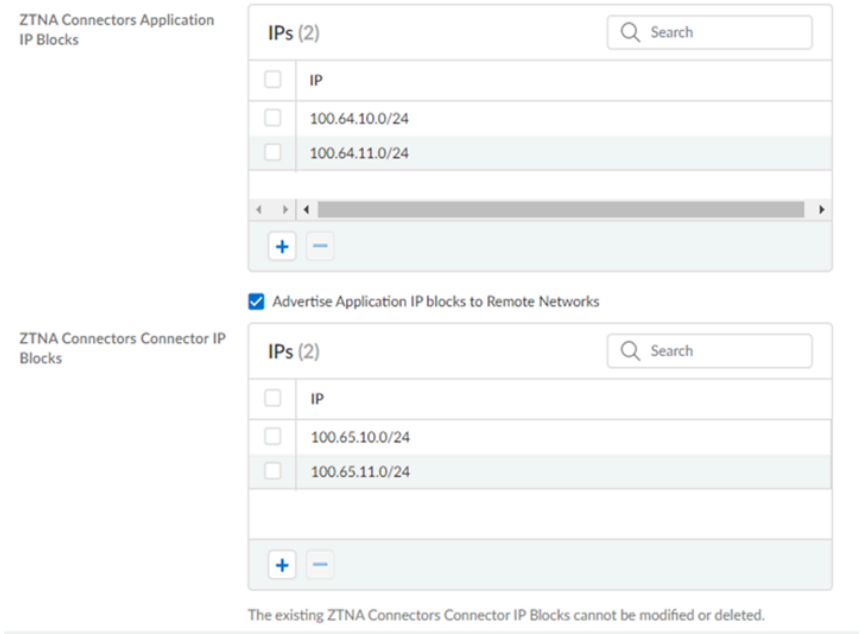
。

- 选择 **ZTNA Connectors Application IP Blocks**（**ZTNA** 连接器应用程序 **IP** 块）以进行添加。

  您可以根据您的部署添加单个应用程序 IP 块或多个块。例如，输入 100.64.10.0/24 和 100.64.11.0/24。还可以选择 **Advertise Application IP blocks to Remote Networks**（向远程网络通告应用程序 **IP** 块）以提供远程网络访问权限。

- 选择 **ZTNA Connectors Connector IP Blocks**（**ZTNA Connectors** 连接器 **IP** 地址块）以进行添加，Prisma Access 内部使用这些地址块在移动用户、远程网络和数据中心中的连接器虚拟机之间路由流量。

  您可以添加单个连接器 IP 块，也可以添加多个块，具体取决于您的部署。例如，输入 100.65.10.0/24 和 100.65.11.0/24。

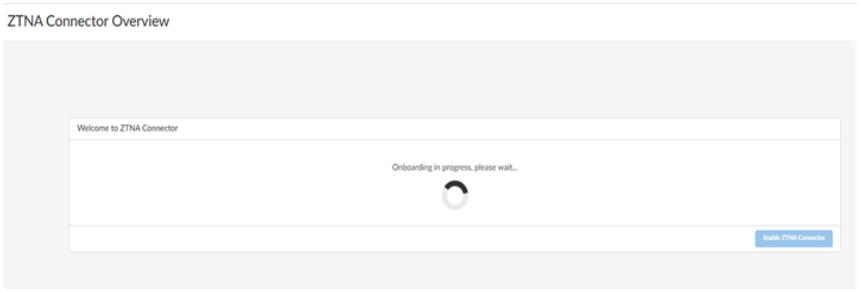


 ©2025 Palo Alto Networks, Inc.

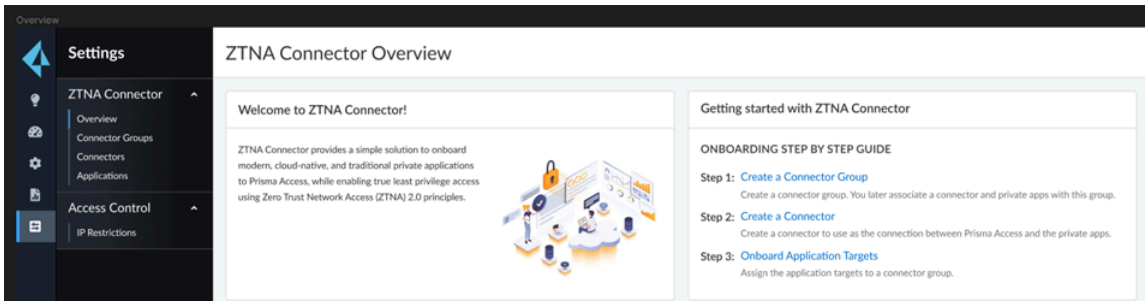
- 单击 **Save**（保存）以保存 IP 地址块配置，然后单击 **Commit**（提交）以提交并推送配置。

STEP 2 | 从 Strata Cloud Manager 启动 ZTNA 连接器。

- 选择 **Workflows**（工作流） > **ZTNA Connector**（**ZTNA** 连接器）。
- Prisma Access 开始设置 ZTNA 连接器的基础设施。这可能需要几分钟时间。



- 当接入完成时，将显示 ZTNA 连接器概述。



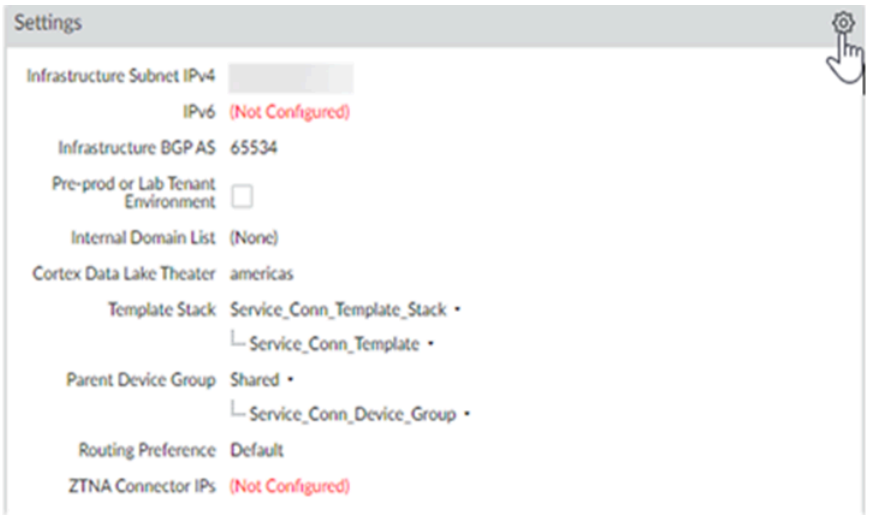
启用 ZTNA 连接器 (Panorama)

使用以下工作流程在 Prisma Access (Managed by Panorama) 中启用 ZTNA 连接器。

 ©2025 Palo Alto Networks, Inc.

STEP 1 | 配置 Prisma Access 内部使用的 IP 地址块，这些地址块用于将流量路由至 ZTNA 连接器和接入的私有应用程序。

- 选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Service Setup**（服务设置），然后单击 **Edit**（编辑）以编辑 **Settings**（设置）选项。



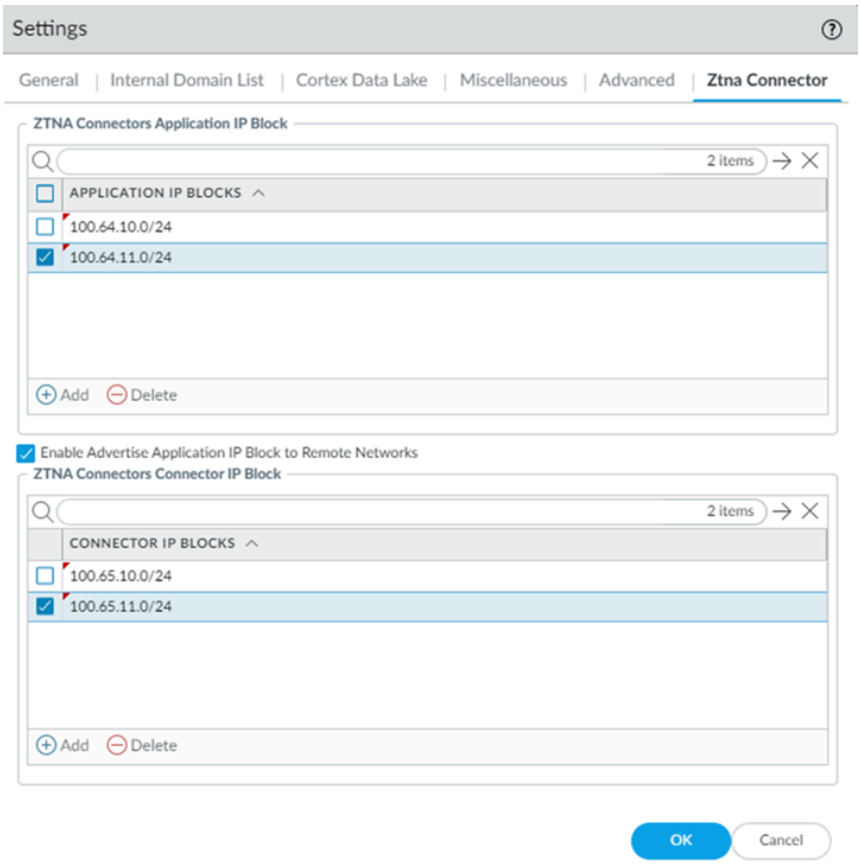
- 选择 **ZTNA Connectors Application IP Blocks**（**ZTNA** 连接器应用程序 **IP** 块）选项上，依次选择 **Add**（添加）和 **Application IP Block**（应用程序 **IP** 块）。

  您可以根据您的部署添加单个应用程序 IP 块或多个块。例如，100.64.10.0/24 和 100.64.11.0/24。还可以选择 **Enable Advertise Application IP Block to Remote Networks**（启用将应用程序 **IP** 块通告给远程网络的功能）。

- 选择 **Connector IP Blocks**（连接器 **IP** 块）以设置供 Prisma Access 内部使用的 IP 块，用于在移动用户、远程网络和数据中心中的连接器虚拟机之间路由流量。

  您可以添加单个连接器 IP 块或多个块，具体取决于您的部署。例如，输入 100.65.10.0/24 和 100.65.11.0/24。

 ©2025 Palo Alto Networks, Inc.

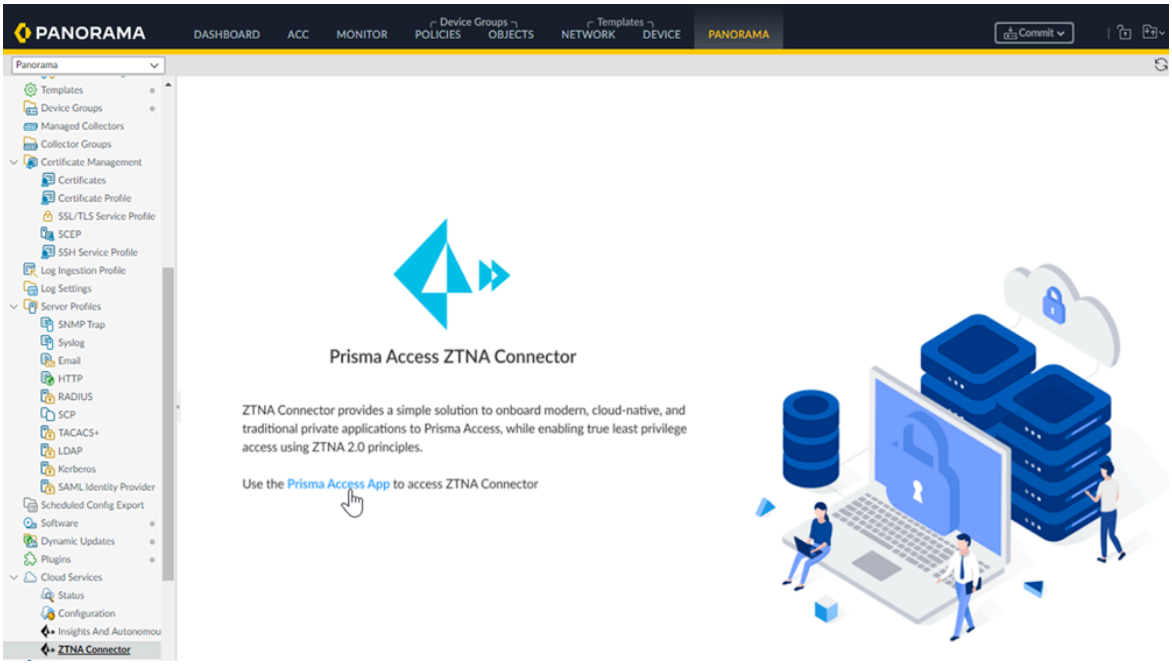


- 单击 **OK**（确定）以保存 IP 地址块配置，然后单击 **Commit**（提交）以提交并推送配置。

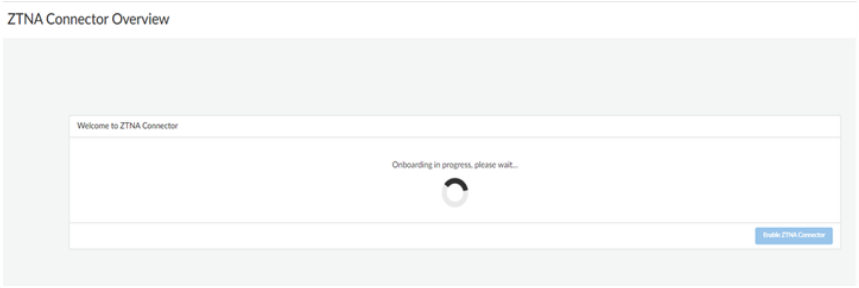
©2025 Palo Alto Networks, Inc.

STEP 2 | 从 Panorama 上的云服务插件启动 ZTNA 连接器。

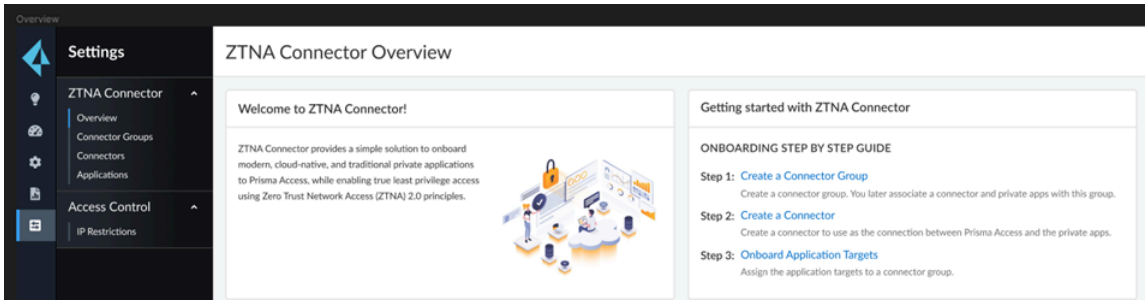
- 选择 **Panorama** > **Cloud Services**（云服务） > **ZTNA Connector**（**ZTNA** 连接器）。
- 单击 Strata Cloud Manager 以在中心内的 Strata Cloud Manager 中启动 ZTNA 连接器。



- 从 Strata Cloud Manager 中 **Settings**（设置） > **ZTNA Connector**（**ZTNA** 连接器）。
- Prisma Access 开始设置 ZTNA 连接器的基础设施。这可能需要几分钟时间。



- 当接入完成时，将显示 ZTNA 连接器概述。



 ©2025 Palo Alto Networks, Inc.

配置 ZTNA 连接器

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ ZTNA 连接器附加许可证 带附加许可证的基础许可证包括 8 个 ZTNA 连接器、100 个 FQDN 和 4 个 IP 子网功能。 带附加许可证的高级许可证包括 40 个 ZTNA 连接器、300 个 FQDN 和 1024 个 IP 子网功能。 带附加许可证的高级许可证包括 200 个 ZTNA 连接器、4000 个 FQDN 和 1024 个 IP 子网功能。 ❑ 如果您不购买 ZTNA 连接器附加许可证，Prisma Access 许可证将包括四个连接器、40 个 FQDN 和四个 IP 子网。此功能旨在让您在自己的环境中尝试 ZTNA 连接器。

启用 ZTNA 连接器后，您可以开始设置 ZTNA 连接器组件：

STEP 1 | 识别您的应用程序 IP 和连接器 IP 地址块，并在 Prisma Access 中添加 IP 地址块。

请参考针对 *IP* 地址块的以下建议：

- 为每个应用程序分配一个单独的 *IP* 地址。
- 为每个连接器分配至少一个 */27 IP* 地址块（每个连接器至少 *32* 个 *IP* 地址）。
- 为每个连接器组分配一个唯一的 *IP* 地址。

您可以根据需要添加更多连接器或应用程序块。

如果您在网络内使用 RFC 6598 地址，则必须保留一个单独的 RFC 6598 IP 地址池供 Prisma Access 内部使用，以将流量路由到您要加入的连接器和私有应用程序。

STEP 2 | 创建连接器组。

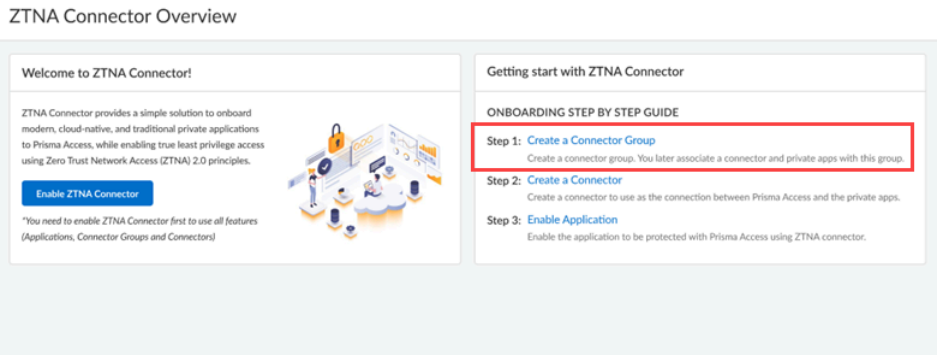
连接器组是连接器和应用程序的逻辑分组。可以使用多种不同的方法对应用程序和连接器进行分组。您可以将连接器分组到不同的地理位置以实现冗余。或者，您可以在同一个数据中心创

 ©2025 Palo Alto Networks, Inc.

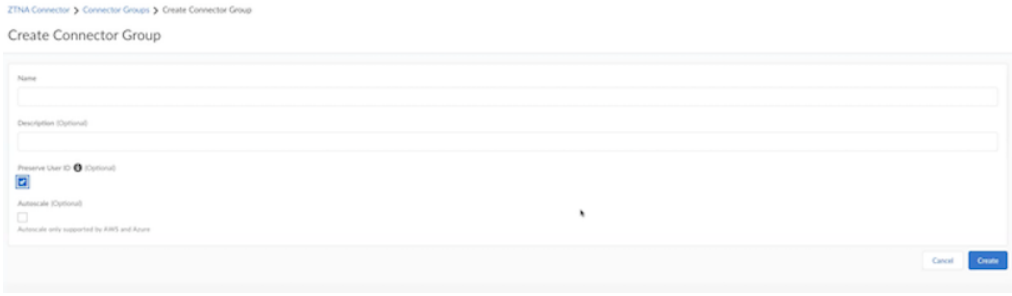
建多个连接器以提高吞吐量。为了简化策略管理，您可能希望对相同的用户组使用的应用程序进行分组。先创建连接器组，然后将连接器和应用程序添加到组中。

根据需要重复此步骤，以创建对连接器和应用程序进行分组所需的所有连接器组。

1. 选择 **Workflows**（工作流） > **ZTNA Connector**（**ZTNA** 连接器），选择 **Overview**（概述）或 **Connector Groups**（连接器组），然后 **Create Connector Group**（创建连接器组）。



2. 为连接器组指定 **Name**（名称）、启用 **Preserve User ID**（保留用户 **ID**），或者提供该连接器组的 **Description**（说明）。



3. （可选）如果数据中心位于 Azure 或 AWS 中，并且您想要使用自动缩放功能，请选择 **Autoscale**（自动缩放）。如果您已启用此功能，则无需创建连接器。
4. **Create**（创建）连接器组

 ©2025 Palo Alto Networks, Inc.

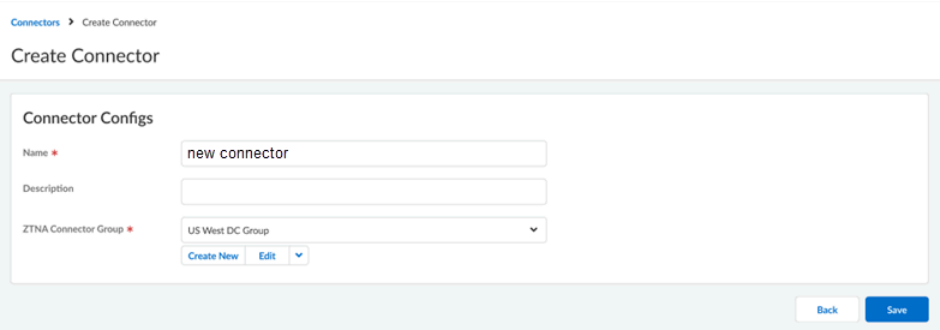
STEP 3 | 仅当您选择非自动缩放连接器组时，才创建连接器并将其添加到连接器组。

创建连接器并将其添加到连接器组。

连接器代表在连接到 Prisma Access 的数据中心内运行的虚拟机。必须在 Prisma Access 中创建连接器，并使用提供的机密/密钥将相应的连接器虚拟机加入数据中心。

根据需要重复此步骤，以创建将数据中心应用程序连接到 Prisma Access 所需的尽可能多的连接器。

- 选择 **Workflows**（工作流） > **ZTNA Connector**（**ZTNA** 连接器），选择 **Overview**（概述）或 **Connectors**（连接器），然后 **Create Connector**（创建连接器）。
- 输入连接器的 **Name**（名称）。



- （可选）添加连接器的 **Description**（说明）。
- 选择要添加连接器的 **Connector Group**（连接器组）。

为了简化路由并以最快速度访问数据中心服务器，*Palo Alto Networks* 建议连接器和服务器位于同一子网中。

- **Create**（创建）连接器。

为了使 *ZTNA* 连接器保持最新状态，您可以更新其软件版本 ***ZTNA Connector***（***ZTNA*** 连接器） > ***Connector Groups***（连接器组）中的图标显示连接器的状态以及是否有可用的升级。

©2025 Palo Alto Networks, Inc.

STEP 4 | 检索用于设置连接器的密钥和机密。

在后续步骤中设置虚拟机时，您将使用密钥和机密值。

1. 自动缩放连接器组 — 按照下面列出的步骤操作：
   1. 转到 **Workflows**（工作流） > **ZTNA Connector**（**ZTNA** 连接器） > **Connector Groups**（连接器组）。
   2. 在自动缩放连接器组的 **Actions**（操作）区域中选择 **Copy Token**（复制令牌），然后复制 **Key**（密钥）和 **Secret**（机密）值。

      使用密钥和机密将创建的云实例或虚拟机与连接器关联。
2. 非自动缩放连接器组 — 请按照下面列出的步骤操作：
   - 选择 **Workflows**（工作流） > **ZTNA Connector**（**ZTNA** 连接器） > **Connectors**（连接器）。
   - 选择您要部署的连接器。
   - 在 **Actions**（操作）区域中选择 **Copy Token**（复制令牌），然后复制 **Key**（密钥）和 **Secret**（机密）值。

     使用密钥和机密将创建的云实例或虚拟机与连接器关联。

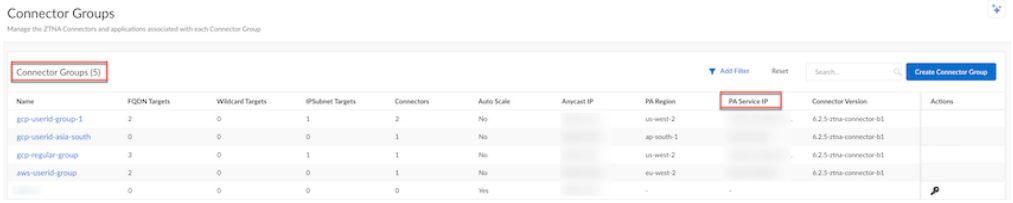


STEP 5 | 在数据中心部署 ZTNA 连接器虚拟机。

STEP 6 | （可选）选择 **Workflows**（工作流） > **ZTNA Connector**（**ZTNA** 连接器） > **Connector Groups**（连接器组），记下连接器组的 **PA Service IP**（**PA** 服务 **IP**）地址，然后将此 IP 地址添加到组织的允许列表中。

只有在您加入连接器后，才能在 ***Connector Groups***（连接器组）下看到 ***PA Service IP***（***PA*** 服务 ***IP***）。

如果需要，请将此 IP 地址添加到允许列表中，以便您的网络可以传输和接收 ZTNA 连接器流量。



 ©2025 Palo Alto Networks, Inc.

STEP 7 | 将目标添加到连接器组。

设置目标以通过 ZTNA 连接器虚拟机访问数据中心内的私有应用程序。可以根据 FQDN 通配符、FQDN 或 IP 子网添加目标；ZTNA 连接器负责设置移动用户和分支机构用户通过 Prisma Access 安全地访问应用程序所需的网络和 DNS 设置。

1. 选择 **Workflows**（工作流） > **ZTNA Connector**（**ZTNA** 连接器） > **Application Targets**（应用程序目标）。
2. 选择要创建的目标类型。



借助无提交应用程序加入增强功能，现在只需不到一分钟的时间即可加入应用程序，以便实现对应用程序的快速访问。此功能还允许您加入更多应用程序。

限制：

- 您不能在多个应用程序目标（具有不同的端口/协议）中添加相同的 *FQDN*。
- 添加或删除通配符目标时，*MU* 或 *RN* 上会进行提交操作以添加或删除 *DNS* 代理转发规则。但是，随后通配符应用程序发现与该通配符匹配的 *FQDN* 不需要任何额外的提交操作，因此可以快速加入应用程序，以便您立即访问这些应用程序。

要启用无提交应用程序加入功能，请将 *Prisma Access* 数据平面更新到版本 *11.2.3* 及更高版本。

- **Wildcard Targets**（通配符目标）— 将通配符（例如，*.example.com）用于目标。当用户访问与该通配符匹配的站点时，这些应用程序将会自动加入，以便移动用户和远程网络用户从 ZTNA 连接器进访问这些应用程序。例如，假设通配符为 *.example.com，当用户访问 app1.example.com 上的应用程序时，ZTNA 连接器会自动创建配置，以使用其特定的 FQDN、协议和端口加入该子应用程序。

  此外，当用户访问基于通配符的应用程序时（例如，基于 *.example.com 通配符的 app1.example.com），系统会发现该应用程序并将其作为 **FQDN Target**（**FQDN** 目标）自动加入。

  1. 转到 **Wildcard Targets**（通配符目标），单击 **Create Wildcard Target**（创建通配符目标）。
  2. 为该目标输入唯一的 **Name**（名称）。
  3. 输入与该目标关联的 **Connector Group**（连接器组）。

     组的类型必须为 **FQDN/Wildcard**（**FQDN/**通配符）。

     从 Prisma Access 5.0.1 开始，您可以为通配符和 FQDN 目标选择多个连接器组，每个通配符或 FQDN 目标最多四个连接器组。为每个目标选择多个连接器组时，请遵循指导原则。

 ©2025 Palo Alto Networks, Inc.

4. 输入要用于目标的 **Wildcard**（通配符）。

   以 .example.com 或 .my.example.com 的格式输入（UI 会在通配符前添加星号）。不要通过指定通配符 *.*、example.*.com 或 *.com 来允许所有站点。

5. 选择 **Protocol**（协议）（**tcp**、**udp** 或两者）。

6. （可选）要启用从 GlobalProtect 用户到 ZTNA 连接器数据中心的 ICMP 协议，请选择 **Allow ICMP Protocol**（允许 **ICMP** 协议）。

7. 选择要用于该应用程序的 **Port**（端口）。

   输入单个端口、使用逗号分隔的多个端口、使用破折号的端口范围，或两者兼而有之。请勿在逗号后添加空格。选择 **Any**（任何）端口以匹配您指定的任何端口，或选择 **Match**（匹配）并输入要匹配的一个或多个端口。

   如果在 **Protocol**（协议）下选择了 **both**（两者），则必须同时将这些端口添加到 **TCP Port**（**TCP** 端口）和 **UDP Port**（**UDP** 端口）

   当您在 **Advanced Settings**（高级设置）下的 **TCP Port**（**TCP** 端口）字段中输入范围时，将激活 **icmp ping** 和 **none**（无）的 **Probing Type**（探测类型）。

8. 根据所选择的协议，输入 **tcp ping**、**icmp ping** 或 **none**（无）的 **Probing Type**（探测类型）。

   如果选择 **tcp ping**，请选择 **probing port**（探测端口），然后输入单个端口。该端口不一定要在您在 **port**（端口）和 **protocol**（协议）区域中输入的端口范围内。ZTNA 连接

©2025 Palo Alto Networks, Inc.

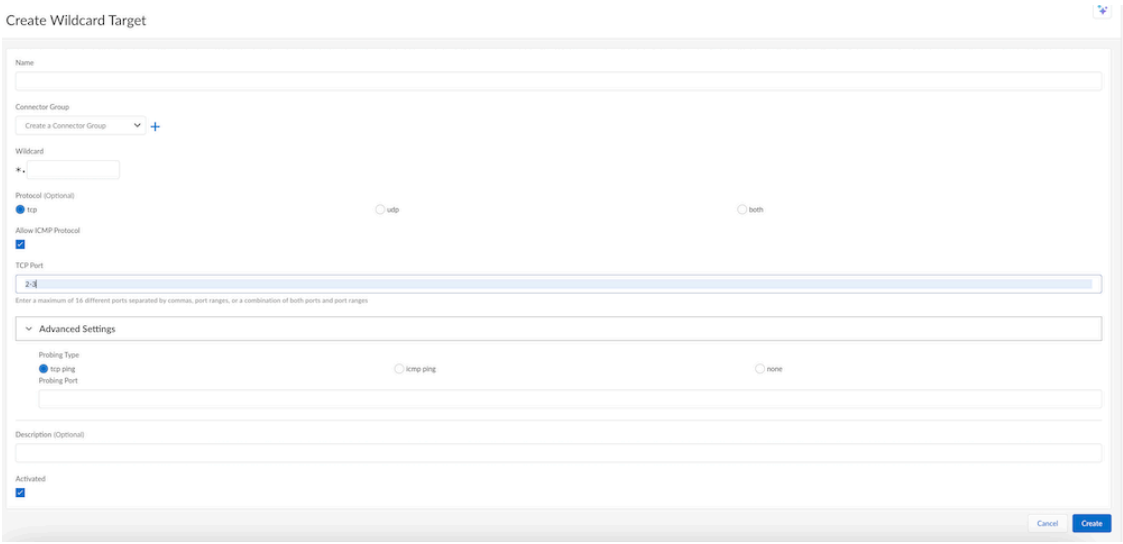
器通过从探测端口到 FQDN 解析的 IP 地址执行 tcp ping 来确定应用程序的可达性。如果 ping 成功，则应用程序被视为 **Up**（正常运行）。

您还可以编辑在应用程序加入期间添加的探测端口。探测端口更新后，ZTNA 连接器会在更新的端口上启动 tcp 探测应用程序，应用程序状态也会相应更新。

如果选择 **icmp ping**，ZTNA 连接器将对 FQDN 解析的 IP 地址执行 ICMP ping。如果收到对 ICMP ping 的响应，则应用程序被视为 **Up**（正常运行）。

如果选择 **none**（无），则不执行探测且应用程序始终标记为 **Up**（正常运行）。

9. 选择 **Activated**（已激活）并 **Create**（创建）目标。



- **FQDN Targets**（**FQDN** 目标）— 要为单个 FQDN 创建目标，请创建 FQDN 目标。

  从 *Prisma Access 5.0* 开始，对于具有 *ZTNA* 连接器 *5.0* 版本或更高版本的连接器组，如果应用程序 *FQDN* 解析为多个专用 *IP* 地址，则 *ZTNA* 连接器将执行应用程序探测以确定所有已解析 *IP* 地址的状态，并在应用程序状态为“运行正常”的多个已解析 *IP* 地址之间实现 *FQDN* 访问负载均衡。

  要创建 FQDN 目标，请转到 **FQDN Targets**（**FQDN** 目标），单击 **Create FQDN Target**（创建 **FQDN** 目标）。创建 FQDN 目标的方式与创建 FQDN 通配符的方式相同，需要用单个 FQDN 替换 FQDN 通配符。

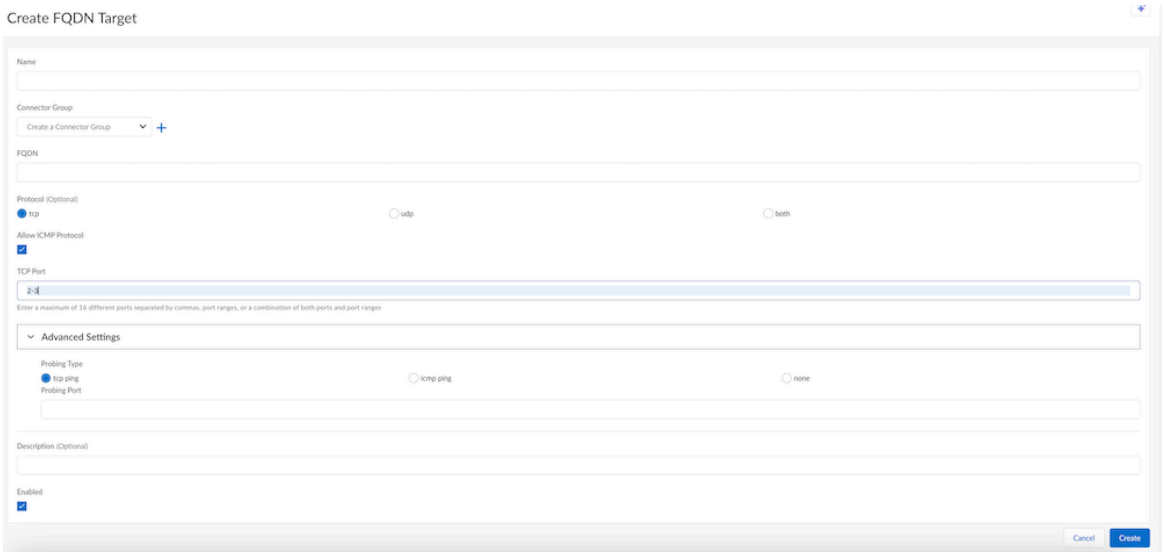
  从 Prisma Access 5.0.1 开始，您可以为每个 FQDN 目标以及通配符目标选择多个连接器组，每个 FQDN 或通配符目标最多四个连接器组。为每个目标配置多个连接器组时，请遵循指导原则。

  通过通配符目标发现的应用程序也显示在此处。当用户访问与该通配符匹配的站点时，这些应用程序将会自动加入，以便移动用户和远程网络用户从 ZTNA 连接器进访问这些应用

 ©2025 Palo Alto Networks, Inc.

程序。例如，假设通配符为 *.example.com，当用户访问 app1.example.com 上的应用程序时，ZTNA 连接器会自动将该应用添加到 FQDN 目标列表中。

通过父类型通配符目标发现 FQDN 应用程序后，不会在发现的应用程序中更新对通配符目标进行的任何更改。此外，不会重新发现相同的已发现 FQDN。如果需要更新已发现 FQDN 应用程序的特征，请按照以下步骤对已发现的应用程序执行手动更新。



- **IP Subnet**（**IP** 子网）— 创建基于 IP 子网的目标，以根据 IP 子网（而不是 FQDN）查找应用程序。

  1. 转到 **IP Subnets**（**IP** 子网），单击 **Create Subnet Rule**（创建子网规则）。
  2. 为该目标输入唯一的 **Name**（名称）。
  3. 输入与该目标关联的 **Connector Group**（连接器组）。

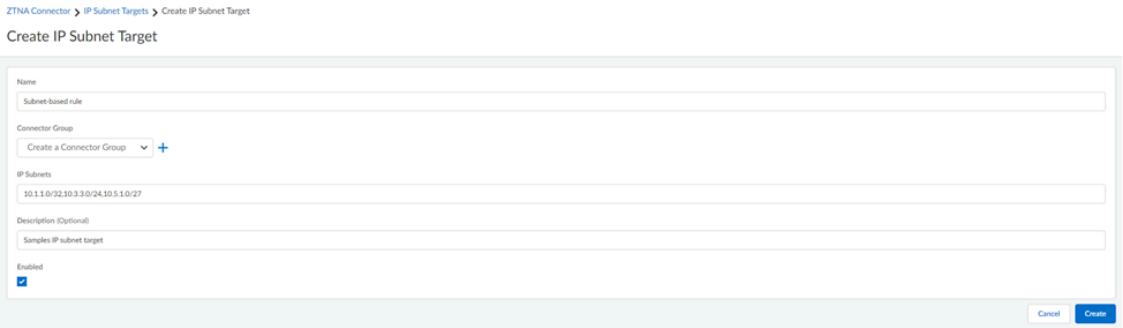
     该组的类型必须为 **IP Subnet**（**IP** 子网）。
  4. 指定该组中的连接器提供 IP 路由访问的数据中心 **IP Subnets**（**IP** 子网）。

     该组中的所有连接器都提供对指定 IP 子网的路由访问。您可以选择单个 IP 地址（格式为 10.1.1.1/32）、单个子网，或用逗号分隔的多个子网。最多输入 16 个子网。

     IP 子网必须可在租户的 IP 架构内路由，并且该 IP 子网不能与租户中的任何其他 IP 子网重叠，包括：

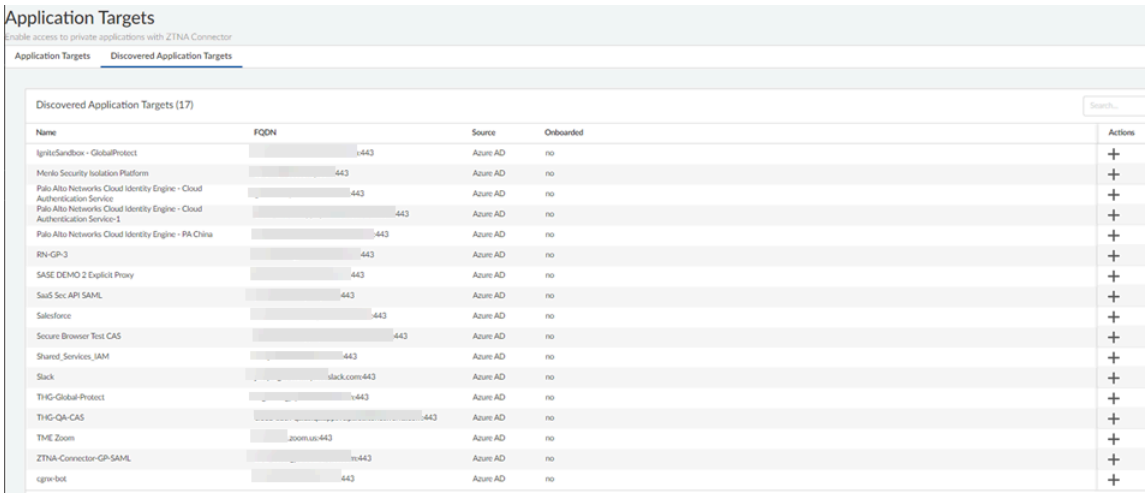
     - 其他 IP 可路由子网，包括用户在 Panorama 上配置的静态路由、从分支机构通告到远程网络的路由或从数据中心通告到服务连接的路由。
     - ZTNA FQDN 应用程序 IP 子网
     - ZTNA 连接器 IP 子网
     - 基础架构子网 IP 地址
     - 移动用户—GlobalProtect IP 地址池
  5. 选择 **Activated**（已激活）并 **Create**（创建）目标。

 ©2025 Palo Alto Networks, Inc.



STEP 8 | 将 ZTNA 连接器自动发现的应用程序添加到该连接器组。

1. 使用 Cloud Identity Engine 设置应用程序的自动发现
2. 选择 **Workflows**（工作流） > **ZTNA Connector**（**ZTNA** 连接器） > **Application Targets**（应用程序目标） > **Discovered Application Targets**（已发现的应用程序目标）。



3. 单击 **Actions**（操作） 下的 +，将应用程序添加到连接器组。
4. 为应用程序指定唯一的 **Name**（名称）。
5. 选择要与该应用程序关联的 **ZTNA Connector Group**（**ZTNA** 连接器组）。
6. 输入 **Probing Type**（探测类型）（**tcp ping**、**icmp ping**或 **none**（无））。
   - 如果选择 **tcp ping**，则还需要选择一个 **probing port**（探测端口）。该端口不一定要在您在 **port**（端口）和 **protocol**（协议）区域中输入的端口范围内。如果选择 **tcp ping**

 ©2025 Palo Alto Networks, Inc.

作为探测类型，Palo Alto Networks 建议您使用同一端口作为 **probing port**（探测端口）。

ZTNA 连接器通过从探测端口到 FQDN 解析的 IP 地址执行 tcp ping 来确定应用程序的可达性。如果 ping 成功，则应用程序被视为 **Up**（正常运行）。

- 您还可以编辑在应用程序加入期间添加的探测端口。探测端口更新后，ZTNA 连接器会在更新的端口上启动 tcp 探测应用程序，应用程序状态也会相应更新。
- 如果选择 **icmp ping**，ZTNA 连接器将对 FQDN 执行 ICMP ping。如果收到对 ICMP ping 的响应，ZTNA 连接器会将该应用程序的状态设置为 **Up**（正常运行）。
- 如果选择 **none**（无），则不执行探测且应用程序始终标记为 **Up**（正常运行）。

7. 选择 **Enabled**（启用）。
8. **Create**（创建）应用程序目标。

STEP 9 | 创建安全策略规则以允许用户访问连接器中的应用程序。

STEP 10 | （可选）查看和监视 ZTNA 连接器，以了解 ZTNA 连接器和连接器组的运行情况。

STEP 11 | （可选）如果您在使用 ZTNA 连接器访问私有应用程序时遇到问题，请使用 ping、traceroute 和 nslookup 诊断工具检查应用程序的可达性。

升级 ZTNA 连接器

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ ZTNA 连接器附加许可证 带附加许可证的基础许可证包括 8 个 ZTNA 连接器、100 个 FQDN 和 4 个 IP 子网功能。 带附加许可证的高级许可证包括 40 个 ZTNA 连接器、300 个 FQDN 和 1024 个 IP 子网功能。 带附加许可证的高级许可证包括 200 个 ZTNA 连接器、4000 个 FQDN 和 1024 个 IP 子网功能。 ❑ 如果您不购买 ZTNA 连接器附加许可证，Prisma Access 许可证将包括四个连接器、40 个 FQDN 和四个 IP 子网。此功能旨在让您在自己的环境中尝试 ZTNA 连接器。

为了使 ZTNA 连接器保持最新状态，您可以更新其软件版本。您可能还需要升级连接器以支持新特性或功能。

©2025 Palo Alto Networks, Inc.

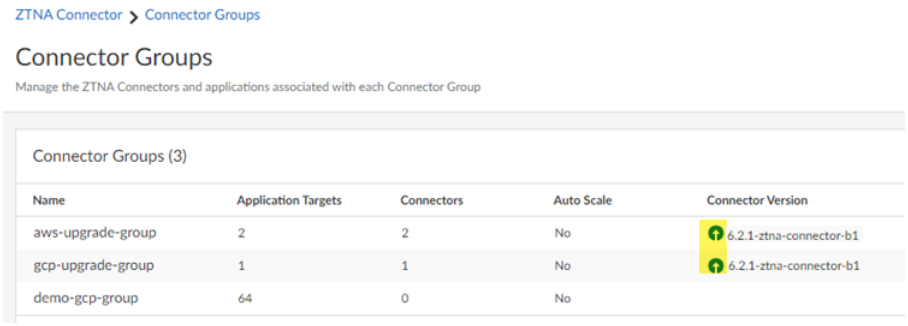
当发布新的 ZTNA 连接器版本时，将检查部署中的连接器，如果发布的版本比现有版本新，或者组中的所有连接器不在同一版本，则连接器组区域中的图标会显示有可用更新。如果您选择更新连接器，则可以选择一起升级整个组。升级一个组会自动并行升级该组中的所有连接器。您无法升级单个连接器。

ZTNA 连接器大约需要 *8* 到 *10* 分钟进行升级，并且在此过程中连接器会重新启动。*Palo Alto Networks* 建议您在停机时间或计划的网络中断期间安排连接器升级。

STEP 1 | 转到 **ZTNA Connector**（**ZTNA** 连接器） > **Connector Groups**（连接器组）。绿色箭头表示可以升级。

您只能升级到租户可用的最新映像版本。

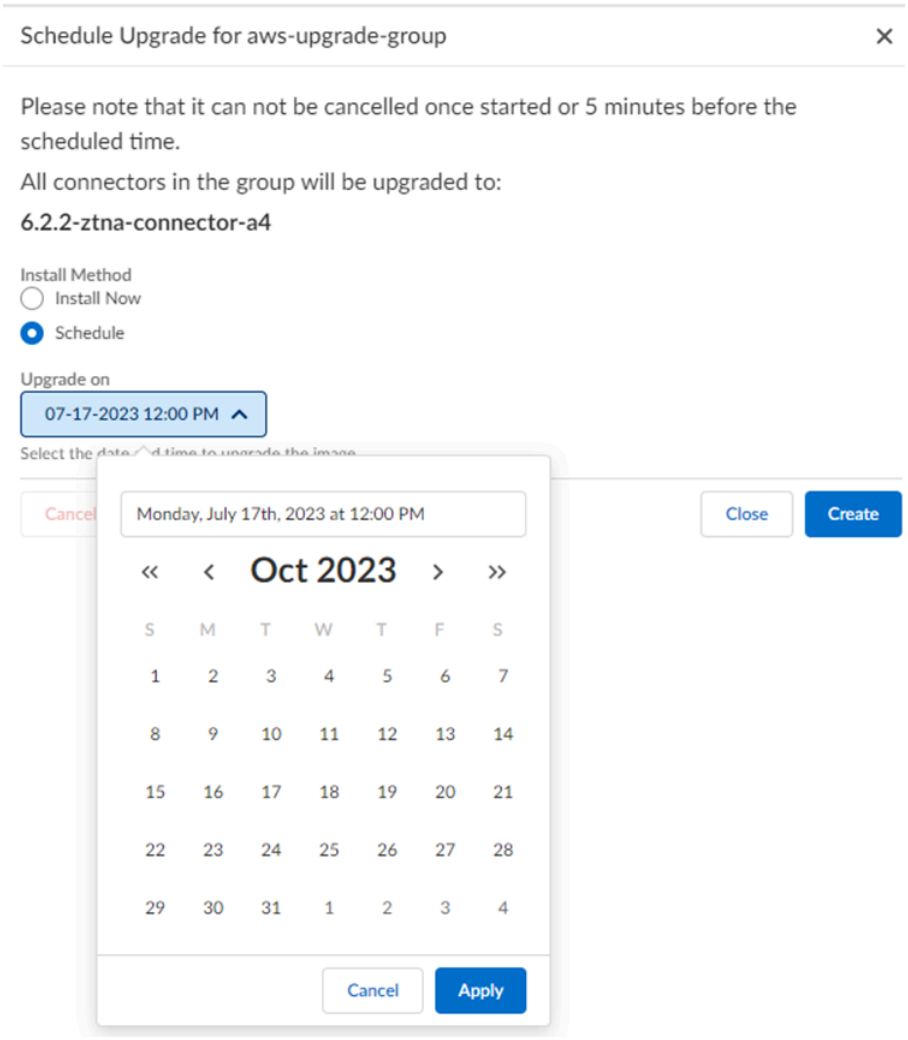
STEP 2 | 单击连接器组旁边的绿色箭头。



 ©2025 Palo Alto Networks, Inc.

STEP 3 | 选择 **Install Now**（立即安装）以立即升级连接器组，或选择 **Schedule**（计划）并提供升级的时间和日期。显示的时间是使用 ZTNA UI 的管理员的当地时区。

您可以在升级开始前五分钟 **Cancel Scheduled Upgrade**（取消预定的升级）。



STEP 4 | 通过查看 **Connector Version**（连接器版本）下的图标可检查连接器的状态。

图标	说明
	可以升级。
	升级已安排好。
	升级已开始且正在进行中。

©2025 Palo Alto Networks, Inc.

图标	说明
无图标（仅显示连接器版本） 6.1.1-ztna-connector-a8	升级成功。
	并非所有连接器都得到了升级。
	升级失败。

ZTNA 连接器诊断工具

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ ZTNA 连接器附加许可证 带附加许可证的基础许可证包括 8 个 ZTNA 连接器、100 个 FQDN 和 4 个 IP 子网功能。 带附加许可证的高级许可证包括 40 个 ZTNA 连接器、300 个 FQDN 和 1024 个 IP 子网功能。 带附加许可证的高级许可证包括 200 个 ZTNA 连接器、4000 个 FQDN 和 1024 个 IP 子网功能。 ❑ 如果您不购买 ZTNA 连接器附加许可证，Prisma Access 许可证将包括四个连接器、40 个 FQDN 和四个 IP 子网。此功能旨在让您在自己的环境中尝试 ZTNA 连接器。

如果您在使用 ZTNA 连接器访问私人应用程序时遇到问题，您可以使用以下网络工具从 ZTNA 连接器 UI 运行测试来帮助您找到问题：

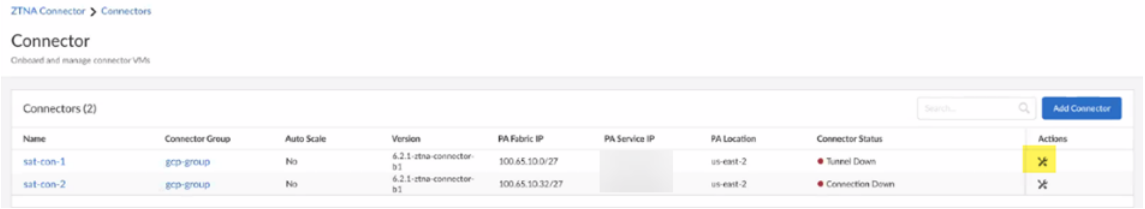
- ping
- TCP Ping
- 路由追踪
- nslookup
- 转储概述
- 您还可以 进行数据包捕获 以帮助确定 ZTNA Connector 任何问题的原因。

©2025 Palo Alto Networks, Inc.

在使用 *ping* 和 *traceroute* 工具之前，请确保您的网络允许 *ICMP*。一些云环境出于安全考虑不允许 *ICMP*，并且这些工具不会显示任何活动。

STEP 1 | 转到 工作流 > **ZTNA** 连接器 > 连接器。

STEP 2 | 为连接器选择 操作 > 诊断 。



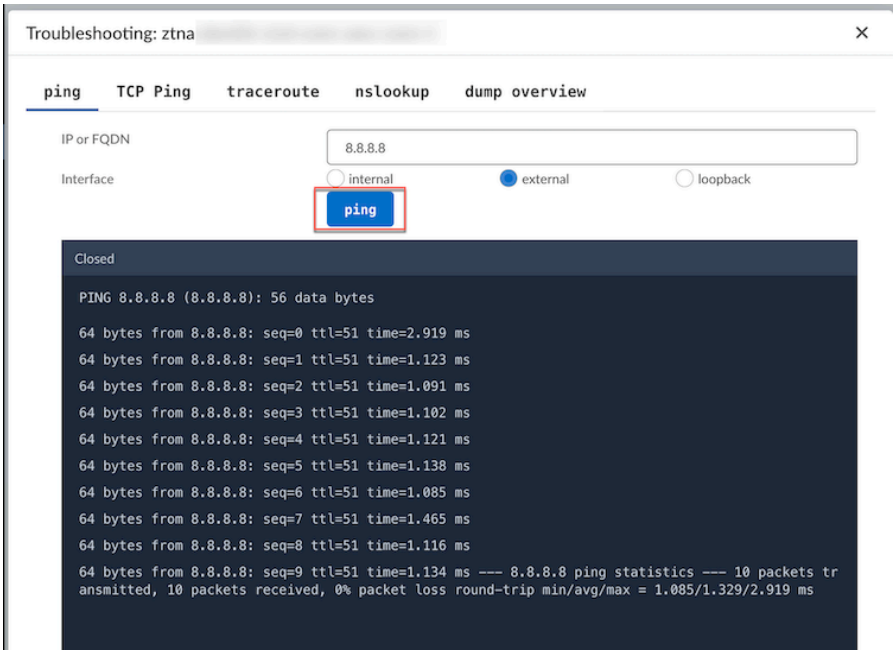
 ©2025 Palo Alto Networks, Inc.

STEP 3 | 运行 ping、TCP Ping、traceroute 或 nslookup 诊断工具。

- **ping**：
  1. 选择您尝试访问的应用程序的 **IP** 或 **FQDN**。
  2. 选择要测试 ping 的 接口 。

     如果您已为 虚拟机配置 了双臂部署，请选择 内部 检查虚拟机的 LAN 端（端口 2），并选择 外部 检查 WAN 端（端口 1）。

     对于单臂部署，请选择 内部 或 外部，因为 WAN 和 LAN 端都映射到端口 1。
  3. 选择 **ping**。

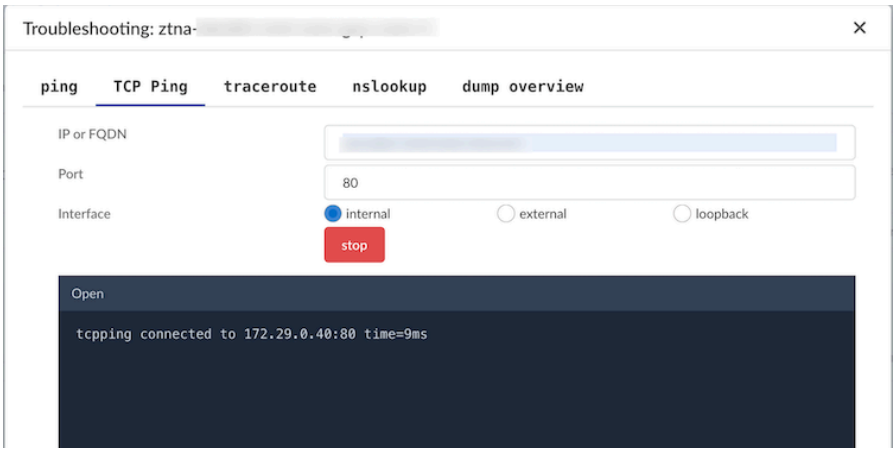
     显示 ping 输出。
  4. 要完成测试， 请停止。
- **TCP Ping**：

  将连接器升级到 *ZTNA* 连接器 *6.2.5-b1* 版本。如果连接器未更新至此版本，则 *Strata Cloud Manager UI* 不会提供 ***TCP Ping*** 作为诊断工具。

  1. 选择您尝试访问的应用程序的 **IP** 或 **FQDN**。
  2. 选择要测试 ping 的 接口 。

     如果您已为 虚拟机配置 了双臂部署，请选择 内部 检查虚拟机的 LAN 端（端口 2），并选择 外部 检查 WAN 端（端口 1）。
  3. 选择 **TCP Ping**。

 ©2025 Palo Alto Networks, Inc.

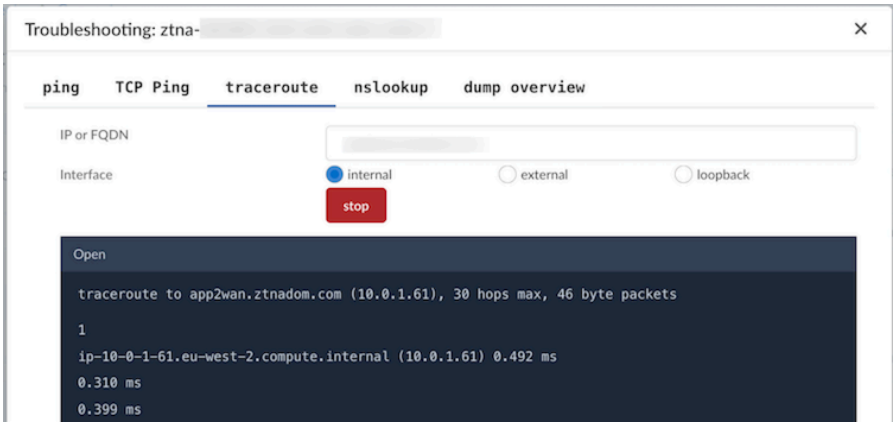


4. 要完成测试，请停止。

- 跟踪路由：

1. 选择您尝试访问的应用程序的 **IP** 或 **FQDN**。
2. 选择要测试 ping 的 接口 。

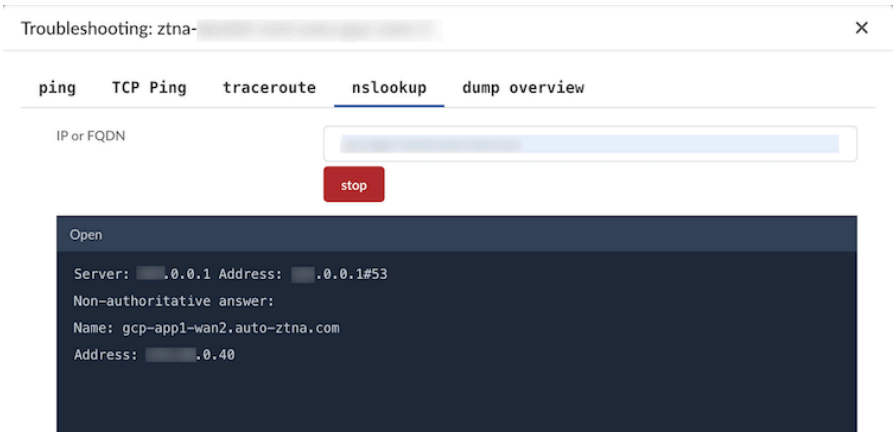
   如果您已为 虚拟机配置 了双臂部署，请选择 内部 检查虚拟机的 LAN 端（端口 2），并选择 外部 检查 WAN 端（端口 1）。
3. 选择 跟踪路由。
4. 要完成测试，请停止。



- **nslookup**：

1. 选择您尝试访问的应用程序的 **IP** 或 **FQDN**。
2. 选择 **nslookup**。
3. 要完成测试，请停止。

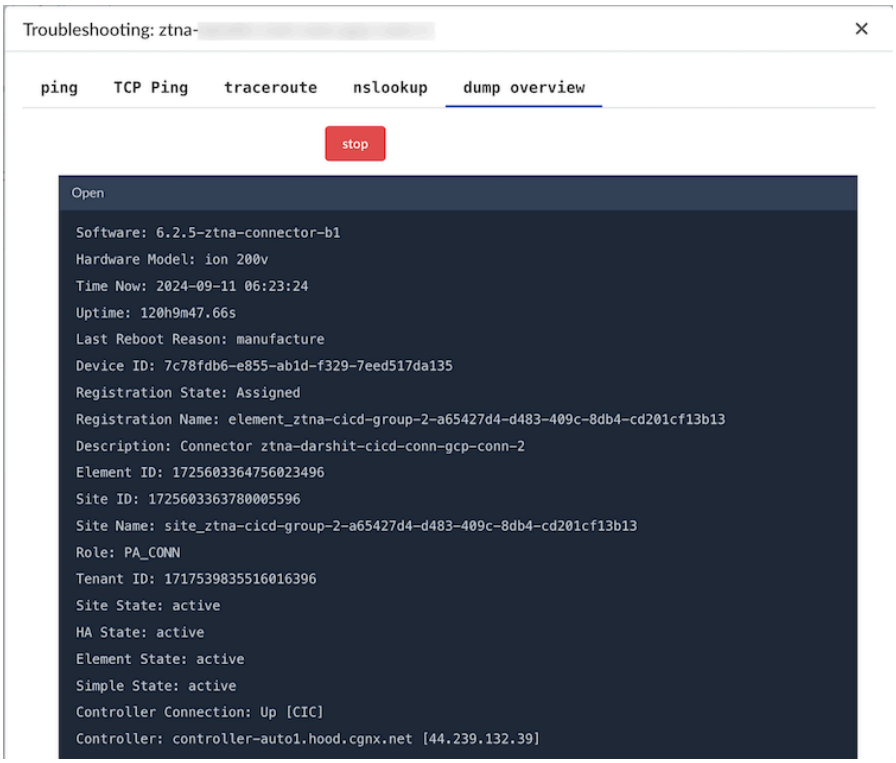
 ©2025 Palo Alto Networks, Inc.



- **dump overview**（转储改述）：

  1. 单击 “开始”下载系统转储，单击“停止”停止 。

     转储概览提供了 PANW 故障排除所需的软件版本、接口和连接状态以及连接器识别信息。



执行数据包捕获

如果您需要进行数据包捕获以进行网络级故障排除，则可以进行数据包捕获以从特定连接器捕获网络数据。您还可以根据特定的 IP 地址或协议（例如 TCP）捕获数据包。

在以下用例中，捕获数据包很有用：

- 如果你的隧道没有建成。捕获连接器和 ZTT 之间的 IKE 协商将有助于确定问题。在这种情况下，选择 互联网 接口并使用服务连接的 IP 地址作为源或目标接口。

 ©2025 Palo Alto Networks, Inc.

- 如果您的应用程序出现故障，您可以通过使用服务器 IP 地址和端口以及数据中心接口上的端口获取 tcpdump 来检查应用程序的探测。
- 如果端到端数据平面不工作，但隧道是应用程序并且应用程序已启动。在这种用例中，获取发往应用程序结构 IP 地址的 IPSec 隧道上的用户流量的 tcpdump 将会很有帮助。

STEP 1 | 转到 工作流 > **ZTNA** 连接器 > 连接器。

STEP 2 | 选择您想要排除故障的连接器的 数据包捕获 （放大镜）。



STEP 3 | 选择 接口 , 其中 的 数据 包 将 被 捕获 (内部, 外部或 隧道).

STEP 4 | （可选）指定捕获数据包的 源或目标 **IPv4** 地址。

如果指定此选项，则只捕获来自该 IP 地址的数据包。

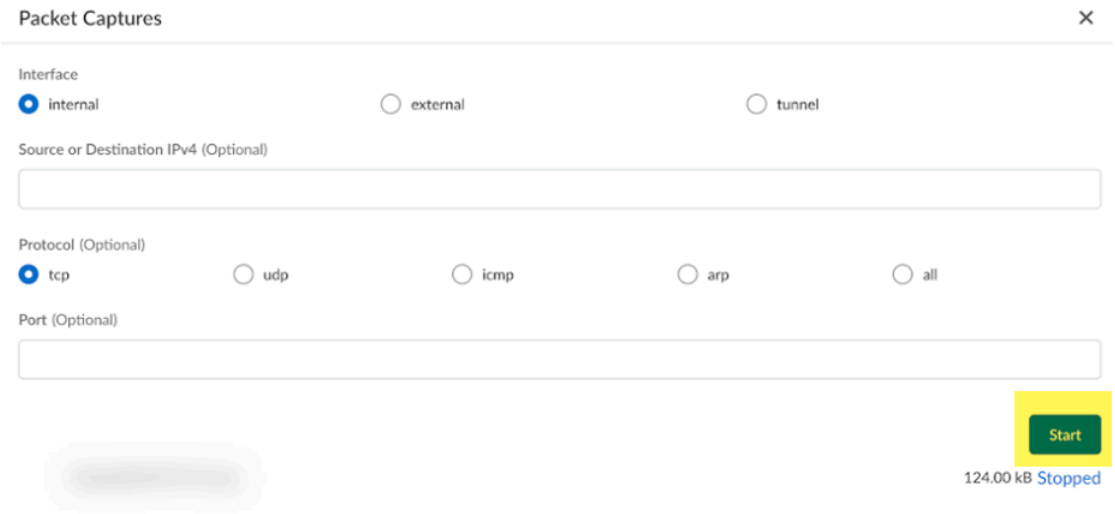
STEP 5 | （可选）选择要捕获的数据包类型。

您可以选择要捕获的特定协议的数据包（**tcp**、**udp**、**icmp**或 **arp**），或选择 全部 以捕获所有数据包。

STEP 6 | （可选）选择要捕获数据包的 端口 。

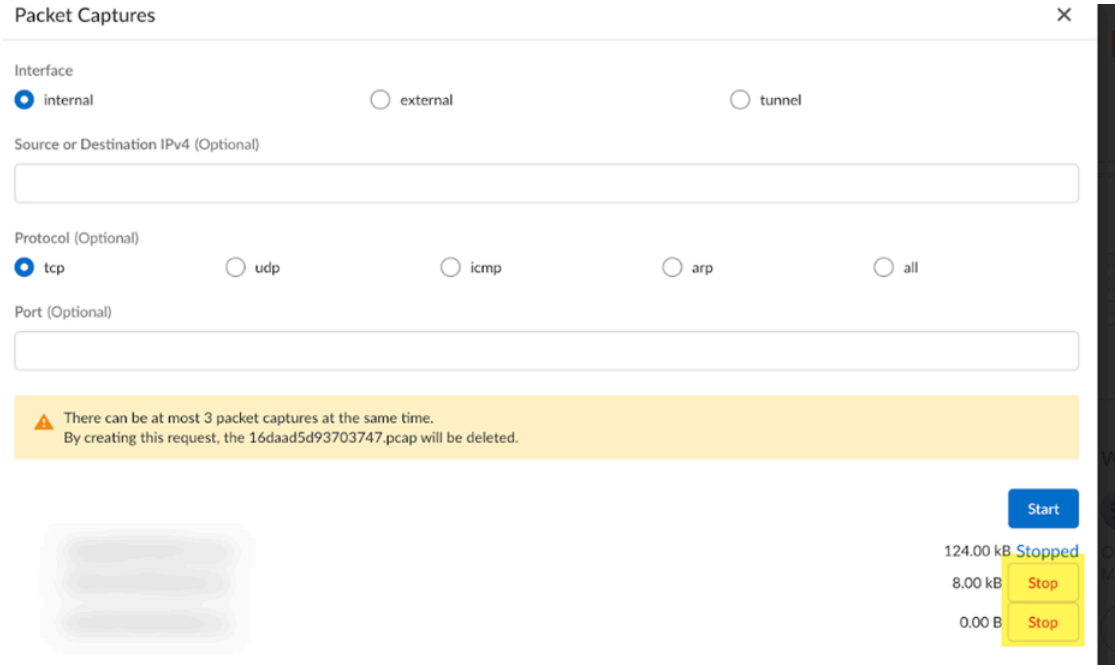
如果指定此选项，则只捕获来自该端口的数据包。

STEP 7 | 开始 数据包捕获。



 ©2025 Palo Alto Networks, Inc.

STEP 8 | 要停止数据包捕获，请单击 停止。



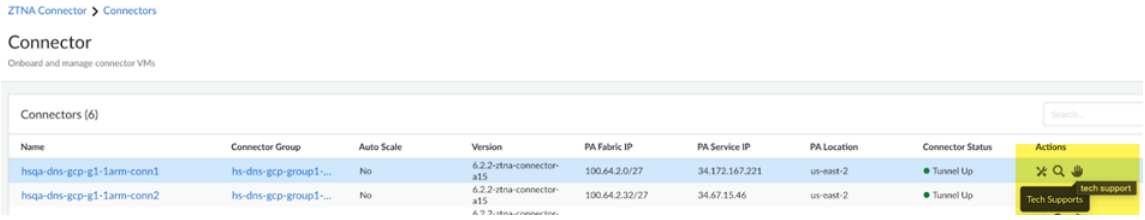
- 数据包捕获的最大文件大小为 5 MB。如果在达到最大大小之前您没有停止捕获，则文件将被覆盖。
- 一个连接器最多允许同时进行三次数据包捕获。如果启动了第四个会话，则第一个正在运行的会话将终止。

收集技术支持文件

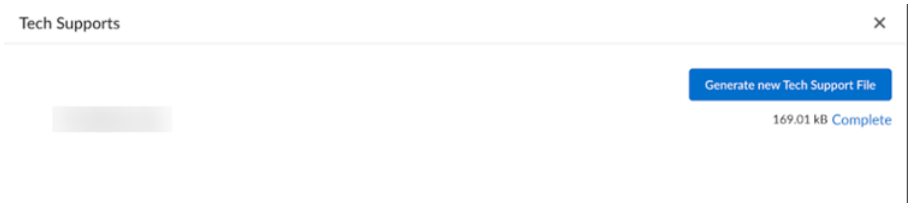
技术支持文件包含您的设备配置、系统信息和一些日志（非流量）。Palo Alto Networks 可以请求您上传技术支持文件，以帮助解决 ZTNA Connector 的问题。

STEP 1 | 转到 工作流 > **ZTNA** 连接器 > 连接器。

STEP 2 | 针对您要排除故障的连接器选择 技术支持 （手）。



STEP 3 | **Generate new Tech Support File**（生成新的技术支持文件）。



STEP 4 | 选择“完成”将技术支持文件下载到本地。

©2025 Palo Alto Networks, Inc.

删除连接器 IP 块

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ ZTNA 连接器附加许可证 带附加许可证的基础许可证包括 8 个 ZTNA 连接器、100 个 FQDN 和 4 个 IP 子网功能。 带附加许可证的高级许可证包括 40 个 ZTNA 连接器、300 个 FQDN 和 1024 个 IP 子网功能。 带附加许可证的高级许可证包括 200 个 ZTNA 连接器、4000 个 FQDN 和 1024 个 IP 子网功能。 ❑ 如果您不购买 ZTNA 连接器附加许可证，Prisma Access 许可证将包括四个连接器、40 个 FQDN 和四个 IP 子网。此功能旨在让您在自己的环境中尝试 ZTNA 连接器。

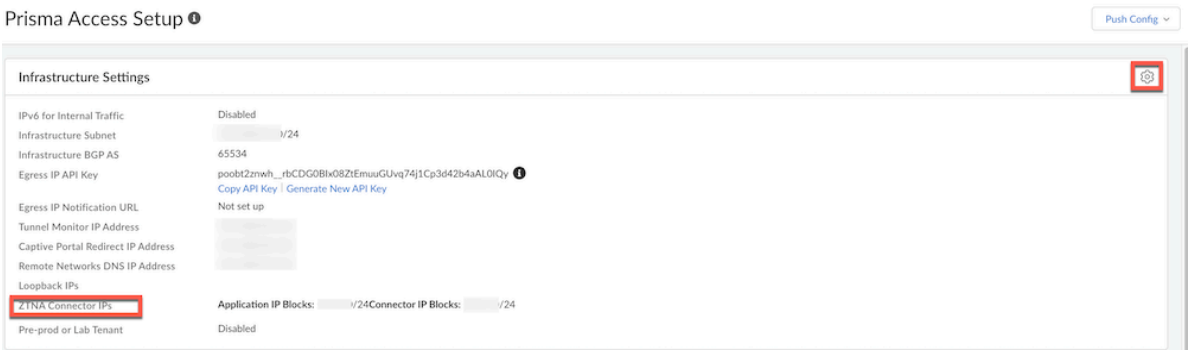
您可以启用 ZTNA 连接器并添加所需的连接器 IP 块，Prisma Access 将在内部使用这些 IP 块在移动用户、远程网络和数据中心中的连接器虚拟机之间路由流量。以前，在创建连接器 IP 块后便无法对其进行任何更改。但现在您可以删除或更新连接器 **IP** 块。按照上述步骤删除或更新块。

- Panorama
- Strata Cloud Manager

删除连接器 IP 块（云托管）

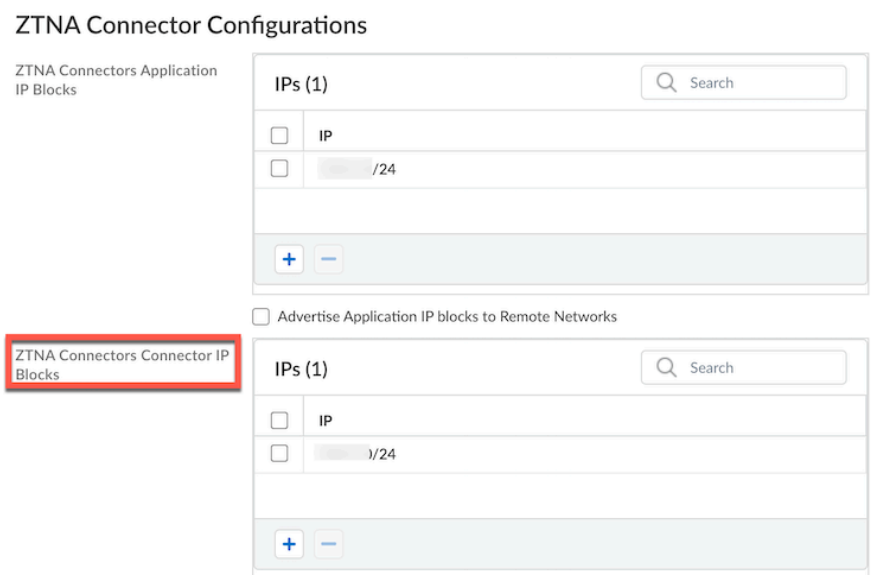
完成以下步骤以删除连接器 IP 块。

STEP 1 | 转到 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Prisma Access** > **Infrastructure Settings**（基础设施设置），然后单击齿轮符号以编辑 **Settings**（设置）。



 ©2025 Palo Alto Networks, Inc.

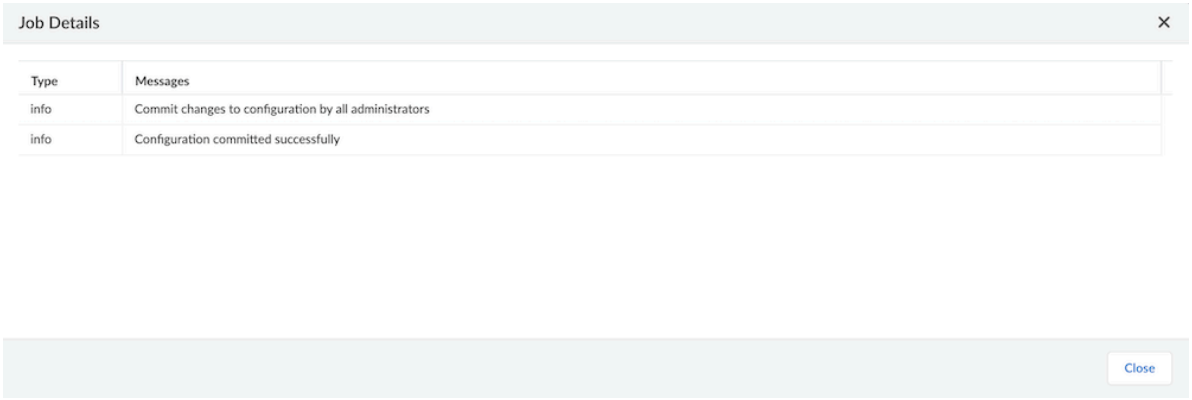
STEP 2 | 从 **ZTNA Connector Configurations**（**ZTNA** 连接器配置） > **ZTNA Connectors Connector IP Blocks**（**ZTNA** 连接器连接器 **IP** 块）中，选中要删除的连接器块旁边的复选框，然后单击 **Save**（保存）。



 ©2025 Palo Alto Networks, Inc.

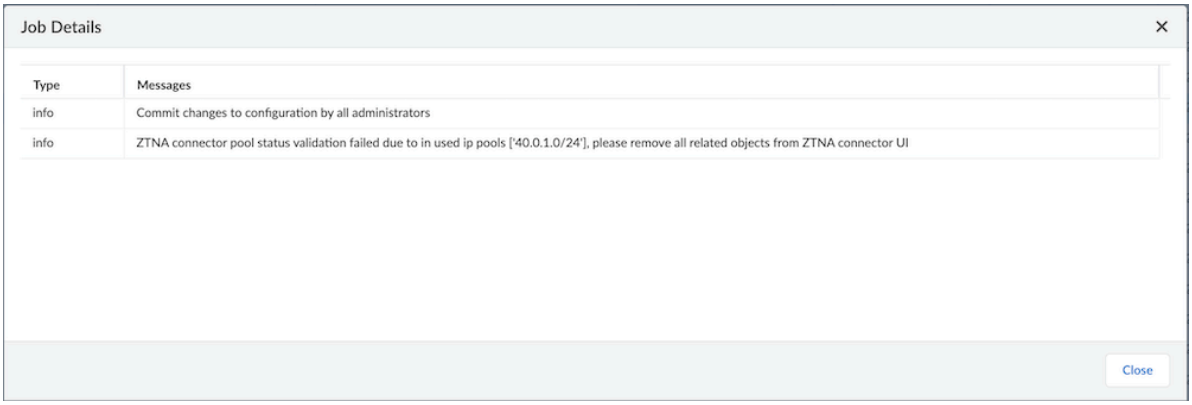
STEP 3 | 单击 **Commit**（提交）以提交并推送配置更改。

提交通过后会显示一条消息。



如果您创建了任何 ZTNA 连接器对象（如连接器、应用程序、通配符和连接器组），并且在没有首先删除 ZTNA 连接器对象的情况下尝试删除连接器 **IP** 块，则提交和推送将失败。

在这种情况下，请删除 ZTNA 连接器对象，删除所需的 连接器 **IP** 块，然后再进行提交。第一次提交失败，但第二次提交会成功。

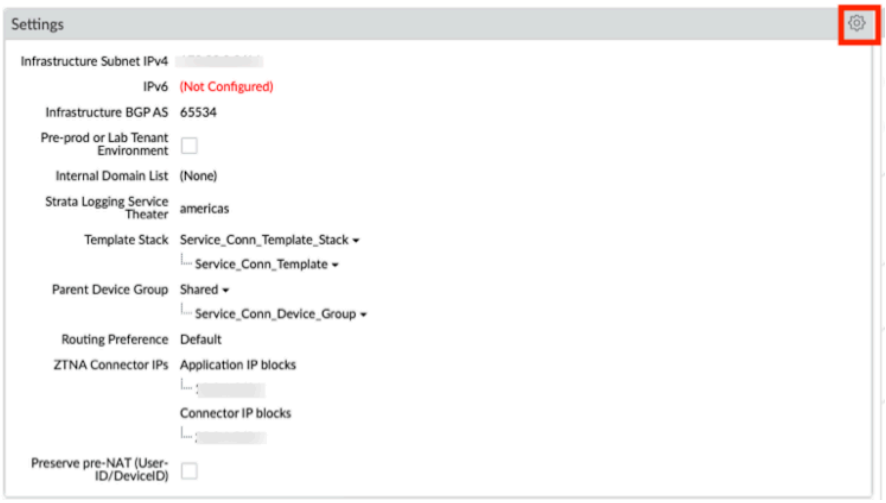


删除连接器 IP 块 (Panorama)

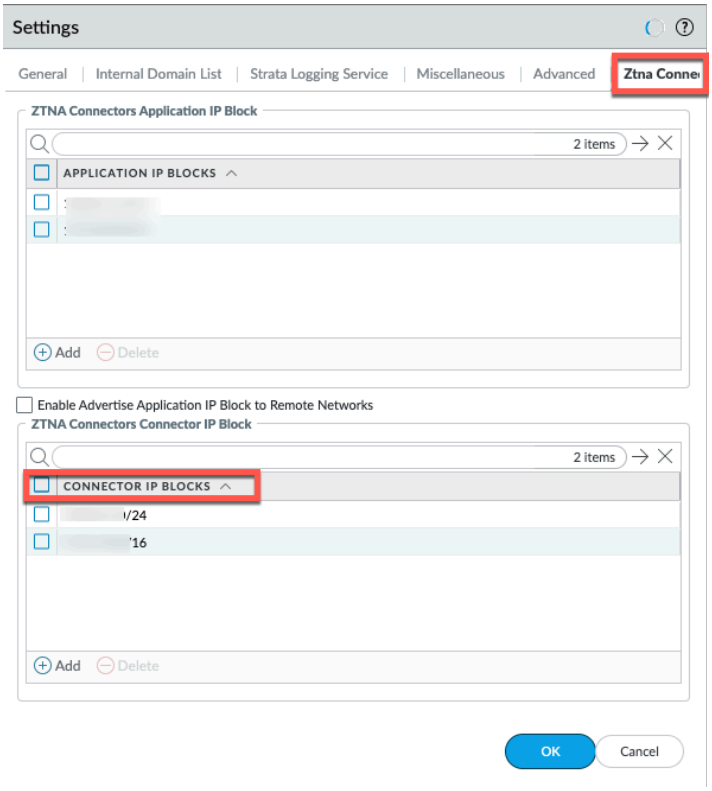
完成以下步骤来删除连接器 IP 块。

©2025 Palo Alto Networks, Inc.

STEP 1 | 转到 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Service Setup**（服务设置），然后单击齿轮来编辑 **Settings**（设置）。



STEP 2 | 选择 **Ztna Connector**（**ZTNA** 连接器）。

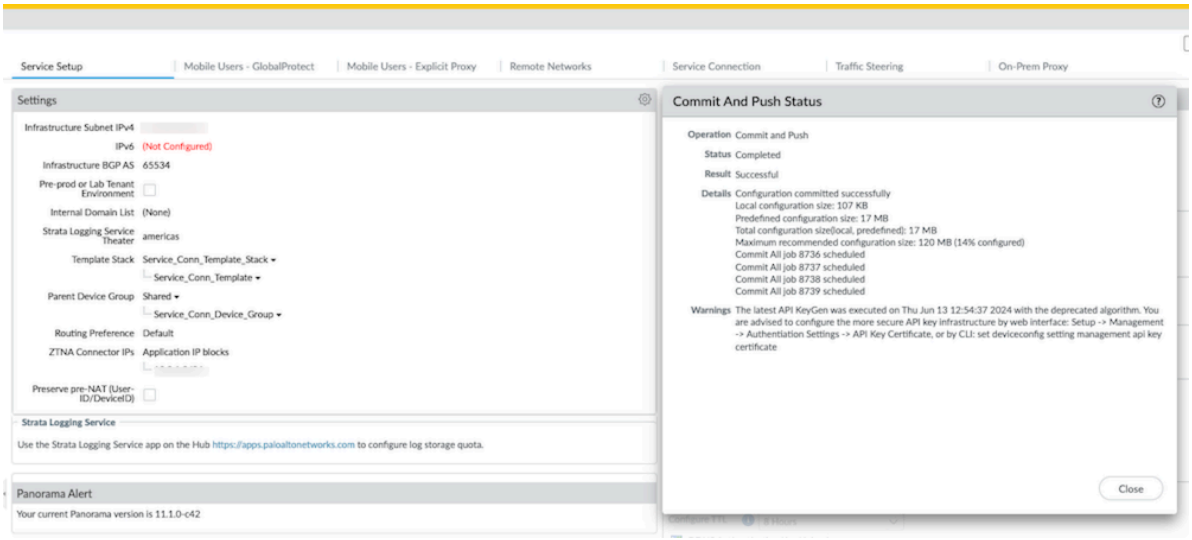


STEP 3 | 选中要删除的连接器块旁边的复选框，然后单击 **OK**（确定）以保存配置。

©2025 Palo Alto Networks, Inc.

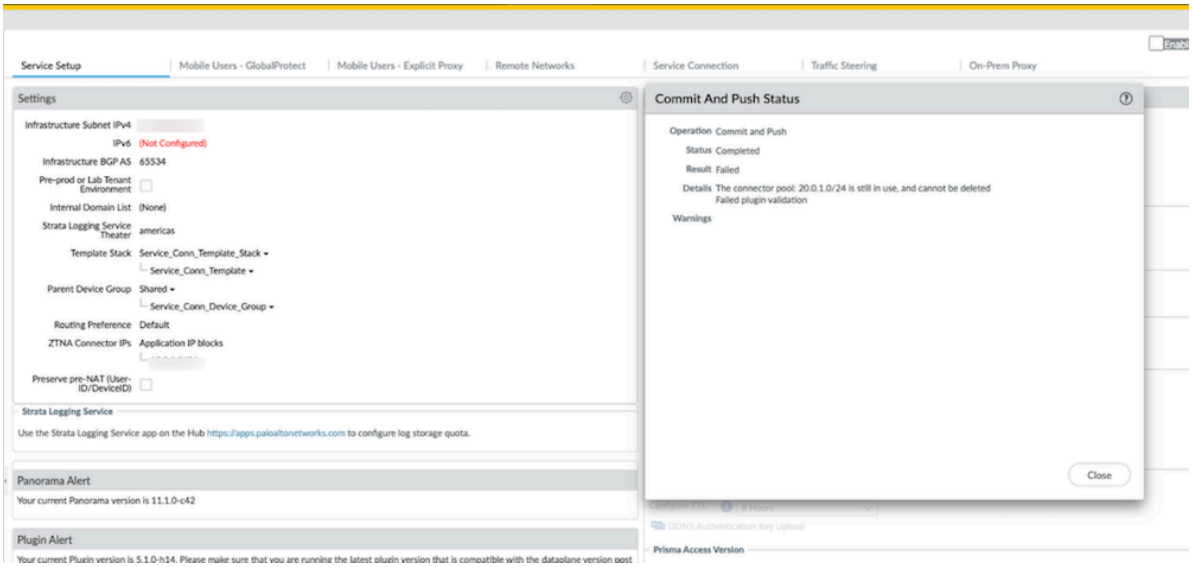
STEP 4 | 选择 **Commit**（提交），然后推送配置更改。

提交成功后会显示一条消息。



如果您创建了任何 ZTNA 连接器对象（如连接器、应用程序、通配符和连接器组），并且在没有首先删除 ZTNA 连接器对象的情况下尝试删除连接器 **IP** 块，则提交和推送将失败。

在这种情况下，请删除 ZTNA 连接器对象，删除所需的 连接器 **IP** 块，然后再进行提交并推送两次。第一次提交失败，但第二次提交会成功。



 ©2025 Palo Alto Networks, Inc.

使用 Cloud Identity Engine 设置应用程序的自动发现

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ ZTNA 连接器附加许可证 带附加许可证的基础许可证包括 8 个 ZTNA 连接器、100 个 FQDN 和 4 个 IP 子网功能。 带附加许可证的高级许可证包括 40 个 ZTNA 连接器、300 个 FQDN 和 1024 个 IP 子网功能。 带附加许可证的高级许可证包括 200 个 ZTNA 连接器、4000 个 FQDN 和 1024 个 IP 子网功能。 ❑ 如果您不购买 ZTNA 连接器附加许可证，Prisma Access 许可证将包括四个连接器、40 个 FQDN 和四个 IP 子网。此功能旨在让您在自己的环境中尝试 ZTNA 连接器。

为了使 ZTNA 连接器能够自动发现在 Azure Active Directory 或 Okta 目录中定义的应用程序，您必须配置以下几项：

- ❑ 在中心激活 Cloud Identity Engine 并创建第一个租户。

  在 Azure 或 Okta 中配置基于云的目录时，您必须选择 **Collect enterprise applications**（收集企业应用程序）。
- ❑ 选择您希望 Cloud Identity Engine 访问的目录类别。
- ❑ 配置基于云的目录，例如 Azure Active 目录 (Azure AD) 或 Okta 目录，以便与 Cloud Identity Engine 通信。

以下 IdP 支持与应用程序发现一起使用：

- Azure AD
- Okta

 ©2025 Palo Alto Networks, Inc.

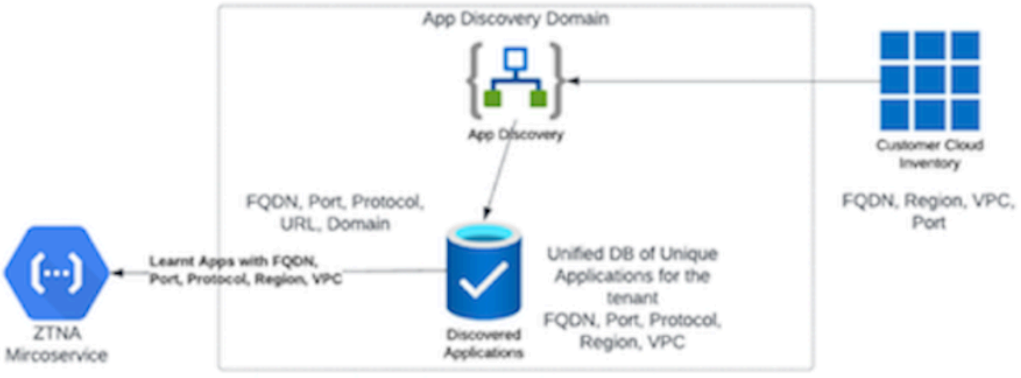
私有应用程序目标发现

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ ZTNA 连接器附加许可证 带附加许可证的基础许可证包括 8 个 ZTNA 连接器、100 个 FQDN 和 4 个 IP 子网功能。 带附加许可证的高级许可证包括 40 个 ZTNA 连接器、300 个 FQDN 和 1024 个 IP 子网功能。 带附加许可证的高级许可证包括 200 个 ZTNA 连接器、4000 个 FQDN 和 1024 个 IP 子网功能。 ❑ 如果您不购买 ZTNA 连接器附加许可证，Prisma Access 许可证将包括四个连接器、40 个 FQDN 和四个 IP 子网。此功能旨在让您在自己的环境中尝试 ZTNA 连接器。

在现代网络基础设施中，成千上万的私有应用程序部署在本地和多云数据中心中。网络团队不知道在其网络中或网络的特定子网内运行的应用程序，这导致缺乏对应用程序的可见性。

为了提供对应用程序的安全访问，您必须手动输入 FQDN、端口、应用程序，并且要注意此应用程序对其他应用程序的依赖性。

私有应用程序目标发现提供了一种发现云环境中托管的应用程序的方法，并允许这些应用程序接入 ZTNA 连接器解决方案。私有应用程序目标发现还连接到云提供商网络，进行发现操作并将发现的目标存储在数据库中。还将为不同的服务提供 API，以获取发现的应用程序。如果用户只有服务连接而没有 ZTNA 连接器，则只会发现应用程序目标。



私有应用程序目标发现可确定以下几个方面：

©2025 Palo Alto Networks, Inc.

- FQDN
- 应用程序的端口
- 应用程序的协议

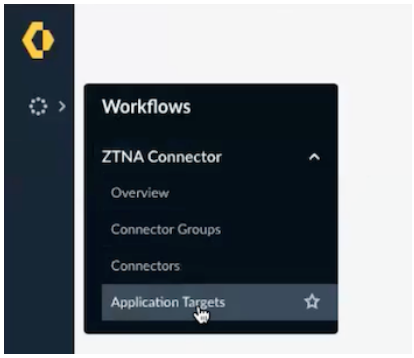
在启用私有应用程序发现功能之前，请务必激活云身份引擎 *(CIE)*。

完成以下步骤以在 AWS 中添加云帐户、IAM 角色并发现目标应用程序。

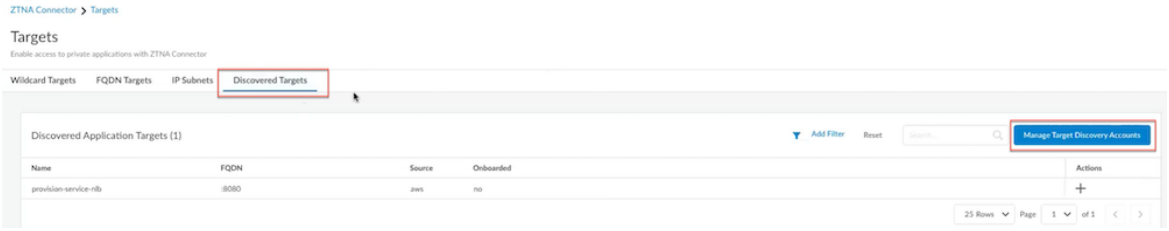
©2025 Palo Alto Networks, Inc.

STEP 1 | 获取 CloudFormation 模板 (CFT) 以添加云帐户。

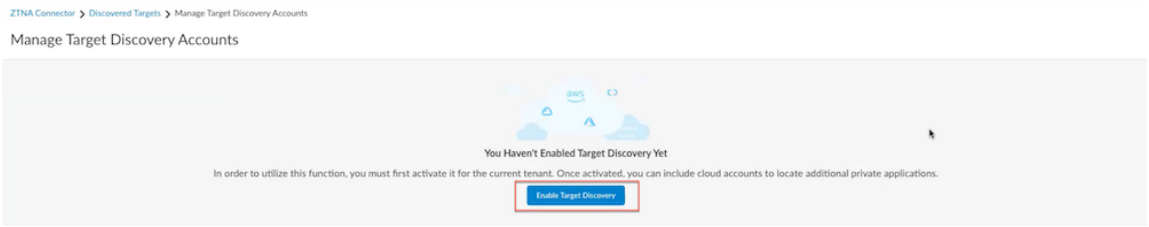
1. 导航到 **Application Targets**（应用程序目标）（**Workflows**（工作流） > **ZTNA Connector**（**ZTNA** 连接器） > **Application Targets**（应用程序目标））。



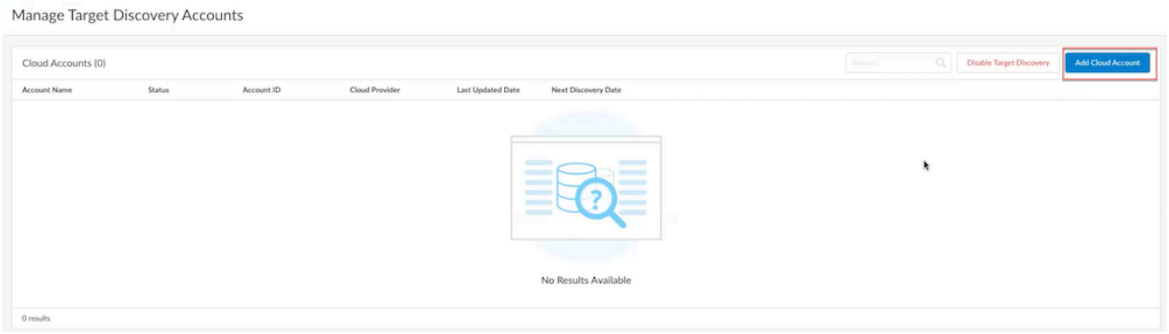
2. 在 **Application Targets**（应用程序目标）页面上，选择 **Discovered Targets**（已发现的目标），然后选择 **Manage Target Discovery Accounts**（管理目标发现帐户）。



3. 选择 **Enable Target Discovery**（启用目标发现），然后选择 **Enable**（启用）。

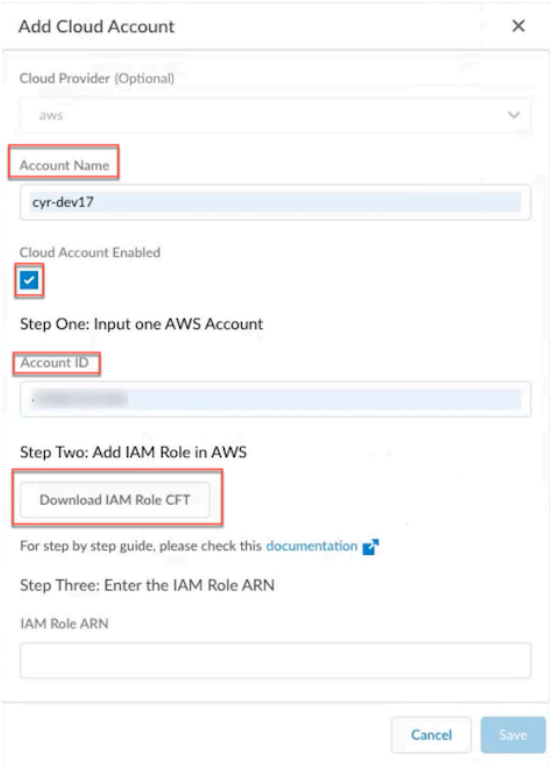


4. 在 **Manage Target Discovery Accounts**（管理目标探索帐户）页面上，选择 **Add Cloud Account**（添加云帐户）。



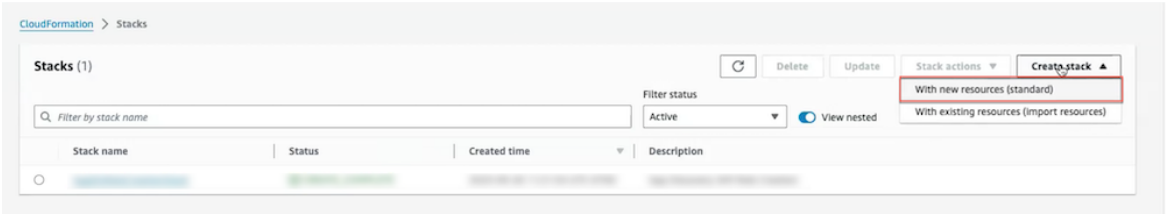
5. 单击 **Account Name**（帐户名称）以添加帐户名称，然后单击 **Cloud Account Enabled**（启用云帐户）下的复选框。添加 AWS 帐户 **ID**，然后单击 **Download IAM Role CFT**（下载 **IAM** 角色 **CFT**）以下载文件。

 ©2025 Palo Alto Networks, Inc.



STEP 2 | 在 AWS 中创建 IAM 角色。

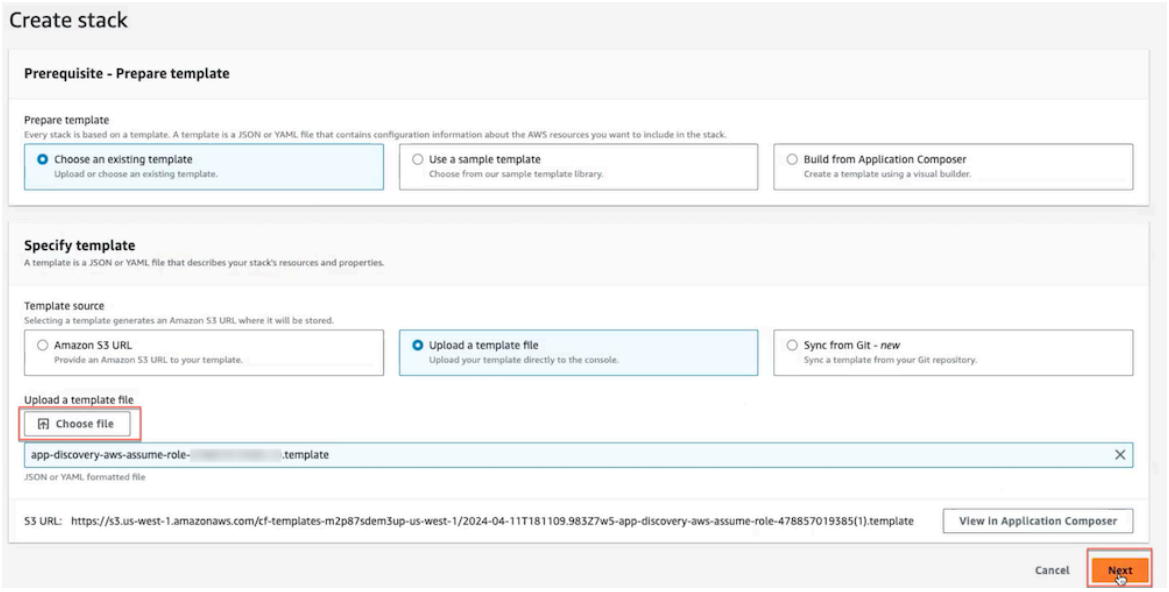
1. 导航到 AWS 应用程序，选择您的帐户，然后选择 **Sign in**（登录）。
2. 导航到 **CloudFormation** > **Stacks**（堆栈） > **Create stack**（创建堆栈） > **With new resources (standard)**（使用新资源（标准））以创建堆栈。



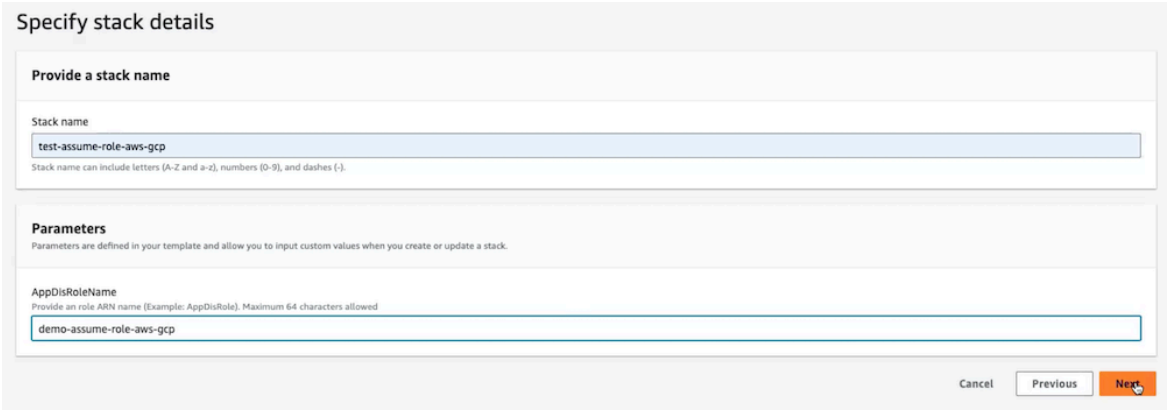
3. 在 **Create stack**（创建堆栈）页面的 **Prerequisite-Prepare template**（**Prerequisite-Prepare** 模板）下面，选择 **Choose an existing template**（选取现有模板）。在 **Specify**

 ©2025 Palo Alto Networks, Inc.

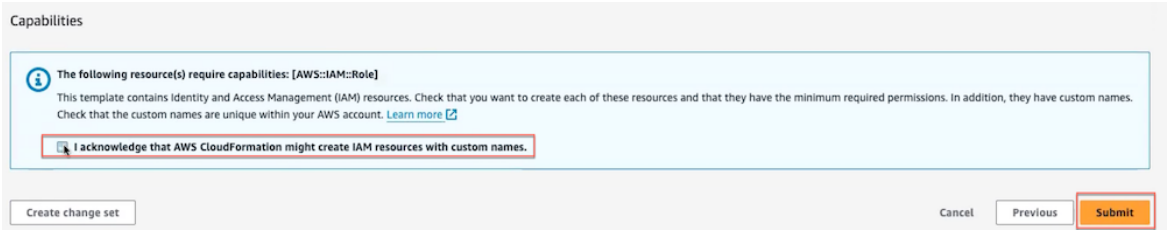
template（指定模板）下，选择 **Upload a template**（上传模板文件）。上传在步骤 1 中下载的文件，然后选择 **Next**（下一步）。



4. 单击 **Stack name**（堆栈名称）以添加堆栈名称 **AppDisRoleName**，然后选择 **Next**（下一步）。

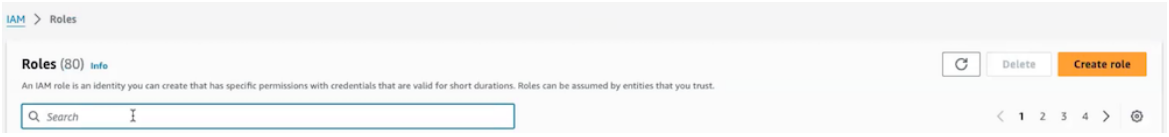


5. 在 **Configure stack options**（配置堆栈选项）页面上，不要进行任何更新，然后选择 **Next**（下一步）。
6. 检查更改。选中 **Capabilities**（能力）下的复选框以确认使用自定义名称创建 IAM 资源，然后选择 **Submit**（提交）。

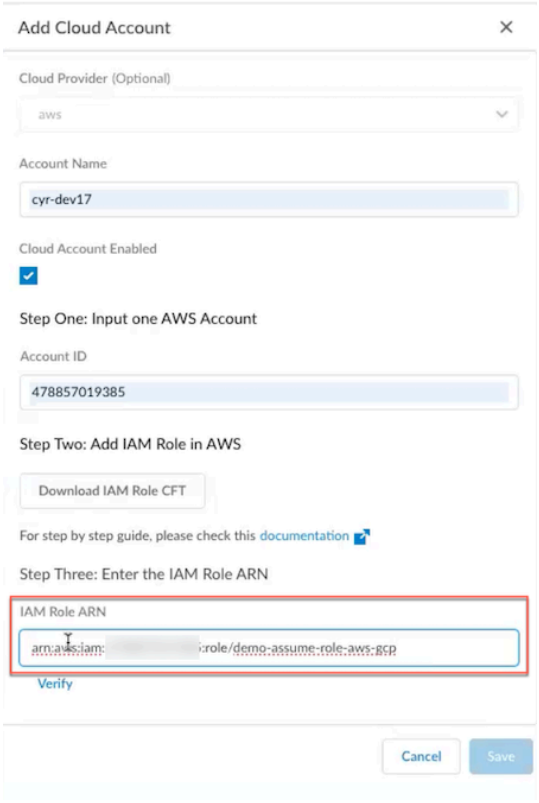


7. 导航到 **IAM > Roles**（角色）并搜索您定义的角色名称。选择角色名称并复制该角色的 **ARN**。

 ©2025 Palo Alto Networks, Inc.



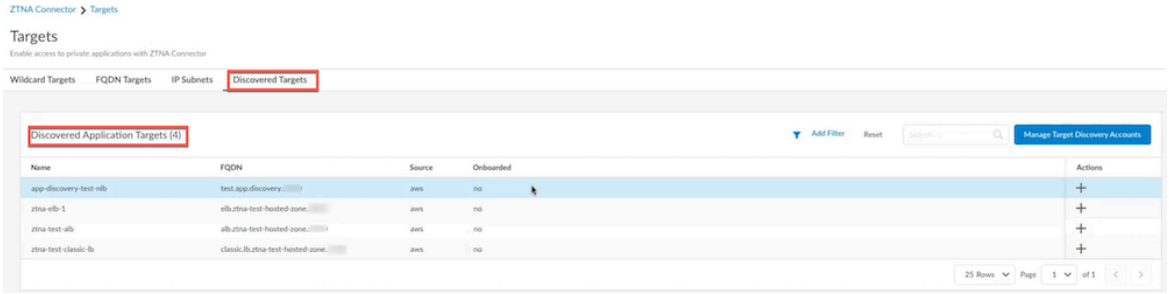
STEP 3 | 将 ARN 粘贴到 **IAM Role ARN**（**IAM** 角色 **ARN**）字段中，然后选择 **Verify**（验证）。验证 ARN 后，选择 **Save**（保存）。



如果在 ***IAM Role ARN***（***IAM*** 角色 ***ARN***）文本字段中添加了错误的 *ARN*，则验证将失败并显示错误消息。

添加帐户后，您可以查看状态、帐户 ID 和其他详细信息。发现的刷新周期为 24 小时。您也可以向同一个租户添加多个帐户。

STEP 4 | 要识别已发现的应用程序，请选择 **Discovered Targets**（已发现的目标）。您可以在 **Discovered Application Targets**（已发现的应用程序目标）下找到已识别应用程序的列表。

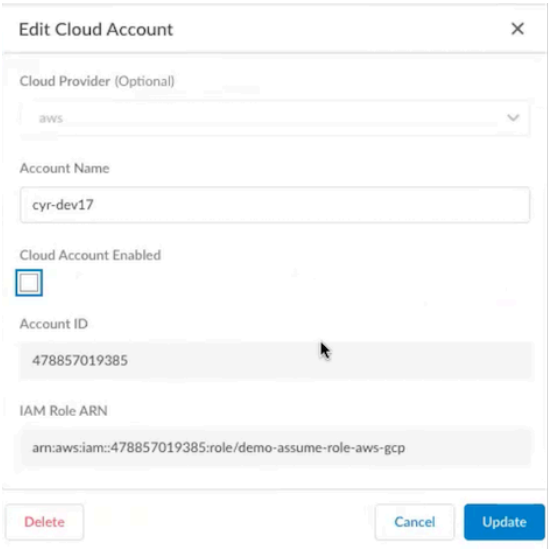


 ©2025 Palo Alto Networks, Inc.

STEP 5 | （可选）删除云帐户。

要在不禁用目标发现的情况下删除您的云帐户并添加新帐户，请按照以下步骤操作。但如果要禁用目标发现功能，则必须执行这些步骤。

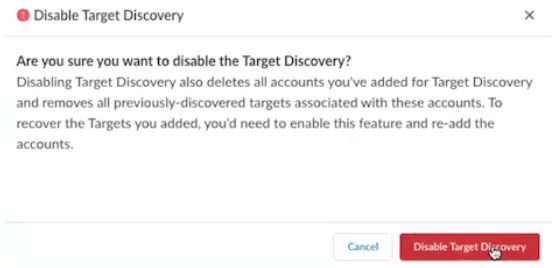
1. 在 **Manage Target Discovery Accounts**（管理目标发现帐户）下，单击 **Account Name**（帐户名称）以选择要删除的帐户名称。
2. 禁用 **Cloud Account Enabled**（启用云帐户），然后选择 **Update**（更新）。更新帐户后，选择 **Delete**（删除）。帐户即已删除。



STEP 6 | （可选）禁用目标发现。

在禁用目标发现之前，请确保删除所有云帐户。

1. 选择 **Disable Target Discovery**（禁用目标发现），然后选择 **Disable Target Discovery**（禁用目标发现）。



 ©2025 Palo Alto Networks, Inc.

启用 ZTNA 连接器的应用程序的安全策略

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ ZTNA 连接器附加许可证 带附加许可证的基础许可证包括 8 个 ZTNA 连接器、100 个 FQDN 和 4 个 IP 子网功能。 带附加许可证的高级许可证包括 40 个 ZTNA 连接器、300 个 FQDN 和 1024 个 IP 子网功能。 带附加许可证的高级许可证包括 200 个 ZTNA 连接器、4000 个 FQDN 和 1024 个 IP 子网功能。 ❑ 如果您不购买 ZTNA 连接器附加许可证，Prisma Access 许可证将包括四个连接器、40 个 FQDN 和四个 IP 子网。此功能旨在让您在自己的环境中尝试 ZTNA 连接器。

ZTNA 连接器不强制执行策略；它会将您现有的 Prisma Access 安全策略无缝扩展到其支持的 Prisma Access 应用程序。这意味着您可以在所有应用程序和数据中心使用通用策略，并且无需为载入到 ZTNA 连接器的应用程序单独编写安全策略。

但是，作为设置 ZTNA 连接器的一部分，您必须确保安全策略：

允许 **Prisma Access** 与 **ZTNA** 连接器之间的流量

为此，请按照ZTNA 连接器要求和指南.确保 ZTNA 连接器可以连接到 Prisma Access。

用户可以访问 **ZTNA** 连接器后的应用程序

为确保您的用户可以访问 ZTNA 连接器应用程序，请按照此处用于管理 Prisma Access 的接口的步骤操作。

- Strata Cloud Manager
- Panorama

启用 ZTNA 连接器的应用程序的安全策略 (Strata Cloud Manager)

将应用程序加入 ZTNA 连接器后，您要设置策略规则来允许和控制这些应用程序的访问。创建和应用策略的过程取决于您的应用程序是通过通配符、IP 子网还是 FQDN 定义的。

 ©2025 Palo Alto Networks, Inc.

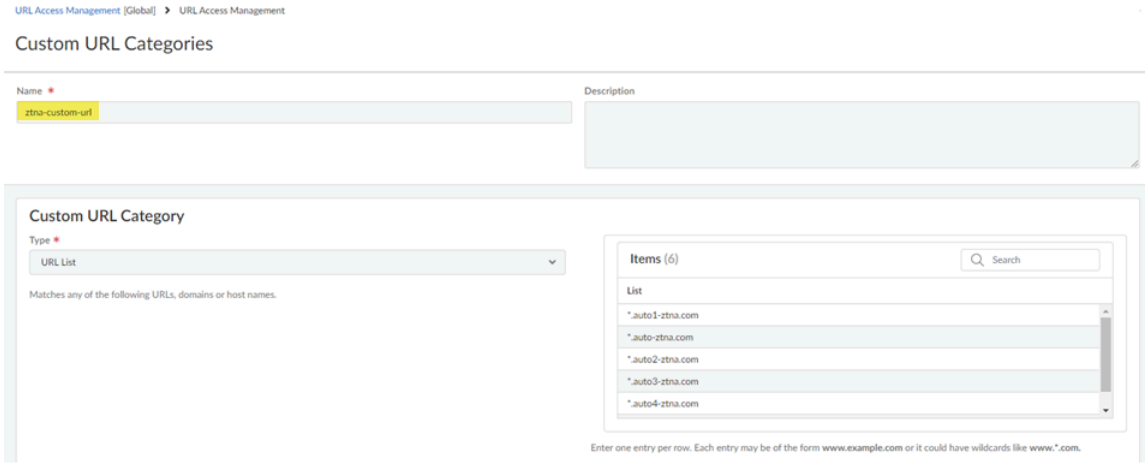
基于通配符的应用程序的安全策略

基于通配符的应用程序（（**Settings**（设置） > **ZTNA Connector**（**ZTNA** 连接器） > **Application Targets**（应用程序目标） > **Wildcard Targets**（通配符目标））要求创建自定义 URL 类别；但是，该类型的类别仅强制执行 HTTP 和 HTTPS 流量的策略，而不允许其他流量（例如 SSH）。因此，您需要通过允许 ZTNA 连接器应用程序 IP 块的流量，以便暂时允许所有应用程序的访问。

在 ZTNA 连接器学习基于通配符的 FQDN 后，您可以禁用允许应用程序 IP 块的流量的策略，并根据学习到的 FQDN 应用策略实施。

STEP 1 | 创建自定义 URL 类别并将通配符 URL 添加到该类别中。

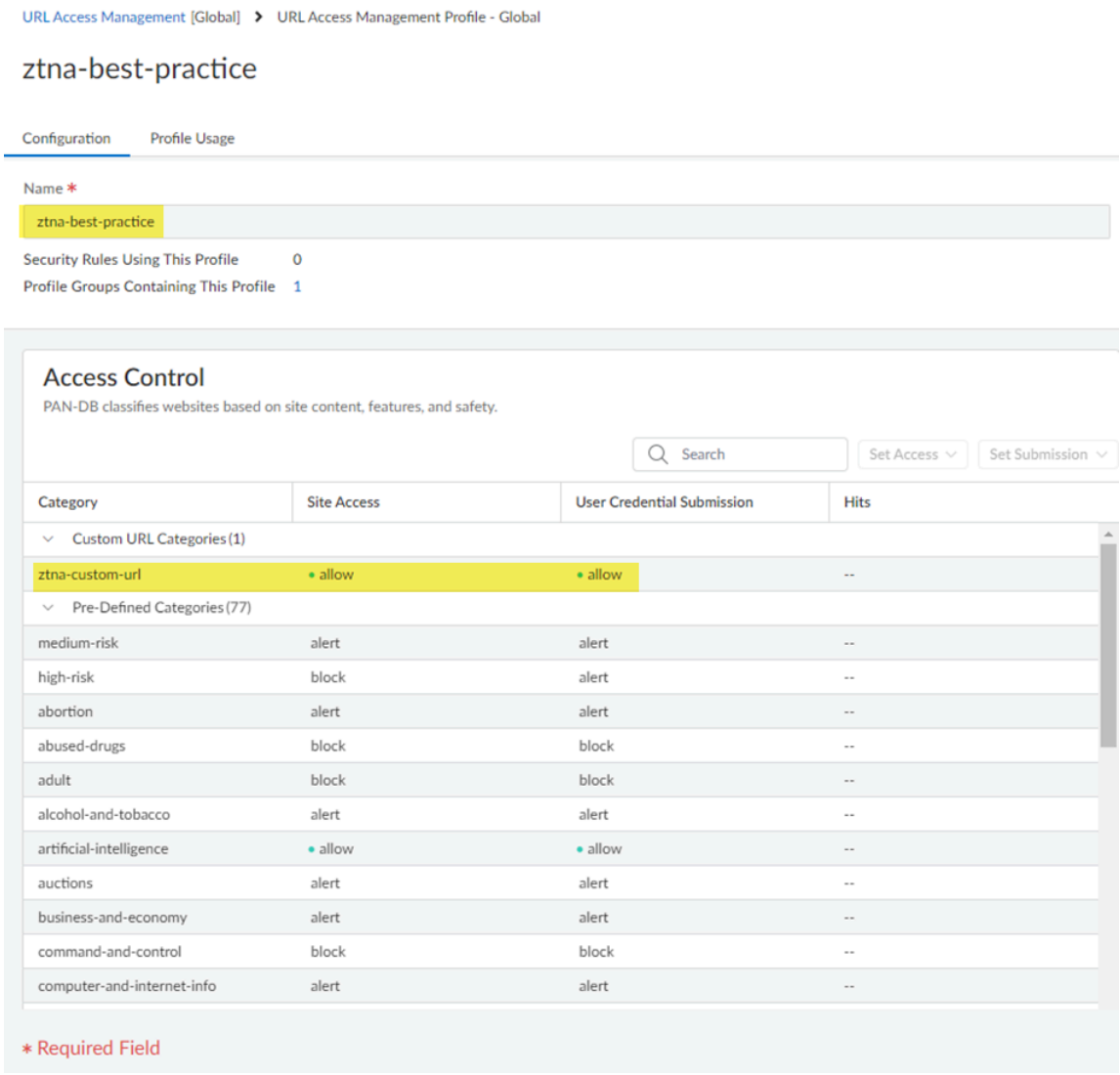
1. 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Security Services**（安全服务） > **URL Access Management**（**URL** 访问管理）。
2. 在“自定义 URL”类别下，选择 **Add Category**（添加类别）。
3. 为自定义 URL 类别提供描述性 **Name**（名称），并选择 **URL List**（**URL** 列表）的 **Type**（类型）。
4. 将您在 ZTNA 连接器中创建的通配符 URL 添加到 **Items**（项目）中。
5. **Save**（保存）更改。



 ©2025 Palo Alto Networks, Inc.

STEP 2 | 创建 URL 访问管理配置文件并将您创建的自定义 URL 类别添加到其中。

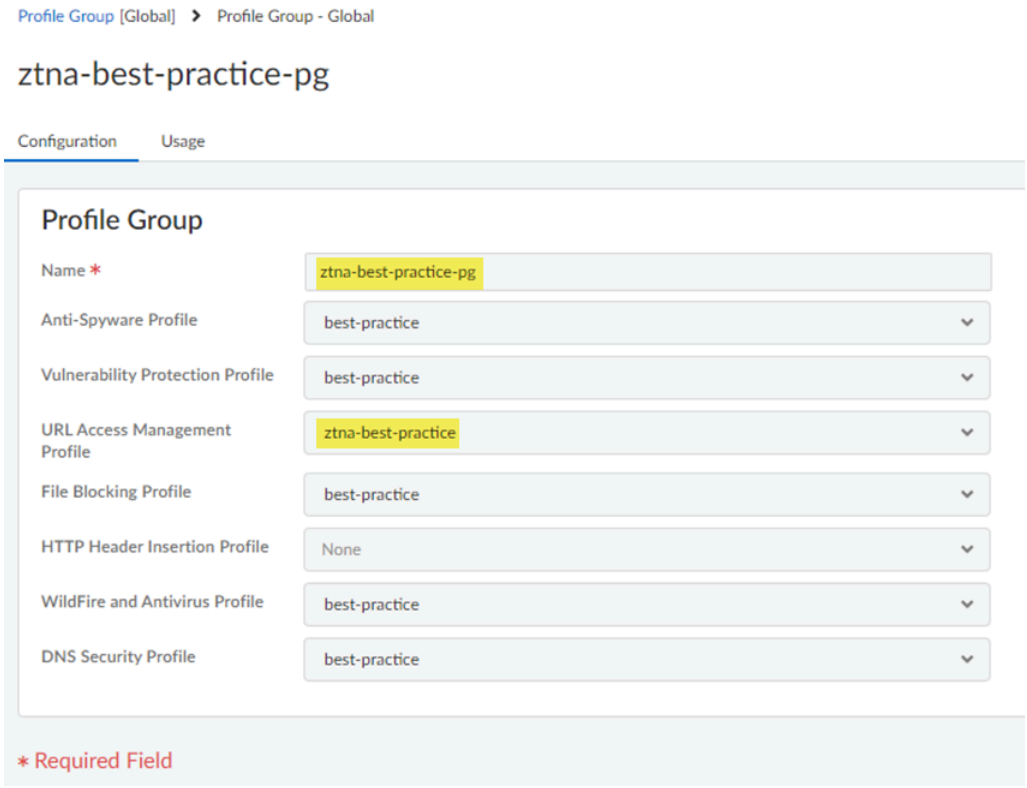
1. 仍在 **URL Access Management**（**URL** 访问管理）区域中，选择 **URL Access Management Profiles**（**URL** 访问管理配置文件）。
2. 选择要修改的现有配置文件，或者单击 **Add Profile**（添加配置文件）。
3. 将您创建的自定义 URL 类别添加到配置文件中。
4. 选择以下参数：
   - **Site Access**（站点访问）：允许
   - **User Credential Submission**（用户凭证提交）：允许
5. **Save**（保存）更改。



 ©2025 Palo Alto Networks, Inc.

STEP 3 | 创建配置文件组并将 URL 访问管理配置文件附加到该组中。

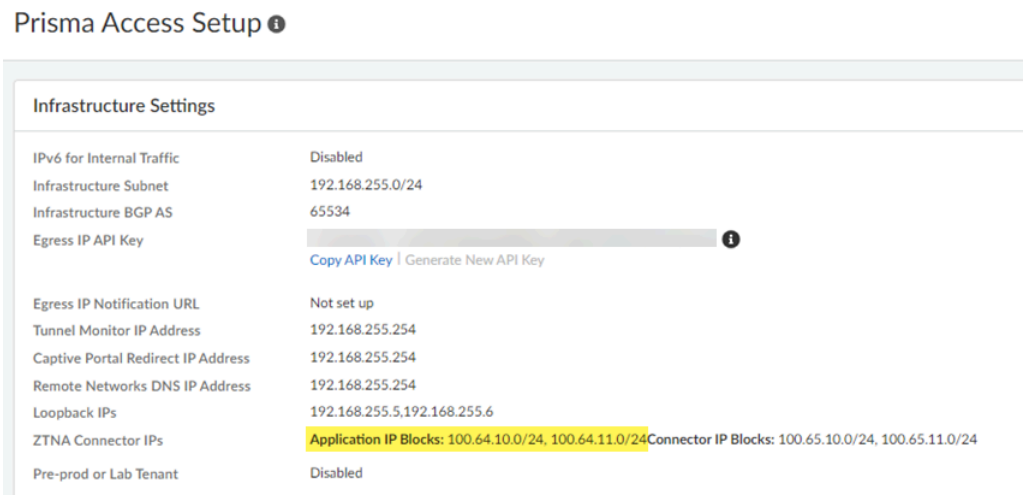
1. 转到 **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Security Services**（安全服务） > **Profile Groups**（配置文件组）。
2. **Add**（添加）配置文件组，指定您创建的 URL 访问管理配置文件。



 ©2025 Palo Alto Networks, Inc.

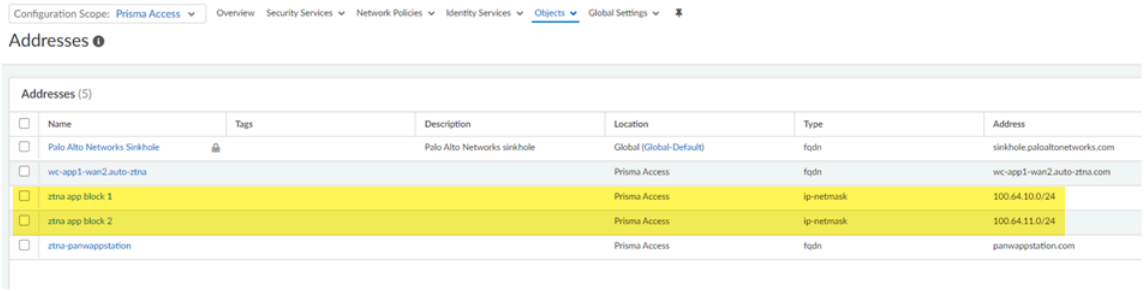
STEP 4 | 创建策略以允许配置文件组和 ZTNA 连接器应用程序 IP 块的 IP 地址。

1. 转到 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Prisma Access** > **Prisma Access Setup**（**Prisma Access** 设置），并确保记录 ZTNA 连接器 IP 下的 **Application IP Blocks**（应用程序 **IP** 块）。

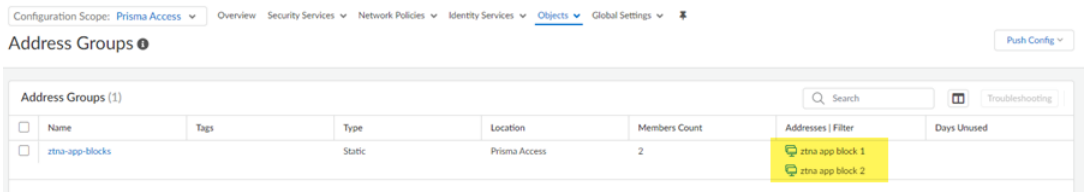


2. 转到 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Objects**（对象） > **Address**（地址） > **Addresses**（地址），并根据检索到的 IP 地址 **Add**（添加）地址对象。

   如果您有基于 IP 子网的应用程序，请同时为这些子网创建地址对象。



3. 转到 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Objects**（对象） > **Address**（地址） > **Address Groups**（地址组），并将创建的地址对象 **Add**（添加）到地址组。



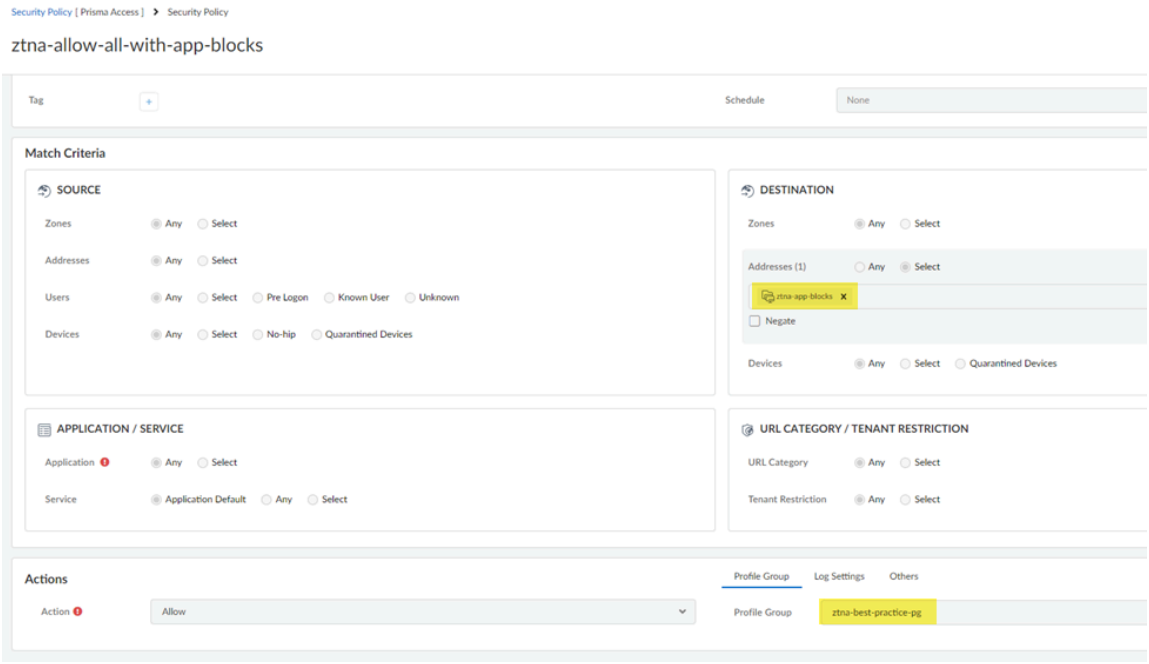
4. 转到 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Security Services**（安全服务） > **Security Policy**（安全策略） > **Pre Rules**（前导规则），并 **Add**（添加）安全策略以允许访问所有应用程序 IP 地址块，

 ©2025 Palo Alto Networks, Inc.

从而指定在之前的步骤中创建的 **Address Group**（地址组）和 **Profile Group**（配置文件组）。

添加此安全策略将允许所有基于通配符的应用程序流量通过，同时 ZTNA 连接器根据通配符发现应用程序。如果没有允许应用程序 IP 块的规则，用户将无法访问基于通配符的应用程序。

您可以保留此策略，直到 ZTNA 连接器发现基于通配符的应用程序。然后，您可以选择禁用此策略，并为每个发现的应用程序添加安全策略规则。



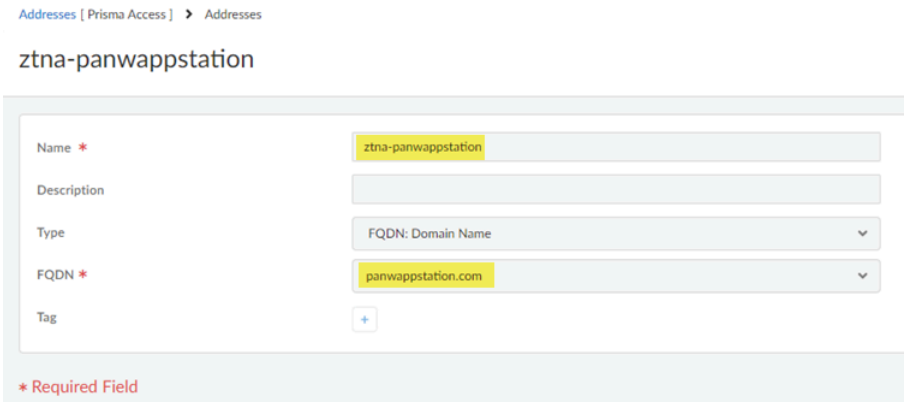
 ©2025 Palo Alto Networks, Inc.

STEP 5 | ZTNA 连接器根据通配符发现应用程序后，为使用 FQDN 添加的应用程序配置安全策略。

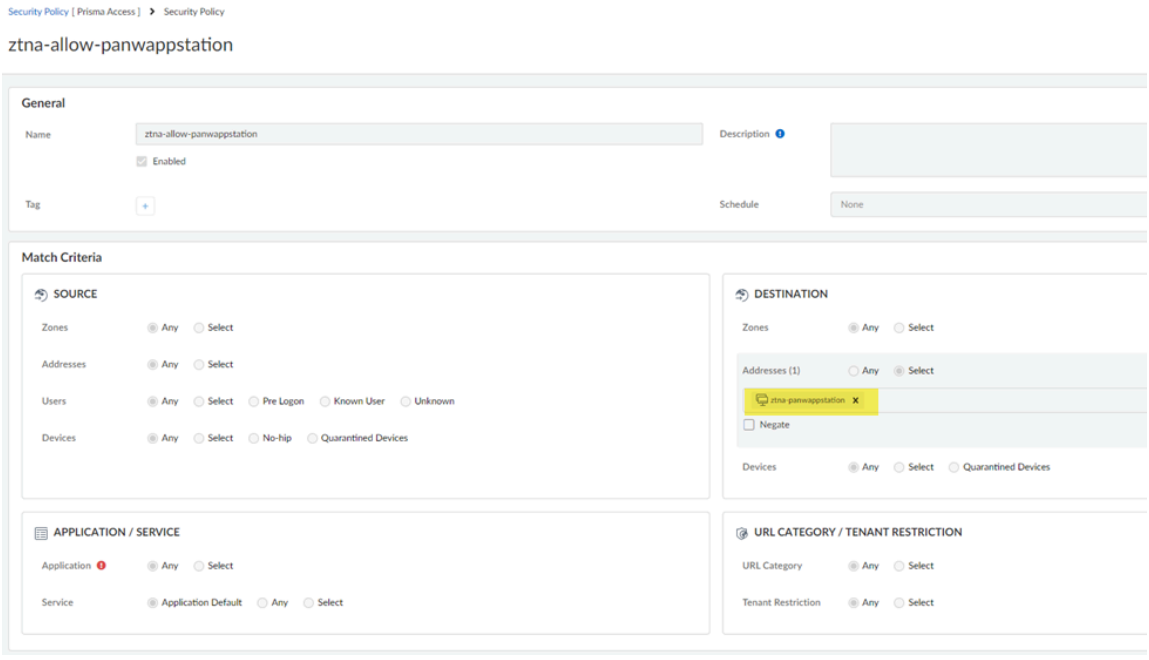
1. 转到 **Workflows**（工作流） > **ZTNA Connector**（**ZTNA** 连接器） > **Application Targets**（应用程序目标） > **FQDN Targets**（**FQDN** 目标），并记录应用程序使用的 FQDN。
2. 为 FQDN 创建一个地址对象（**Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Objects**（对象） > **Address**（地址） > **Addresses**（地址））。

   选择 **Prisma Access** 的配置范围。
3. **Add**（添加）具有以下 **Type**（类型）的地址对象：**FQDN:Domain Name**（**FQDN**：域名），并输入发现的应用程序的 **FQDN**。

   输入 FQDN 目标的 FQDN。



4. 转到 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Security Services**（安全服务） > **Security Policy**（安全策略） > **Pre Rules**（前导规则），并 **Add**（添加）一条安全策略，以便允许访问发现的应用程序。



 ©2025 Palo Alto Networks, Inc.

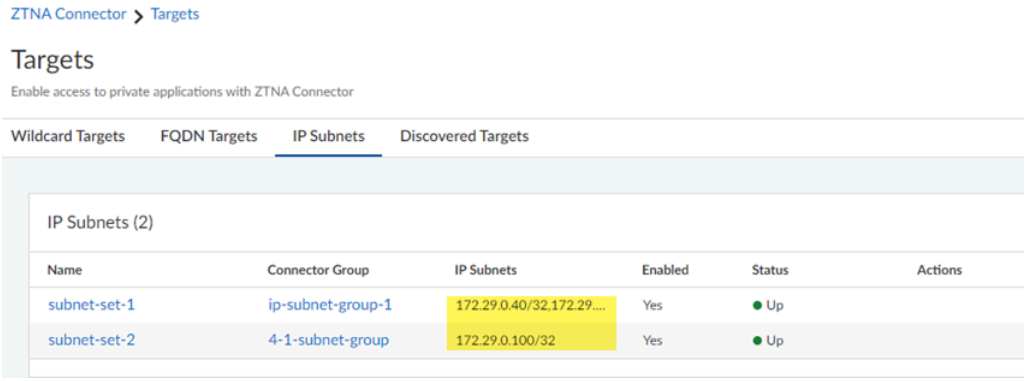
STEP 6 | 单击 **Push Config**（推送配置）以保存并推送配置更改。

STEP 7 | （可选）创建基于 FQDN 的安全策略后，删除基于 IP 应用程序块的策略。

基于 IP 子网的应用程序的安全策略

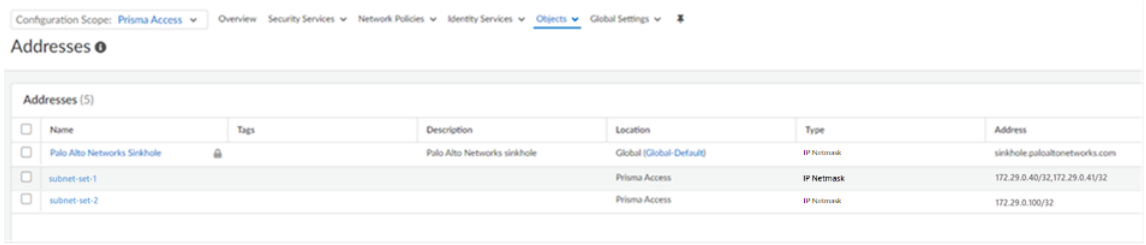
如果您基于 IP 子网创建了 ZTNA 连接器应用程序目标（**Settings**（设置） > **ZTNA Connector**（**ZTNA** 连接器） > **Connectors**（连接器） > **Application Targets**（应用程序目标） > **IP Subnets**（**IP** 子网）），请完成以下步骤以允许访问应用程序。

STEP 1 | 转到 **Workflows**（工作流） > **ZTNA Connector**（**ZTNA** 连接器） > **Application Targets**（应用程序目标） > **IP Subnets**（**IP** 子网），并记录应用程序使用的 IP 子网。

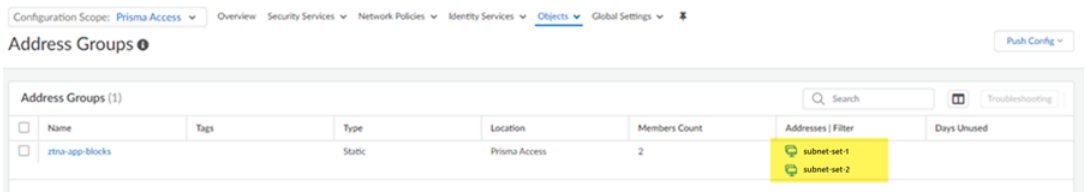


STEP 2 | 创建策略以允许应用程序使用的 IP 子网的 IP 地址。

1. 转到 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Objects**（对象） > **Address**（地址） > **Addresses**（地址），并根据检索到的 IP 地址 **Add**（添加）地址对象。



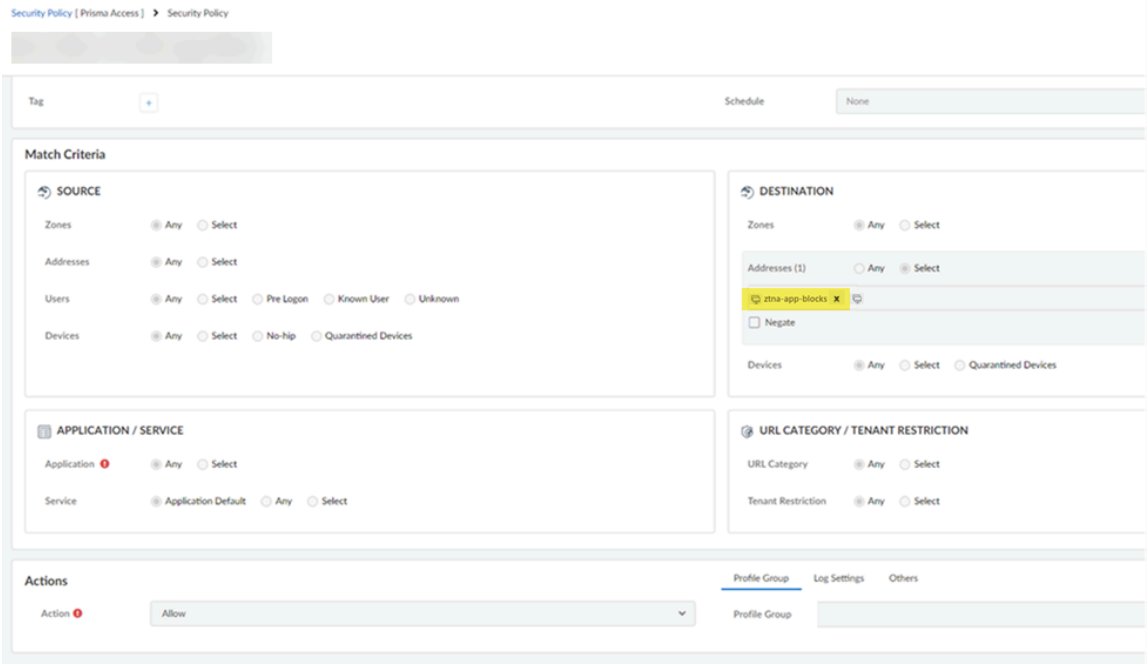
2. 转到 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Objects**（对象） > **Address**（地址） > **Address Groups**（地址组），并将创建的地址 **Add**（添加）到地址组中。



3. 转到 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Security Services**（安全服务） > **Security Policy**（安全策略） >

 ©2025 Palo Alto Networks, Inc.

Pre Rules（前导规则），并 **Add**（添加）一条安全策略，以便允许访问应用程序的 IP 子网，从而指定在之前的步骤中创建的 **Addresses**（地址）。



STEP 3 | 单击 **Push Config**（推送配置）以保存并推送配置更改。

基于 FQDN 的应用程序的安全策略

如果您已基于 FQDN 添加目标（**Settings**（设置） > **ZTNA Connector**（**ZTNA** 连接器） > **Connectors**（连接器） > **Application Targets**（应用程序目标） > **FQDN Targets**（**FQDN** 目标）），请完成以下步骤，以便创建地址对象和安全策略来允许访问应用程序。

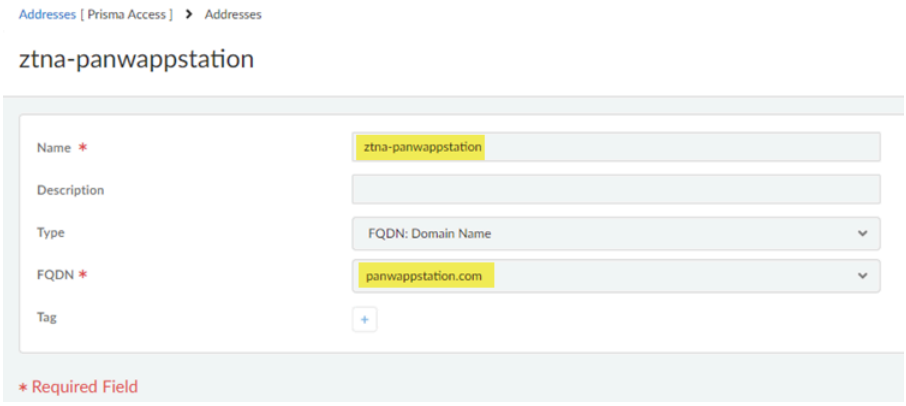
©2025 Palo Alto Networks, Inc.

STEP 1 | 为使用 FQDN 添加的应用程序配置安全策略。

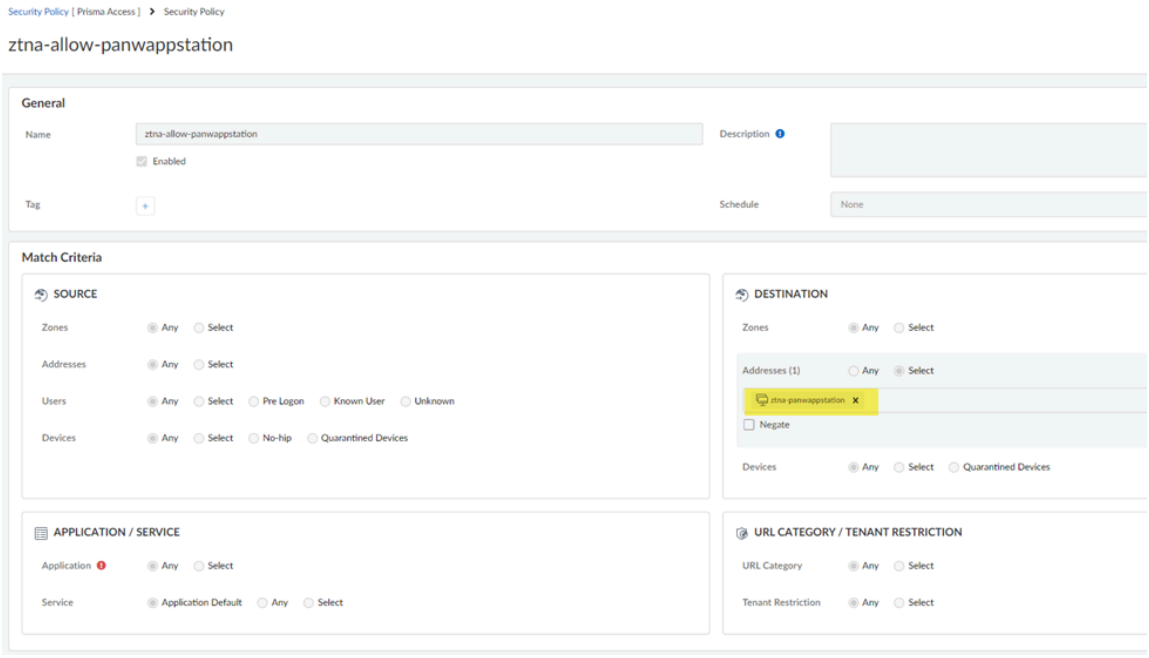
1. 转到 **Workflows**（工作流） > **ZTNA Connector**（**ZTNA** 连接器） > **Application Targets**（应用程序目标） > **FQDN Targets**（**FQDN** 目标），并记录应用程序使用的 FQDN。
2. 为 FQDN 创建一个地址对象（**Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Objects**（对象） > **Address**（地址） > **Addresses**（地址））。

   选择 **Prisma Access** 的配置范围。
3. **Add**（添加）具有以下 **Type**（类型）的地址对象：**FQDN:Domain Name**（**FQDN**：域名），并输入发现的应用程序的 **FQDN**。

   输入所有已发现应用程序的 FQDN。



4. 可选转到 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Security Services**（安全服务） > **Security Policy**（安全策略） > **Pre Rules**（前导规则），并 **Add**（添加）一条安全策略，以便允许访问发现的应用程序。



 ©2025 Palo Alto Networks, Inc.

STEP 2 | 单击 **Push Config**（推送配置）以保存并推送配置更改。

启用 ZTNA 连接器的应用程序的安全策略 (Panorama)

将应用程序加入 ZTNA 连接器后，您要设置策略规则来允许和控制这些应用程序的访问。创建和应用策略的过程取决于您的应用程序是通过通配符、IP 子网还是 FQDN 定义的。

基于通配符的应用程序的安全策略

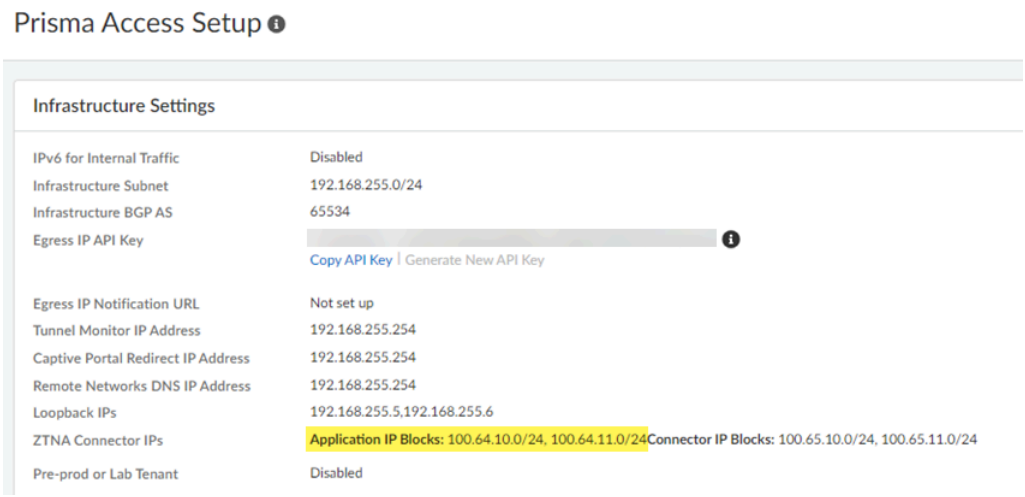
基于通配符的应用程序（（**Settings**（设置） > **ZTNA Connector**（**ZTNA** 连接器） > **Application Targets**（应用程序目标） > **Wildcard Targets**（通配符目标））要求创建自定义 URL 类别；但是，该类型的类别仅强制执行 HTTP 和 HTTPS 流量的策略，而不允许其他流量（例如 SSH）。因此，您需要通过允许 ZTNA 连接器应用程序 IP 块的流量，以便暂时允许所有应用程序的访问。

在 ZTNA 连接器学习基于通配符的 FQDN 后，您可以禁用允许应用程序 IP 块的流量的策略，并根据学习到的 FQDN 应用策略实施。

©2025 Palo Alto Networks, Inc.

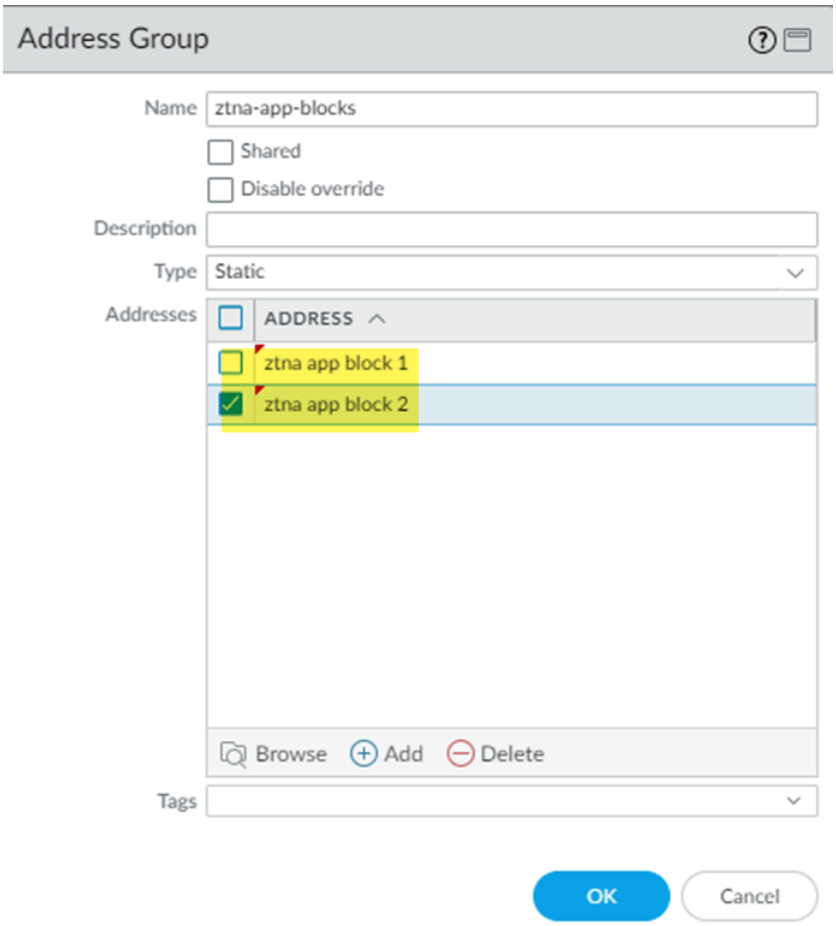
STEP 1 | 创建策略以允许 ZTNA 连接器应用程序 IP 块的 IP 地址。

1. 从 ZTNA 连接器用户界面中，转到 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Prisma Access** > **Prisma Access Setup**（**Prisma Access** 设置），并记录 **Application IP Blocks**（应用程序 **IP** 块）。



2. 转到 **Objects**（对象） > **Addresses**（地址），并根据检索到的 IP 地址 **Add**（添加）地址对象。
3. 转到 **Objects**（对象） > **Address Groups**（地址组），并将创建的地址对象 **Add**（添加）到地址组。

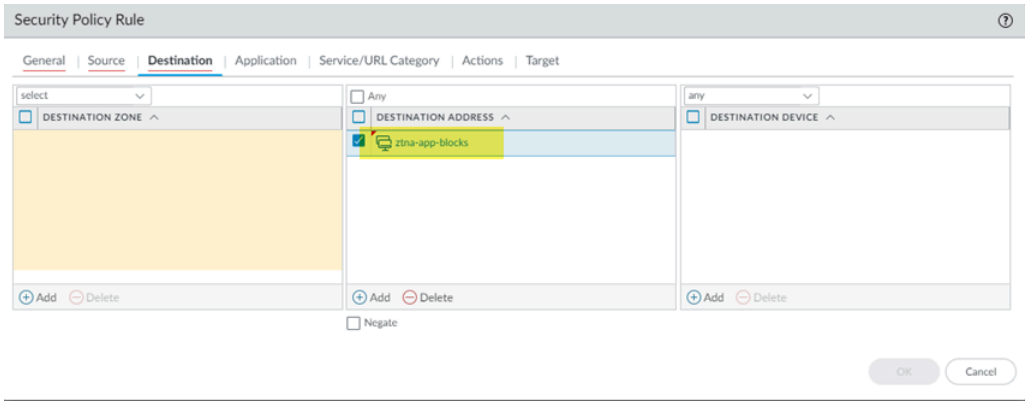
 ©2025 Palo Alto Networks, Inc.



4. 转到 **Policies**（策略） > **Security**（安全） > **Pre Rules**（前导规则），并 **Add**（添加）一条安全策略，以便允许访问所有应用程序 IP 地址块，从而指定在之前的步骤中创建的 **Address Group**（地址组）。

   添加此安全策略将允许所有基于通配符的应用程序流量通过，同时 ZTNA 连接器根据通配符发现应用程序。如果没有允许应用程序 IP 块的规则，用户将无法访问基于通配符的应用程序。

   您可以保留此策略，直到 ZTNA 连接器发现基于通配符的应用程序。然后，您可以选择禁用此策略，并为每个发现的应用程序添加安全策略规则。



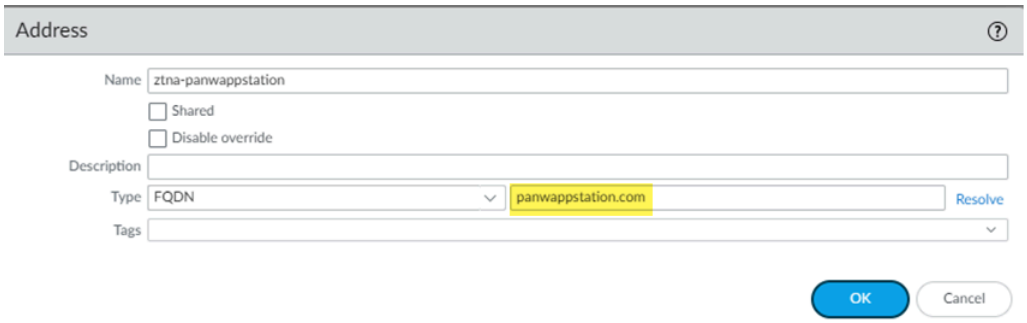
 ©2025 Palo Alto Networks, Inc.

STEP 2 | ZTNA 连接器根据通配符发现应用程序后，为使用 FQDN 添加的应用程序配置安全策略。

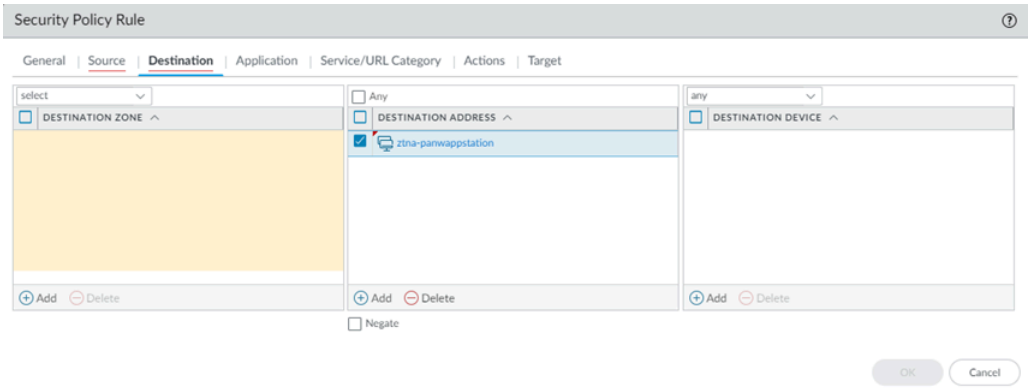
1. 转到 **Workflows**（工作流） > **ZTNA Connector**（**ZTNA** 连接器） > **Application Targets**（应用程序目标） > **FQDN Targets**（**FQDN** 目标），并记录应用程序使用的 FQDN。
2. 为 FQDN 创建地址对象（**Objects**（对象） > **Addresses**（地址））。

   选择 **Mobile_User_Device_Group** 或 **Remote_Network_Device_Group**，具体取决于移动用户或分支站点的用户是否将访问 ZTNA 连接器后的私有应用程序。
3. **Add**（添加）具有 **FQDN Type**（类型）的地址对象，并输入发现的应用程序的 **FQDN**。

   输入 FQDN 目标的 FQDN。



4. 转到 **Policies**（策略） > **Security**（安全） > **Pre Rules**（前导规则），并 **Add**（添加）一条安全策略，以便允许访问发现的应用程序。



STEP 3 | **Commit and Push**（提交并推送）更改。

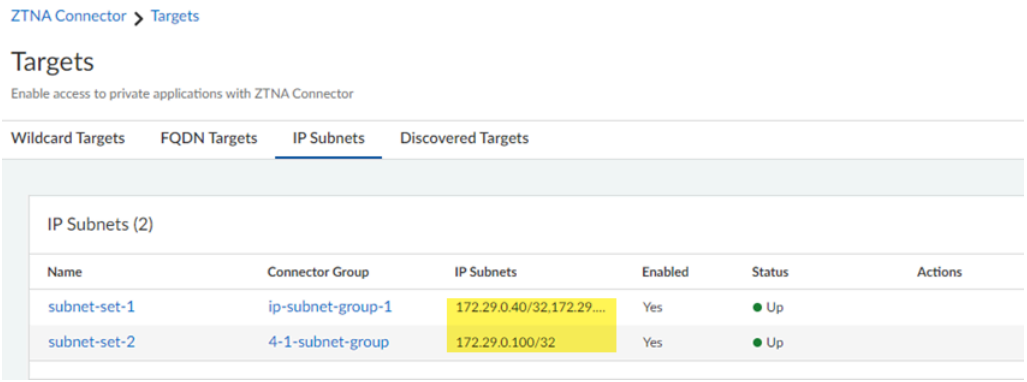
STEP 4 | （可选）创建基于 FQDN 的安全策略后，删除基于 IP 应用程序块的策略。

基于 IP 子网的应用程序的安全策略

如果您基于 IP 子网创建了 ZTNA 连接器应用程序目标（**Settings**（设置） > **ZTNA Connector**（**ZTNA** 连接器） > **Connectors**（连接器） > **Application Targets**（应用程序目标） > **IP Subnets**（**IP** 子网）），请完成以下步骤以允许访问应用程序。

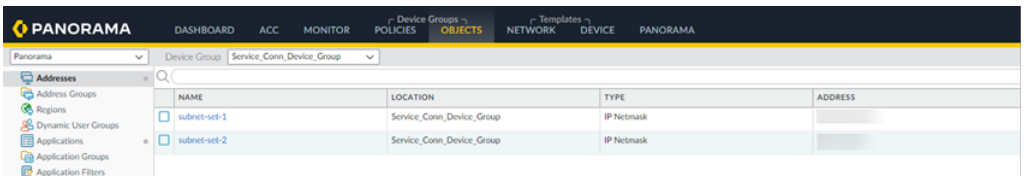
©2025 Palo Alto Networks, Inc.

STEP 1 | 转到 **Workflows**（工作流） > **ZTNA Connector**（**ZTNA** 连接器） > **Application Targets**（应用程序目标） > **IP Subnets**（**IP** 子网），并记录应用程序使用的 IP 子网。

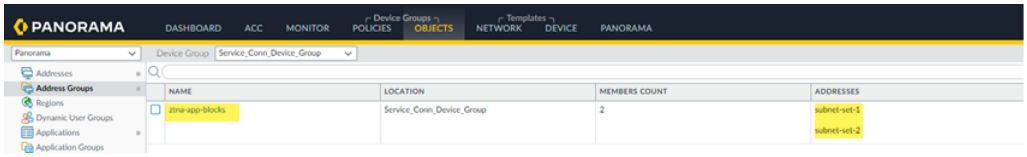


STEP 2 | 创建策略以允许应用程序使用的 IP 子网的 IP 地址。

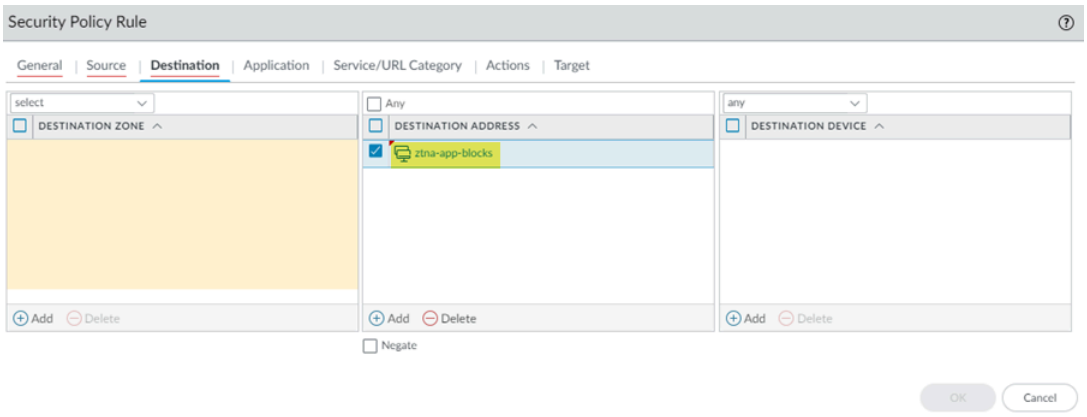
1. 转到 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Objects**（对象） > **Address**（地址） > **Addresses**（地址），并根据检索到的 IP 地址 **Add**（添加）地址对象。



2. 转到 **Objects**（对象） > **Address Groups**（地址组），并将创建的地址 **Add**（添加）到地址组中。



3. 转到 **Policies**（策略） > **Security**（安全） > **Pre Rules**（前导规则），并 **Add**（添加）一条安全策略，以便允许访问应用程序的 IP 子网，从而指定在之前的步骤中创建的 **Addresses**（地址）。



STEP 3 | 单击 **Push Config**（推送配置）以保存并推送配置更改。

 ©2025 Palo Alto Networks, Inc.

基于 FQDN 的应用程序的安全策略

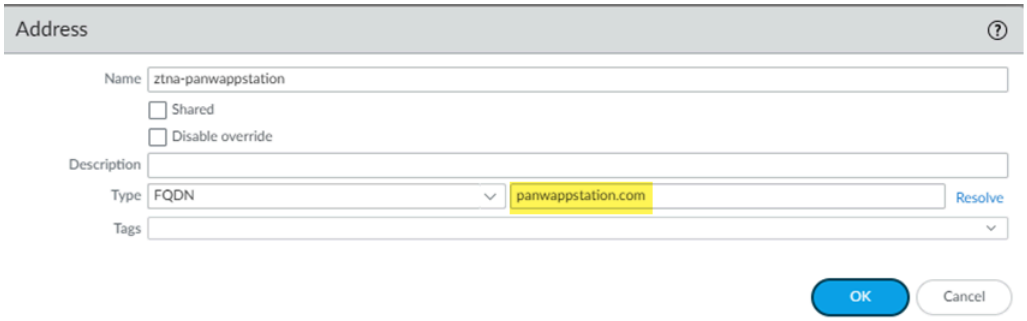
如果您已基于 FQDN 添加目标（**Settings**（设置） > **ZTNA Connector**（**ZTNA** 连接器） > **Connectors**（连接器） > **Application Targets**（应用程序目标） > **FQDN Targets**（**FQDN** 目标）），请完成以下步骤，以便创建地址对象和安全策略来允许访问应用程序。

STEP 1 | 为使用 FQDN 添加的应用程序配置安全策略。

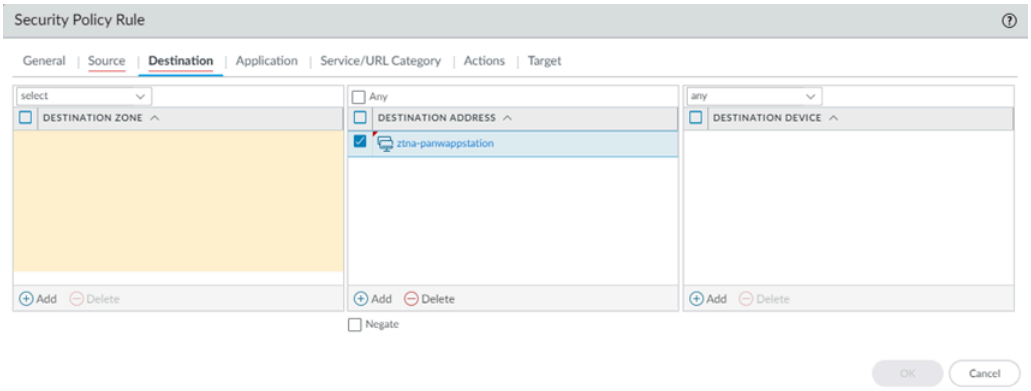
1. 转到 **Workflows**（工作流） > **ZTNA Connector**（**ZTNA** 连接器） > **Application Targets**（应用程序目标） > **FQDN Targets**（**FQDN** 目标），并记录应用程序使用的 FQDN。
2. 为 FQDN 创建地址对象（**Objects**（对象） > **Addresses**（地址））。

   选择 **Mobile_User_Device_Group** 或 **Remote_Network_Device_Group**，具体取决于移动用户或分支站点的用户是否将访问 ZTNA 连接器后的私有应用程序。
3. **Add**（添加）具有 **FQDN Type**（类型）的地址对象，并输入发现的应用程序的 **FQDN**。

   输入所有已发现应用程序的 FQDN。



4. 可选转到 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Security Services**（安全服务） > **Security Policy**（安全策略） > **Pre Rules**（前导规则），并 **Add**（添加）一条安全策略，以便允许访问发现的应用程序。



STEP 2 | 单击 **Push Config**（推送配置）以保存并推送配置更改。

©2025 Palo Alto Networks, Inc.

在您的数据中心内接入 ZTNA Connector 虚拟机

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ ZTNA 连接器附加许可证 带附加许可证的基础许可证包括 8 个 ZTNA 连接器、100 个 FQDN 和 4 个 IP 子网功能。 带附加许可证的高级许可证包括 40 个 ZTNA 连接器、300 个 FQDN 和 1024 个 IP 子网功能。 带附加许可证的高级许可证包括 200 个 ZTNA 连接器、4000 个 FQDN 和 1024 个 IP 子网功能。 ❑ 如果您不购买 ZTNA 连接器附加许可证，Prisma Access 许可证将包括四个连接器、40 个 FQDN 和四个 IP 子网。此功能旨在让您在自己的环境中尝试 ZTNA 连接器。

在 Prisma Access 中配置连接器组、连接器和应用程序目标后，必须在数据中心中部署连接器 VM。为了简化连接器接入，可以从 Palo Alto Networks 客户支持门户或云提供商市场获得每个数据中心环境的部署模板。您使用的模板取决于您是否打算使用单臂部署还是双臂部署。

支持的 ZTNA 连接器部署

ZTNA 连接器会发起与云端 Prisma Access 公共 IP 地址的连接，而且您无需定义任何入站防火墙安全规则。但由于 ZTNA 连接器会启动连接，因此您需要添加出口规则，以允许 ZTNA 连接器访问云控制器，并允许 IPSec 连接到云控制器 Prisma Access 数据平面。ZTNA 连接器启动与 Prisma Access 云中的公有 IP 地址。因此，您需要以下出口规则，以便 ZTNA 连接器可以创建到 Prisma Access 的 IPSec 隧道：

- 面向互联网—允许 HTTPS (TCP 443) 和 IKE/IPSec（UDP 500 和 4500）的出口
- 面向数据中心—允许出口应用程序端口。

  例如，允许出口应用程序端口 HTTP (80) 和 HTTPS (443)。这些示例端口是 TCP 端口。如果您的数据中心使用其他端口，请改为允许您使用的端口。

您可以在以下部署拓扑中部署连接器虚拟机：

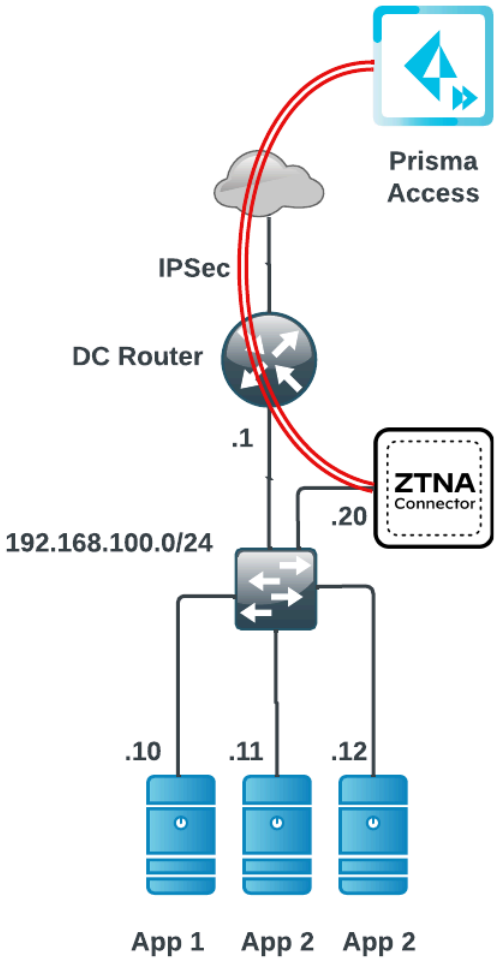
 ©2025 Palo Alto Networks, Inc.

单臂部署

仅在 *AWS*、*Azure* 或 *GCP* 等云原生环境中支持单臂部署。对于本地部署（如 *ESXi* 或基于内核的虚拟机 *(KVM)* 或 *Microsoft Hyper-V*），请使用双臂部署。

在此部署中，您的 ZTNA 连接器位于私有数据中心子网上，可通过数据中心路由器访问互联网。可以在同一子网上本地访问应用程序，也可以通过数据中心路由器访问应用程序。

下图显示了使用单臂部署的 ZTNA 连接器网络部署示例。



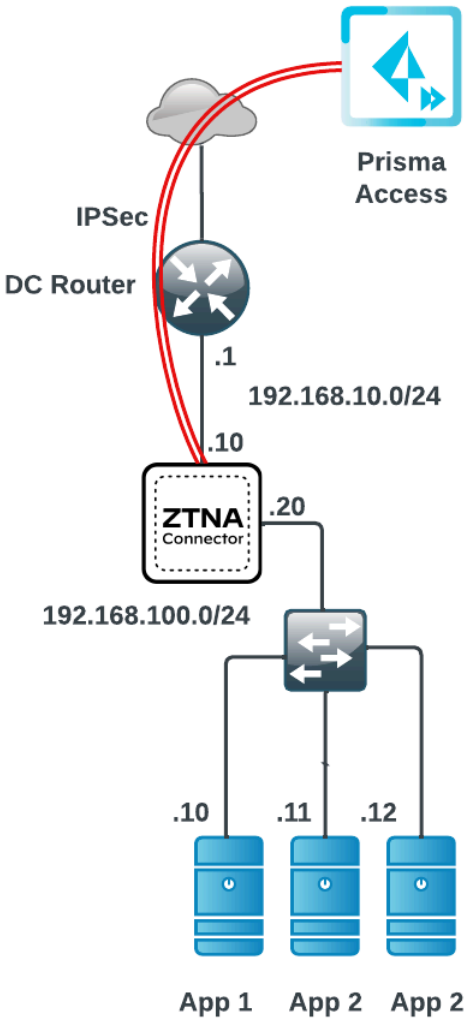
 ©2025 Palo Alto Networks, Inc.

双臂部署

如果您想更好地控制入口和出口安全规则，或者如果您拥有本地 VM 部署，则可以使用双臂部署，其中一个接口面向互联网，另一个接口面向数据中心。

在双臂连接器上设置 *IP* 地址时，请确保在启动虚拟机之前已正确设置 *ZTNA* 连接器的 *IP* 地址分配。例如，以下示例图使用 *IP* 地址 *192.168.10.10* 和 *192.168.10.20*。给定这些示例地址，请在 *ZTNA* 连接器上为 *192.168.10.10* 和 *192.168.100.20* 设置端口，否则 *Prisma Access* 无法通过 *ZTNA* 连接器访问数据中心中的应用程序。*192.168.10.10* 和 *192.168.100.20* 只是 *IP* 地址示例，您不必使用这些 *IP* 地址即可使部署正常运行。

下图显示了使用双臂部署的 ZTNA 连接器网络部署示例。

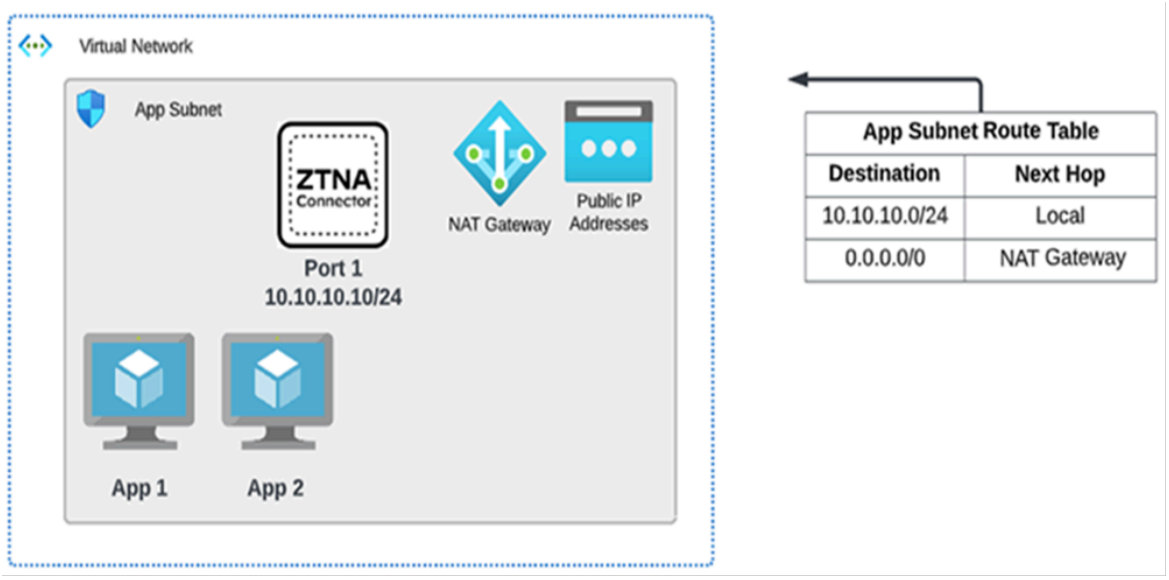


ZTNA 连接器支持的 Microsoft Azure 部署

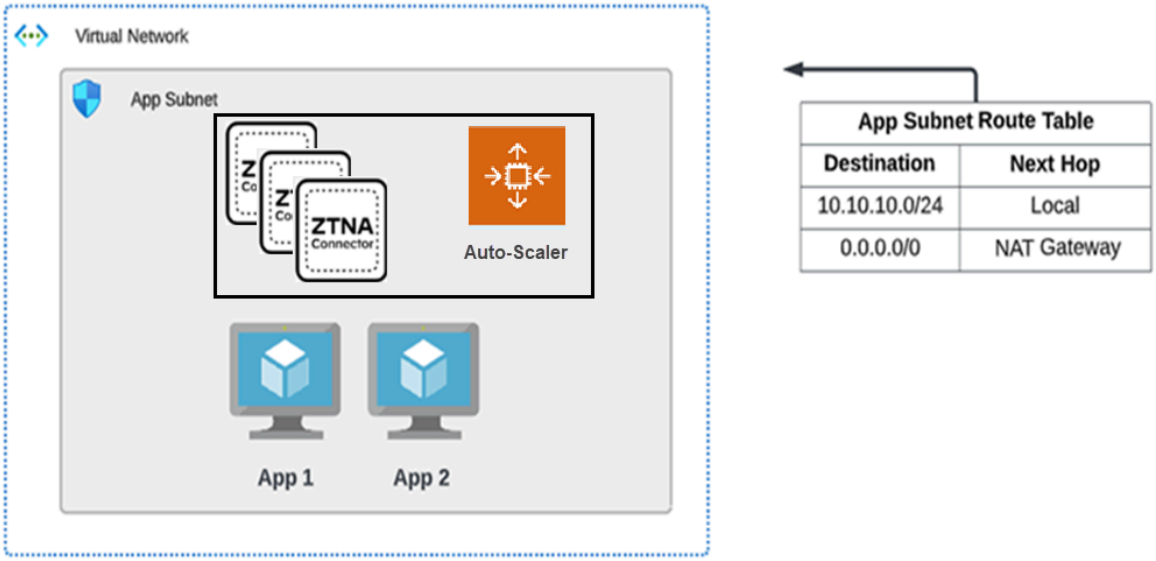
Prisma Access Microsoft Azure 中的 ZTNA 连接器网络部署支持两个部署以及每个部署对应的模板。

©2025 Palo Alto Networks, Inc.

下图显示了使用单臂模式和 NAT 网关在 Azure 中部署 Prisma Access ZTNA 连接器的示例。

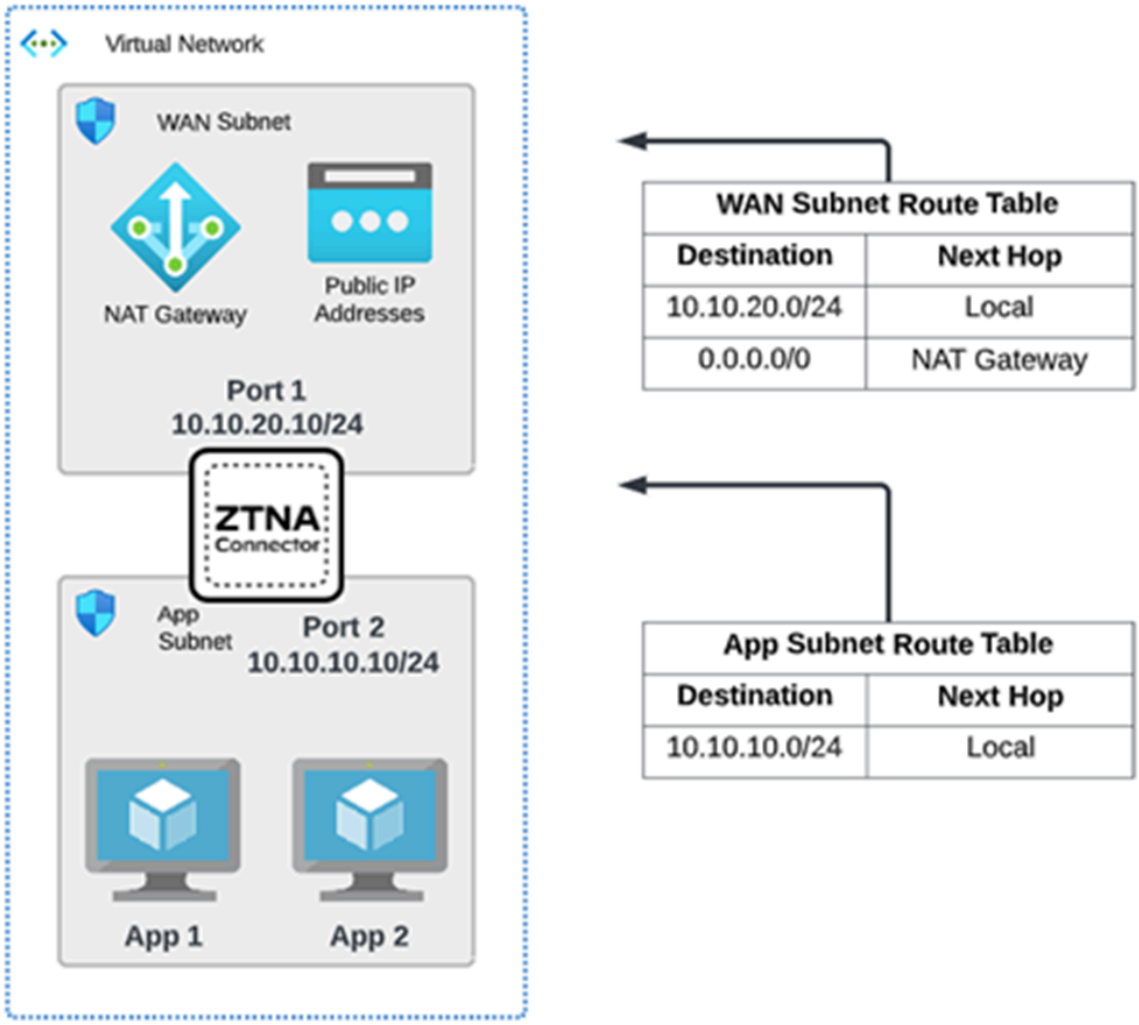


下图展示了在 AWS 中使用单臂自动缩放和 NAT 网关进行 ZTNA 连接器部署的示例。



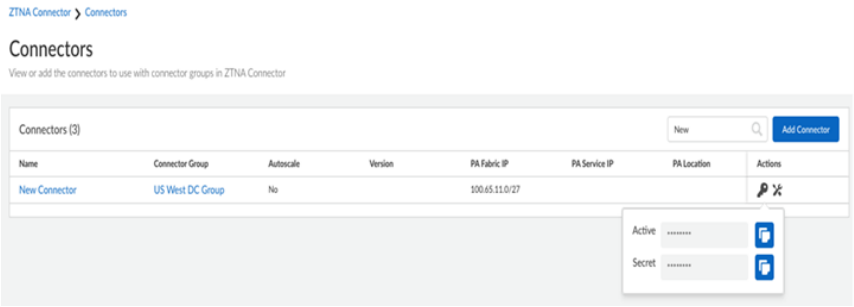
下图显示了使用双臂模式和 NAT 网关在 Azure 中部署 Prisma Access ZTNA 连接器的示例。

©2025 Palo Alto Networks, Inc.



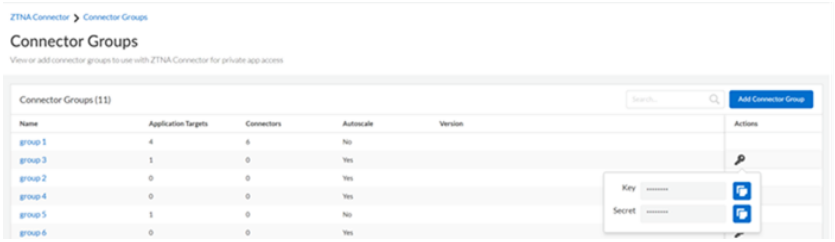
在 Microsoft Azure 中接入 ZTNA 连接器

- 查看要求和指南，以及为了在 Microsoft Azure 中使用 ZTNA 连接器而需要配置的 FQDN 和端口。
- 在Prisma SASE 平台上，检索并复制连接器密钥和机密值：在 **Workflows**（工作流） > **ZTNA Connector**（**ZTNA** 连接器） > **Connectors**（连接器）中，找到您在 Prisma Access 中创建的要与该虚拟机关联的连接器对象，选择 **Copy Token**（复制令牌）；然后，复制 **Key**（密钥） 和 **Secret**（机密）值。



 ©2025 Palo Alto Networks, Inc.

- 对于 **Prisma Access ZTNA** 连接器单臂自动扩展部署，必须检索并复制连接器组密钥和机密值在 **Workflows**（工作流） > **ZTNA Connector**（**ZTNA** 连接器） > **Connectors Groups**（连接器组）中，找到您在 Prisma Access 中创建的要与该虚拟机关联的连接器对象，选择 **Copy Token**（复制令牌）；然后，复制 **Key**（密钥）和 **Secret**（机密）值。



满足所有先决条件后，请按照以下步骤在 Microsoft Azure 中接入 ZTNA 连接器。

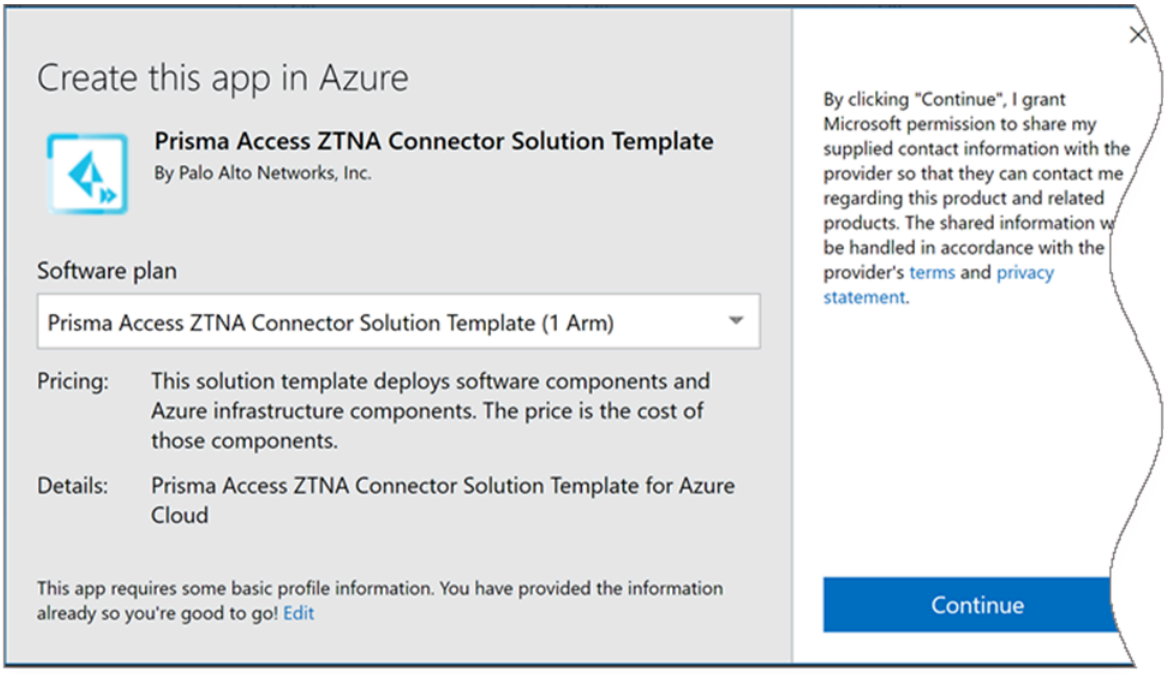
STEP 1 | 登录 Azure Marketplace，然后搜索 **Prisma Access ZTNA** 连接器。

STEP 2 | 单击 **Get it now**（立即获取）。



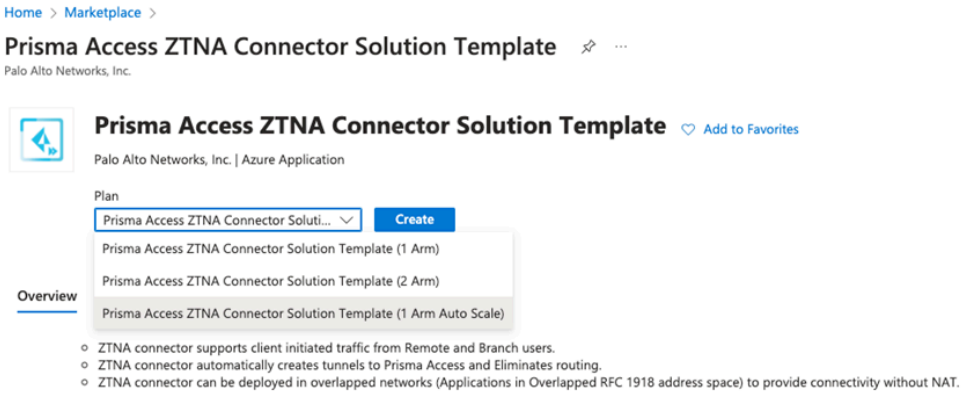
 ©2025 Palo Alto Networks, Inc.

STEP 3 | 选择 **Continue**（继续）以继续创建过程。



STEP 4 | 选择软件计划，然后选择 **Create**（创建）以在 Azure 中创建此应用程序：

- Prisma Access ZTNA 连接器解决方案模板（单臂）
- 在 Microsoft Azure 中部署具有自动缩放功能的 ZTNA 连接器单臂
- Prisma Access ZTNA 连接器解决方案模板（双臂）



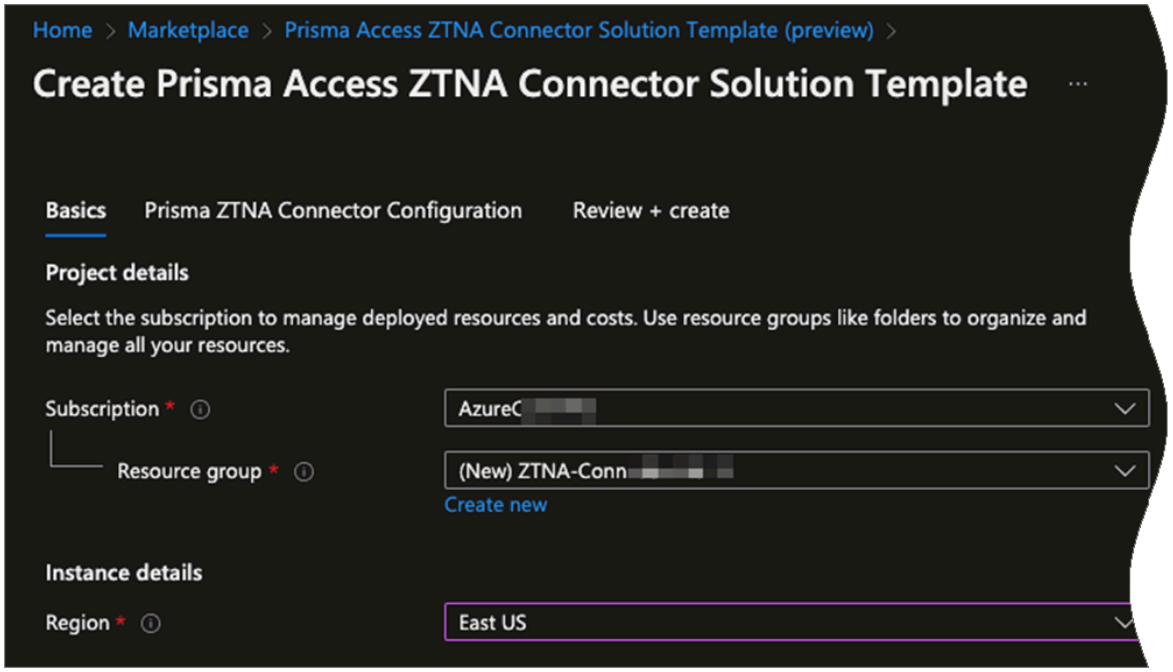
在 **Microsoft Azure** 中部署 **ZTNA** 连接器单臂

按照以下步骤在 Microsoft Azure 中部署单臂 ZTNA 连接器：

 ©2025 Palo Alto Networks, Inc.

STEP 1 | 在 **Basics**（基础）选项卡上配置以下内容：

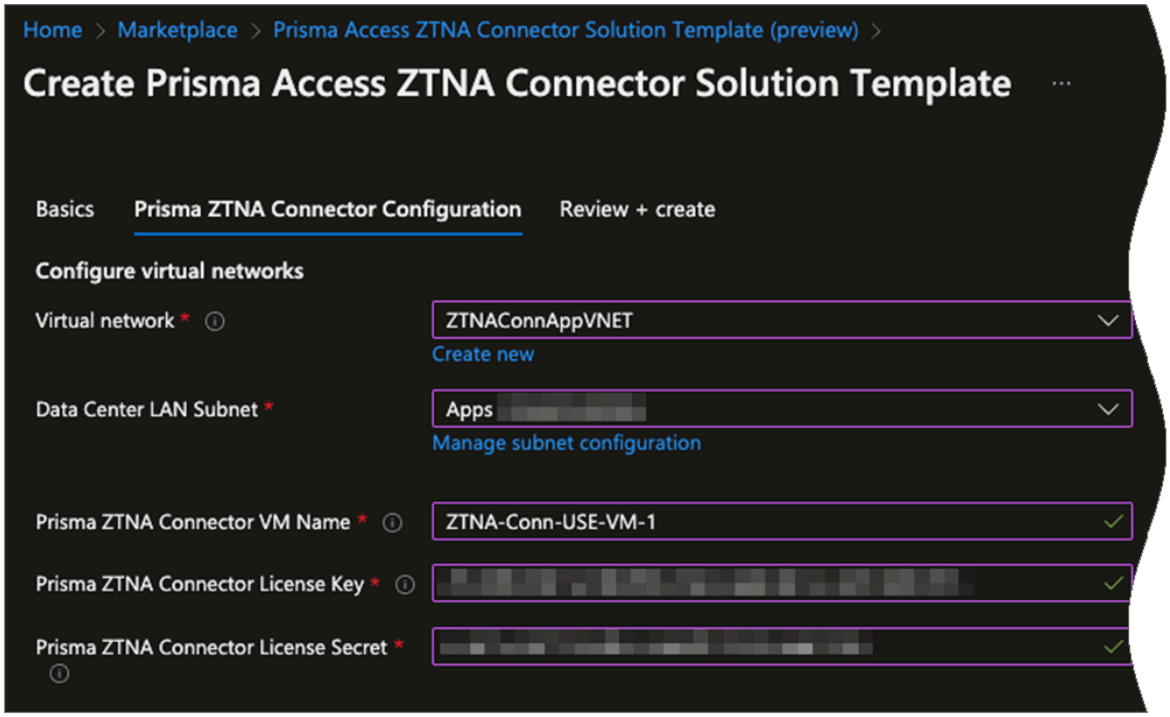
- 选择您的 Azure 订阅以管理已部署的资源。
- 选择现有 **Resource Group**（资源组），或选择 **Create new**（新建）。
- 选择与您的位置相关的 Azure **Region**（区域）。
- 单击 **Next:Prisma ZTNA Connector Configuration**（下一步：**Prisma ZTNA** 连接器配置）。



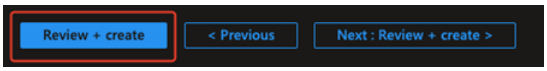
 ©2025 Palo Alto Networks, Inc.

STEP 2 | 在 **Prisma ZTNA Connector Configuration**（**Prisma ZTNA** 连接器配置）选项卡上配置虚拟网络：

- 创建新虚拟网络，或选择 **Virtual network**（虚拟网络以选择现有虚拟网络。
- 选择 **Data Center LAN Subnet**（数据中心 **LAN** 子网），您已在其中配置了应用程序以接入此连接器。
- 在 **Prisma ZTNA Connector VM Name**（**Prisma ZTNA** 连接器虚拟机名称）中输入名称。
- 输入您从 Prisma SASE 门户获取的 **Prisma ZTNA Connector License Key**（**ZTNA** 连接器许可证密钥）和 **Prisma ZTNA Connector License Secret**（**ZTNA** 连接器许可证机密）值。



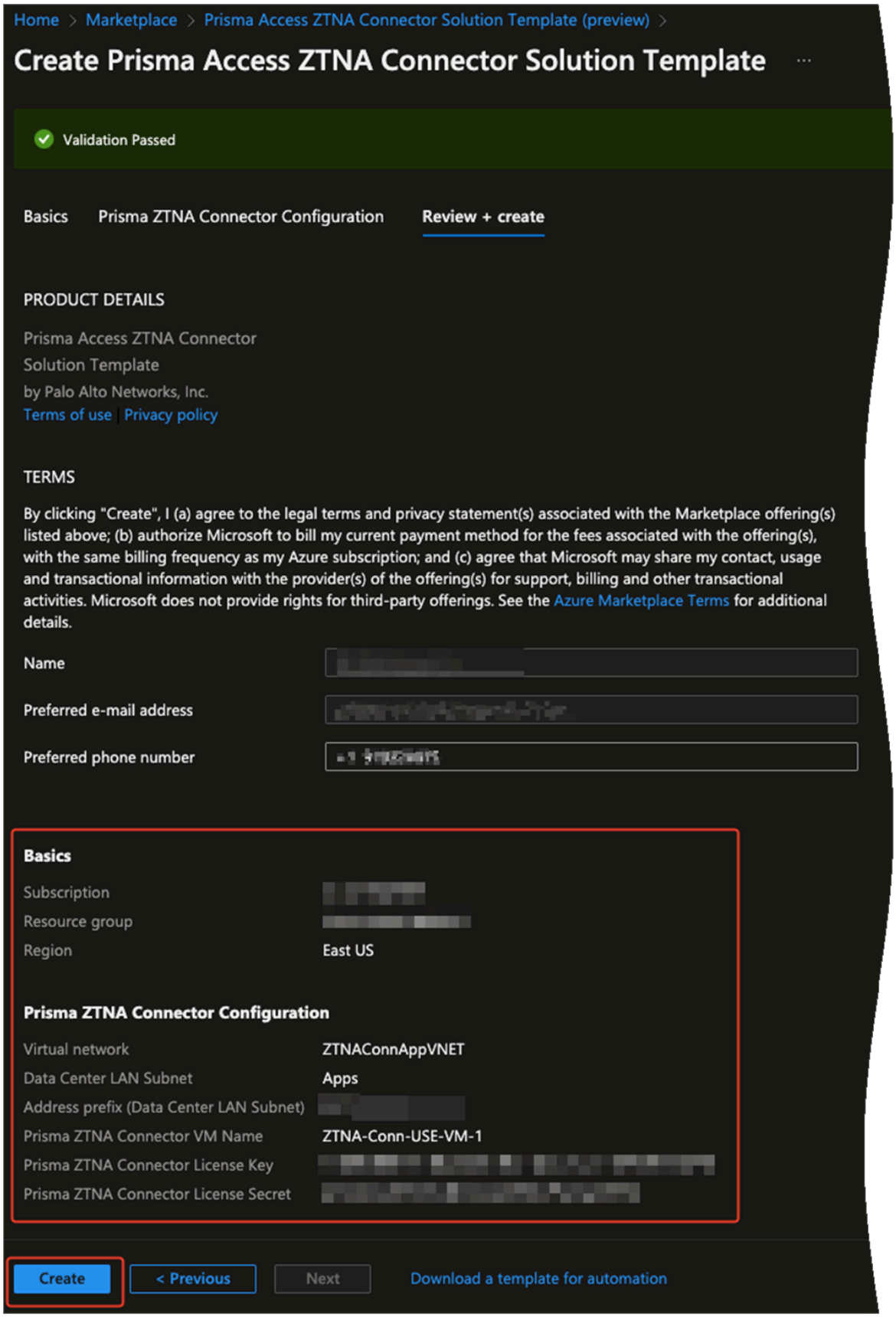
- 选择 **Review + create**（审查 + 创建）查看托管的 Prisma ZTNA 连接器配置。



 ©2025 Palo Alto Networks, Inc.

STEP 3 | 确认您提供的详细信息，然后单击 **Create**（创建）以开始虚拟机部署。

 ©2025 Palo Alto Networks, Inc.



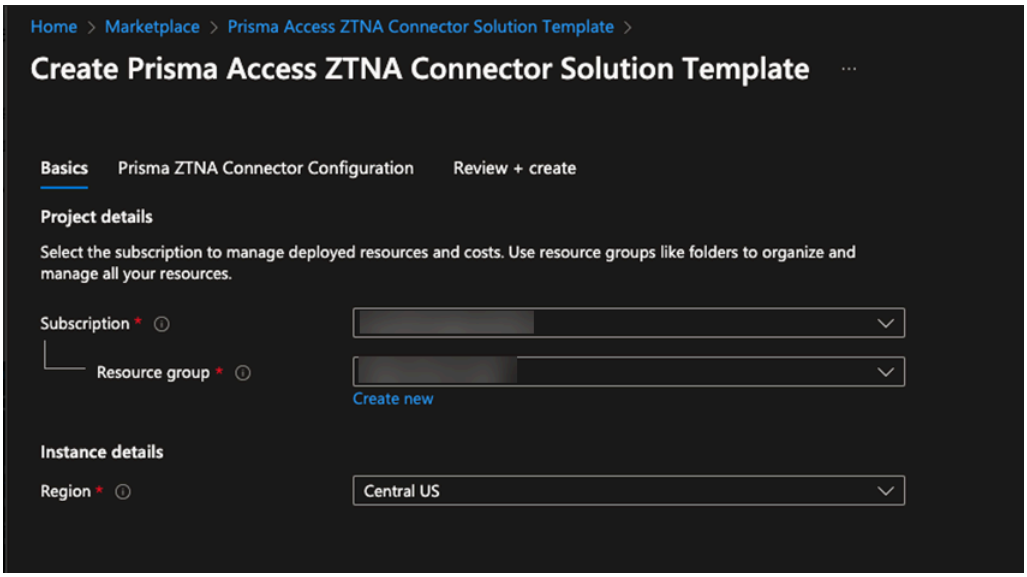
 ©2025 Palo Alto Networks, Inc.

STEP 4 | 部署完成后，请选择 **Go to resource**（转到资源）。

在 **Microsoft Azure** 中部署具有自动缩放功能的 **ZTNA** 连接器单臂

STEP 1 | 在 **Basics**（基础）选项卡上配置以下内容：

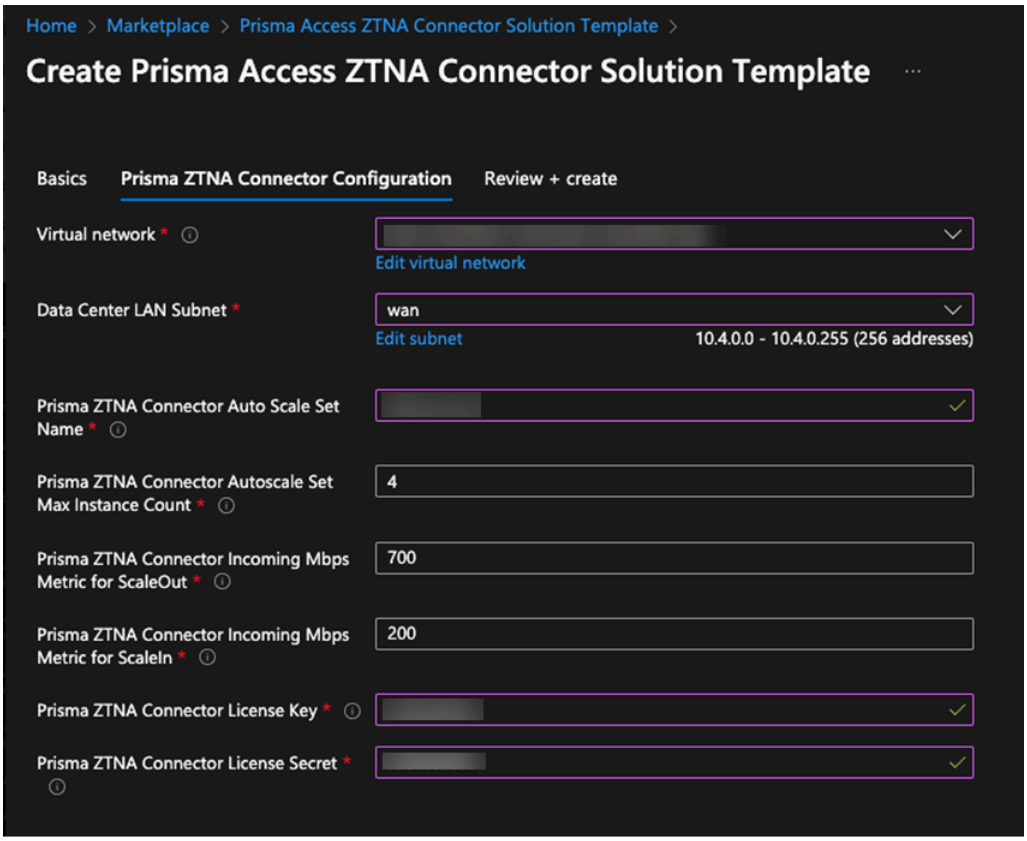
- 选择您的 Azure 订阅以管理已部署的资源。
- 选择现有 **Resource Group**（资源组），或选择 **Create new**（新建）。
- 选择与您的位置相关的 Azure **Region**（区域）。
- 单击 **Next:Prisma ZTNA Connector Configuration**（下一步：**Prisma ZTNA** 连接器配置）。



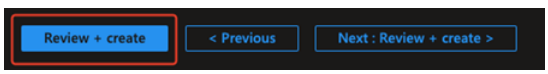
 ©2025 Palo Alto Networks, Inc.

STEP 2 | 在 **Next:Prisma ZTNA Connector Configuration**（下一步：**Prisma ZTNA** 连接器配置）选项卡上配置虚拟网络：

- 创建新虚拟网络，或选择 **Virtual network**（虚拟网络以选择现有虚拟网络。
- 选择 **Data Center LAN Subnet**（数据中心 **LAN** 子网），您已在其中配置了应用程序以接入此连接器。
- 在 **Prisma ZTNA Connector Auto Scale Set Name**（**Prisma ZTNA** 连接器自动缩放集名称）中输入名称，指定在 Azure 中创建的缩放集名称。
- 在 **Prisma ZTNA Connector Autoscale Set Max Instance Count**（**Prisma ZTNA** 连接器自动缩放设置最大实例数量）中输入数量。连接器组中允许的最大 ZTNA 连接器数量为 4。
- 在 **Prisma ZTNA Connector Incoming Mbps Metric for ScaleOut**（用于横向扩展的 **Prisma ZTNA** 连接器输入 **Mbps** 指标）中输入值。请输入一个介于 100 到 1000 之间的值。
- 在 **Prisma ZTNA Connector Incoming Mbps Metric for ScaleIn**（用于纵向扩展的 **Prisma ZTNA** 连接器输入 **Mbps** 指标）中输入值。请输入一个介于 1 到 500 之间的值。
- 输入您从连接器组的 Prisma SASE 门户（要在其中接入连接器）获取的 **Prisma ZTNA Connector License Key**（**ZTNA** 连接器许可证密钥）和 **Prisma ZTNA Connector License Secret**（**ZTNA** 连接器许可证机密）值。

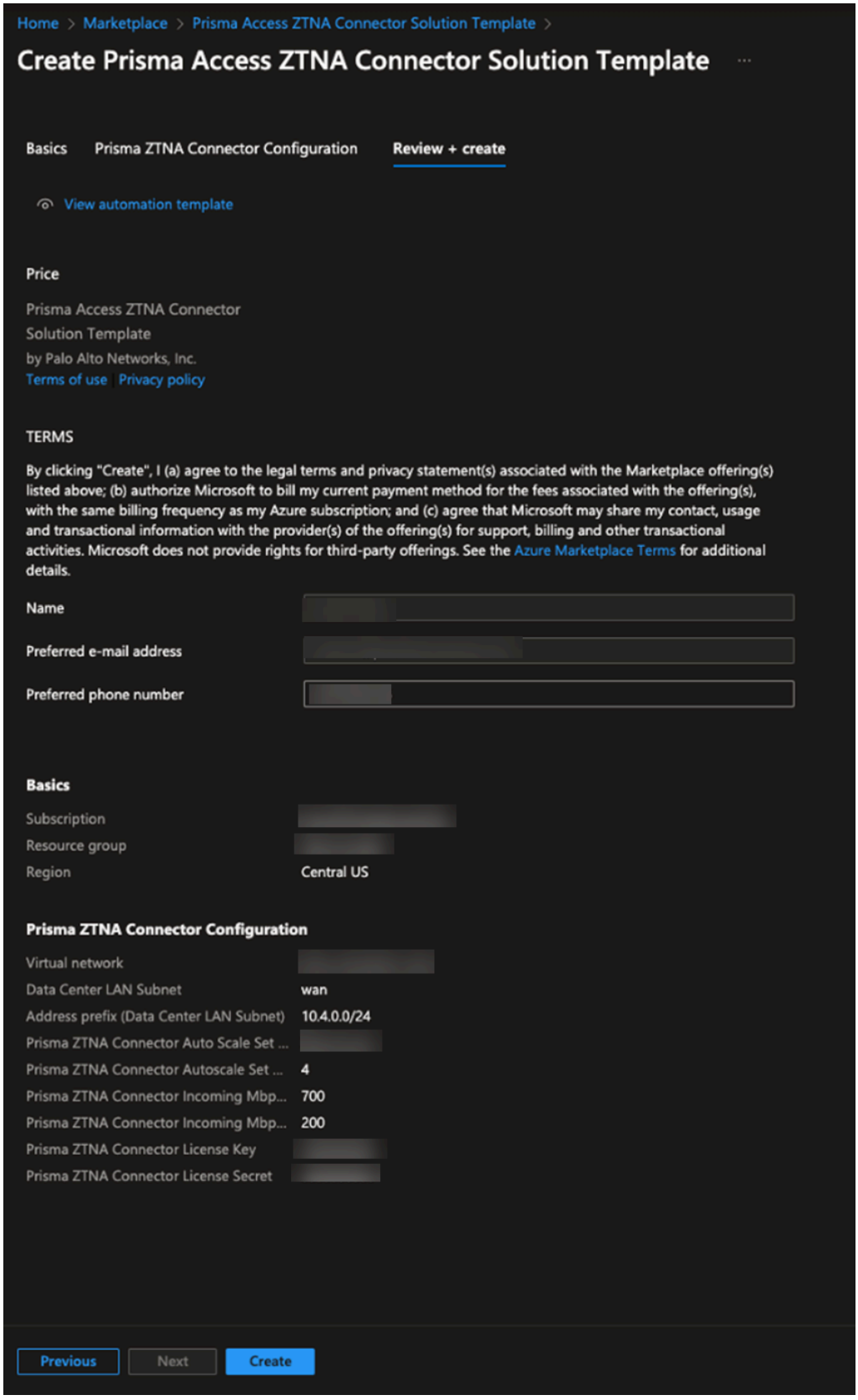


- 选择 **Review + create**（审查 + 创建）查看托管的 Prisma ZTNA 连接器配置。



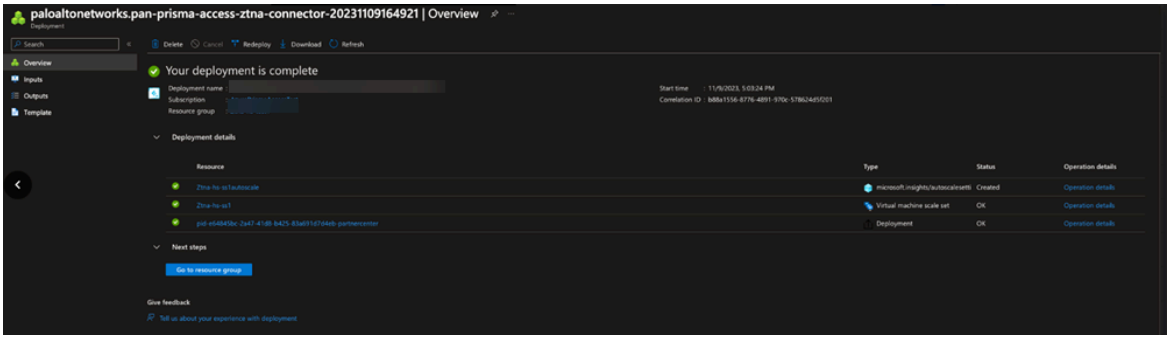
 ©2025 Palo Alto Networks, Inc.

STEP 3 | 确认您提供的详细信息，然后单击 **Create**（创建）以开始虚拟机部署。



 ©2025 Palo Alto Networks, Inc.

STEP 4 | 部署完成后，选择 **Go to resource group**（转到资源组）。

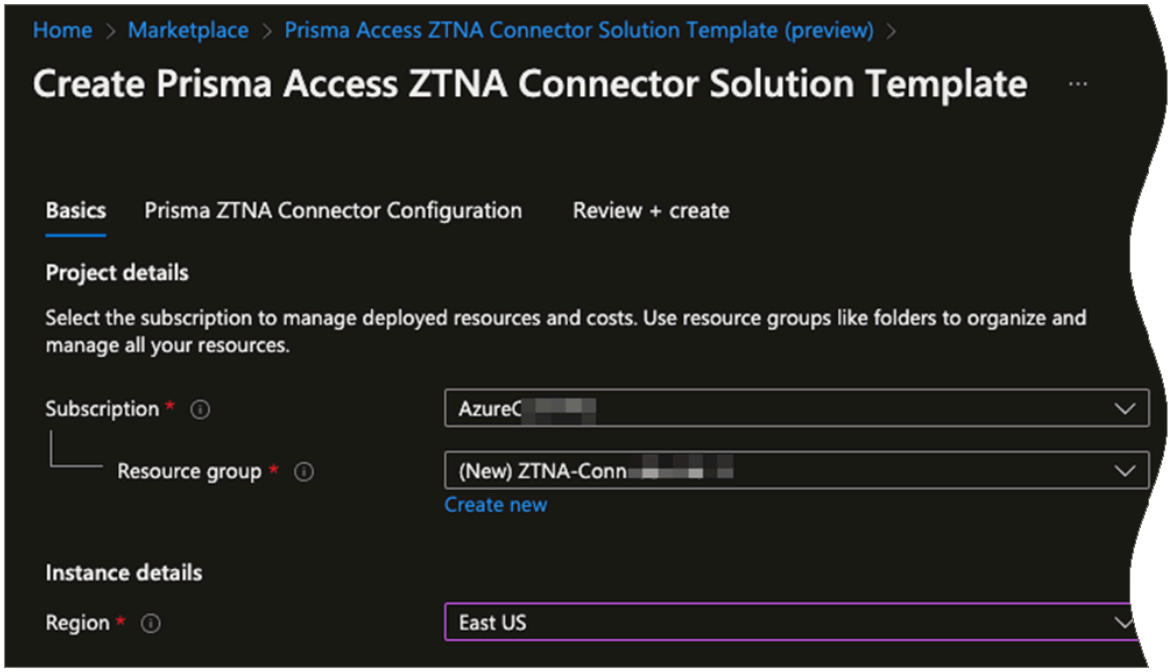


在 **Microsoft Azure** 中部署 **ZTNA** 连接器双臂

按照以下步骤在 Microsoft Azure 中部署双臂 ZTNA 连接器：

STEP 1 | 在 **Basics**（基础）选项卡上配置以下内容：

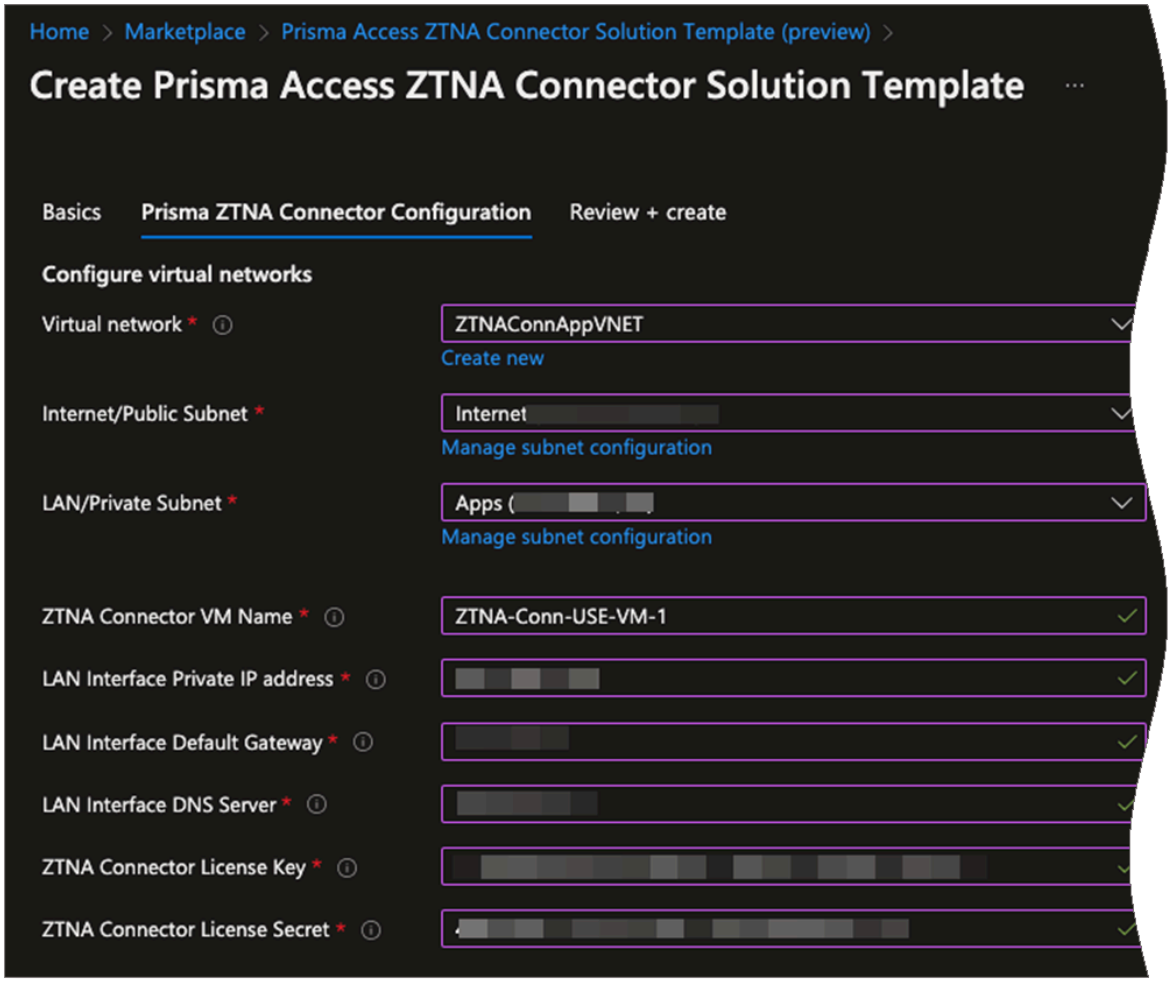
- 选择您的 Azure 订阅以管理已部署的资源。
- 选择现有 **Resource Group**（资源组），或选择 **Create new**（新建）。
- 选择与您的位置相关的 Azure **Region**（区域）。
- 单击 **Next:Prisma ZTNA Connector Configuration**（下一步：**Prisma ZTNA** 连接器配置）。



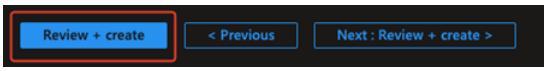
 ©2025 Palo Alto Networks, Inc.

STEP 2 | 在 **Next:Prisma ZTNA Connector Configuration**（下一步：**Prisma ZTNA** 连接器配置）选项卡上配置虚拟网络：

- 创建新虚拟网络或使用现有虚拟网络。
- 选择用于 WAN 与 IPSec 连接的 **Internet/Public Subnet**（互联网/公共子网）。您需要将子网与 NAT 网关关联，以便实现互联网连接。
- 选择 **Data Center LAN Subnet**（数据中心 **LAN** 子网），您已在其中配置了应用程序以接入此连接器。
- 在 **Prisma ZTNA Connector VM Name**（**Prisma ZTNA** 连接器虚拟机名称）中输入名称。
- 在 **LAN Interface Private IP address**（**LAN** 接口私有 **IP** 地址）中输入地址。
- 在 **LAN Interface Default Gateway**（**LAN** 接口默认网关）中输入 IP 地址。
- 在 **LAN Interface DNS Server**（**LAN** 接口 **DNS** 服务器）中输入 IP 地址。
- 输入您从 Prisma SASE 门户获取的 **Prisma ZTNA Connector License Key**（**ZTNA** 连接器许可证密钥）和 **Prisma ZTNA Connector License Secret**（**ZTNA** 连接器许可证机密）值。



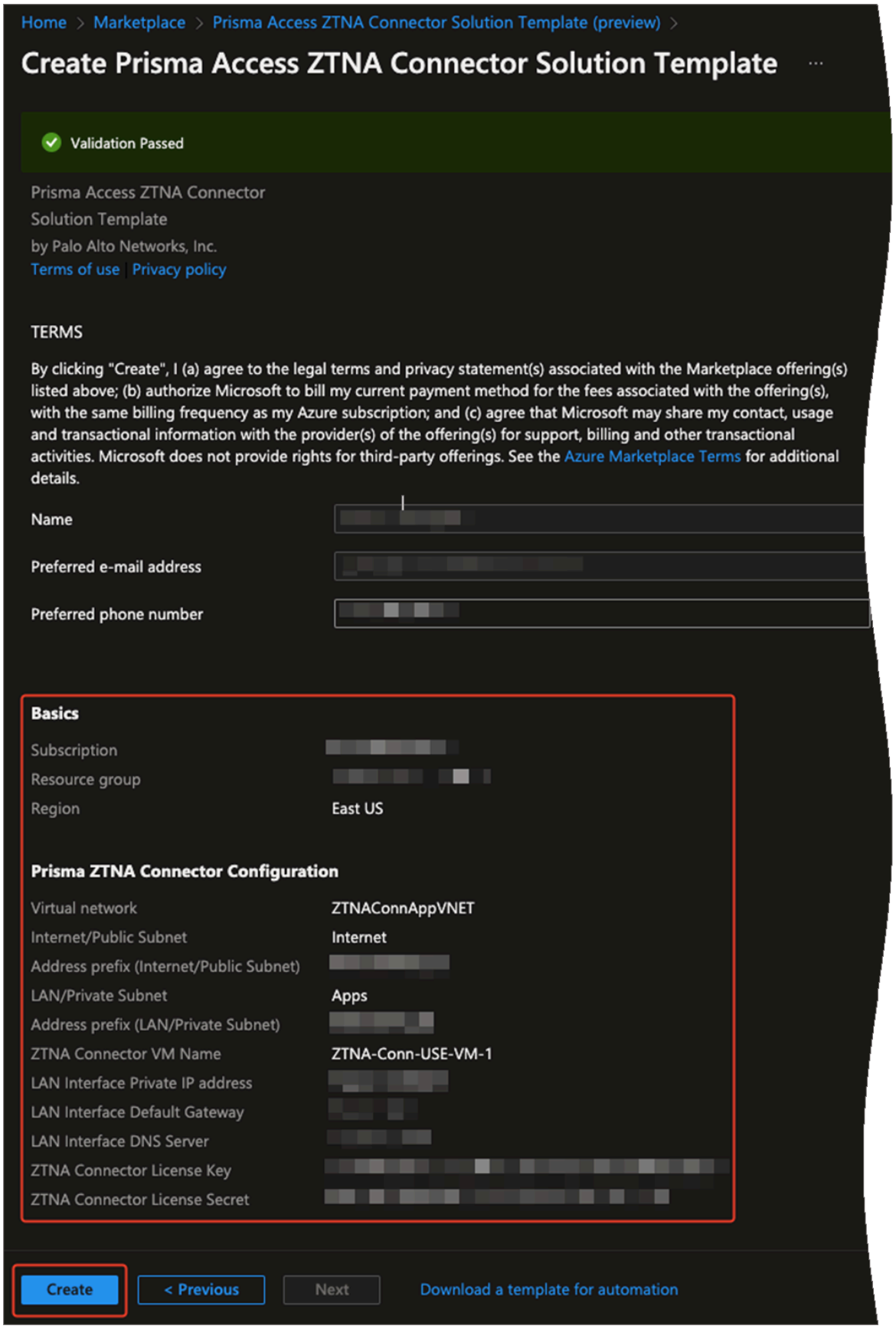
- 选择 **Review + create**（审查 + 创建）查看托管的 Prisma ZTNA 连接器配置。



 ©2025 Palo Alto Networks, Inc.

STEP 3 | 确认您提供的详细信息，然后单击 **Create**（创建）以开始虚拟机部署。

 ©2025 Palo Alto Networks, Inc.



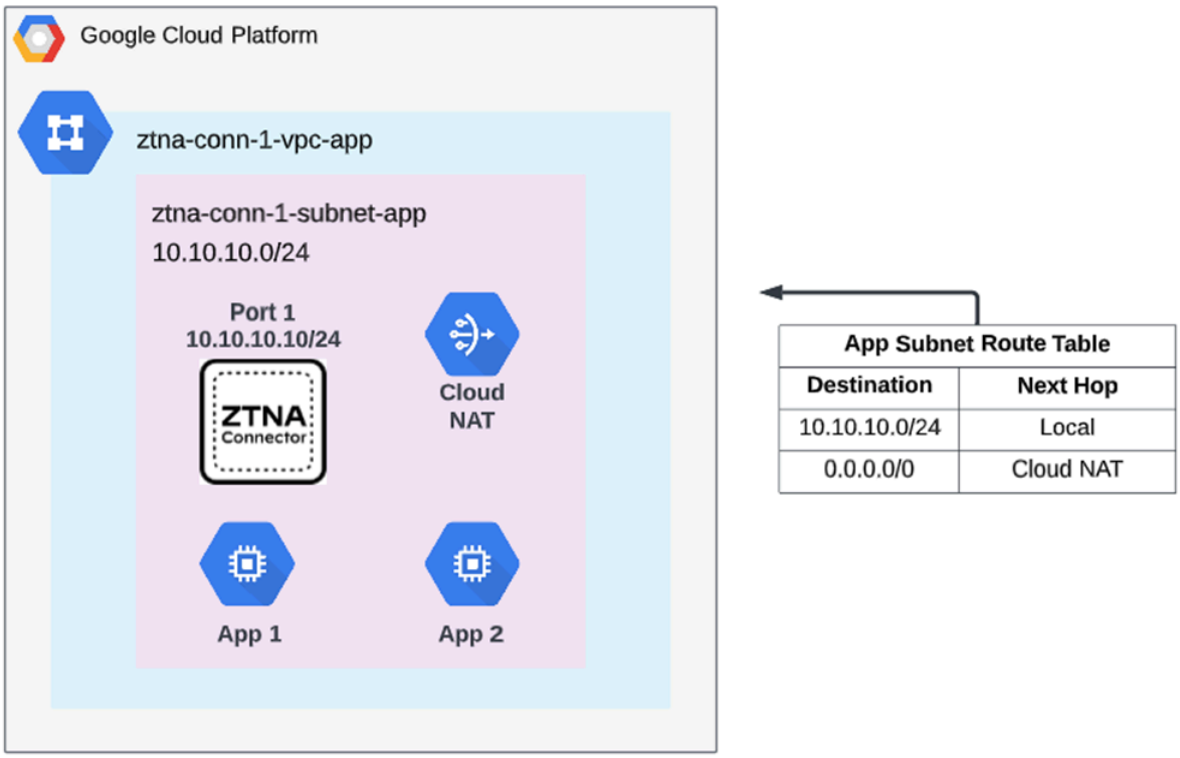
 ©2025 Palo Alto Networks, Inc.

STEP 4 | 部署完成后，请选择 **Go to resource**（转到资源）。

ZTNA 连接器支持的 Google Cloud Platform 部署

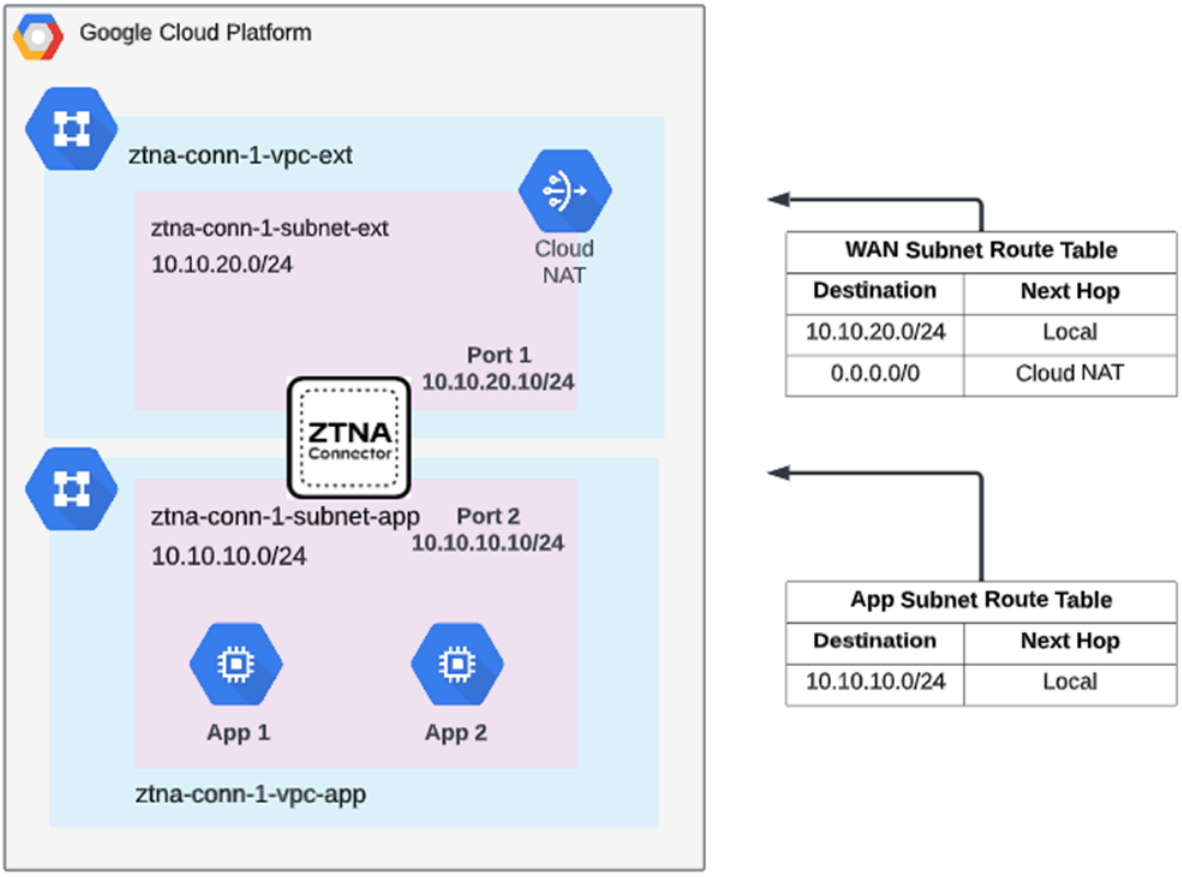
Google Cloud Platform (GCP) 中的 Prisma Access ZTNA 连接器网络部署支持两种部署，还支持每种部署对应的模板。

下图展示了在 GCP 中使用单臂模式和 NAT 网关进行 Prisma Access ZTNA 连接器部署的示例。



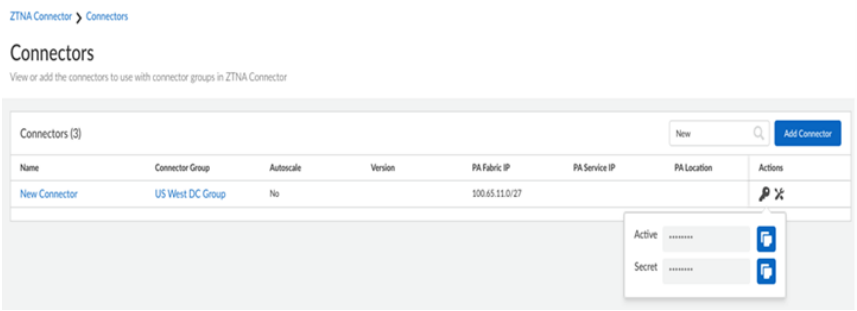
下图展示了在 GCP 中使用双臂模式和 NAT 网关进行 Prisma Access ZTNA 连接器部署的示例。

©2025 Palo Alto Networks, Inc.



在 Google Cloud Platform 中接入 ZTNA 连接器

- 查看要求和指南，以及为了在 Google Cloud Platform (GCP) 中使用 Prisma Access ZTNA 连接器而需要配置的 FQDN 和端口。
- 在Prisma SASE 平台上，检索并复制连接器密钥和机密值：在 **Workflows**（工作流） > **ZTNA Connector**（**ZTNA** 连接器） > **Connectors**（连接器）中，找到您在 Prisma Access 中创建的要与该虚拟机关联的连接器对象，选择 **Copy Token**（复制令牌）；然后，复制 **Key**（密钥） 和 **Secret**（机密）值。



满足所有先决条件后，请按照以下步骤在 GCP 中接入 Prisma Access ZTNA 连接器。

STEP 1 | 转到 GCP Marketplace，然后搜索 **Prisma Access ZTNA** 连接器。

 ©2025 Palo Alto Networks, Inc.

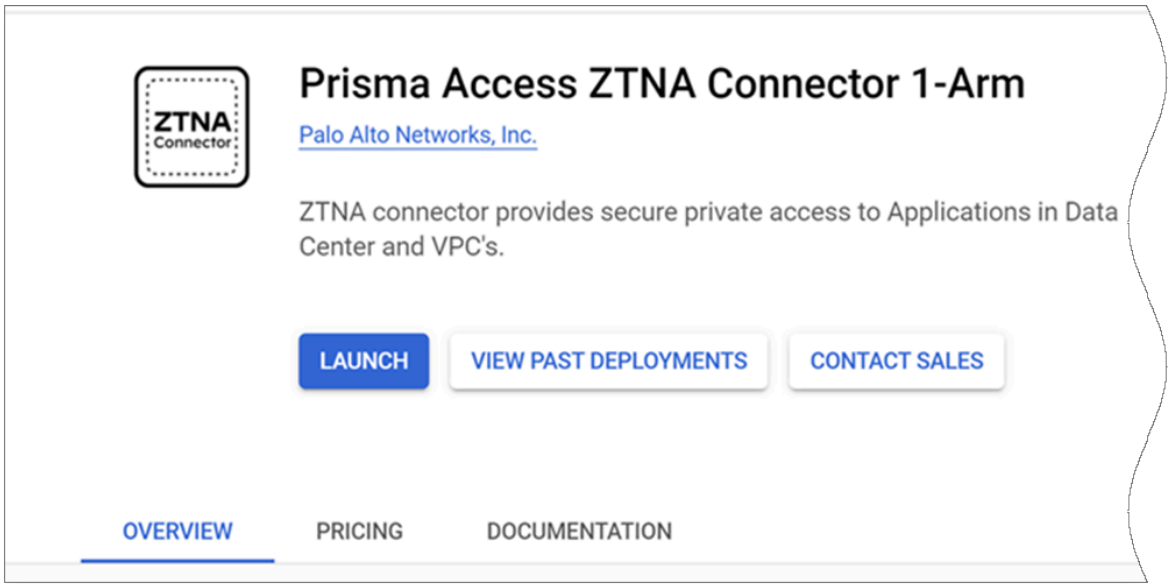
STEP 2 | 选择最适合您需求的软件计划。

- Prisma Access ZTNA 连接器单臂
- Prisma Access ZTNA 连接器双臂

在 **GCP** 中部署 **ZTNA** 连接器单臂

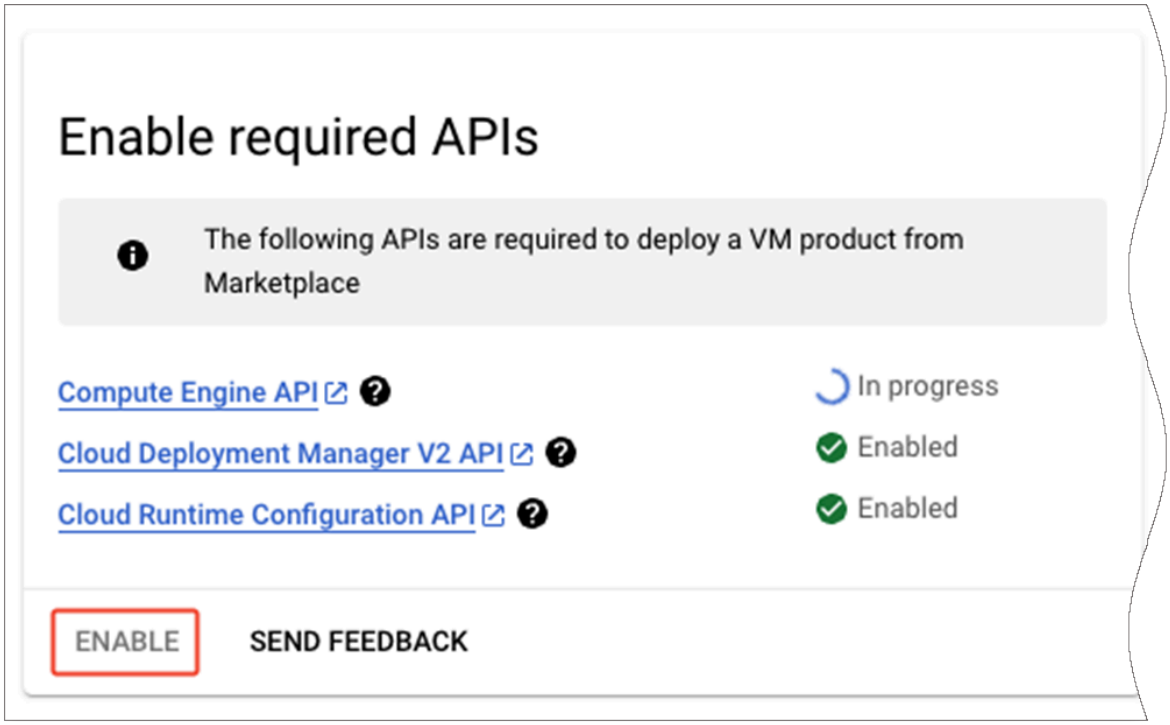
按照以下步骤在 GCP 中部署 ZTNA 连接器单臂：

STEP 1 | 单击 **LAUNCH**（启动）以配置 ZTNA 连接器单臂。



 ©2025 Palo Alto Networks, Inc.

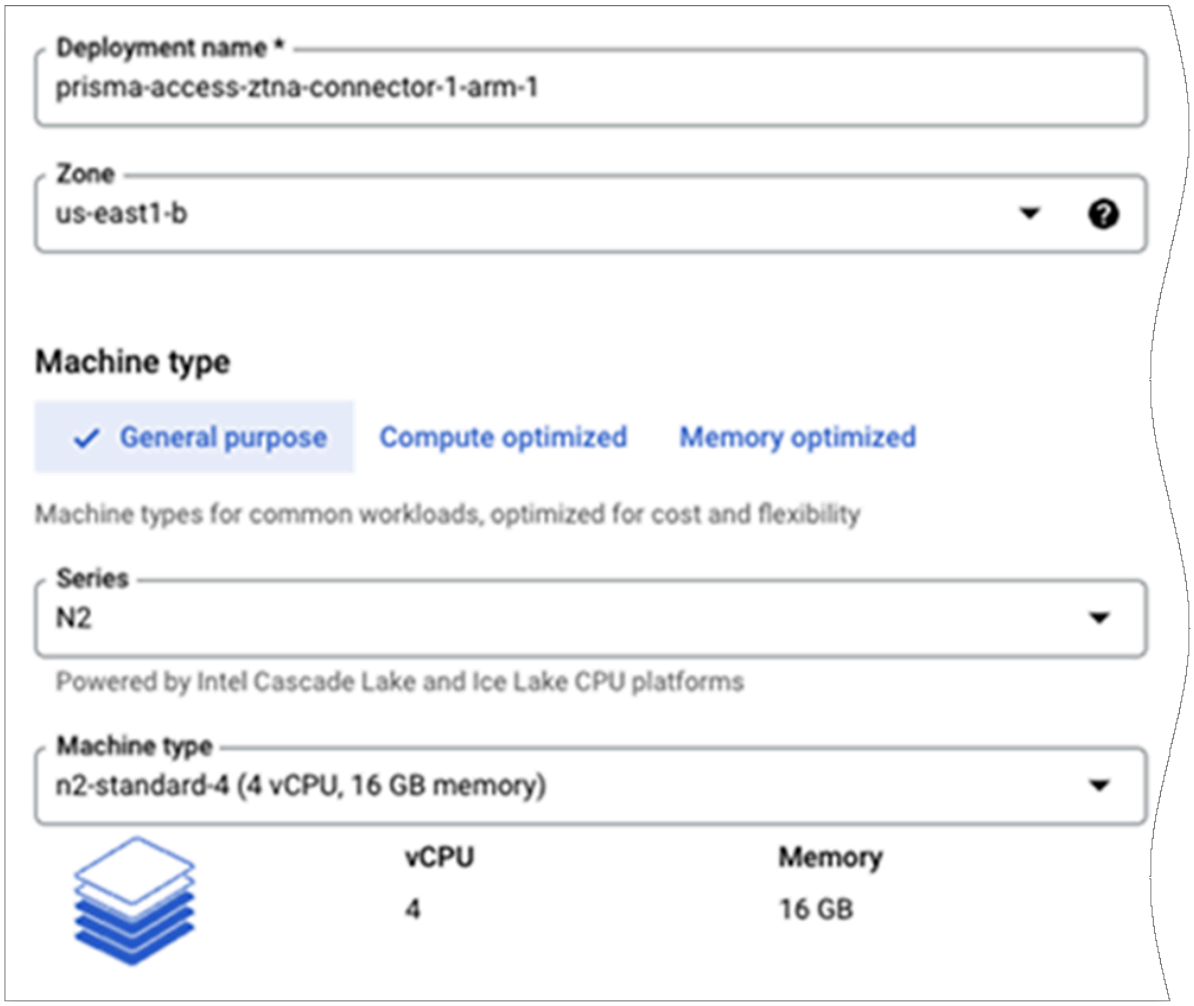
STEP 2 | （可选）单击 **Enable**（启用）以启用从 Marketplace 部署虚拟机所需的 GCP API。



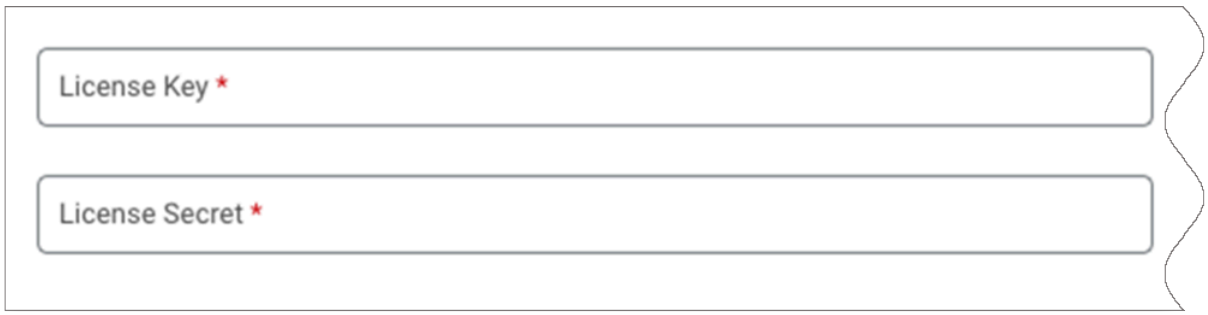
©2025 Palo Alto Networks, Inc.

STEP 3 | 配置以下设置：

- 在 **Deployment Name**（部署名称）中输入可用于标识虚拟机的部署名称。
- 选择 **Zone**（区域），其中包含了此连接器所在的应用程序。
- 对于 **Machine type**（机器类型），使用默认值。此连接器的限定机器类型是 **n2-standard-4**。

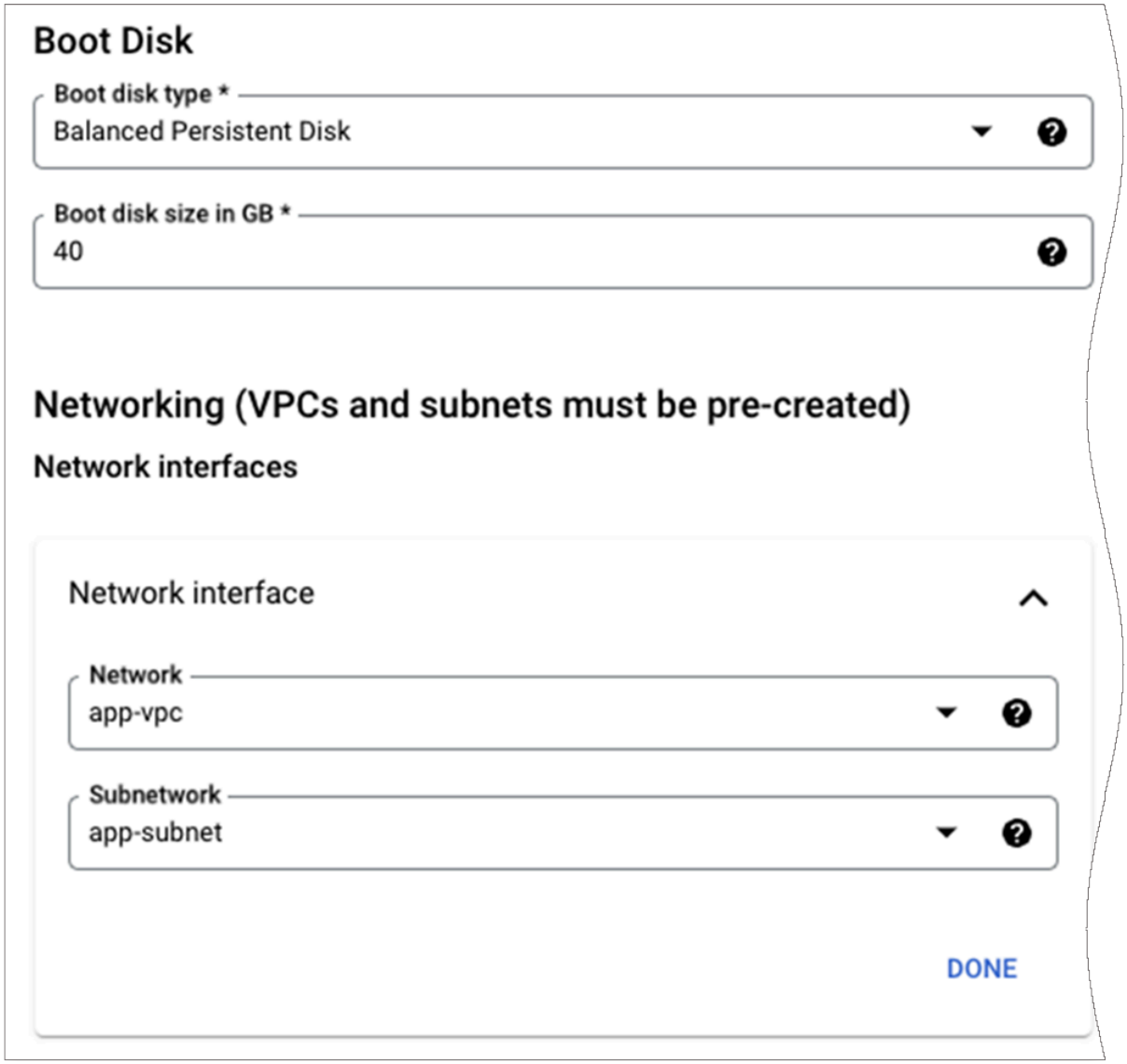


- 输入您从 Prisma SASE 门户获取的 **Prisma ZTNA Connector License Key**（**ZTNA** 连接器许可证密钥）和 **Prisma ZTNA Connector License Secret**（**ZTNA** 连接器许可证机密）值。



 ©2025 Palo Alto Networks, Inc.

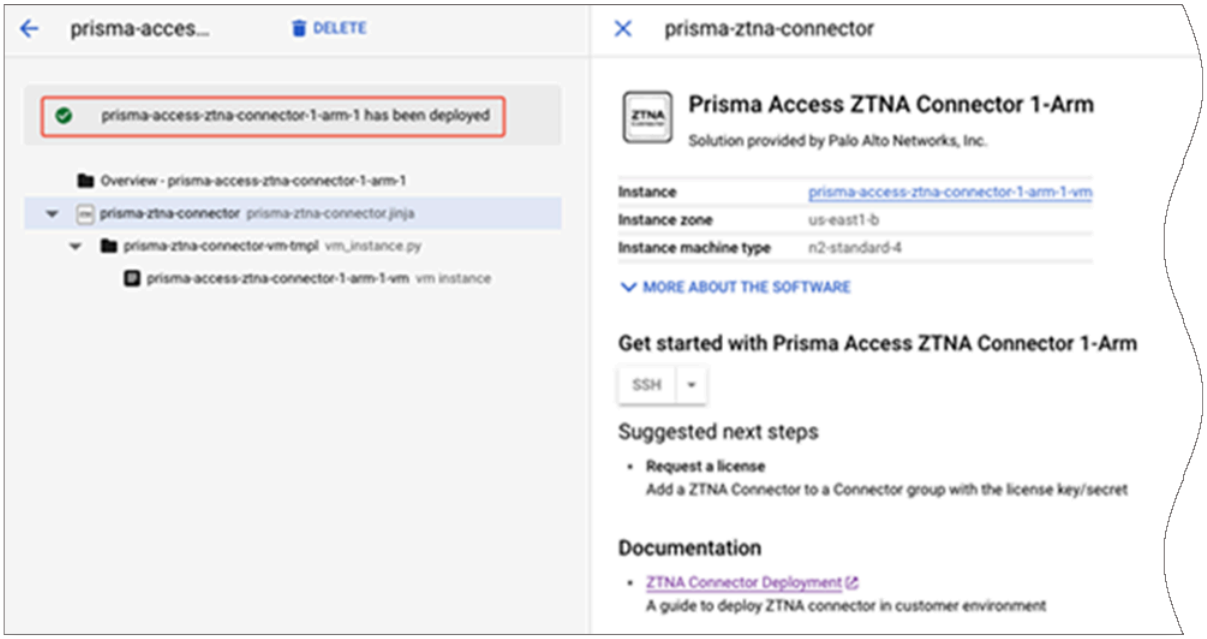
- 在 **Boot Disk**（启动磁盘）部分中，配置以下参数：
  - 使用默认的 **Boot disk type**（启动磁盘类型）。
  - 对于 **Boot disk size in GB**（启动磁盘大小 **(GB)**），选择 **40 GB**。
- 展开 **Networking (VPCs and subnets must be pre-created)**（网络（必须预先创建 **VPC** 和子网））部分，然后选择 **Network interface**（网络接口）详细信息。
  - 选择包含您创建的子网的 **Network**（网络）。
  - 选择虚拟机要使用的 **Subnetwork**（子网）。



STEP 4 | 单击 **Done**（完成）。

©2025 Palo Alto Networks, Inc.

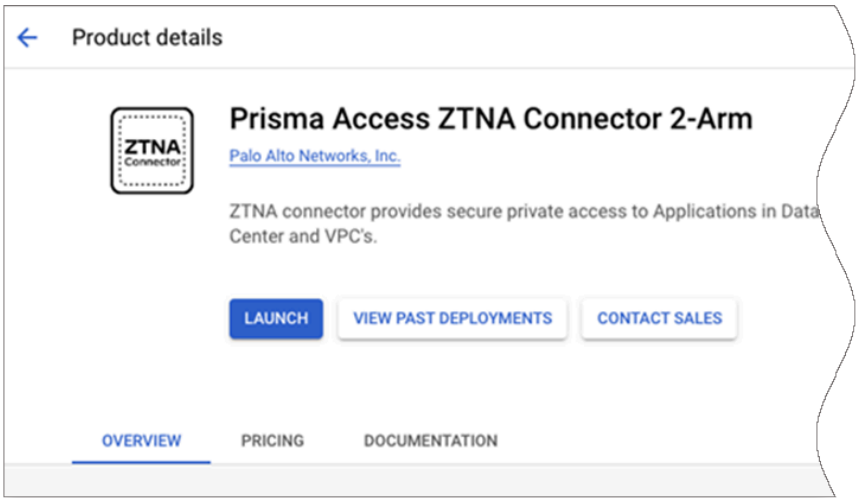
STEP 5 | 单击 **Deploy**（部署）以完成接入流程。



在 **GCP** 中部署 **ZTNA** 连接器双臂

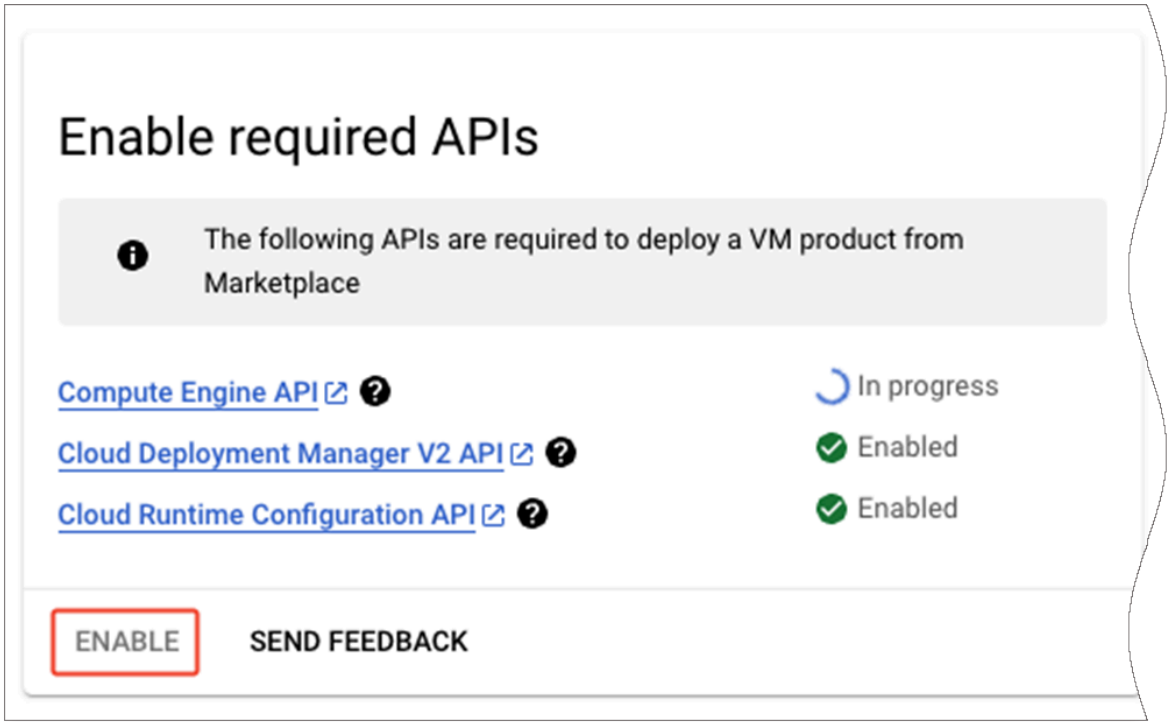
按照以下步骤在 GCP 中部署 ZTNA 连接器：

STEP 1 | 选择 **LAUNCH**（启动）以进行配置。



 ©2025 Palo Alto Networks, Inc.

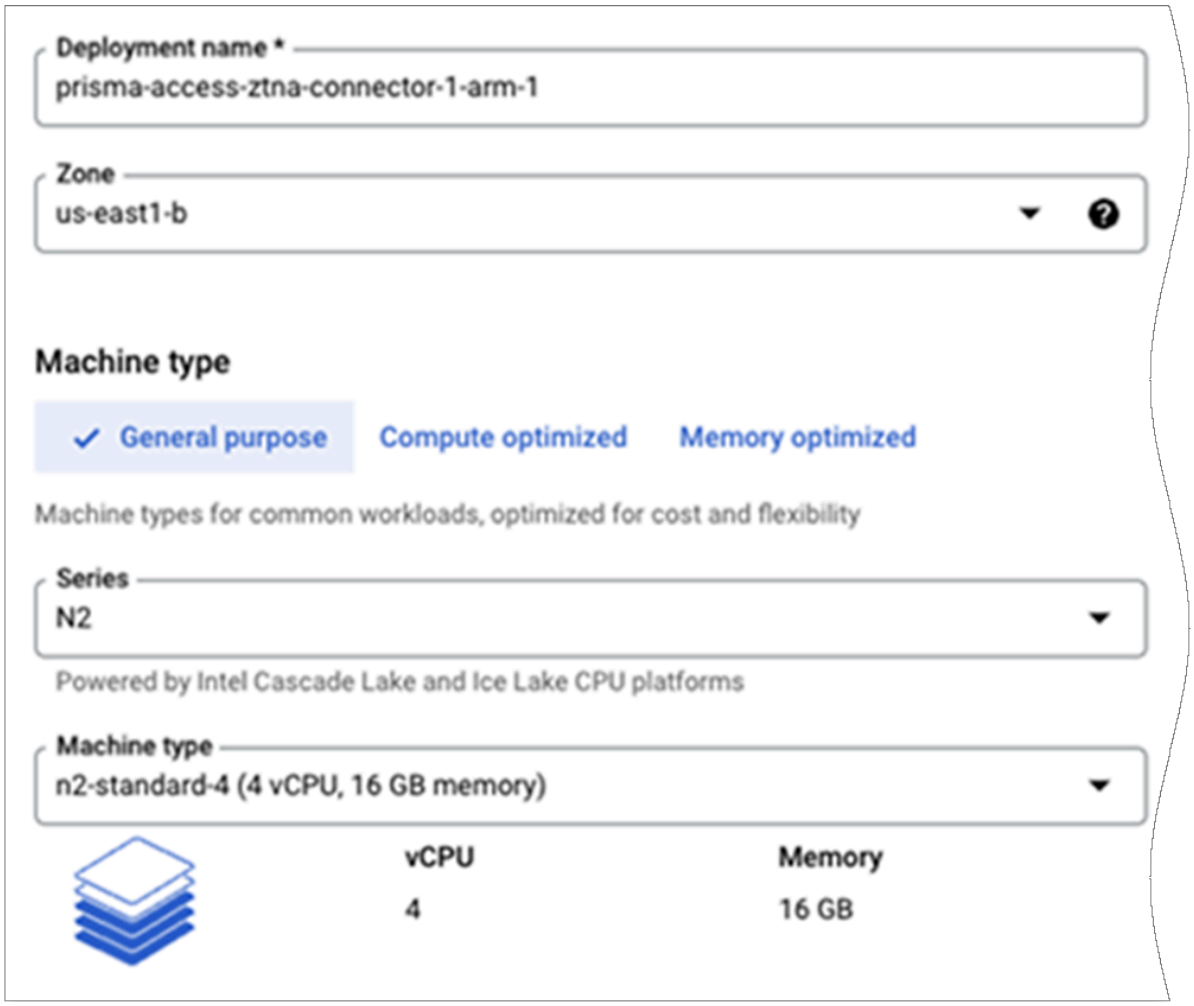
STEP 2 | （可选）单击 **Enable**（启用）以启用从 Marketplace 部署虚拟机所需的 API。



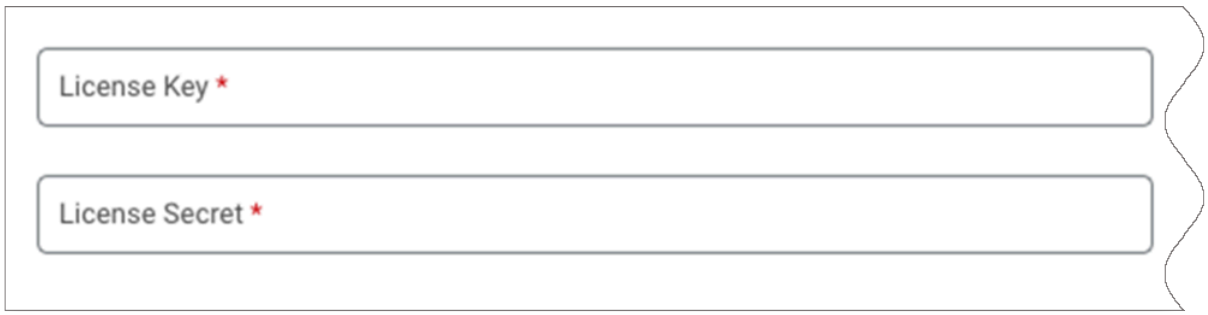
©2025 Palo Alto Networks, Inc.

STEP 3 | 配置以下设置：

- 在 **Deployment Name**（部署名称）中输入可用于标识虚拟机的部署名称。
- 选择 **Zone**（区域），其中包含了此连接器所在的应用程序。
- 对于 **Machine type**（机器类型），使用默认值。此连接器的限定机器类型是 **n2-standard-4**。

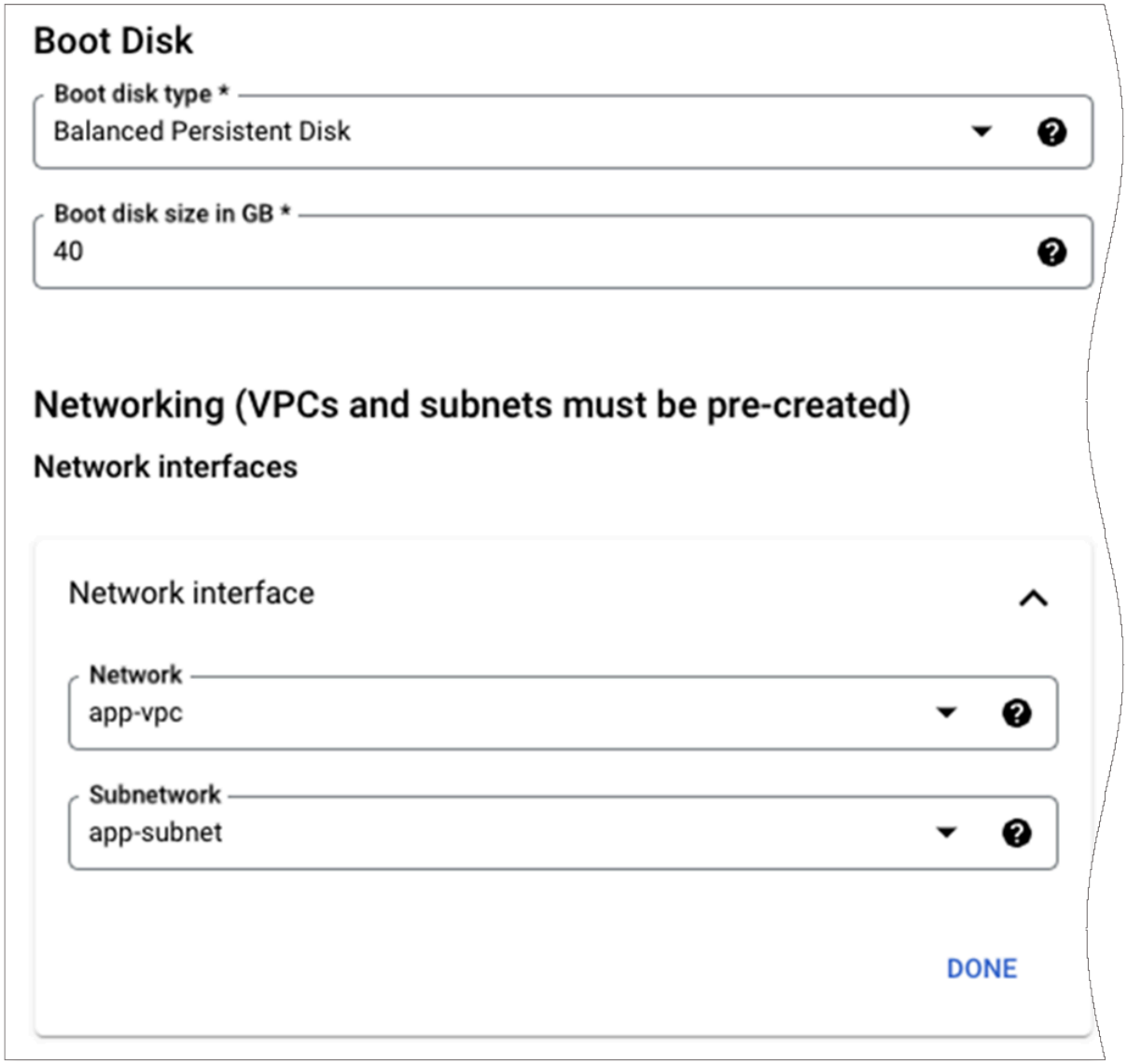


- 输入您从 Prisma SASE 门户获取的 **Prisma ZTNA Connector License Key**（**ZTNA** 连接器许可证密钥）和 **Prisma ZTNA Connector License Secret**（**ZTNA** 连接器许可证机密）值。



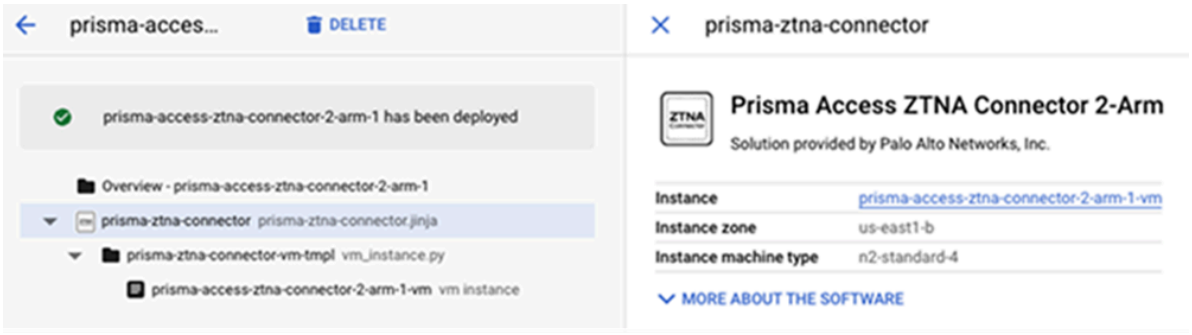
 ©2025 Palo Alto Networks, Inc.

- 在 **Boot Disk**（启动磁盘）部分中：
  - 使用默认的 **Boot disk type**（启动磁盘类型）。
  - 对于 **Boot disk size in GB**（启动磁盘大小 **(GB)**），选择 **40 GB**。
- 展开 **Networking (VPCs and subnets must be pre-created)**（网络（必须预先创建 **VPC** 和子网））部分，然后选择 **Network interface**（网络接口）详细信息。
  - 选择包含您创建的子网的 **Network**（网络）。
  - 选择虚拟机要使用的 **Subnetwork**（子网）。



 ©2025 Palo Alto Networks, Inc.

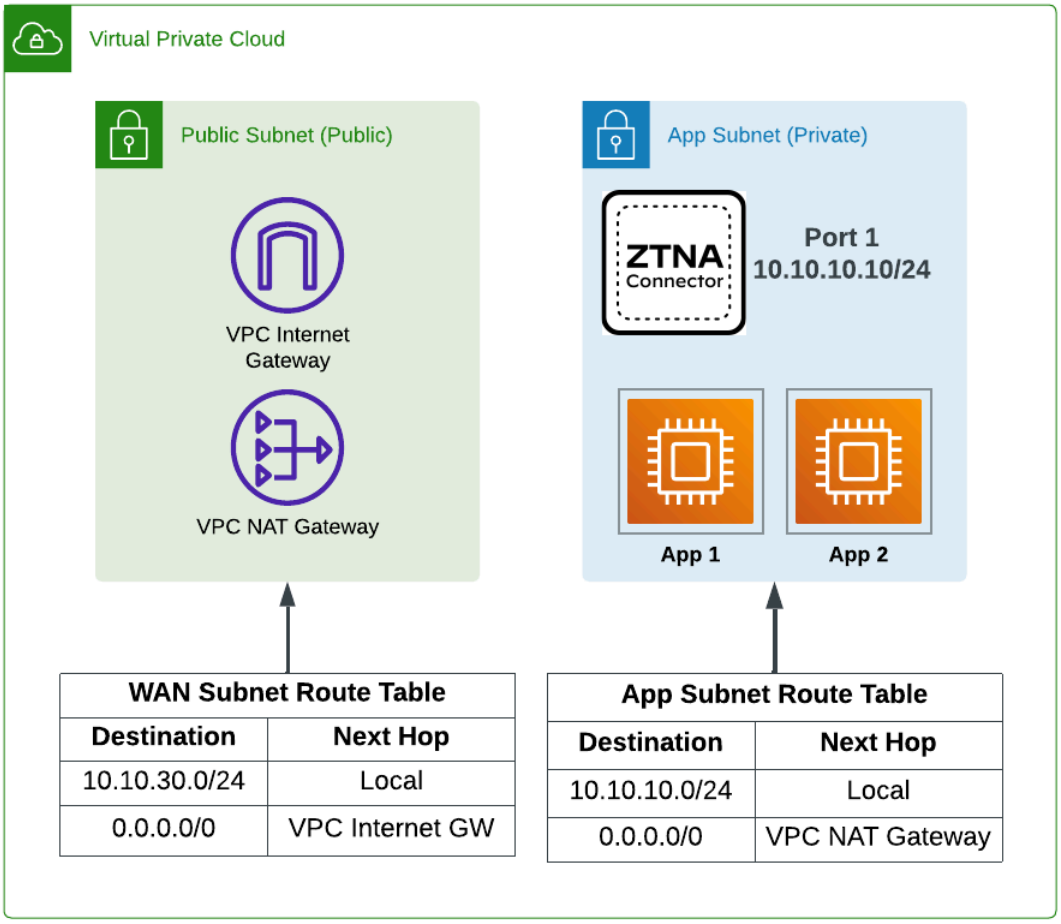
STEP 4 | 单击 **Deploy**（部署）以完成接入流程。



ZTNA 连接器支持的 Amazon Web Services 部署

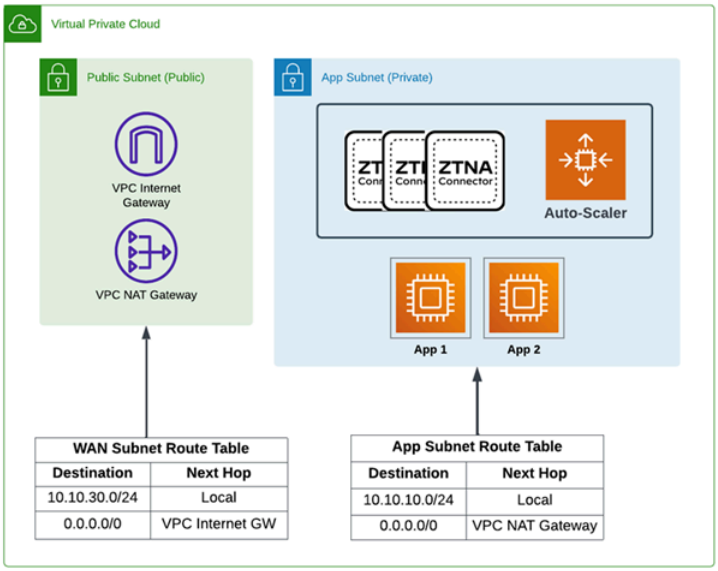
Amazon Web Services (AWS) 中的 Prisma Access ZTNA 连接器网络部署支持三种部署，每种部署都有一个对应的模板。

下图展示了在 AWS 中使用单臂模式和 NAT 网关进行 Prisma Access ZTNA 连接器部署的示例。

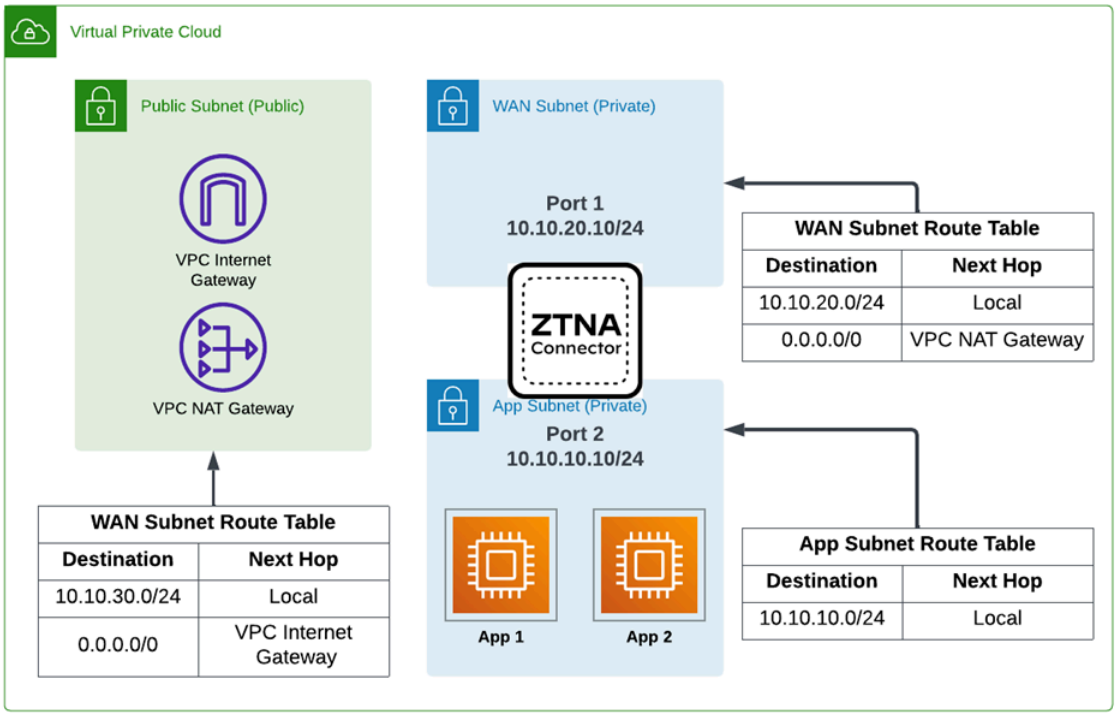


下图展示了在 AWS 中使用单臂自动缩放和 NAT 网关进行 ZTNA 连接器部署的示例。

©2025 Palo Alto Networks, Inc.



下图展示了在 AWS 中使用双臂模式和 NAT 网关进行 ZTNA 连接器部署的示例。

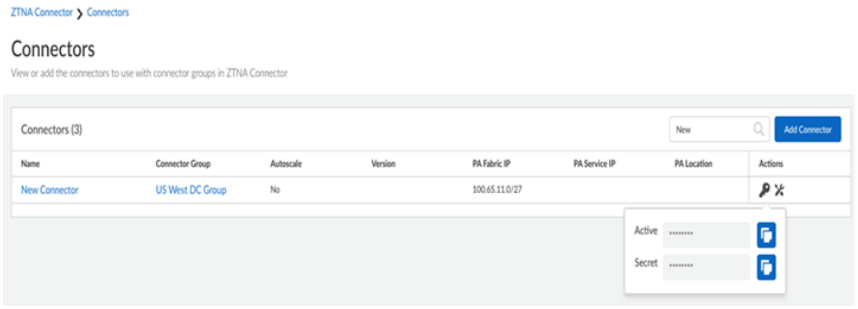


在 Amazon Web Services 中接入 ZTNA 连接器

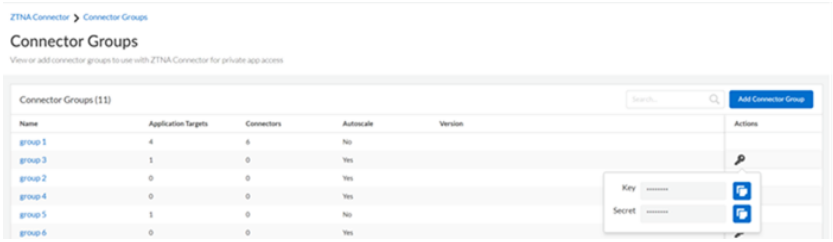
- 查看要求和指南，以及为了在 Amazon Web Services (AWS) 中使用 ZTNA 连接器而需要配置的 FQDN 和端口。
- 在Prisma SASE 平台上，检索并复制连接器密钥和机密值：在 **Workflows**（工作流） > **ZTNA Connector**（**ZTNA** 连接器） > **Connectors**（连接器）中，找到您在 Prisma Access 中创建的要

©2025 Palo Alto Networks, Inc.

与该虚拟机关联的连接器对象，选择 **Copy Token**（复制令牌）；然后，复制 **Key**（密钥）和 **Secret**（机密）值。



- 对于 **Prisma Access ZTNA** 连接器单臂自动扩展部署，必须检索并复制连接器组密钥和机密值在 **Workflows**（工作流） > **ZTNA Connector**（**ZTNA** 连接器） > **Connectors Groups**（连接器组）中，找到您在 Prisma Access 中创建的要与该虚拟机关联的连接器对象，选择 **Copy Token**（复制令牌）；然后，复制 **Key**（密钥）和 **Secret**（机密）值。



满足所有先决条件后，请按照以下步骤在 AWS 中接入 Prisma Access ZTNA 连接器。

STEP 1 | 转到 AWS Marketplace 并搜索 **Prisma Access ZTNA Connector**（**Prisma Access ZTNA** 连接器）。

STEP 2 | 选择最适合您需求的软件计划。

- Prisma Access ZTNA 连接器单臂
- Prisma Access ZTNA 连接器单臂自动扩展
- Prisma Access ZTNA 连接器双臂

在 **AWS** 中部署 **ZTNA** 连接器单臂

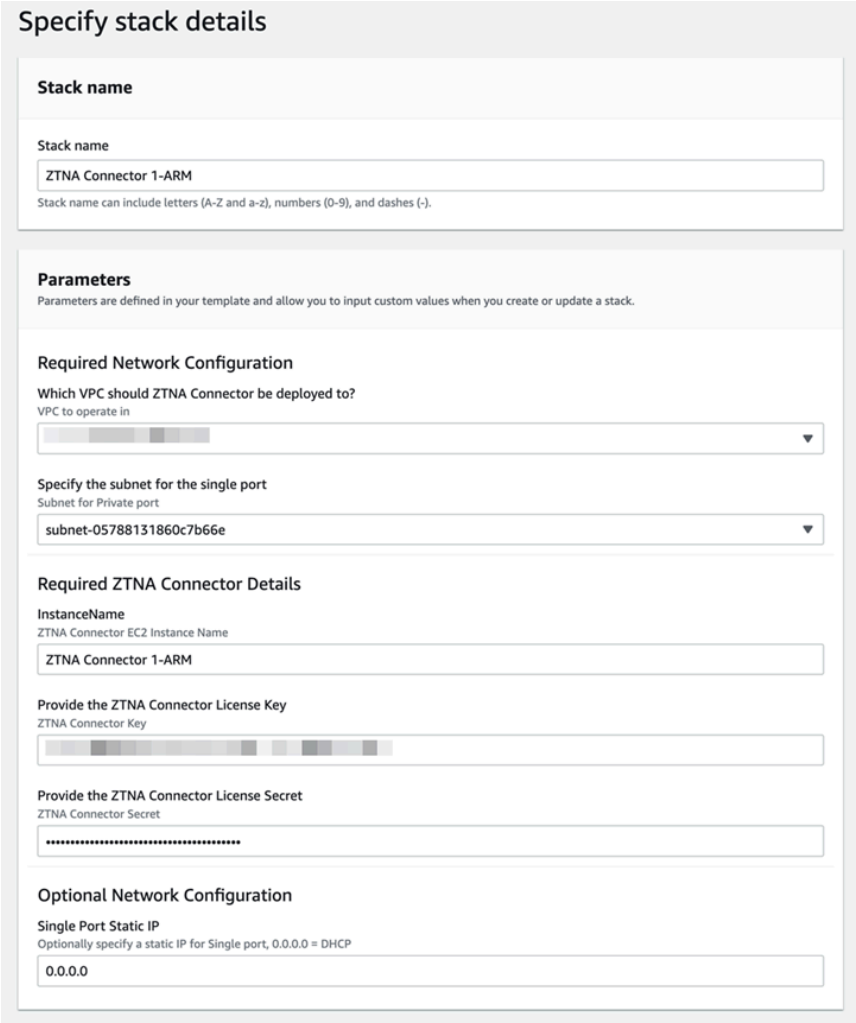
按照以下步骤在 AWS 中部署 ZTNA 连接器单臂。

STEP 1 | 选择 **Prisma Access ZTNA** 连接器单臂云信息模板。

©2025 Palo Alto Networks, Inc.

STEP 2 | 在 **Specify stack details**（指定堆栈详细信息）页上配置以下参数：

- 在 **Stack name**（堆栈名称）中输入堆栈名称以标识堆栈。
- 在 **Parameters**（参数）部分中，指定堆栈模板中定义的参数。
  - 选择 **Which VPC should ZTNA Connector be deployed to**（**ZTNA** 连接器应部署到哪个 **VPC**）。
  - 指定单个端口的子网，您在其中配置了要接入此连接器的应用程序。您需要通过 NAT 网关从该子网访问互联网。
- 输入您从 Prisma SASE 门户获取的 Prisma **ZTNA Connector License Key**（**ZTNA** 连接器许可证密钥）和 Prisma **ZTNA Connector License Secret**（**ZTNA** 连接器许可证机密）值。



在 AWS 中部署具有自动缩放功能的 ZTNA 连接器单臂

按照以下步骤在 AWS 中部署具有自动缩放功能的 ZTNA 连接器单臂。

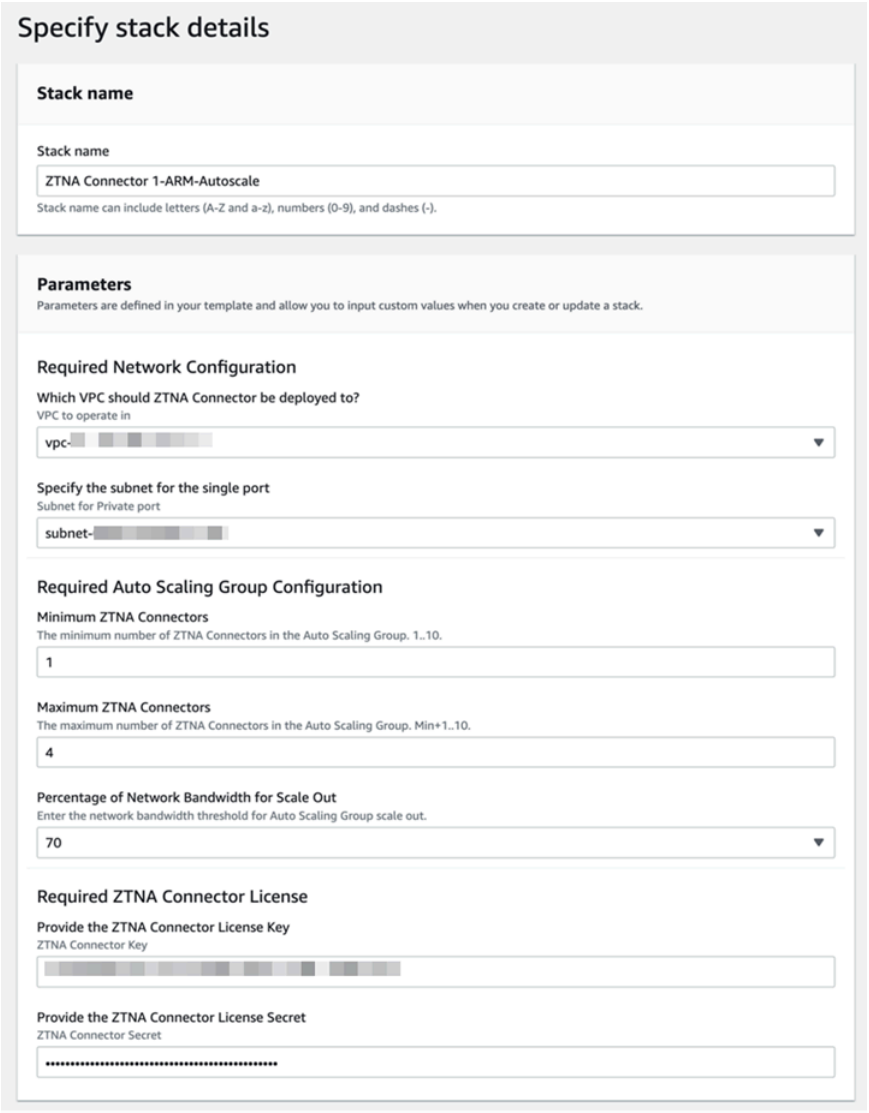
STEP 1 | 选择 **Prisma Access ZTNA** 连接器单臂自动缩放云信息模板。

 ©2025 Palo Alto Networks, Inc.

STEP 2 | 在 **Specify stack details**（指定堆栈详细信息）页上配置以下参数：

- 在 **Stack name**（堆栈名称）中输入部署的唯一堆栈名称。
- 在 **Parameters**（参数）部分中，指定堆栈模板中定义的参数。
  - 选择 **Which VPC should ZTNA Connector be deployed to**（**ZTNA** 连接器应部署到哪个 **VPC**）。
  - 指定单个端口的子网，您在其中配置了要接入此连接器的应用程序。您需要通过 NAT 网关从该子网访问互联网。
- 在 **Required Auto Scaling Group Configuration**（所需的自动扩展组配置）中：
  - 在自动扩展组中输入所需的 **Minimum ZTNA Connectors**（**ZTNA** 连接器最小数量）。
  - 在自动扩展组中输入所需的 **Maximum ZTNA Connectors**（**ZTNA** 连接器最大数量）。连接器组中允许的最大 ZTNA 连接器数量为 4。
  - 设置 **Percentage of Network Bandwidth for Scale Out**（用于横向扩展的网络带宽百分比）。默认值（也是推荐值）为 70%。
- 输入您从 Prisma SASE 门户获取的 Prisma **ZTNA Connector License Key**（**ZTNA** 连接器许可证密钥）和 **ZTNA Connector License Secret**（**ZTNA** 连接器许可证机密）值。

©2025 Palo Alto Networks, Inc.



在 **AWS** 中部署 **ZTNA** 连接器双臂

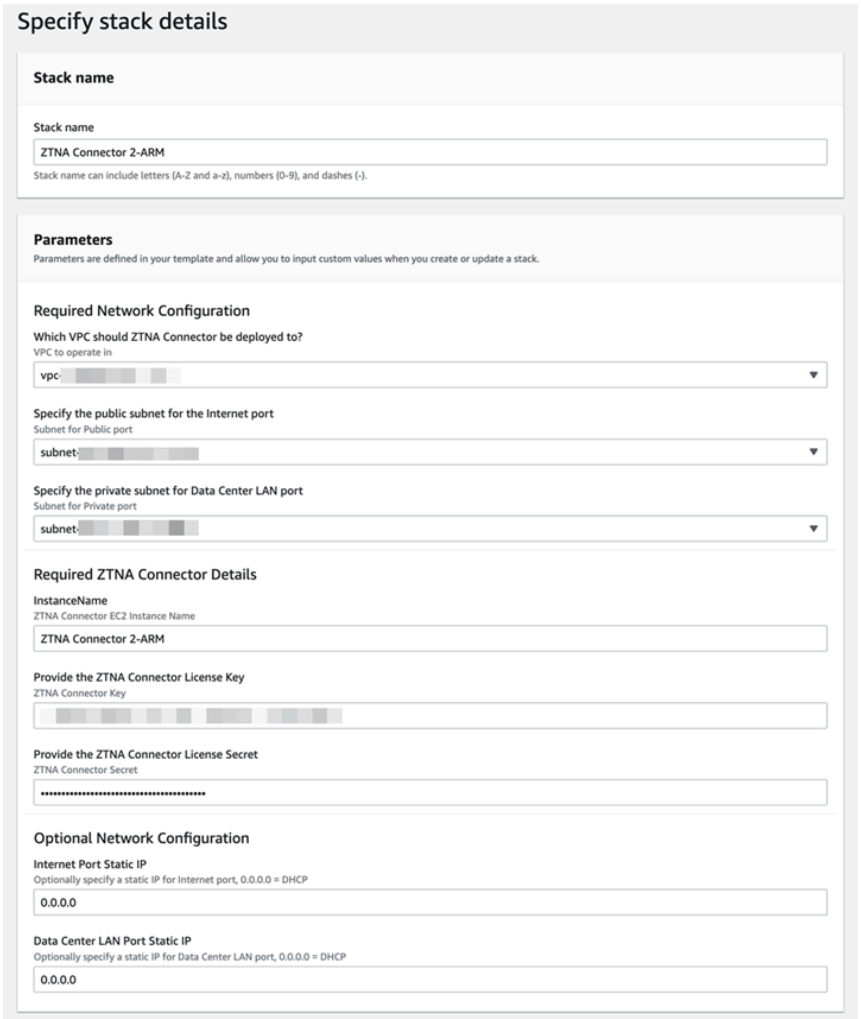
按照以下步骤在 AWS 中部署 ZTNA 连接器双臂。

STEP 1 | 选择 Prisma Access ZTNA 连接器单臂部署云信息模板。

©2025 Palo Alto Networks, Inc.

STEP 2 | 在 **Specify stack details**（指定堆栈详细信息）页中：

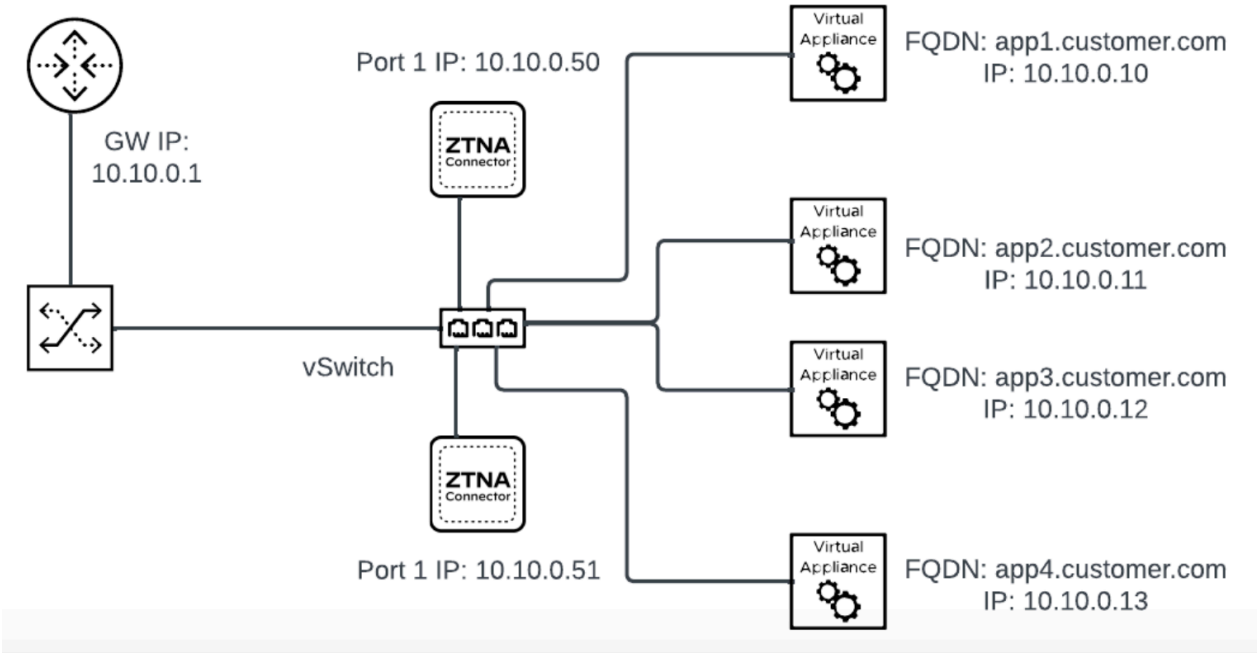
- 在 **Stack name**（堆栈名称）中输入部署的堆栈名称。
- 在 **Parameters**（参数）部分中，指定堆栈模板中定义的参数。
  - 选择 **Which VPC should ZTNA Connector be deployed to**（**ZTNA** 连接器应部署到哪个 **VPC**）。
  - 针对 WAN 与 IPSec 的连接，指定互联网端口的公共子网。此子网需要与 NAT 网关关联才能连接到互联网。
  - 指定数据中心 **LAN** 端口的专用子网，您已在其中配置了要接入此连接器的应用程序。
- 输入 **Instance Name**（实例名称）
- 输入您从 Prisma SASE 门户获取的 Prisma **ZTNA Connector License Key**（**ZTNA** 连接器许可证密钥）和 Prisma **ZTNA Connector License Secret**（**ZTNA** 连接器许可证机密）值。



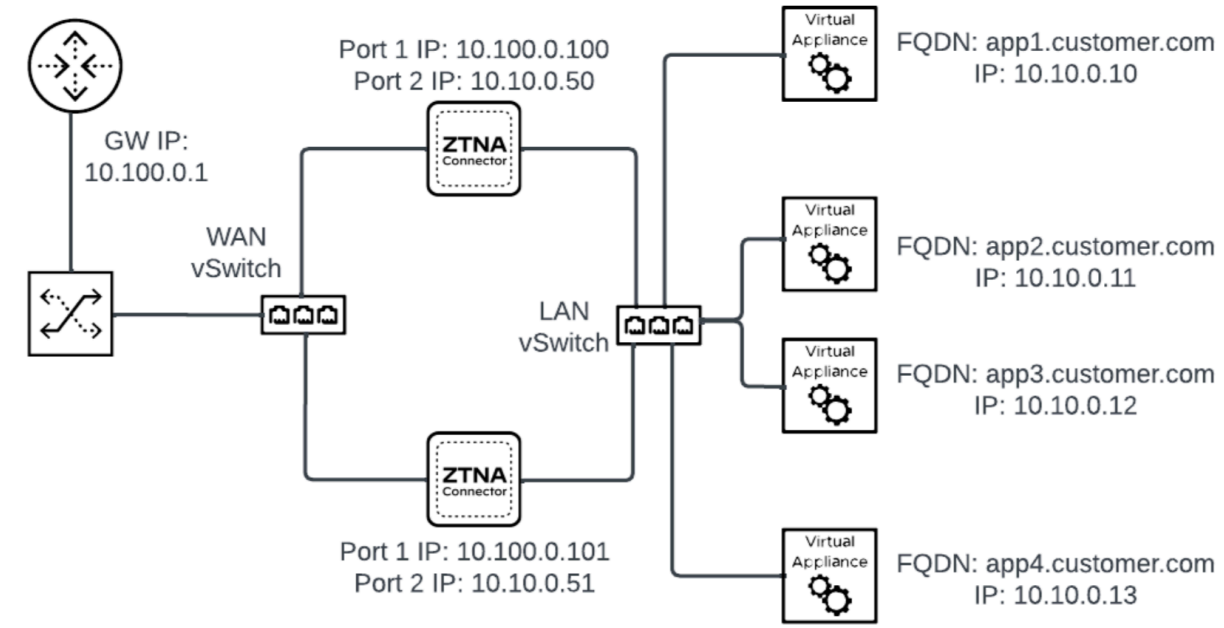
Prisma Access ZTNA 连接器支持的 VMware ESXi 部署

下图显示了使用 VMware ESXi 在单臂模式下与 NAT 网关结合使用的 ZTNA 连接器网络部署示例。

 ©2025 Palo Alto Networks, Inc.



下图显示了使用 VMware ESXi 在双臂模式下与 NAT 网关结合使用的 ZTNA 连接器网络部署示例。



在 VMware ESXi 中接入 ZTNA 连接器

要在 VMware ESXi 中接入 ZTNA 连接器，请完成以下步骤。在开始之前，请务必查看 ZTNA 的一般要求和指南，特别是 VMware ESXi 部署。

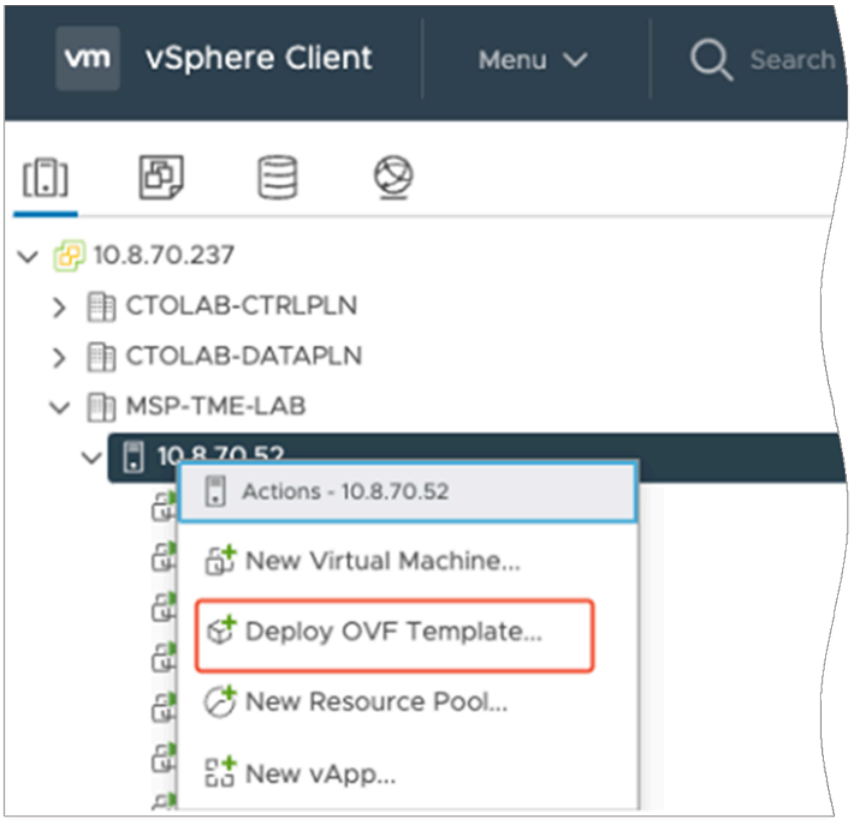
开始前，请查看要求和指南，以及为了在 VMware ESXi 中使用 ZTNA 连接器而需要配置的 FQDN 和端口。

©2025 Palo Alto Networks, Inc.

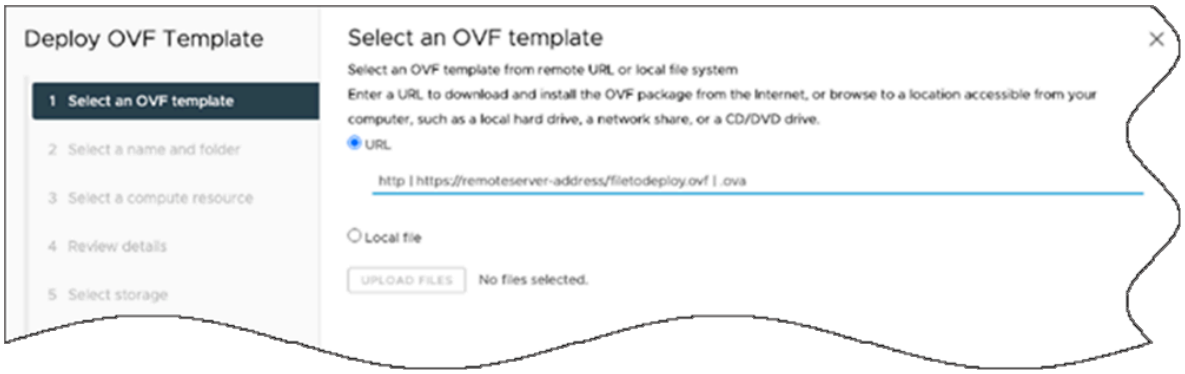
STEP 1 | 在客户支持门户 (CSP) 中，在 **Updates**（更新） > **Software Updates**（软件更新） > **Prisma Access ZTNA Connector for VMware**（适用于 **KVM** 的 **Prisma Access ZTNA** 连接器）下面下载 ZTNA 连接器 VMware ESXi 映像。

对于单臂部署，请下载 *1-nic* 版本文件；对于双臂部署，请下载 *2-nic* 版本文件。

STEP 2 | 打开 VMware vCenter，选择并右键单击主机，然后选择 **Deploy OVF Template**（部署 **OVF** 模板）。

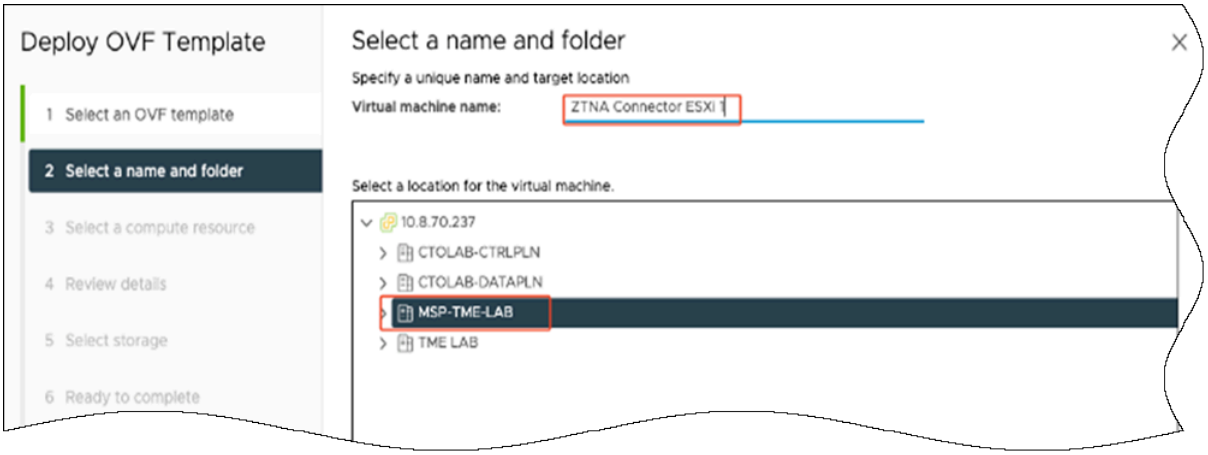


STEP 3 | 从连接器 OVA 中选择位置（URL 或本地文件），然后选择 **Next**（下一步）。

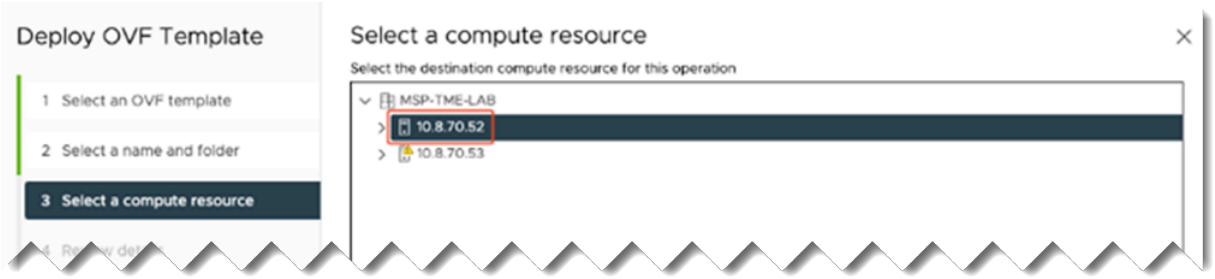


 ©2025 Palo Alto Networks, Inc.

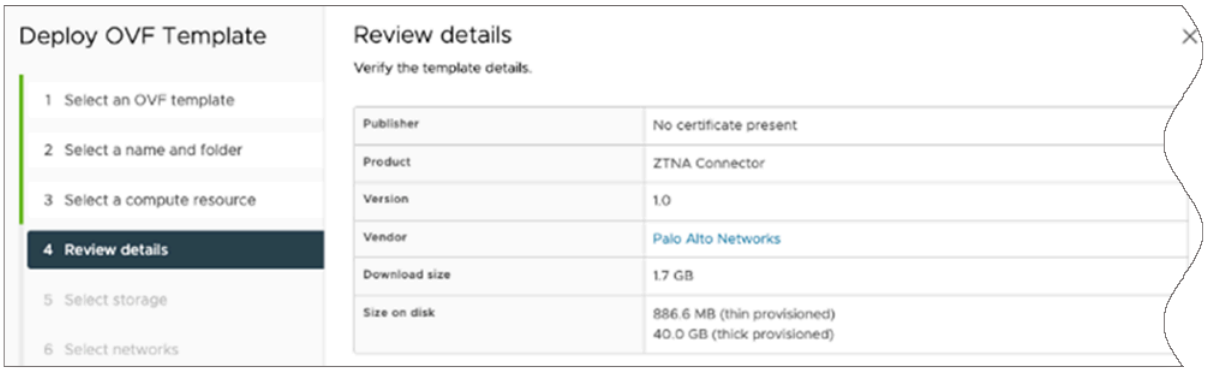
STEP 4 | 输入虚拟机 (VM) 的名称和位置。



STEP 5 | 选择虚拟机的计算资源。

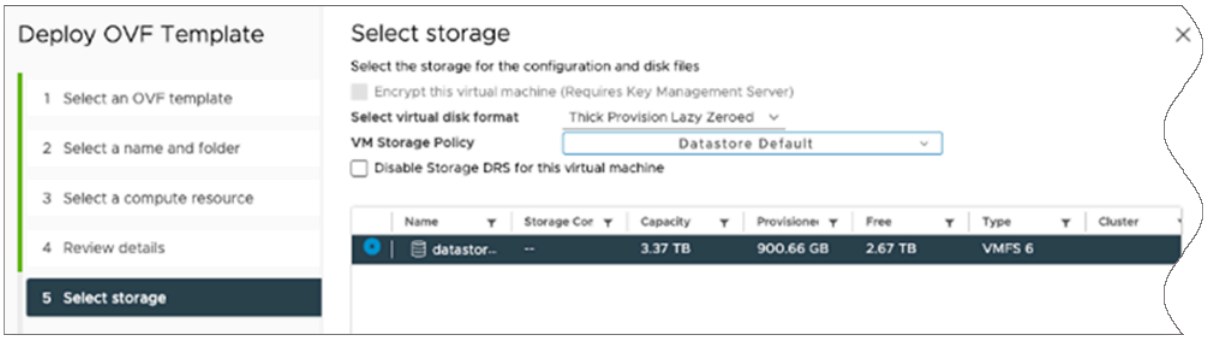


STEP 6 | 查看模板的详细信息，然后选择 **Next**（下一步）。



 ©2025 Palo Alto Networks, Inc.

STEP 7 | 选择 **Thick Provision Lazy Zeroed**（密集配置延迟置零）作为虚拟磁盘格式，并为 ZTNA 连接器 VM 选择适当的数据存储。



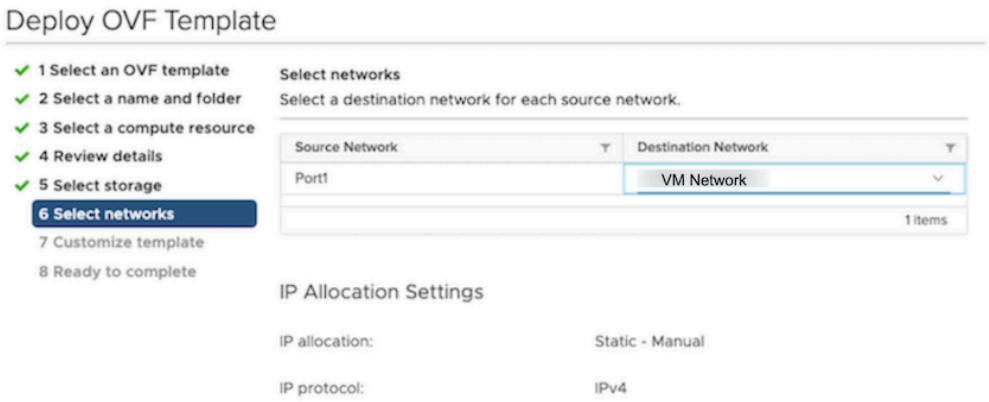
可选 选择 **Thin Provision**（精简配置）作为虚拟磁盘格式和 ZTNA 连接器虚拟机的适当数据存储，其中根据要求，服务器仅分配主机所需的空间。



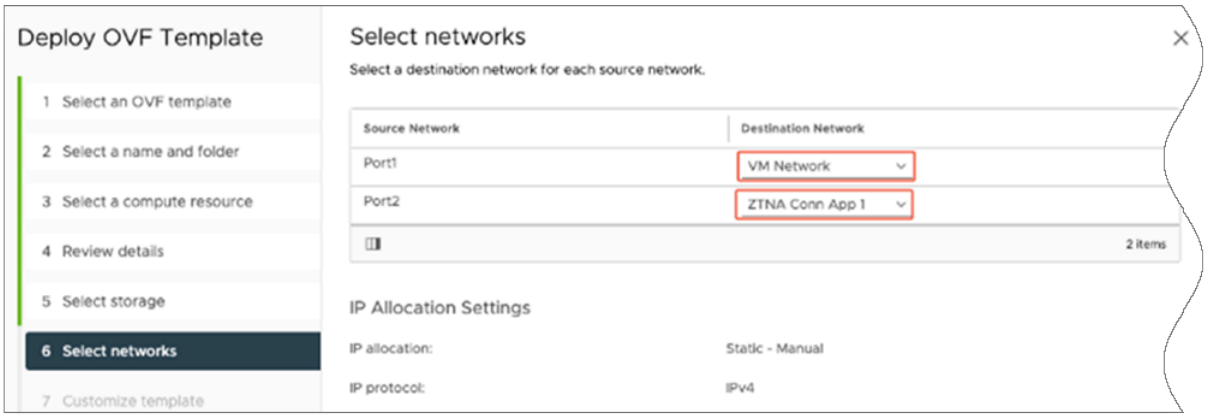
 ©2025 Palo Alto Networks, Inc.

STEP 8 | 为使用 OVA 配置模板创建的接口选择网络（用于端口 1 和端口 2）。

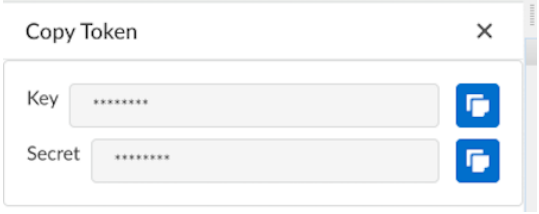
1. 如果您正在部署单臂连接器，**Port 1**（端口 **1**）是可连接到 WAN 和 LAN 应用服务器的网络。为 **Port 1**（端口 **1**）选择 WAN/LAN 网络。



2. 如果您正在部署双臂连接器，为 **Port 1**（端口 **1**）选择面向互联网的端口，为 **Port 2**（端口 **2**）选择面向应用服务器的网络。
   - 端口 1 是面向 Wan 的端口，用于到 Prisma Access 的 IPSec 连接。
   - 端口 2 是面向应用程序的端口。



STEP 9 | 如果您还未操作，请转到 **Workflows**（工作流） > **ZTNA Connector**（**ZTNA** 连接器） > **Connectors**（连接器），找到您在 Prisma Access 中创建且要与该虚拟机关联的连接器对象，从 **Actions**（操作）选项卡（钥匙图标）选择 **Copy Token**（复制令牌），然后复制 **Key**（密钥）和 **Secret**（机密）的值。



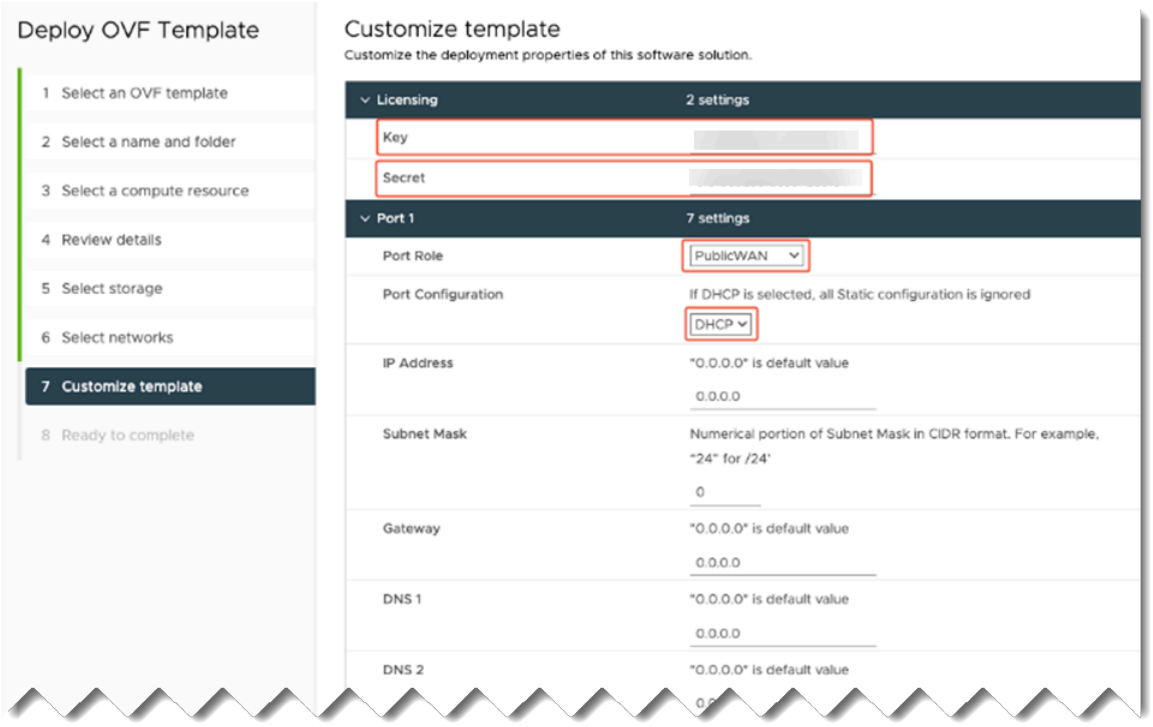
 ©2025 Palo Alto Networks, Inc.

STEP 10 | 在 **Customize template**（自定义模板）屏幕中，进行以下配置更改：

- **Licensing**（许可）区域—输入您从 Prisma SASE 门户检索到的 **Key**（密钥）和 **Secret**（机密）值。
- **Port 1**（端口 **1**）（面向 Prisma Access 的端口）区域—进行以下更改：
  - **Role**（角色）—公共 WAN。
  - **Port Configuration**（端口配置）—**DHCP** 或 **Static**（静态）。

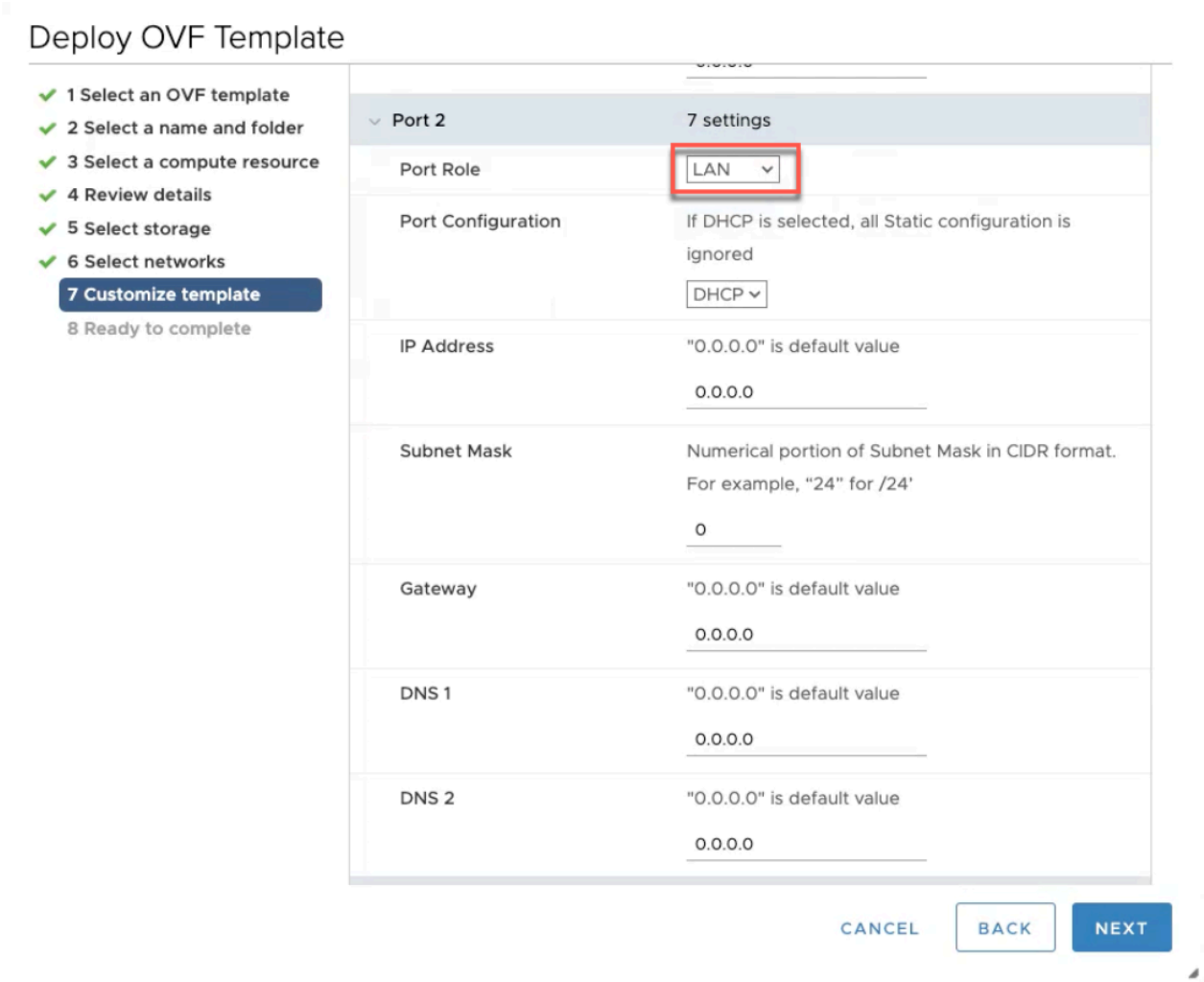
    如果选择 **Static**（静态），请输入 IP 地址、子网掩码、网关以及一个或两个 DNS 服务器值。

    如果使用 DHCP，请保留字段中的默认零，如以下屏幕截图所示。



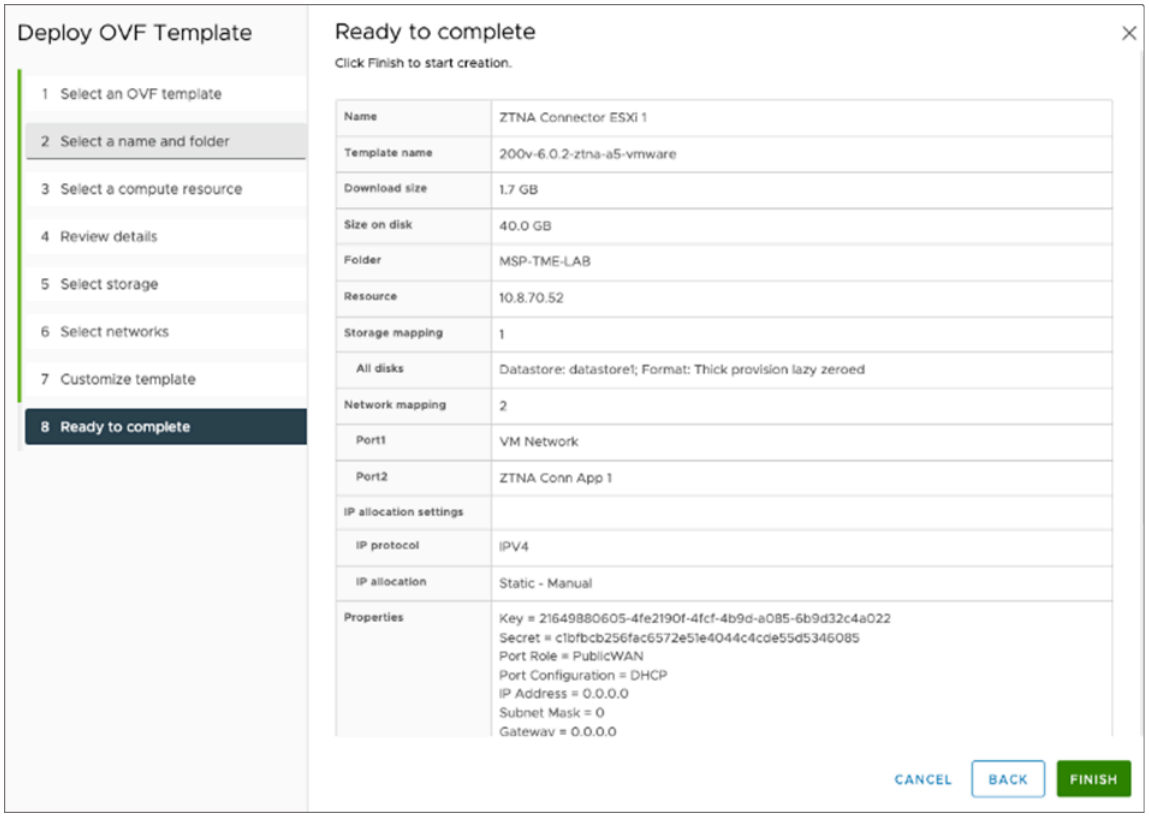
- 仅限双臂 ESXi 部署如果您进行的是双臂部署，使用与步骤 10 中应用于 **Port 1**（端口 **1**）的相同规则，来配置 **Port 2**（端口 **2**）的 LAN IP 接口。

 ©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.

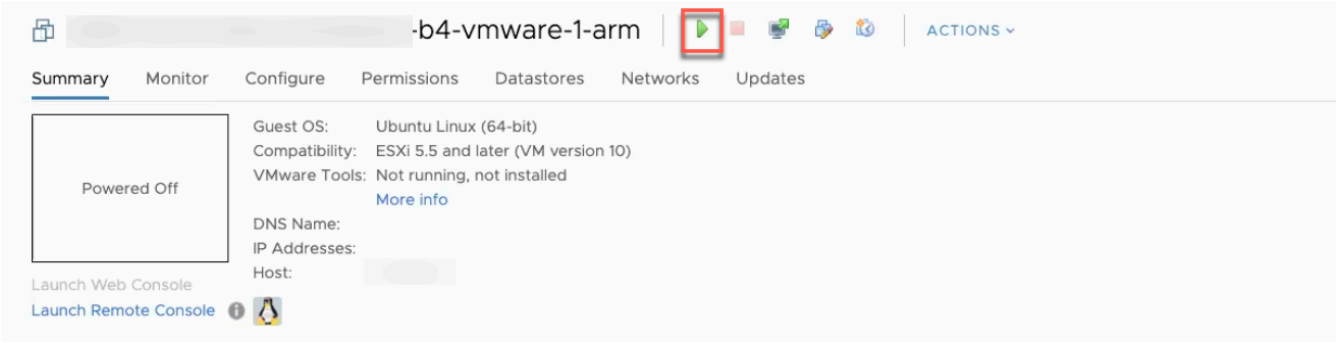
STEP 11 | 查看摘要，然后选择 **Finish**（完成）。



 ©2025 Palo Alto Networks, Inc.

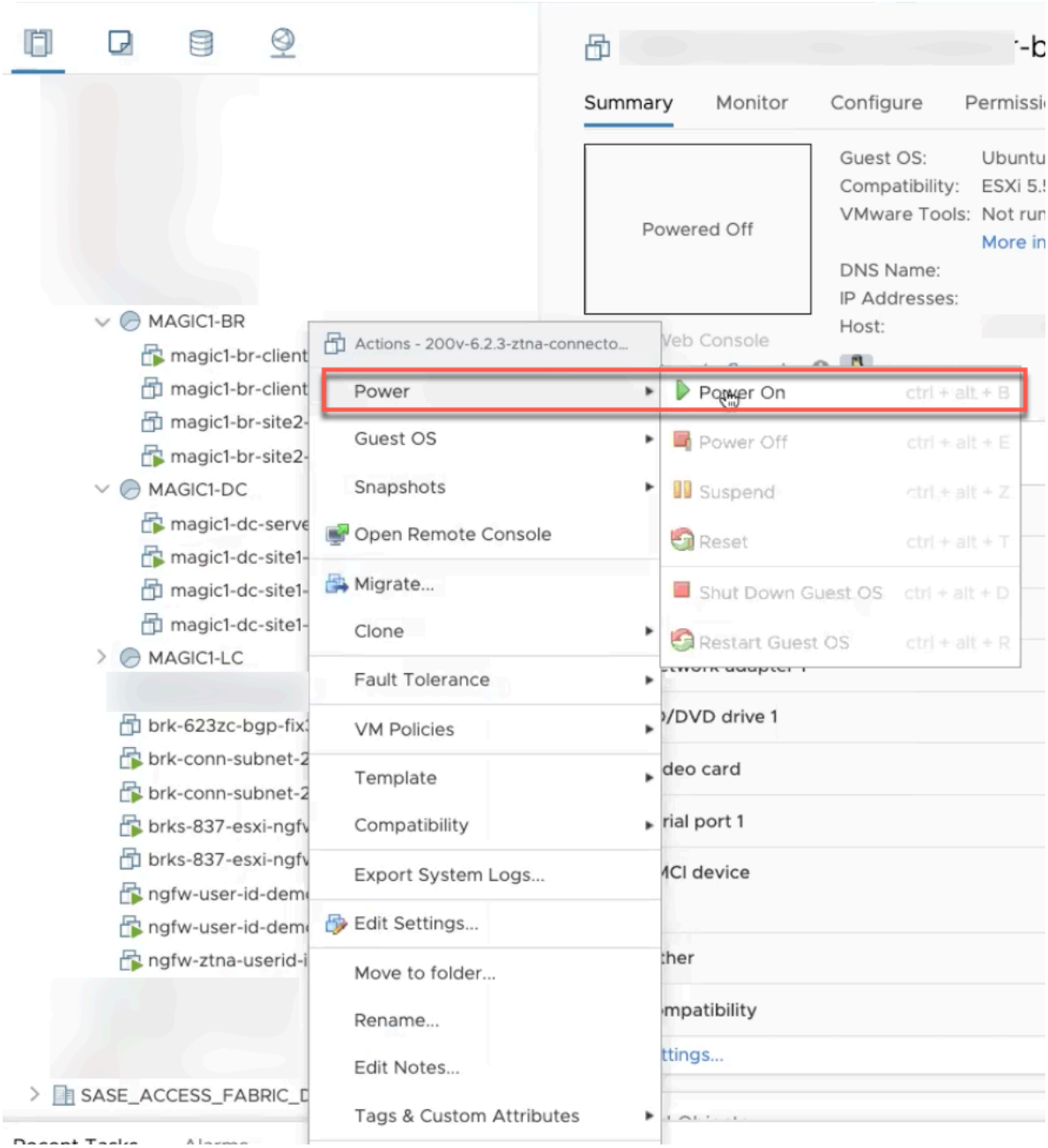
STEP 12 | 使用以下方法之一启动虚拟机。

- 选择 **Power On**（启动）来启动虚拟服务器。



- 右键单击接口，并选择 **Power On**（启动）（**Power**（电源） > **Power On**（启动））。

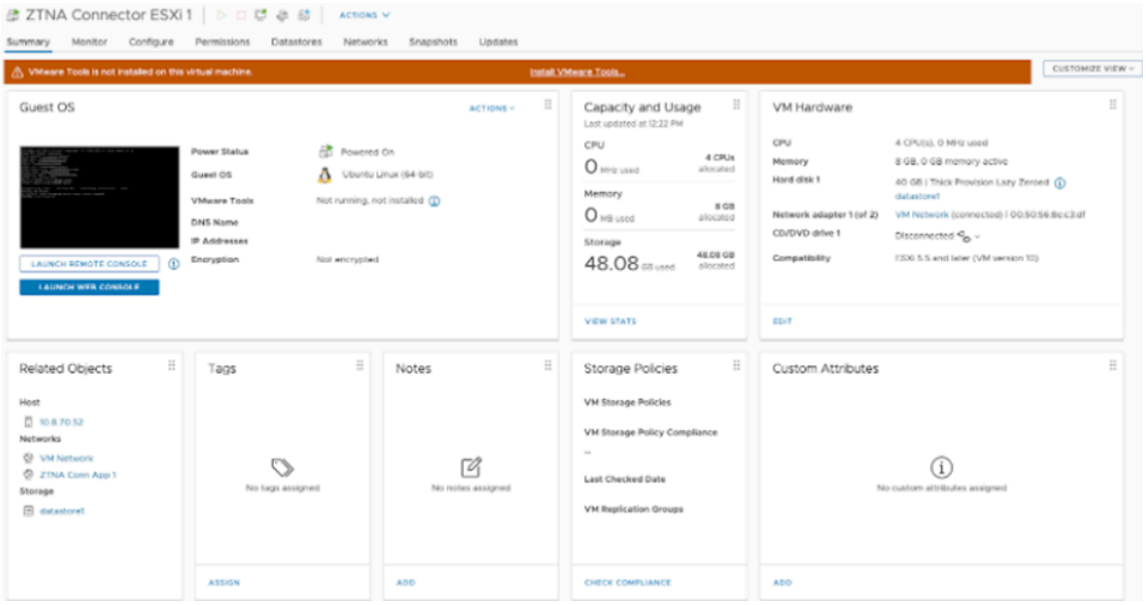
©2025 Palo Alto Networks, Inc.



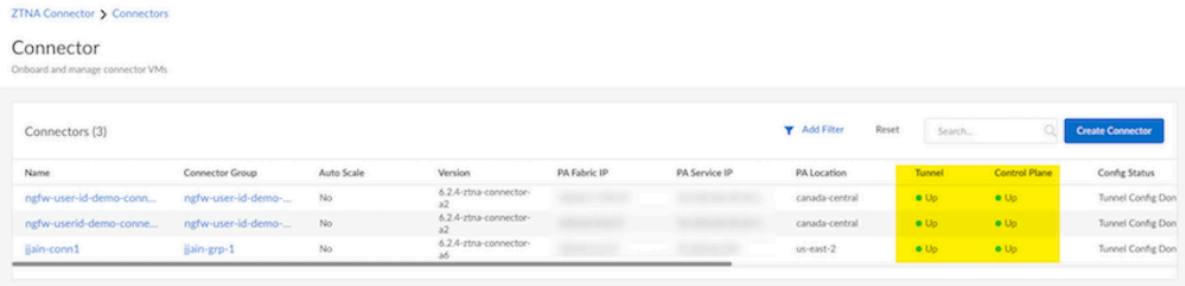
 ©2025 Palo Alto Networks, Inc.

STEP 13 | 部署虚拟机后，确认它已启动。

ESXi 虚拟服务器启动后，Prisma Access 完成要用作 ZTNA 连接器的设备的配置。



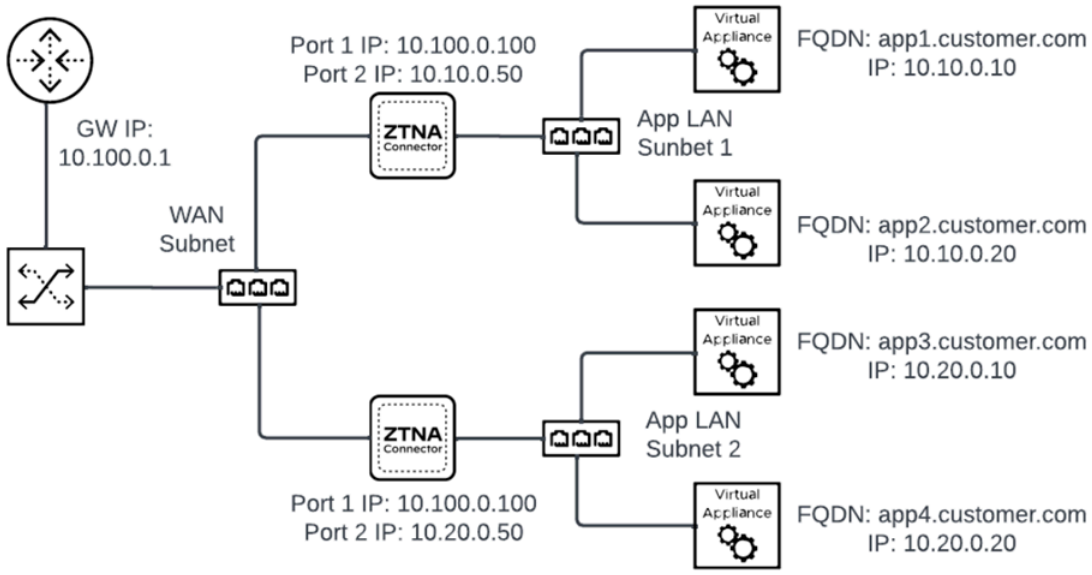
STEP 14 | 在 Prisma SASE 门户上，转到 **Workflows**（工作流） > **ZTNA Connector**（**ZTNA** 连接器） > **Connectors**（连接器），找到要使用的连接器，并确保其显示 **tunnel up**（隧道已启动）。



Prisma Access ZTNA 连接器支持的 KVM 部署

您使用双臂部署来部署基于内核的虚拟机 (KVM)。下图显示了在双臂模式下使用 KVM 和 NAT 网关的 ZTNA 连接器网络部署示例。

©2025 Palo Alto Networks, Inc.



使用 KVM 接入 ZTNA 连接器

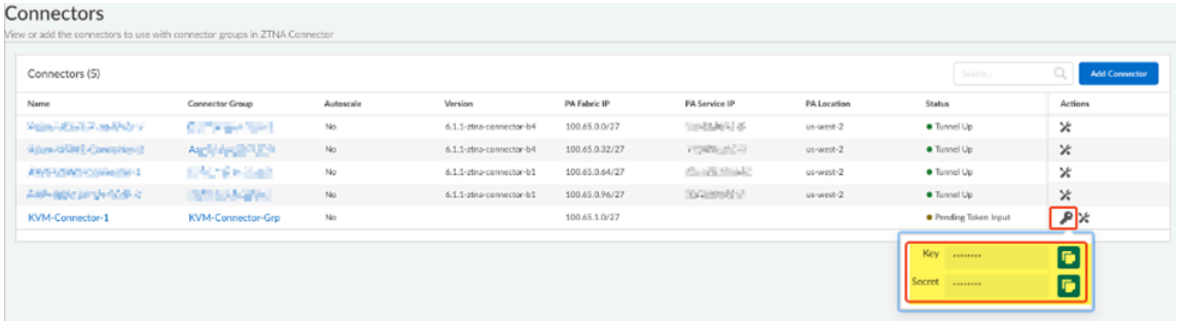
要使用基于内核的虚拟机 (KVM) 接入 ZTNA 连接器，请完成以下步骤。

在开始之前，请确保您满足以下先决条件：

- 在客户支持门户 (CSP) 中，在 **Updates**（更新） > **Software Updates**（软件更新） > 适用于 **KVM** 的 **Prisma Access ZTNA** 连接器。
- 确保您拥有满足 ZTNA 连接器最低托管环境的 KVM 主机。

STEP 1 | 为 KVM 主机创建连接器组和连接器。

STEP 2 | 选择 **Workflows**（工作流） > **ZTNA Connector**（**ZTNA** 连接器） > **Connectors**（连接器），找到您为 KVM 主机创建的连接器，在 **Status**（状态）区域中单击 **Copy Token**（复制令牌），并复制 **Key**（密钥）和 **Secret**（机密值）。



STEP 3 | 将从 CSP 下载的 **qcow** 映像上传到 KVM 主机。

 ©2025 Palo Alto Networks, Inc.

STEP 4 | 如果尚未执行此操作，请在 KVM 主机上构建并关联虚拟桥接接口，然后通过输入以下命令准备主机：

- `brctl addbr virbr0`
- `brctl addbr virbr0`
- `brctl addbr virbr1`
- `brctl addif virbr1 ens192`

STEP 5 | 通过运行 `virt-install` 命令并设置以下选项，在 KVM 主机上部署 VM：

- `-name` 是虚拟机的名称。
- `-vcpu` 是 **4**。
- `-内存` 为 **16384**（16 GB）。
- `-disk` 是 KVM 主机上 **qcow** 映像的位置和名称。
- `-network` 引用要连接到此 VM 的虚拟接口（您需要为 ZTNA 连接器部署接口）。

以下是用于部署 KVM 主机的示例命令，其中 **<kvm-file-name>** 是您从 CSP 下载的 qcow 文件的名称：

```
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 | 输入以下命令连接到 VM 控制台：

```
virsh console ztna-conn-1
```

交互式 CLI 安装程序启动。

STEP 7 | 配置 ION 模型、密钥和机密。

1. 从显示的选项中选择 **1**（**ion 200v** 的 ION 型号）。

```
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 选择一个数字或选择 Q 退出：1 CPU：已通过（需要 4）内存：已
通过（需要 8.0G）磁盘：无法验证（需要 40.0G）网络：通过（需要 1 个）选
择要修改的项目，或提交配置：1) 型号：ion 200v 2) ION 密钥：3) 机密密
钥：4) 控制器 1：控制器 - DHCP 5) 端口 1：已禁用/未使用 6) 端口 2：已
禁用/未使用 7) 端口 3：已禁用/未使用 8) 端口 4：已禁用/未使用 9) 端口
 5：已禁用/未使用 10) 端口 6：已禁用/未使用 11) 端口 7：已禁用/未使用
 12) 端口 8：已禁用/未使用 13) 端口 9：已禁用/未使用 14) 提交并重新启动
```

2. 从连接器输入密钥，方法如下：选择选项 **2** 并输入从 ZTNA 连接器 UI 保存的密钥。

```
选择一个数字或选择 Q 退出:2 输入 ION 密钥[无]: xxxxxxxxxx-yyyyyyyy-
zzz-1234-1234-abcdefghijkl 选择要修改的项目，或提交配置：1) 型号：ion
 200v 2) ION 密钥：xxxxxxxxx-yyyyyyyy-zzz-1234-1234-abcdefghijkl
 3) 机密密钥：4) 控制器 1：控制器 - DHCP 5) 端口 1：已禁用/未使用
```

 ©2025 Palo Alto Networks, Inc.

```
6) 端口 2：已禁用/未使用 7) 端口 3：已禁用/未使用 8) 端口 4：已禁用/未使用 9) 端口 5：已禁用/未使用 10) 端口 6：已禁用/未使用 11) 端口 7：已禁用/未使用 12) 端口 8：已禁用/未使用 13) 端口 9：已禁用/未使用 14) 提交并重新启动
```

3. 输入 ZTNA 连接器机密，方法如下：选择选项 **3** 并输入从 ZTNA 连接器 UI 保存的机密。

```
选择一个数字或选择 Q 退出:3 输入 ION 机密[无]: abcde12345 选择要修改的项目，或提交配置：1) 模型：ion 200v 2) ION 密钥：xxxxxxxxx-yyyyyyyy-zzz-1234-1234-abcdefghijkl 3) 机密密钥：abcde12345 4) 控制器 1：控制器 - DHCP 5) 端口 1：已禁用/未使用 6) 端口 2：已禁用/未使用 7) 端口 3：已禁用/未使用 8) 端口 4：已禁用/未使用 9) 端口 5：已禁用/未使用 10) 端口 6：已禁用/未使用 11) 端口 7：已禁用/未使用 12) 端口 8：已禁用/未使用 13) 端口 9：已禁用/未使用 14) 提交并重新启动
```

STEP 8 | 配置 WAN 端口选项。

1. 选择选项 **5**（端口 1）。

```
选择一个数字或选择 Q 退出:5 端口 1：1) 角色：禁用 2) 取消端口更改 3) 申请并返回
```

2. 选择选项 **1**（公共/WAN）。

```
选择一个数字或选择 Q 退出:1 选择端口角色：1) 面向互联网的端口（公共 WAN）2) 私有 WAN 端口（私有 WAN）3) 旁路端口对 1（WAN 端口）4) 旁路端口对 1（LAN 端口）5) 旁路端口对 2（WAN 端口）6) 旁路端口对 2（LAN 端口）7) 旁路端口对 3（WAN 端口）8) 旁路端口对 3（LAN 端口）9) 旁路端口对 4（WAN 端口）10) 绕过端口对 4（LAN 端口）11) 禁用/未使用
```

3. （可选）如果您需要设置静态 IP 地址，请选择选项**2** 并设置 IP 地址、网关和 DNS 服务器参数；否则，请选择 **1**。

```
选择一个数字或选择 Q 退出:1 端口 1：1) 角色：公共 WAN 2) 配置方式：DHCP 3) 取消端口更改 4) 应用并返回
```

4. 选择选项 **4** 返回主菜单。

```
选择一个数字或选择 Q 退出:4 选择要修改的项目，或提交配置：1) 模型：ion 200v 2) ION 密钥：xxxxxxxxx-yyyyyyyy-zzz-1234-1234-abcdefghijkl 3) 机密密钥：abcde12345 4) 控制器 1：控制器 - DHCP 5) 端口 1：公共 WAN - DHCP 6) 端口 2：已禁用/未使用 7) 端口 3：已禁用/未使用 8) 端口 4：已禁用/未使用 9) 端口 5：已禁用/未使用 10) 端口 6：已禁用/未使用 11) 端口 7：已禁用/未使用 12) 端口 8：已禁用/未使用 13) 端口 9：禁用/未使用 14) 提交并重启 选择要修改的项目，或提交配置：1) 模型：ion 200v 2) ION 密钥：xxxxxxxxx-yyyyyyyy-zzz-1234-1234-abcdefghijkl 3) 机密密钥：abcde12345 4) 控制器 1：控制器 - DHCP 5) 端口 1：公共 WAN - DHCP 6) 端口 2：已禁用/未使用 7) 端口 3：已禁用/未使用 8) 端口 4：已禁用/未使用 9) 端口 5：已禁用/未使用 10) 端口 6：已禁用/未使用 11) 端口 7：已禁用/未使用 12) 端口 8：已禁用/未使用 13) 端口 9：已禁用/未使用 14) 提交并重新启动
```

 ©2025 Palo Alto Networks, Inc.

STEP 9 | 配置 LAN 端口选项。

1. 选择选项 **6**（端口 2）。

   ```
   选择一个数字或选择 Q 退出:6 端口 2：1) 角色：禁用 2) 取消端口更改 3) 申请并返回
   ```

2. 选择选项 **2**（私有 WAN）。

   ```
   选择一个数字或选择 Q 退出:2 选择端口角色：1) 面向互联网的端口（公共 WAN）2) 私有 WAN 端口（私有 WAN）3) 旁路端口对 1（WAN 端口）4) 旁路端口对 1（LAN 端口）5) 旁路端口对 2（WAN 端口）6) 旁路端口对 2（LAN 端口）7) 旁路端口对 3（WAN 端口）8) 旁路端口对 3（LAN 端口）9) 旁路端口对 4（WAN 端口）10) 绕过端口对 4（LAN 端口）11) 禁用/未使用
   ```

3. （可选）如果您需要设置静态 IP 地址，请选择选项**2** 并设置 IP 地址、网关和 DNS 服务器参数；否则，请选择 **1**。

   ```
   选择一个数字或选择 Q 退出:2 端口 2：1) 角色：私有 WAN 2) 配置方式：DHCP 3) 取消端口更改 4) 应用并返回
   ```

4. 选择选项 **4** 返回主菜单。

   ```
   选择一个数字或选择 Q 退出:4 选择要修改的项目，或提交配置：1) 模型：ion 200v 2) ION 密钥：xxxxxxxxx-yyyyyyyy-zzz-1234-1234-abcdefghijkl 3) 机密密钥：abcde12345 4) 控制器 1：控制器 - DHCP 5) 端口 1：公共 WAN - DHCP 6) 端口 2：私有 WAN - DHCP 7) 端口 3：已禁用/未使用 8) 端口 4：已禁用/未使用 9) 端口 5：已禁用/未使用 10) 端口 6：已禁用/未使用 11) 端口 7：已禁用/未使用 12) 端口 8：已禁用/未使用 13) 端口 9：已禁用/未使用 14) 提交并重新启动
   ```

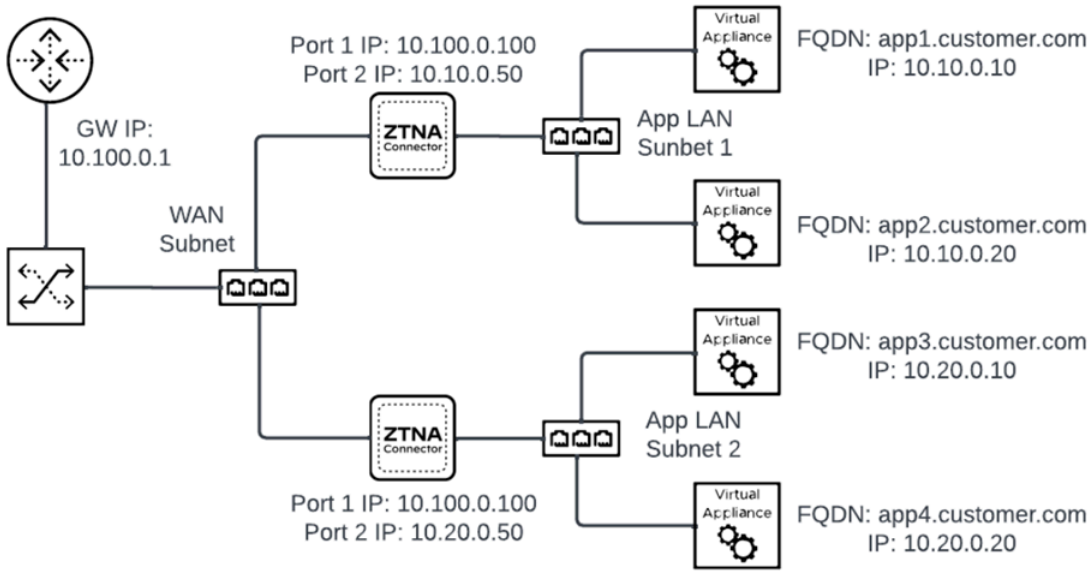
STEP 10 | 保存并重启连接器。

```
选择一个数字或选择 Q 退出:14 警告#提交此配置后，所有硬件将被签名、记录并永久绑定到 Prisma SDWAN 云控制器中的 ION 密钥/机密。这意味着在此使用“提交”功能之后，便无法再添加/删除硬件（磁盘、网卡）。如果需要在进行“提交”之后进行任何硬件更改，则需要使用新的 ION 密钥和机密来重新部署 ION。如果需要添加或删除硬件，请在下面选择 “N”，然后关闭 ION 并立即进行更改。是否立即提交这些更改？[N]: y 正在构建配置... [VFF:CFG] 零接触配置启动 - 配置文件解析器 [VFF:CFG] 尝试加载/解析为配置/INI 文件。[VFF:CFG] 成功加载配置样式文件。[VFF:CFG] 控制器 1 成功设置为 CONTROLLER/DHCP。[VFF:CFG] 端口 1 成功设置为 PUBLICWAN/DHCP。[VFF:CFG] 端口 2 成功设置为 PRIVATEWAN/DHCP。[VFF:CFG] 警告：端口 3 没有配置部分。默认为禁用。[VFF:CFG] 警告：端口 4 没有配置部分。默认为禁用。[VFF:CFG] 警告：端口 5 没有配置部分。默认为禁用。[VFF:CFG] 警告：端口 6 没有配置部分。默认为禁用。[VFF:CFG] 警告：端口 7 没有配置部分。默认为禁用。[VFF:CFG] 警告：端口 8 没有配置部分。默认为禁用。[VFF:CFG] 警告：端口 9 没有配置部分。默认为禁用。[VFF:CFG] Config/INI 文件解析成功。[VFF:KVM] 菜单配置结束，继续正常启动...重启原因：制造
```

 ©2025 Palo Alto Networks, Inc.

Prisma Access ZTNA 连接器支持的 Hyper-V 部署

使用双臂部署来部署 Microsoft Hyper-V 管理程序。下图显示了在双臂模式下使用 Hyper-V 和 NAT 网关的 ZTNA 连接器网络部署示例。



使用 Hyper-V 接入 ZTNA 连接器

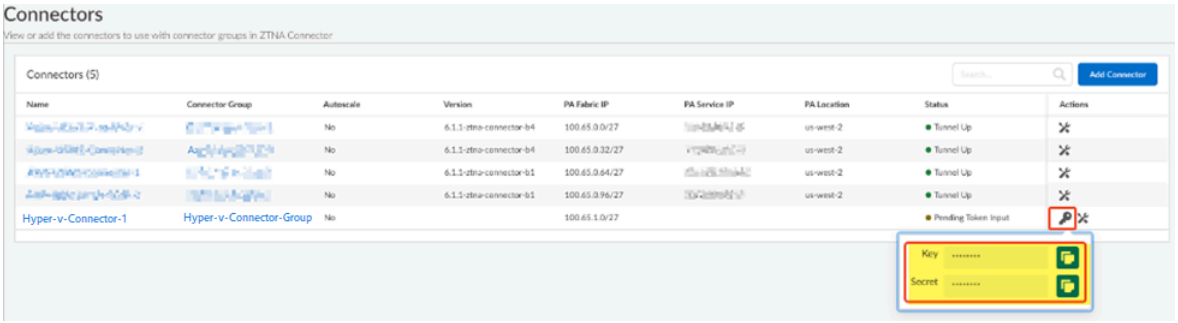
要使用 Microsoft Hyper-V 虚拟机 (VM) 接入 ZTNA 连接器，请完成以下步骤。

在开始之前，请确保您满足以下先决条件：

- 在 客户支持门户 (CSP) 中，在 **Updates**（更新） > **Software Updates**（软件更新） > 适用于 **Hyper-V** 的 **Prisma Access ZTNA** 连接器。
- 确保您拥有满足 ZTNA 连接器最低托管环境的 Hyper-V 虚拟机。

STEP 1 | 为 Hyper-V 虚拟机创建连接器组和连接器。

STEP 2 | 选择 **Workflows**（工作流） > **ZTNA Connector**（**ZTNA** 连接器） > **Connectors**（连接器），找到您为 Hyper-V 虚拟机创建的连接器，在 **Status**（状态）区域中单击 **Copy Token**（复制令牌），并复制 **Key**（密钥）和 **Secret**（机密值）。



©2025 Palo Alto Networks, Inc.

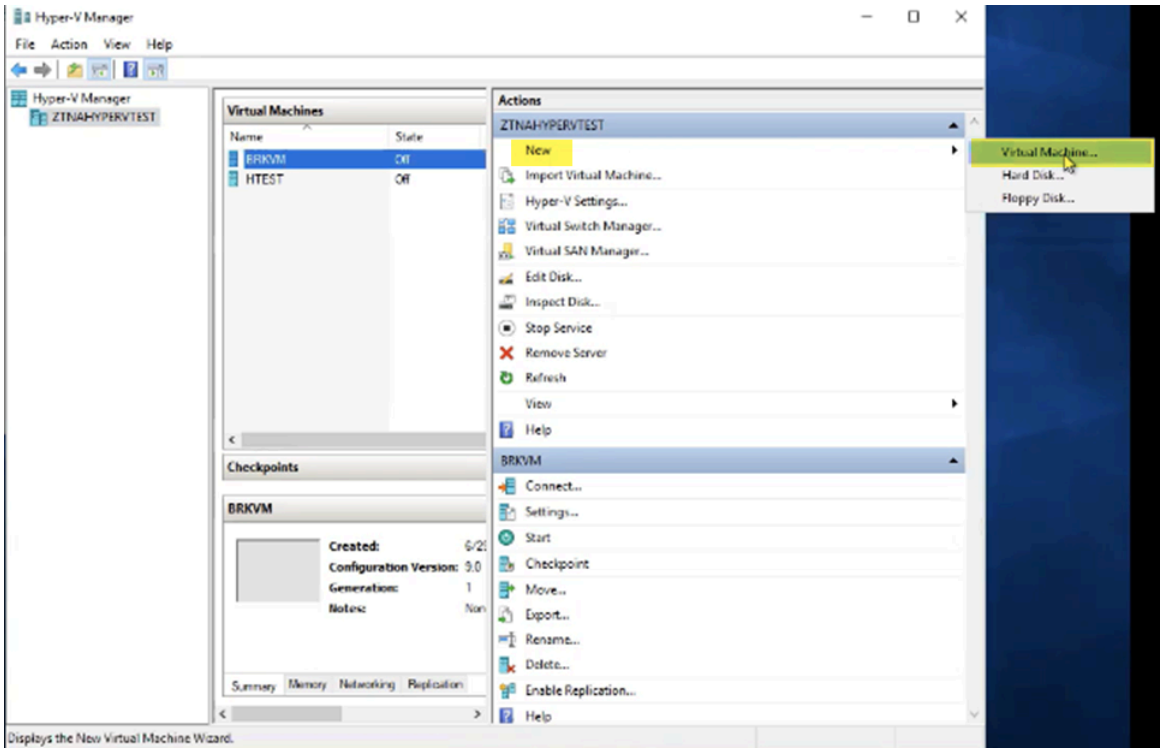
STEP 3 | 将从 CSP 下载的 **vhd** 映像上传到 Hyper-V 虚拟机。

确保您选择的位置可以从 Hyper-V 虚拟机访问。

每个 Hyper-V 虚拟机需要一个 (vhd) 文件。

STEP 4 | 前往 Hyper-V 管理器，选择 **Actions**（操作） > **New**（新建） > **Virtual Machine**（虚拟机）来创建新的虚拟机。

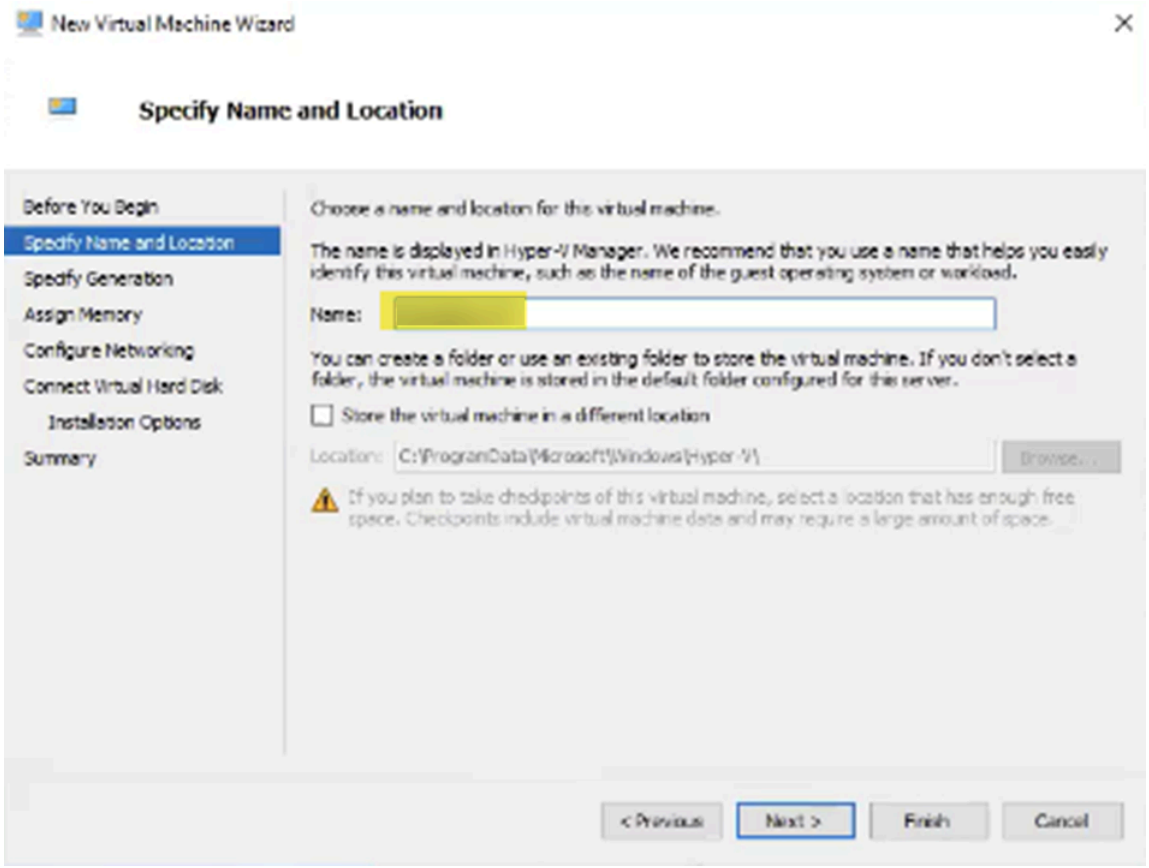
此工作流展示了您在 Microsoft 服务器上部署 Hyper-V 虚拟机所执行的步骤。Hyper-V UI 在您的环境中可能看起来不同。



STEP 5 | 选择 **Next**（下一步）以转到下一个屏幕并输入虚拟机的唯一名称，然后选择 **Next**（下一步）。

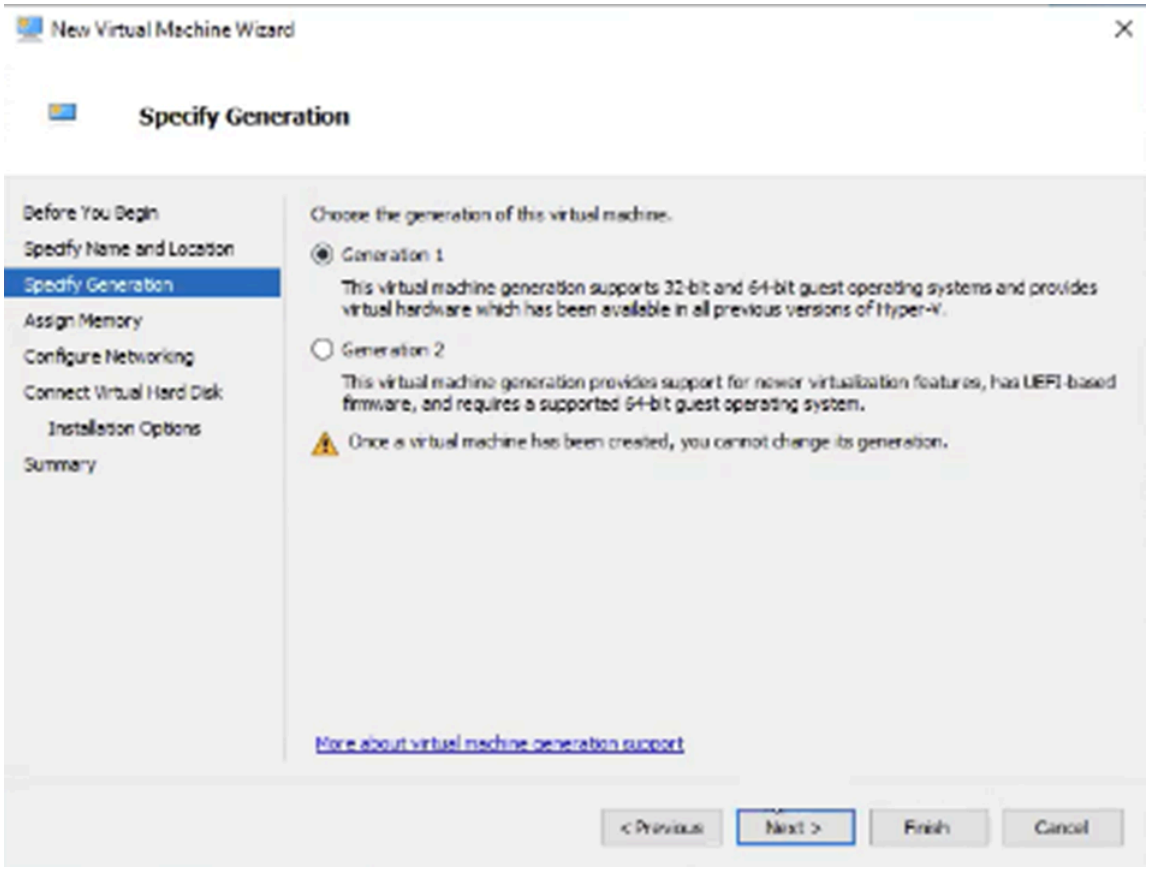
 ©2025 Palo Alto Networks, Inc.

STEP 6 | （可选）要更改虚拟机的位置，请选择 **Store the virtual machine in a different location**（将虚拟机存储在其他位置），然后选择该位置。



 ©2025 Palo Alto Networks, Inc.

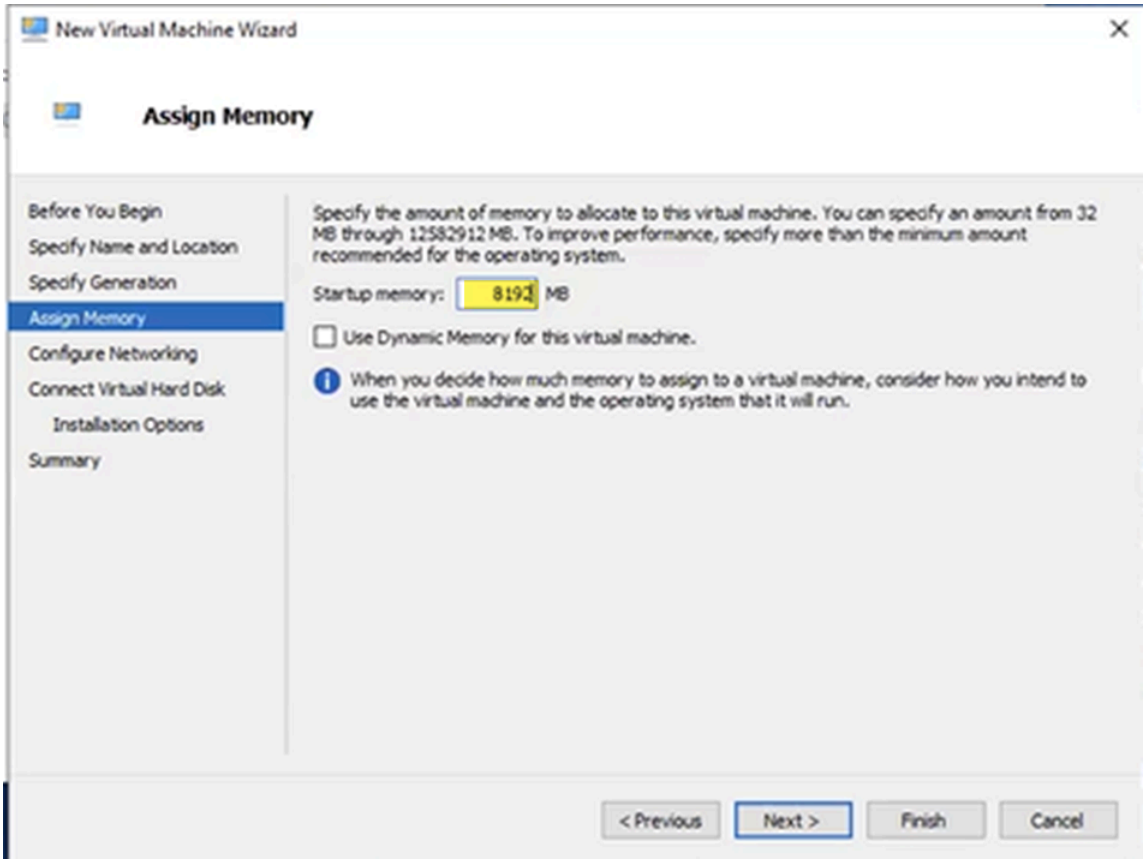
STEP 7 | 选择 **Generation 1**（第一代） 作为虚拟机代系，然后选择 **Next**（下一步）以转到下一页。这是 ZTNA 连接器 vhd 文件支持的代系。



 ©2025 Palo Alto Networks, Inc.

STEP 8 | 为虚拟机分配内存。

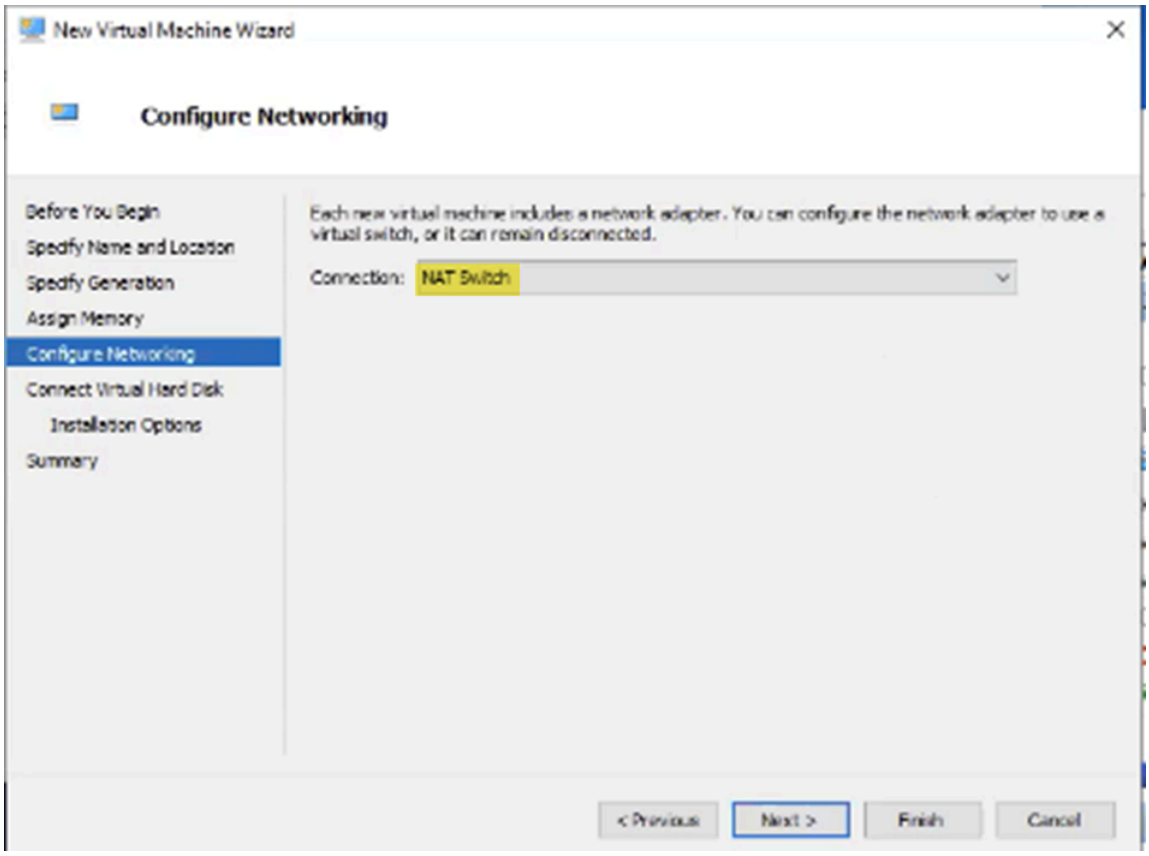
分配至少 **8192** 兆字节（8GB）的内存，这满足了 Hyper-V 虚拟机的最低要求，然后选择 **Next**（下一步）以转到下一页。



 ©2025 Palo Alto Networks, Inc.

STEP 9 | 为您的虚拟机配置网络；然后选择 **Next**（下一步）以转到下一页。

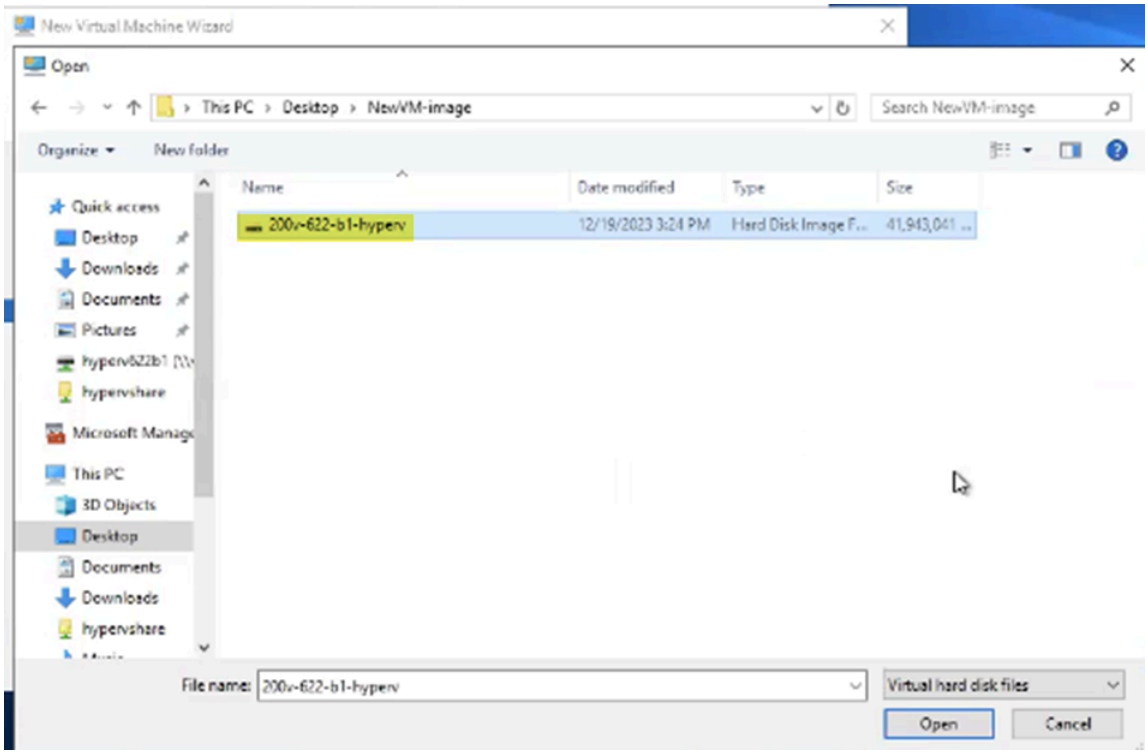
您使用的网络取决于您的配置。本示例使用 **NAT** 交换机进行网络连接。



©2025 Palo Alto Networks, Inc.

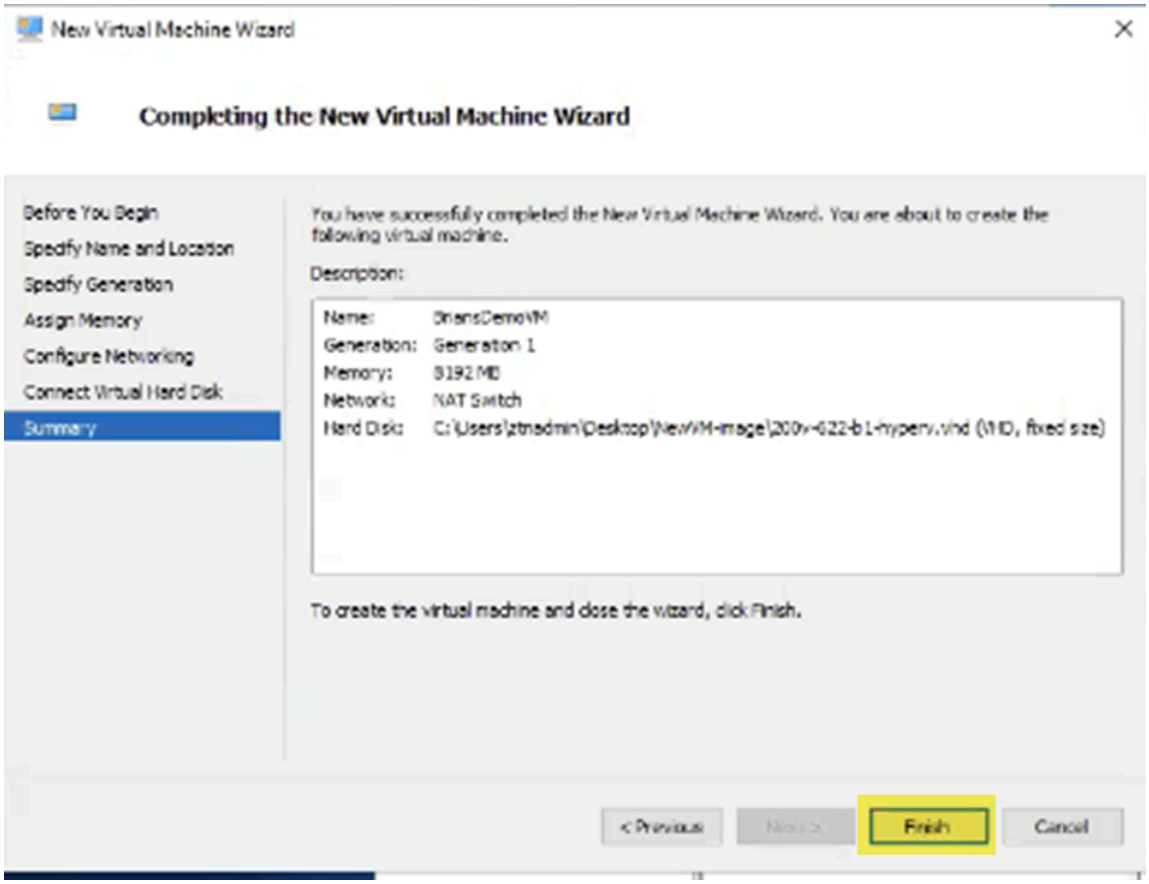
STEP 10 | 连接虚拟硬盘。

1. 选择 **Use an existing virtual hard disk**（使用现有虚拟硬盘），然后选择 **Browse**（浏览）以找到下载的 vhd 文件。
2. 选择您下载的 vhd 文件，然后单击 **Open**（打开）将其打开；然后选择 **Next**（下一步）以转到下一页。



©2025 Palo Alto Networks, Inc.

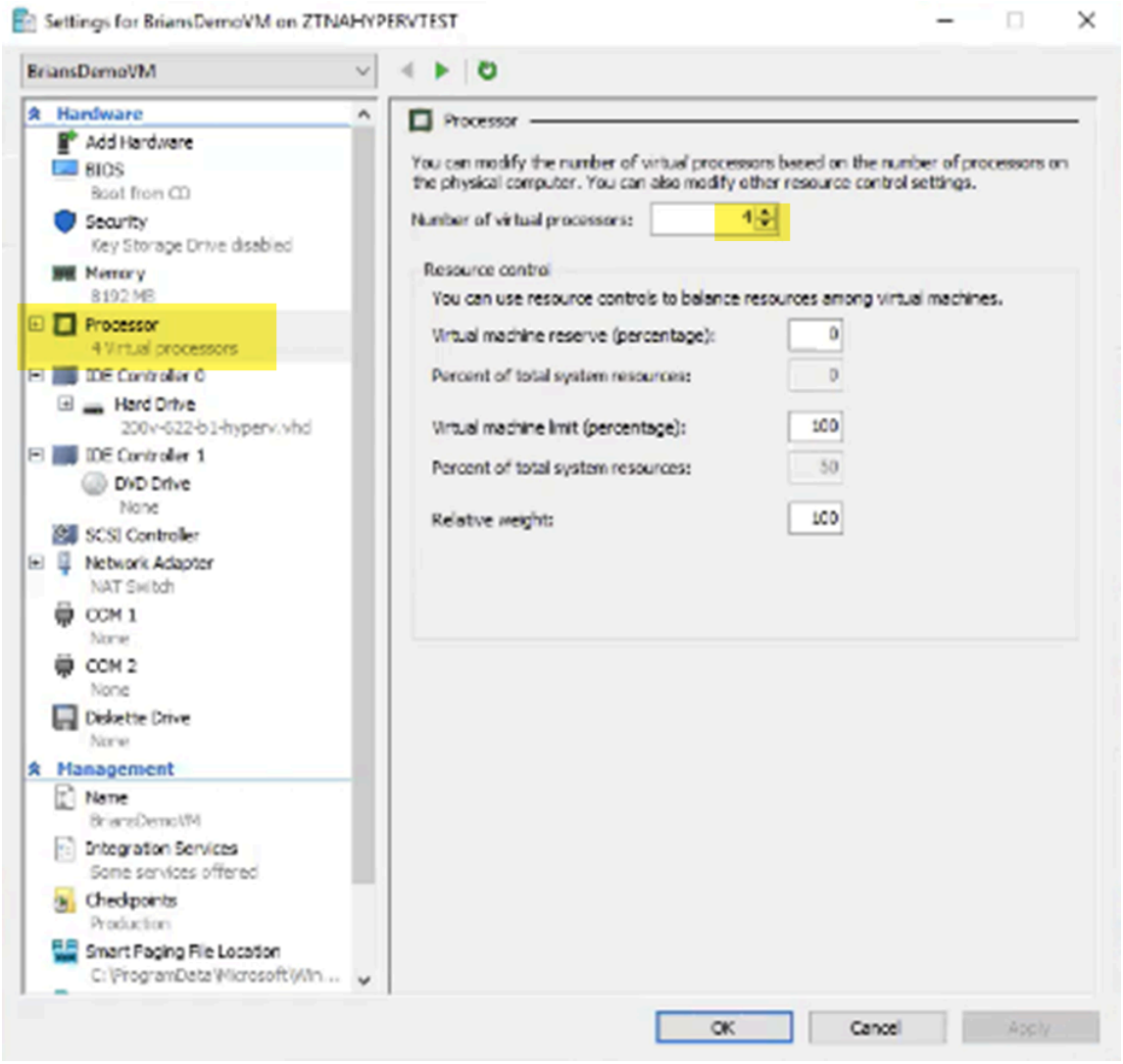
STEP 11 | 单击 **Finish**（完成）以完成新的虚拟机向导。



Hyper-V 将创建虚拟机。

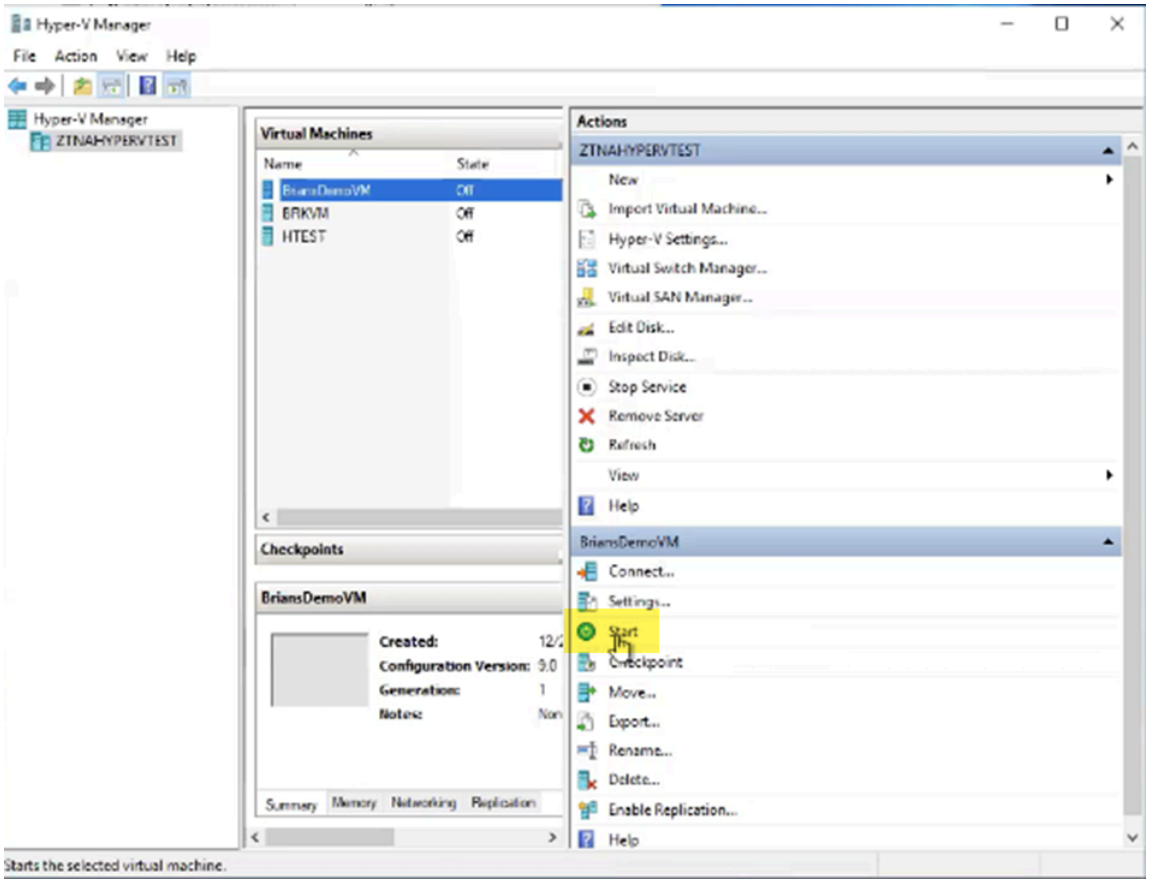
 ©2025 Palo Alto Networks, Inc.

STEP 12 | 确保您的虚拟机至少有四个处理器，方法是转到 **Processor**（处理器）区域并确保选择至少 **4** 个虚拟处理器。

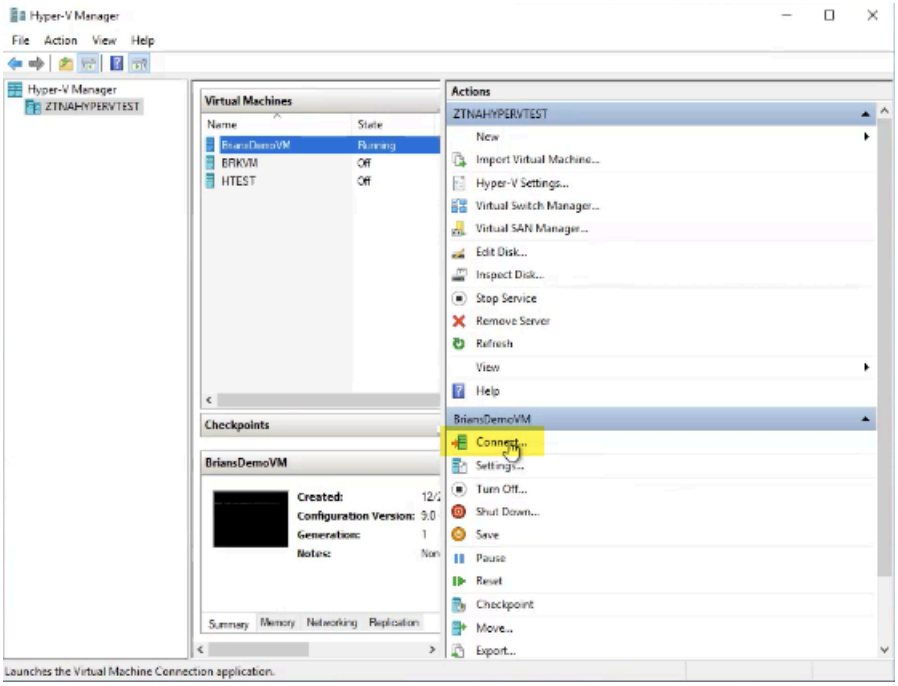


 ©2025 Palo Alto Networks, Inc.

STEP 13 | 选择 **Start**（启动）以启动虚拟机。



STEP 14 | 选择 **Connect**（连接）以连接到串行控制台。



 ©2025 Palo Alto Networks, Inc.

STEP 15 | 等待交互式 CLI 安装程序初始化，然后配置 ION 模型、密钥和机密。

1. 从显示的选项中选择 **1**（**ion 200v** 的 ION 型号）。

```
选择一个 ION 模型：1) ion 200v 2) ion 3102v 3) ion 3104v 4) ion
 3108v 5) ion 7108v 6) ion 7116v 7) ion 7132v 8) ion 9100v 选择
一个数字或选择 Q 退出：1 CPU：已通过（需要 4）内存：已通过（需要 8.0G）
磁盘：无法验证（需要 40.0G）网络：通过（需要 1 个）选择要修改的项目，或
提交配置：1) 型号：ion 200v 2) ION 密钥：3) 机密密钥：4) 控制器 1：
控制器 - DHCP 5) 端口 1：已禁用/未使用 6) 端口 2：已禁用/未使用 7) 端
口 3：已禁用/未使用 8) 端口 4：已禁用/未使用 9) 端口 5：已禁用/未使用
 10) 端口 6：已禁用/未使用 11) 端口 7：已禁用/未使用 12) 端口 8：已禁
用/未使用 13) 端口 9：已禁用/未使用 14) 提交并重新启动
```

2. 从连接器输入密钥，方法如下：选择选项 **2** 并输入从 ZTNA 连接器 UI 保存的密钥。

```
选择一个数字或选择 Q 退出:2 输入 ION 密钥[无]: xxxxxxxxxx-yyyyyyyy-
zzz-1234-1234-abcdefghijkl 选择要修改的项目，或提交配置：1) 型号：ion
 200v 2) ION 密钥：xxxxxxxxx-yyyyyyyy-zzz-1234-1234-abcdefghijkl
 3) 机密密钥：4) 控制器 1：控制器 - DHCP 5) 端口 1：已禁用/未使用
 6) 端口 2：已禁用/未使用 7) 端口 3：已禁用/未使用 8) 端口 4：已禁用/未
使用 9) 端口 5：已禁用/未使用 10) 端口 6：已禁用/未使用 11) 端口 7：已
禁用/未使用 12) 端口 8：已禁用/未使用 13) 端口 9：已禁用/未使用 14) 提
交并重新启动
```

3. 输入 ZTNA 连接器机密，方法如下：选择选项 **3** 并输入从 ZTNA 连接器 UI 保存的机密。

```
选择一个数字或选择 Q 退出:3 输入 ION 机密[无]: abcde12345 选择要修改的
项目，或提交配置：1) 模型：ion 200v 2) ION 密钥：xxxxxxxxx-yyyyyyyy-
zzz-1234-1234-abcdefghijkl 3) 机密密钥：abcde12345 4) 控制器 1：
控制器 - DHCP 5) 端口 1：已禁用/未使用 6) 端口 2：已禁用/未使用 7) 端
口 3：已禁用/未使用 8) 端口 4：已禁用/未使用 9) 端口 5：已禁用/未使用
 10) 端口 6：已禁用/未使用 11) 端口 7：已禁用/未使用 12) 端口 8：已禁
用/未使用 13) 端口 9：已禁用/未使用 14) 提交并重新启动
```

STEP 16 | 配置 WAN 端口选项。

1. 选择选项 **5**（端口 1）。

```
选择一个数字或选择 Q 退出:5 端口 1：1) 角色：禁用 2) 取消端口更改 3) 申
请并返回
```

2. 选择选项 **1**（公共/WAN）。

```
选择一个数字或选择 Q 退出:1 选择端口角色：1) 面向互联网的端口（公共
 WAN）2) 私有 WAN 端口（私有 WAN）3) 旁路端口对 1（WAN 端口）4) 旁路
端口对 1（LAN 端口）5) 旁路端口对 2（WAN 端口）6) 旁路端口对 2（LAN 端
口）7) 旁路端口对 3（WAN 端口）8) 旁路端口对 3（LAN 端口）9) 旁路端口对
 4（WAN 端口）10) 绕过端口对 4（LAN 端口）11) 禁用/未使用
```


©2025 Palo Alto Networks, Inc.

3. （可选）如果您需要设置静态 IP 地址，请选择选项**2** 并设置 IP 地址、网关和 DNS 服务器参数；否则，请选择 **1**。

```
选择一个数字或选择 Q 退出:1 端口 1：1) 角色：公共 WAN 2) 配置方式：DHCP
 3) 取消端口更改 4) 应用并返回
```

4. 选择选项 **4** 返回主菜单。

```
选择一个数字或选择 Q 退出:4 选择要修改的项目，或提交配置：1) 模型：ion
 200v 2) ION 密钥：xxxxxxxxx-yyyyyyyy-zzz-1234-1234-abcdefghijkl
 3) 机密密钥：abcde12345 4) 控制器 1：控制器 - DHCP 5) 端口 1：公共
 WAN - DHCP 6) 端口 2：已禁用/未使用 7) 端口 3：已禁用/未使用 8) 端
口 4：已禁用/未使用 9) 端口 5：已禁用/未使用 10) 端口 6：已禁用/未使
用 11) 端口 7：已禁用/未使用 12) 端口 8：已禁用/未使用 13) 端口 9：
禁用/未使用 14) 提交并重启 选择要修改的项目，或提交配置：1) 模型：ion
 200v 2) ION 密钥：xxxxxxxxx-yyyyyyyy-zzz-1234-1234-abcdefghijkl
 3) 机密密钥：abcde12345 4) 控制器 1：控制器 - DHCP 5) 端口 1：公共
 WAN - DHCP 6) 端口 2：已禁用/未使用 7) 端口 3：已禁用/未使用 8) 端
口 4：已禁用/未使用 9) 端口 5：已禁用/未使用 10) 端口 6：已禁用/未使用
 11) 端口 7：已禁用/未使用 12) 端口 8：已禁用/未使用 13) 端口 9：已禁
用/未使用 14) 提交并重新启动
```

STEP 17 | 配置 LAN 端口选项。

1. 选择选项 **6**（端口 2）。

```
选择一个数字或选择 Q 退出:6 端口 2：1) 角色：禁用 2) 取消端口更改 3) 申
请并返回
```

2. 选择选项 **2**（私有 WAN）。

```
选择一个数字或选择 Q 退出:2 选择端口角色：1) 面向互联网的端口（公共
 WAN）2) 私有 WAN 端口（私有 WAN）3) 旁路端口对 1（WAN 端口）4) 旁路
端口对 1（LAN 端口）5) 旁路端口对 2（WAN 端口）6) 旁路端口对 2（LAN 端
口）7) 旁路端口对 3（WAN 端口）8) 旁路端口对 3（LAN 端口）9) 旁路端口对
 4（WAN 端口）10) 绕过端口对 4（LAN 端口）11) 禁用/未使用
```

3. （可选）如果您需要设置静态 IP 地址，请选择选项**2** 并设置 IP 地址、网关和 DNS 服务器参数；否则，请选择 **1**。

```
选择一个数字或选择 Q 退出:2 端口 2：1) 角色：私有 WAN 2) 配置方式：DHCP
 3) 取消端口更改 4) 应用并返回
```

4. 选择选项 **4** 返回主菜单。

```
选择一个数字或选择 Q 退出:4 选择要修改的项目，或提交配置：1) 模型：ion
 200v 2) ION 密钥：xxxxxxxxx-yyyyyyyy-zzz-1234-1234-abcdefghijkl
 3) 机密密钥：abcde12345 4) 控制器 1：控制器 - DHCP 5) 端口 1：公
共 WAN - DHCP 6) 端口 2：私有 WAN - DHCP 7) 端口 3：已禁用/未使用
 8) 端口 4：已禁用/未使用 9) 端口 5：已禁用/未使用 10) 端口 6：已禁
```

 ©2025 Palo Alto Networks, Inc.

用/未使用 11) 端口 7：已禁用/未使用 12) 端口 8：已禁用/未使用 13) 端口 9：已禁用/未使用 14) 提交并重新启动

STEP 18 | 保存并重启连接器。

选择一个数字或选择 Q 退出:14 警告#提交此配置后，所有硬件将被签名、记录并永久绑定到 Prisma SDWAN 云控制器中的 ION 密钥/机密。这意味着在此使用“提交”功能之后，便无法再添加/删除硬件（磁盘、网卡）。如果需要在进行“提交”之后进行任何硬件更改，则需要使用新的 ION 密钥和机密来重新部署 ION。如果需要添加或删除硬件，请在下面选择 “N”，然后关闭 ION 并立即进行更改。是否立即提交这些更改？[N]: y 正在构建配置... [VFF:CFG] 零接触配置启动 - 配置文件解析器 [VFF:CFG] 尝试加载/解析为配置/INI 文件。[VFF:CFG] 成功加载配置样式文件。[VFF:CFG] 控制器 1 成功设置为 CONTROLLER/DHCP。[VFF:CFG] 端口 1 成功设置为 PUBLICWAN/DHCP。[VFF:CFG] 端口 2 成功设置为 PRIVATEWAN/DHCP。[VFF:CFG] 警告：端口 3 没有配置部分。默认为禁用。[VFF:CFG] 警告：端口 4 没有配置部分。默认为禁用。[VFF:CFG] 警告：端口 5 没有配置部分。默认为禁用。[VFF:CFG] 警告：端口 6 没有配置部分。默认为禁用。[VFF:CFG] 警告：端口 7 没有配置部分。默认为禁用。[VFF:CFG] 警告：端口 8 没有配置部分。默认为禁用。[VFF:CFG] 警告：端口 9 没有配置部分。默认为禁用。[VFF:CFG] Config/INI 文件解析成功。[VFF:KVM] 菜单配置结束，继续正常启动...重启原因：制造

 ©2025 Palo Alto Networks, Inc.

监控 ZTNA 连接器

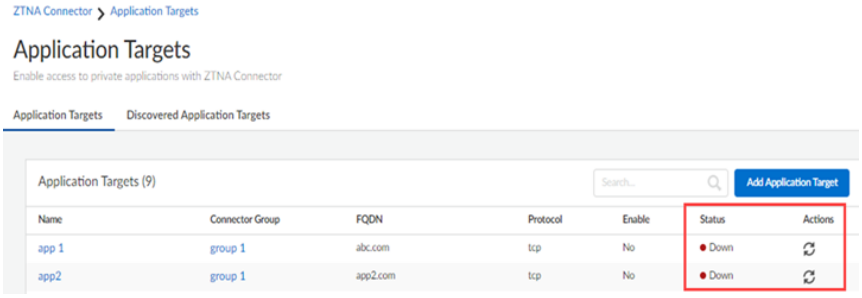
在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ ZTNA 连接器附加许可证 带附加许可证的基础许可证包括 8 个 ZTNA 连接器、100 个 FQDN 和 4 个 IP 子网功能。 带附加许可证的高级许可证包括 40 个 ZTNA 连接器、300 个 FQDN 和 1024 个 IP 子网功能。 带附加许可证的高级许可证包括 200 个 ZTNA 连接器、4000 个 FQDN 和 1024 个 IP 子网功能。 ❑ 如果您不购买 ZTNA 连接器附加许可证，Prisma Access 许可证将包括四个连接器、40 个 FQDN 和四个 IP 子网。此功能旨在让您在自己的环境中尝试 ZTNA 连接器。

所有 ZTNA 连接器组件都提供清晰的状态信息、日志和诊断工具，以帮助您解决出现的任何问题。使用以下工具来监控您的 ZTNA 连接器部署。

©2025 Palo Alto Networks, Inc.

从 Prisma SASE 平台内部查看应用程序和连接器的状态。

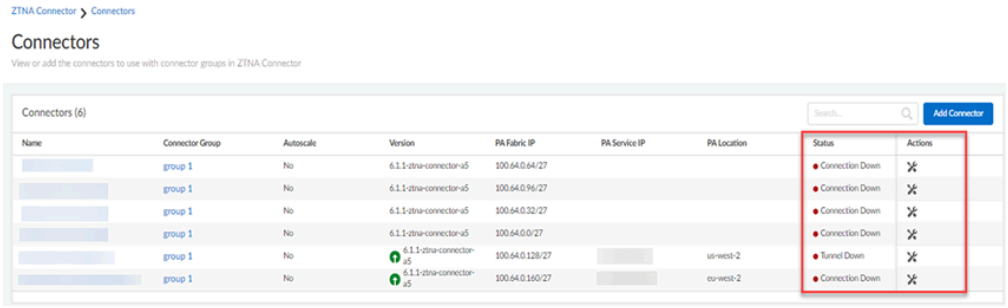
- 选择 **Workflows**（工作流） > **ZTNA Connector**（**ZTNA** 连接器） > **Application Targets**（应用程序目标），并验证所有应用程序目标的 **Status**（状态） 为 **Up**（正常运行）。



如果状态显示为 **Down**（停机），则连接器无法访问您的应用程序。在您解决应用程序的问题后，单击 **Action**（操作） 列中的刷新状态按钮，并验证 **Status**（状态） 是否变为 **Up**（正常运行）（状态每分钟自动刷新一次）。

如果可以从 ZTNA 连接器访问应用程序（使用上次成功的 DNS 解析结果），但从 ZTNA 连接器对应用程序的 FQDN 进行 DNS 解析失败，状态也会显示为“Up（正常运行）”。

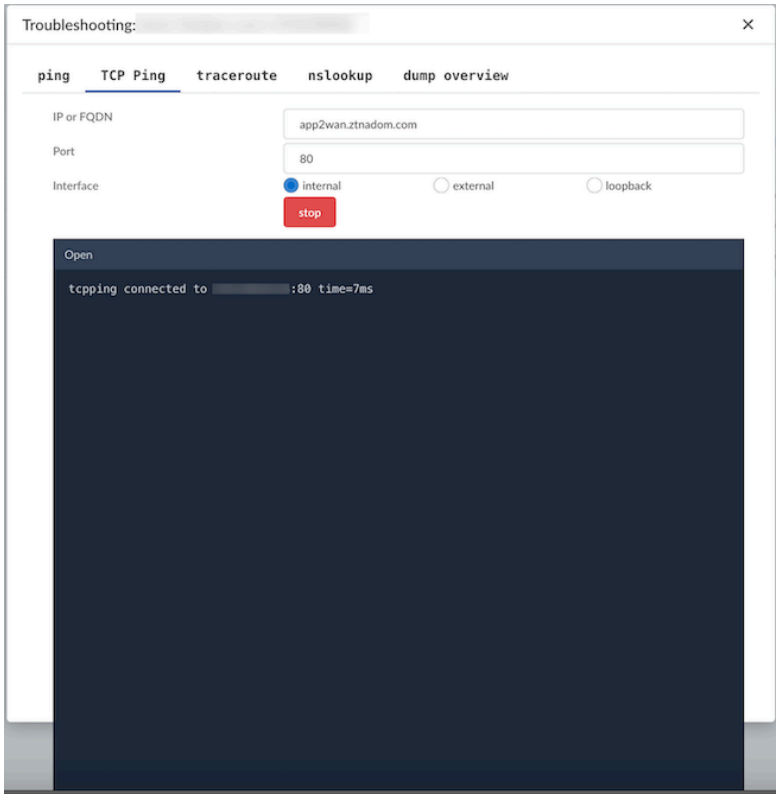
- 选择 **Workflows**（工作流） > **ZTNA Connector**（**ZTNA** 连接器） > **Connectors**（连接器），并确保所有连接器的 **Status**（状态） 为 **Up**（正常运行）。



如果 **Status**（状态） 显示为 **Tunnel Down**（隧道关闭），则表明连接器虚拟机与 Prisma Access 之间的 IPSec 隧道已关闭。如果 **Status**（状态） 显示为 **Connection Down**（连接关闭），则表明连接器虚拟机已关闭。单击诊断图标 以启动与连接器的远程 shell 连接来解

©2025 Palo Alto Networks, Inc.

决问题。您可以运行 **ping**、**TCP Ping**、**traceroute**、**nslookup** 或 **dump overview** 来帮助您诊断连接问题。



©2025 Palo Alto Networks, Inc.

查看 ZTNA 连接器日志

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 4.0 ❑ ZTNA 连接器附加许可证 带附加许可证的基础许可证包括 8 个 ZTNA 连接器、100 个 FQDN 和 4 个 IP 子网功能。 带附加许可证的高级许可证包括 40 个 ZTNA 连接器、300 个 FQDN 和 1024 个 IP 子网功能。 带附加许可证的高级许可证包括 200 个 ZTNA 连接器、4000 个 FQDN 和 1024 个 IP 子网功能。 ❑ 如果您不购买 ZTNA 连接器附加许可证，Prisma Access 许可证将包括四个连接器、40 个 FQDN 和四个 IP 子网。此功能旨在让您在自己的环境中尝试 ZTNA 连接器。

所有 ZTNA 连接器流量均记录到 Strata Logging Service。要在 Strata Logging Service 中存储 Prisma Access 日志，您必须估计并在 Strata Logging Service 中购买适当数量的日志存储空间。我们建议您将 Strata Logging Service 总容量存储空间增加 10%，以用于存储 ZTNA 连接器日志。

确保已配置日志转发配置文件，将所需的日志类型转发至 Strata 日志记录服务。当日志存储空间配额达到 90% 时，Strata Logging Service 将发送电子邮件来通知购买更多存储空间。如果您不购买更多存储空间，旧日志将被清除。

无论您使用 Prisma Access 的哪种管理界面（Panorama 或云管理），您都可以在 Prisma Access (Managed by Strata Cloud Manager) 的 **Incidents & Alerts**（事件和警报） > **Log Viewer**（日志查看器）下查看日志。

ZTNA 连接器提供以下网络日志。

©2025 Palo Alto Networks, Inc.

- 审计日志 — 可通过 Prisma SASE 平台获取，用于提供管理员在 ZTNA 连接器中配置更改的记录。这些日志可用于合规性和故障排除目的。

  您可以按时间范围、站点、设备和类型筛选审计日志。审计日志提供以下详细信息：

  - 特定用户从特定 IP 地址尝试登录企业门户的次数。
  - 应用程序或应用程序连接器是否已加入或被删除。
  - 当计划进行连接器升级时。
  - 查看所有系统变化和访问尝试。

  ZTNA 连接器审计日志在 Prisma Access Web 界面上不可用。要查看审计日志，您必须向 Palo Alto Networks 技术支持部门开立支持案例。
- 流量日志 — 在每个会话开始和结束时显示一个条目。每个条目都包含日期和时间、源和目标服务区、地址和端口，应用程序名称，应用到流的安全规则名称，规则操作（允许、拒绝或丢弃）、传入和传出接口、字节数和会话结束原因。
  - “类型”列指示条目是会话开始条目还是结束条目。
  - 操作”列指示防火墙已允许、拒绝还是丢弃了会话。
  - 丢弃表示阻止通信的安全规则指定了任意应用程序，而拒绝则表示规则标识了特定应用程序。
  - 如果在标识应用程序之前防火墙丢弃流量，例如当规则丢弃特定服务的所有流量时，Application（应用程序）列将显示为“not-applicable（不适用）”。
  - ZTNA 连接器的 App-ID 是自定义 App-ID。
  - 如果流量到达移动用户网关，**Destination Address**（目标地址）列将显示 RFC 6598 IP 地址。
- 日志 — 显示 ZTNA 连接器配置更改的条目。每个条目均包括日期和时间、管理员用户名、管理员执行更改的 IP 地址、客户端类型、执行的命令类型、命令状态（成功或失败）、配置路径以及更改前后的值。
- Strata Cloud Manager
- Panorama

查看 ZTNA 连接器日志 (Panorama)

按照以下工作流程在 Prisma Access (Managed by Panorama) Access 中查看 ZTNA 连接器日志。

STEP 1 | 登录 Prisma Access。

STEP 2 | 选择 **Monitor**（监控） > **Logs**（日志）。

STEP 3 | 从列表中选择日志类别：**Audit**（审计）、**Traffic**（流量）和 **Config**（配置）日志

STEP 4 | 单击任意列标题右侧的箭头，然后选择 **Columns**（列）。

STEP 5 | 从列表中选择要显示的列。日志自动更新，以匹配您的选择。

STEP 6 | 单击特定日志条目的 **spyglass**（望远镜）图标。**Detailed Log View**（详细日志视图）包含更多有关会话的源和目标的信息，以及与该日志条目相关的会话列表的信息。

 ©2025 Palo Alto Networks, Inc.

查看 ZTNA 连接器日志 (Strata Cloud Manager)

按照以下工作流程在云托管 Prisma Access 中查看 ZTNA 连接器日志。

STEP 1 | 登录 Prisma Access (Managed by Strata Cloud Manager)。

STEP 2 | 选择 **Incidents & Alerts**（事件和警报） > **Log Viewer**（日志查看器）。

STEP 3 | 选择要查看的日志类型：审计、防火墙/流量和配置日志。

STEP 4 | 选择要查看日志的时间范围。

STEP 5 | 提供此查询字符串以缩小 ZTNA 连接器日志列表的范围：**Subtype = 'netflow' AND Device Name = 'PA_CONN'**（子类型 = **'netflow' AND** 设备名称 = **'PA_CONN'**）。

日志包括以下详细信息：

- 时间戳
- 连接器名称
- 客户端的原始源 IP 地址
- 客户端的原始源端口
- 连接器的转换 IP 地址
- 连接器的转换端口
- 转换后的目标 IP 地址
- 转换后的目标端口

 ©2025 Palo Alto Networks, Inc.

保留使用源 NAT 的 ZTNA 连接器连接的 User-ID 映射

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 5.1.1

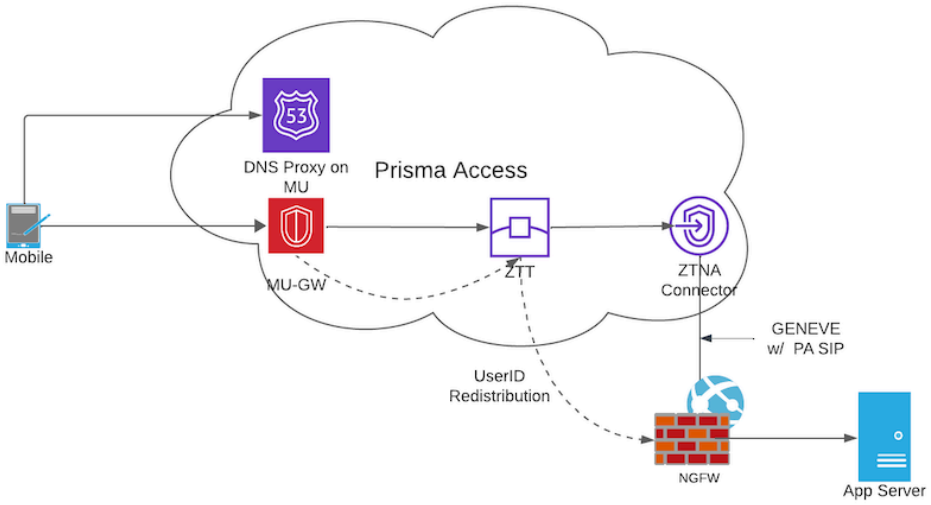
您可以在 Prisma Access 中使用 ZTNA 连接器来保护私有应用程序。要根据 User-ID 限制对应用程序的访问，您可以在私有应用程序所在的数据中心或总部位置部署新一代防火墙 (NGFW)；然后，根据 User-ID 映射在 NGFW 上配置策略规则。

如果您的部署在数据中心或总部位置使用新一代防火墙 (NGFW)，并且私有应用程序位于该位置，同时 ZTNA 连接器执行源 NAT，则 NGFW 无法检索 User-ID 映射。源 NAT 在 ZTNA 连接器上阻止 NGFW 获取客户端 IP 地址，这对映射至关重要。如果 NGFW 无法检索此客户端 IP 地址，则无法根据 User-ID 映射强制执行您在其上创建的基于区域的安全策略规则。

ZTNA 连接器在 NGFW 安全数据中心内启用 User-ID 的职责如下：

1. 为 NGFW 提供与区域 ZTNA 连接器隧道终端 (ZTT) 的安全连接，以便 NGFW 连接到其 User-ID 重新分发代理。
2. 对于 FQDN 应用程序，健康状况探测设置为 tcpping，应用程序探测数据中心应用程序，以便确定该应用程序是否正常运行，并且可以从此单个连接器访问。
3. 在 Geneve 数据包中封装用户到应用程序的后 NAT 数据中心空间 IP 数据包，包括原始源 IP 地址选项。

下图说明了将源 IP 地址提供给 NGFW 的 User-ID 映射的网络元素，并将 Generic Network Virtualization Encapsulation (Geneve) 封装的数据包（包括原始 Prisma Access 源 IP 地址选项）到 NGFW。这些元素使 NGFW 能够有效地根据 User-ID 执行安全策略规则。



限制：

 ©2025 Palo Alto Networks, Inc.

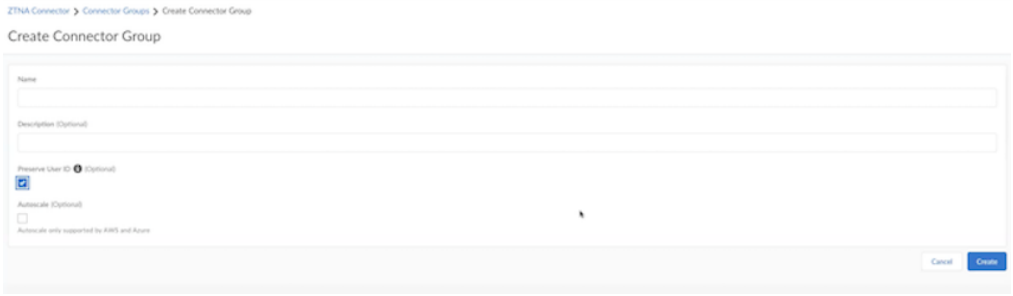
- 具有 ZTNA 连接器的 User-ID 支持仅在高于以下版本的版本中可用：
  - Prisma Access 数据平面：10.2.4 版本及更高版本
  - Saas_agent：5.1.0 版本及更高版本
  - NGFW 版本：11.2.0 版本及更高版本
  - 连接器版本：6.2.4-ztna-connector-b3 版本及更高版本
- ICMP 探测不支持 FQDN 目标，这些目标附加在基于 User-ID 的连接器组上。
- NGFW 服务路由配置仅支持具有静态 IP 地址的 UID 代理接口。如果 NGFW 接口配置为动态模式（通过 DHCP 分配 IP 地址），则 NGFW 到 ZTT 的 User-ID 通道无法支持 ZTNA 连接器 User-ID。要解决此问题，您必须在 NGFW 上为 UID 代理设置要使用的接口，并分配一个静态 IP 地址。
- 基于 User-ID 的连接器不支持 ping 和 traceroute 等诊断工具。

此过程假设您已配置以下网络设置：

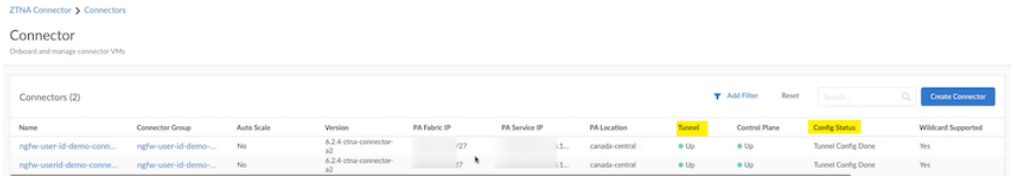
- 您已在总部或私有应用程序所在的数据中心部署 NGFW。
- 您已根据在 NGFW 中创建的区域（不受信任区域和受信任区域）应用安全策略规则。这些安全政策规则包括 User-ID 强制执行。

为了确保您的网络将 User-ID 映射分发到总部或数据中心，请完成以下程序，这样，NGFW 将能够根据其从 GlobalProtect 学到的 User-ID 映射来执行安全策略规则。

STEP 1 | 创建连接器组，启用**Preserve User ID**（保留 **User-ID**），并添加 Connectors（连接器）。

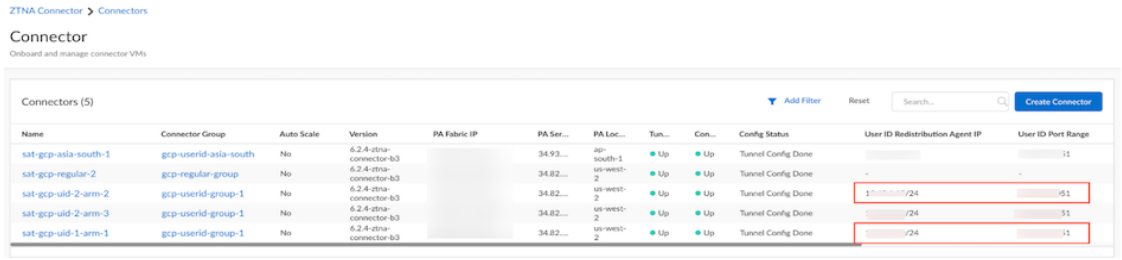


STEP 2 | 在您的数据中心部署和引导连接器，并检查隧道是否正常运行。

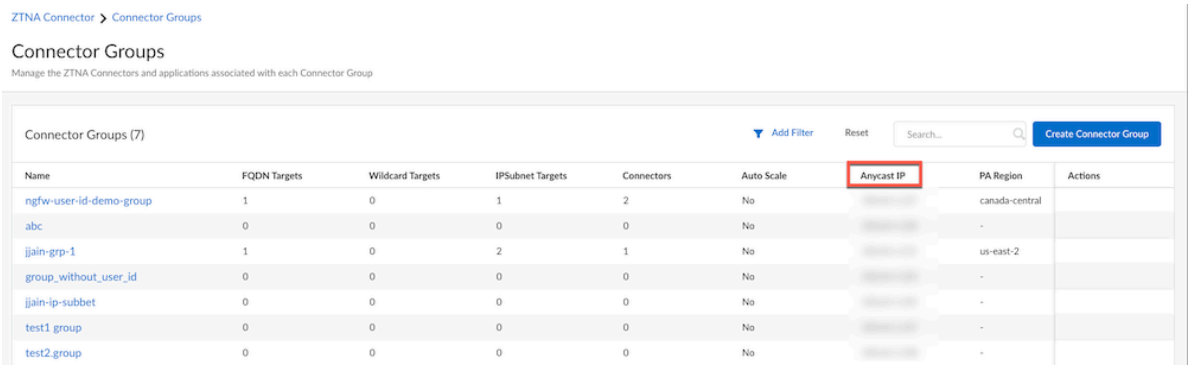


 ©2025 Palo Alto Networks, Inc.

STEP 3 | 转到 **Connector**（连接器），并记录连接器的 **User ID Redistribution Agent IP**（**User-ID** 重新分发代理 **IP**）和 **User ID Port Range**（**User-ID** 端口范围）。您需要这些 IP 地址和端口范围来配置 NGFW 上的 User-ID 重新分发代理。



此外，请转到 **Connector Groups**（连接器组），并记录 **Anycast IP**（任播 **IP**）。此 IP 地址是配置 NGFW 安全策略规则所必需的，用于允许来自此源 IP 地址的 TCP 应用程序探测。



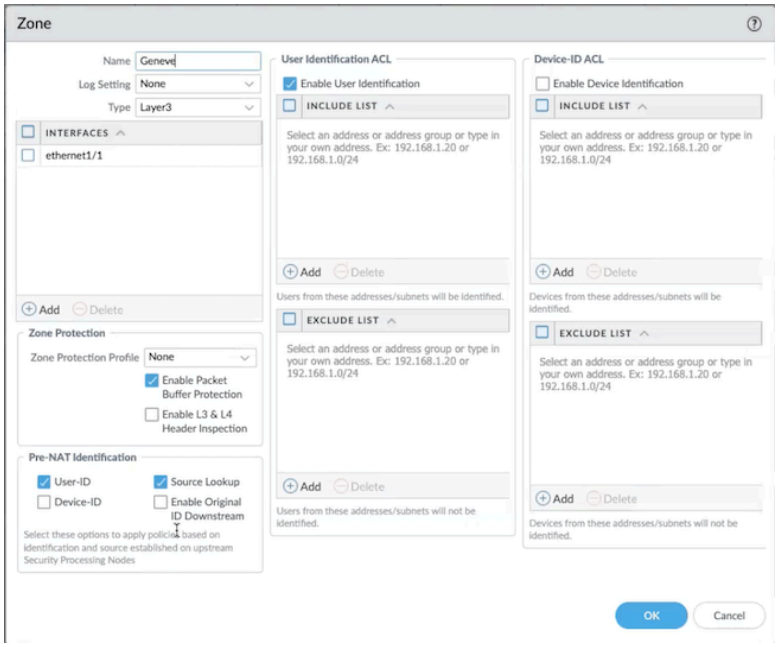
 ©2025 Palo Alto Networks, Inc.

STEP 4 | 在 NGFW 上输入 Pre-NAT 识别参数。

1. 登录到 NGFW 用户界面，转到 **Network**（网络） > **Zones**（服务区）并 **Add**（添加）两个服务区（连接 ZTNA 连接器的接口服务区和连接应用服务器的接口服务区），或选择现有服务区。

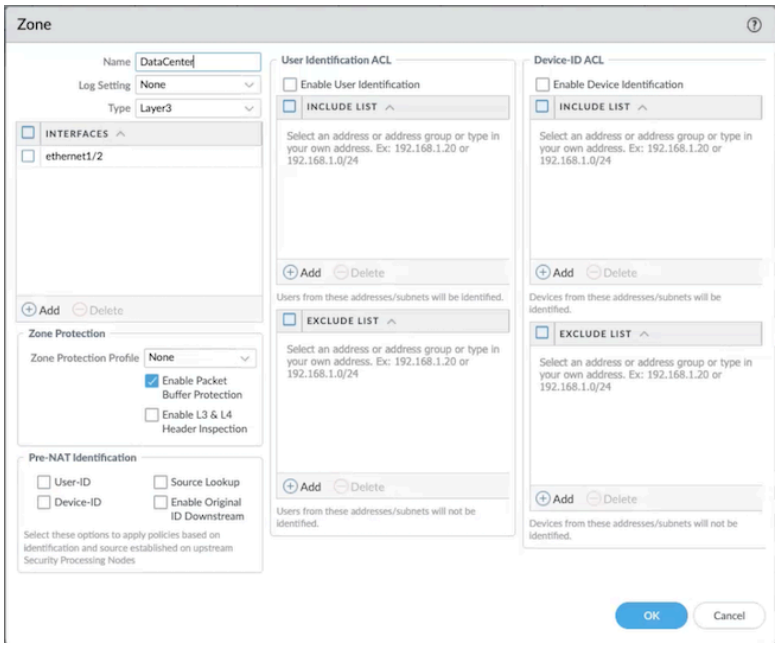
   1. 对于具有连接 ZTNA 连接器的接口的服务区，选择以下 **Pre-NAT Identification**（**NAT** 前导标识）：

      - **User-ID** — 保留在 IP 地址进行 NAT 之前使用的移动用户 User-ID 映射。如果您在安全策略规则中使用 User-ID，请启用此选项。
      - 源查找 — 可以匹配从 GlobalProtect 收到的原始来源 IP 地址。

   2. 对于连接到应用程序服务器服务区的接口，您不必选择任何 **Pre-NAT Identification**（**NAT** 前导标识）参数。

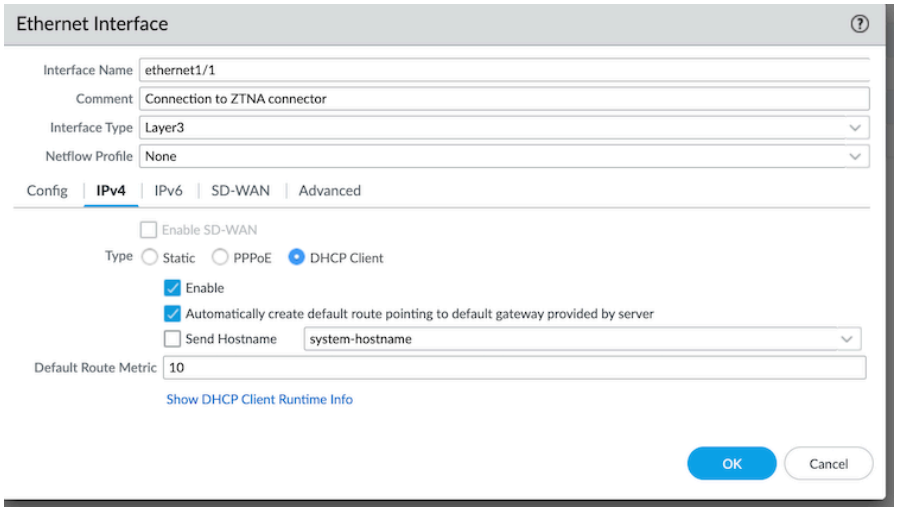
 ©2025 Palo Alto Networks, Inc.



3. 单击 **OK**（确定）并 **Commit**（提交）更改。

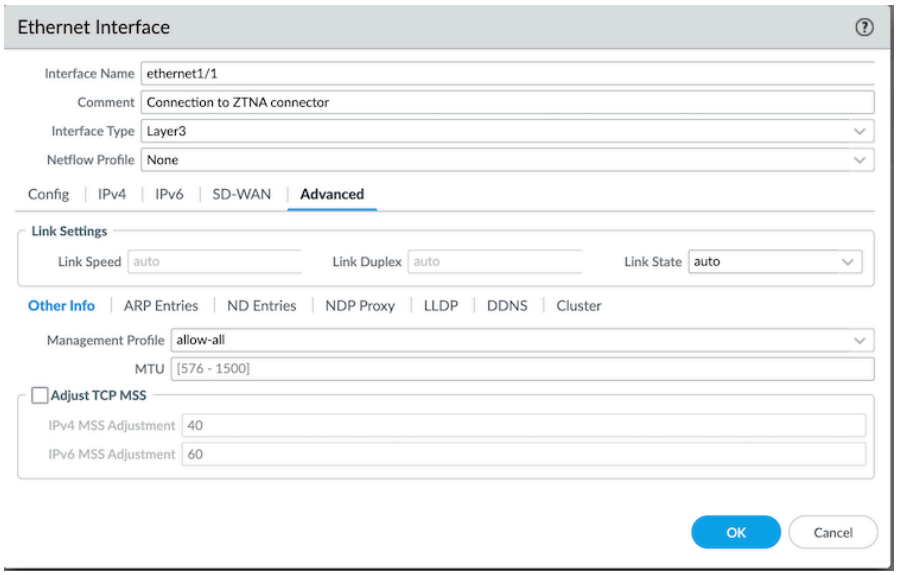
2. 将 IP 地址添加到接口。

   1. 转到 **Network**（网络） > **Interfaces**（接口） > **Ethernet**（以太网）。
   2. 选择连接到 ZTNA 连接器和应用服务器的接口，并进行配置。添加 **Interface name**（接口名称）和 **Interface type**（接口类型）到 **Layer 3**（第 3 层）。



   3. 对于连接到应用程序服务器的以太网接口，请取消选择**Automatically create default route pointing to default gateway provided by server**（自动创建指向服务器提供的默认网关的默认路由）复选框。

 ©2025 Palo Alto Networks, Inc.



3. 前往 **Interfaces**（接口）并将静态 IP 地址添加到接口。将面向 ZTNA 连接器的接口添加到 ZTNA 连接器区域 (Geneve)，并将面向应用程序服务器的接口添加到应用程序服务器区域（数据中心）。

STEP 5 | 创建与 NGFW 的命令行界面 (CLI) 会话，并在配置模式下输入以下命令：

```
set deviceconfig setting preserve-prenat-feature yes
```

如果您将来需要禁用此功能，请输入 `set deviceconfig setting preserve-prenat-feature no`。

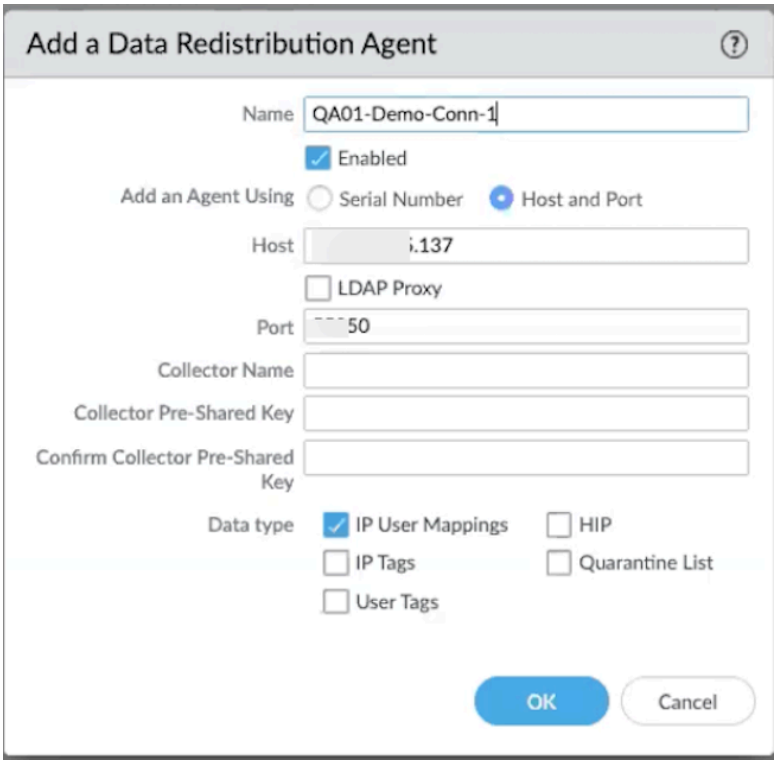
©2025 Palo Alto Networks, Inc.

STEP 6 | 在设置 *User-ID* 重新分发时，您必须在第 *3* 步 ***User ID Port Range***（***User-ID*** 端口范围）中为指定范围内的每个端口添加一个重新分发代理条目。例如，如果范围是 *55050-55055*，则必须配置 *6* 个条目，以便与已部署的 *ZTNA* 连接器区域的数量保持一致。

对于该范围内的每个端口，请在第 *3* 步的 ***User ID Redistribution Agent IP***（***User-ID*** 重新分发代理 ***IP***）中为 ***Host***（主机）字段选择一个 *IP* 地址。如果您希望在 *ZTNA* 连接器级别实现冗余，可以从 ***User ID Redistribution Agent IP***（***User-ID*** 重新分发代理 ***IP***）中选择两个地址，并为这两个 *IP* 地址应用完整的端口范围。或者，可以配置 ***User ID Redistribution Agent IP***（***User-ID*** 重新分发代理 ***IP***）中的所有 *IP* 地址上的所有端口。

为 **User ID Port Range**（**User-ID** 端口范围）内的每个端口添加一个重新分发代理，并使用 **User ID Redistribution Agent IP**（**User-ID** 重新分发代理 **IP**）中的一个或多个地址。

1. 在 NGFW 用户界面中，转到 **Device**（设备），然后选择 **Data Redistribution**（数据重新分发）。
2. 单击 **Add**（添加）并添加 **Name**（名称），然后选择 **Enabled**（已启用）复选框。
3. 选择 **Host and Port**（主机和端口），在第 3 步的 **Host**（主机）中添加 **User ID Redistribution Agent IP**（**User-ID** 重新分发代理 **IP**），然后添加 **User ID Port Range**（**User-ID** 端口范围）。
4. 启用 **IP User Mappings**（**IP** 用户映射）复选框，然后单击 **OK**（确定）。

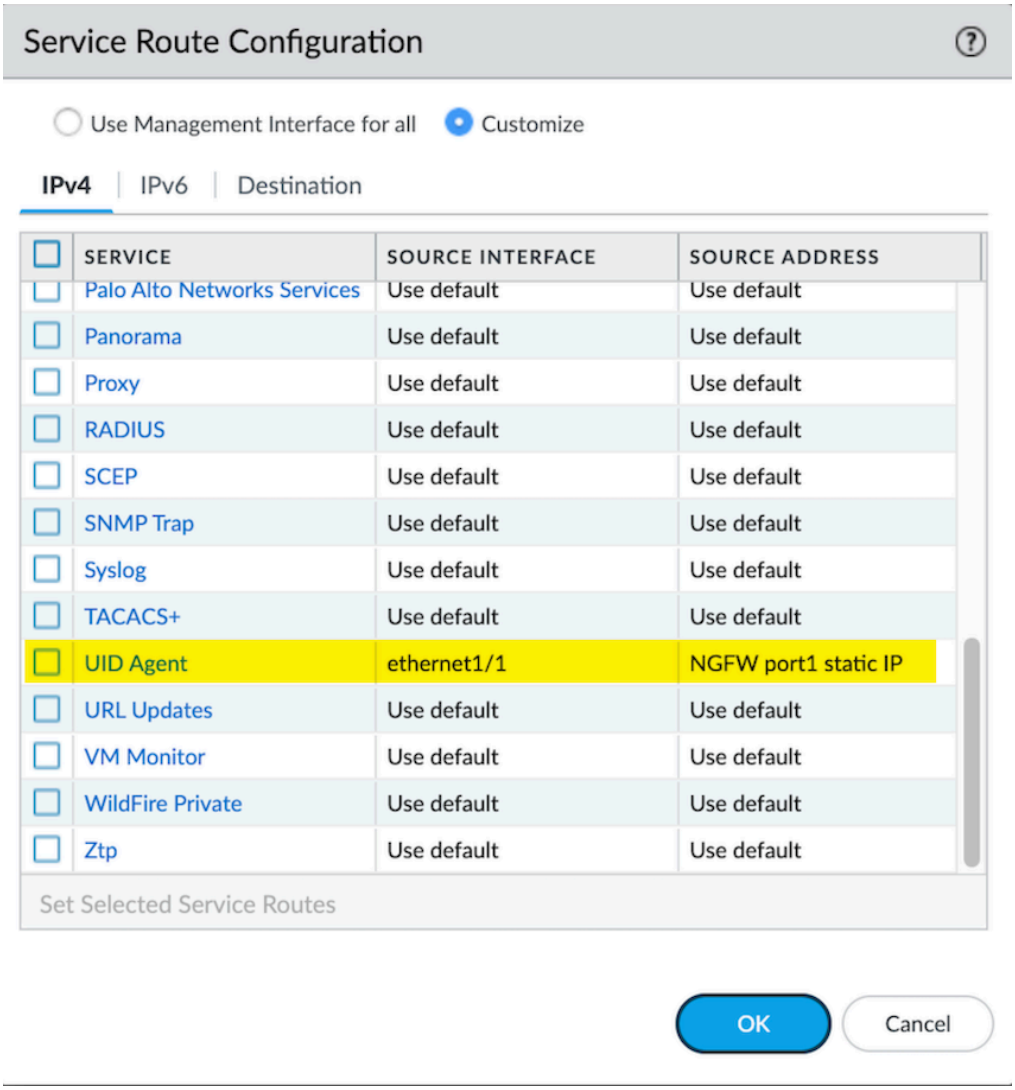


5. 单击 **Commit**（提交）以保存配置。

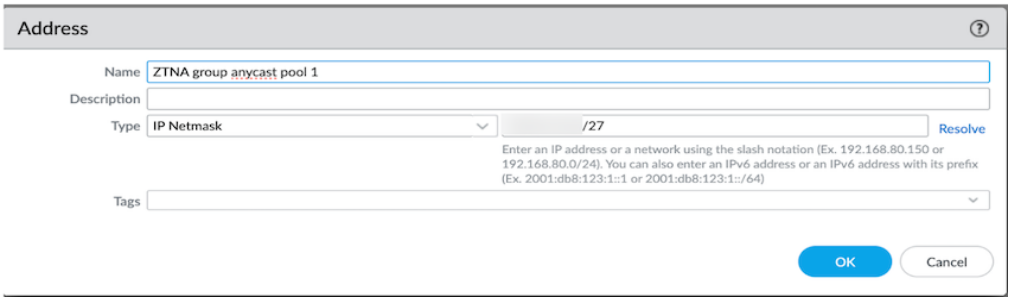
©2025 Palo Alto Networks, Inc.

STEP 7 | 在 NGFW 用户界面中，转到 **Device**（设备） > **Setup**（设置） > **Services**（服务） > **Service Route Configuration**（服务路由配置） > **Customize**（自定义） > **UID agent**（**UID** 代理）。

1. 在 **IPv4** 下，选择 **SOURCE INTERFACE**（源接口）作为 **Ethernet1/1**（面相 ZTNA 连接器的接口），然后添加 **SOURCE ADDRESS**（源地址）。



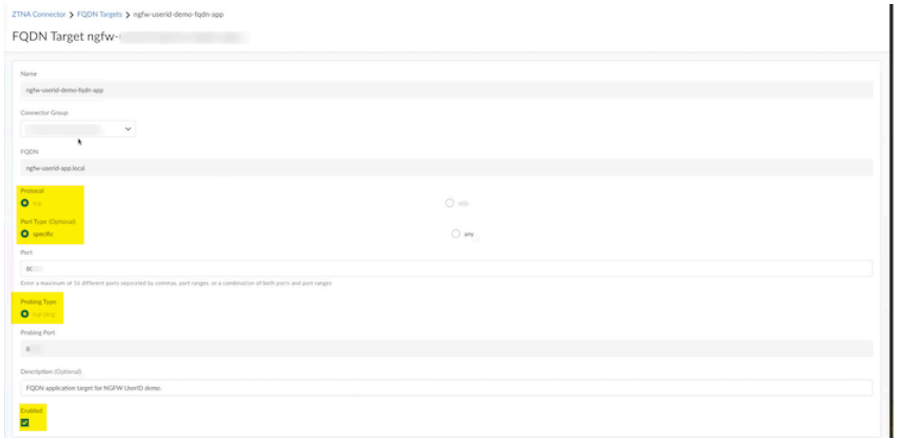
STEP 8 | 添加安全策略规则以允许具有源 IP 地址的 TCP 数据包。添加源 IP 地址，即在第 3 步中复制的任播 IP 地址，然后单击 **OK**（确定）。



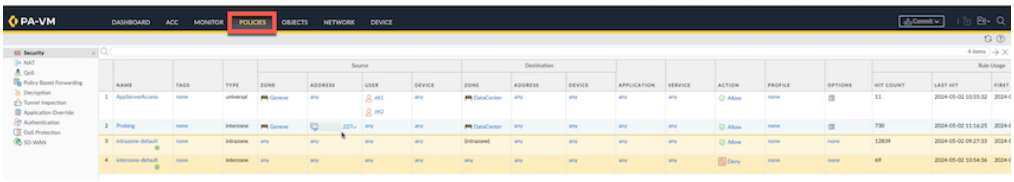
 ©2025 Palo Alto Networks, Inc.

STEP 9 | ）启用 TCP 探测。

1. 要创建一个 FQDN 目标：
   1. 转到 **Workflows**（工作流） > **Application Targets**（应用程序目标） > **FQDN Targets**（**FQDN** 目标），然后单击 **Create FQDN Target**（创建 **FQDN** 目标）。
   2. 添加 **Name**（名称）并选择 **Connector Group**（连接器组）。
   3. 启用 **tcp**、**specific**、**tcp ping** 和 **Enabled**（已启用）。添加 **Port**（端口），然后单击 **Create**（创建）。



STEP 10 | 在 NGFW 用户界面中，转到 **Policies**（策略）并定义基于 User-ID 的策略。



 ©2025 Palo Alto Networks, Inc.

 ©2025 Palo Alto Networks, Inc.

配置动态特权访问设置

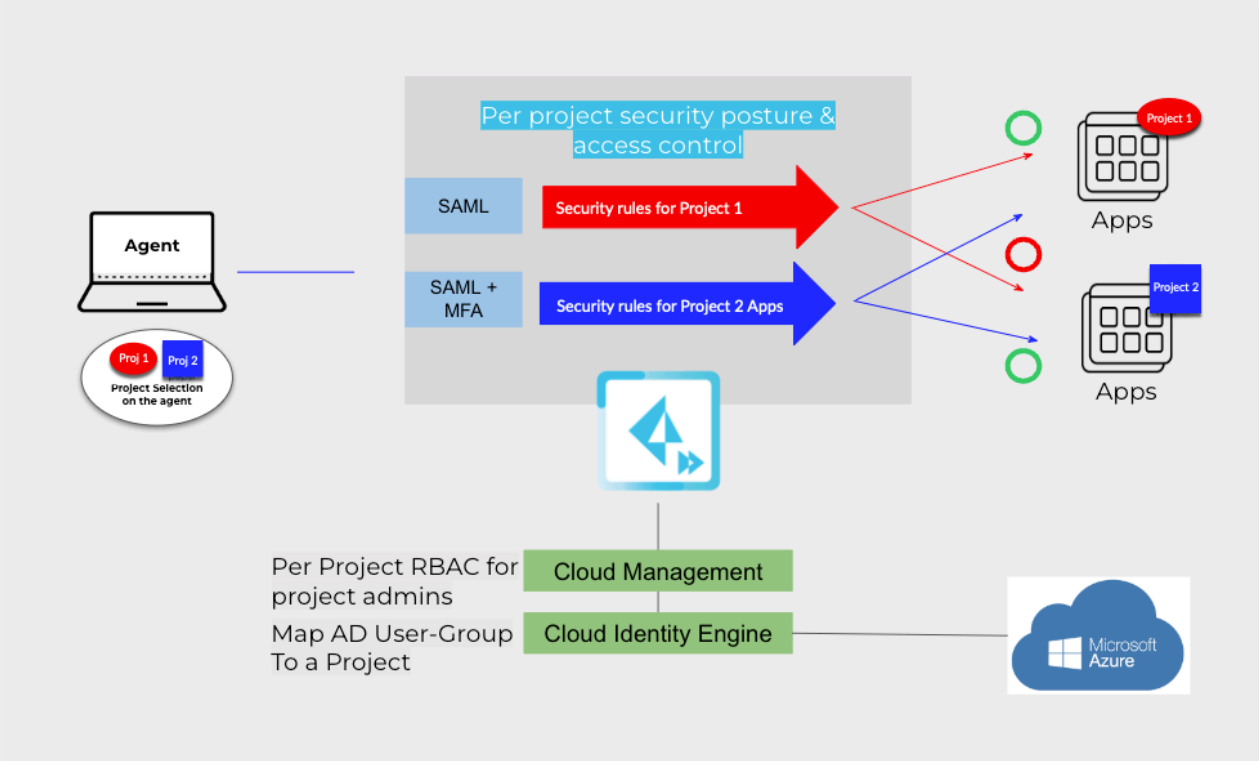
在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 许可证 ❑ Prisma Access 5.1 ❑ 角色：超级用户

对于需要控制哪些用户可以访问其客户项目的 IT 企业和基于 IT 的服务 (ITES) 公司，动态特权访问为您的用户提供了一种无缝、安全且独立的方式，使其只能访问分配给他们的项目。这些公司通常会将多个客户项目分配给员工，并提供对这些项目的孤立访问权限，以便授权用户一次只能访问一个客户项目。

什么是动态特权访问？

动态特权访问是 Prisma Access 中的一项功能，它根据用户在 Prisma Access Agent 中选择的工作流或项目为用户提供动态特权。根据分配给项目的用户组和 IP 池的组合来确定用户的动态特权。通过这种唯一的组合来定义项目。使用动态特权访问，您可以隔离网络中的资源，用户只能根据所分配的项目来访问这些资源。

Prisma Access 上提供一个称为 **Project Admin**（项目管理员）的新的预定义角色，允许项目管理员创建和管理项目定义。项目管理员可以将项目映射到所选的 Prisma Access 地点组，并根据项目和地点组使用 DHCP 创建 IP 地址分配。项目管理员只能在 Strata Cloud Manager 中管理分配给他们的项目。



当最终用户登录到在其托管设备上启用了动态特权访问的 Prisma Access Agent 时，将执行以下工作流：

1. 最终用户选择分配给他们的项目（例如，项目 1）。
2. 在 Cloud Identity Engine 中对其进行身份验证，以便将该用户的用户组映射到项目。
3. 身份验证成功并且其用户组符合项目管理员设置的项目条件后，用户可以通过项目 1 的项目特定设置以及提供每个项目的安全状况和访问控制的安全规则来访问网络中的资源。安全基础架构应用安全规则来限制用户仅访问属于该项目的资源和应用程序。不允许访问其他项目的资源和应用程序。
4. 当用户切换到其他项目（例如，项目 2）时，他们将退出上一个项目（项目 1）。然后，他们可以根据该项目的项目特定设置和安全规则访问第二个项目的资源。

您可以使用 Strata Cloud Manager 监控用户的项目活动，并查看网络中的服务消耗和安全状况，从而了解 Prisma Access Agent 部署。

©2025 Palo Alto Networks, Inc.

通过 Common Services 为 Prisma Access 启用动态权限访问

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 许可证（含移动用户订阅） ❑ 激活链接 ❑ Strata Logging Service ❑ 云身份引擎 ❑ Prisma Access Agent ❑ 角色：多租户 Superuser 或有权访问客户支持门户的 Superuser

借助动态权限访问权限，IT 管理员可以将最终用户映射到多个客户项目。授权用户一次只能访问一个客户项目。

动态权限访问是激活新 Prisma Access 租户期间的一项可选功能。启用此功能并激活租户后，DPA 将在租户生命周期内有效，您无法将其禁用。

启用 DPA 的选项只有在首次激活新的 Prisma Access 租户期间可以使用一次。激活租户后，将以下所有激活（包括附加组件和续订）隐藏该选项。该选项不适用于现有租户。

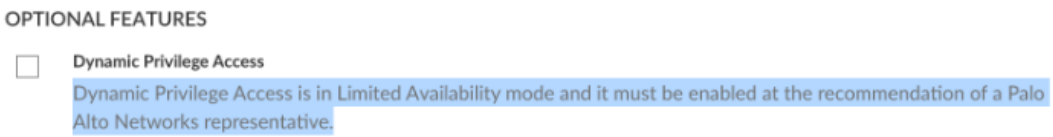
STEP 1 | 要为您的租户启用此功能，请联系您的 Palo Alto Networks 客户代表。

STEP 2 | 为 Prisma Access (Managed by Strata Cloud Manager) 激活许可证。

STEP 3 | 请务必分配许可证，规划服务连接，并相应地添加其他位置。

STEP 4 | 启用可用的附加程序。

STEP 5 | 选中 **Dynamic Privilege Access**（动态权限访问）复选框。



STEP 6 | 同意条款和条件。

STEP 7 | 立即激活。您正在激活的产品和附加程序（例如 Prisma Access 或 Strata Logging Service）现已预配置完毕。激活订阅时会显示进度。该过程完成后，租户状态显示为 Up（已启动）。现在，您已经为租户配置了购买的产品实例。租户有一个用户，即您在开始此过程时使用的帐户。

©2025 Palo Alto Networks, Inc.

STEP 8 | 要完成剩余的产品设置，您必须访问所购买的产品并执行所有必需的安装后配置。有关您的产品的信息，请参阅：

- 打开 API
- Strata Logging Service 入门指南
- Prisma Access (Managed by Strata Cloud Manager) 管理员指南
- 云身份引擎入门指南

STEP 9 | 添加用户访问权限并分配角色。

基于项目为用户提供项目管理员的访问权限。

 ©2025 Palo Alto Networks, Inc.

在 Cloud Identity Engine 中授权用户组映射进行动态特权访问

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 许可证 ❑ 要求的最低 Prisma Access 版本：5.1 ❑ 角色：超级用户

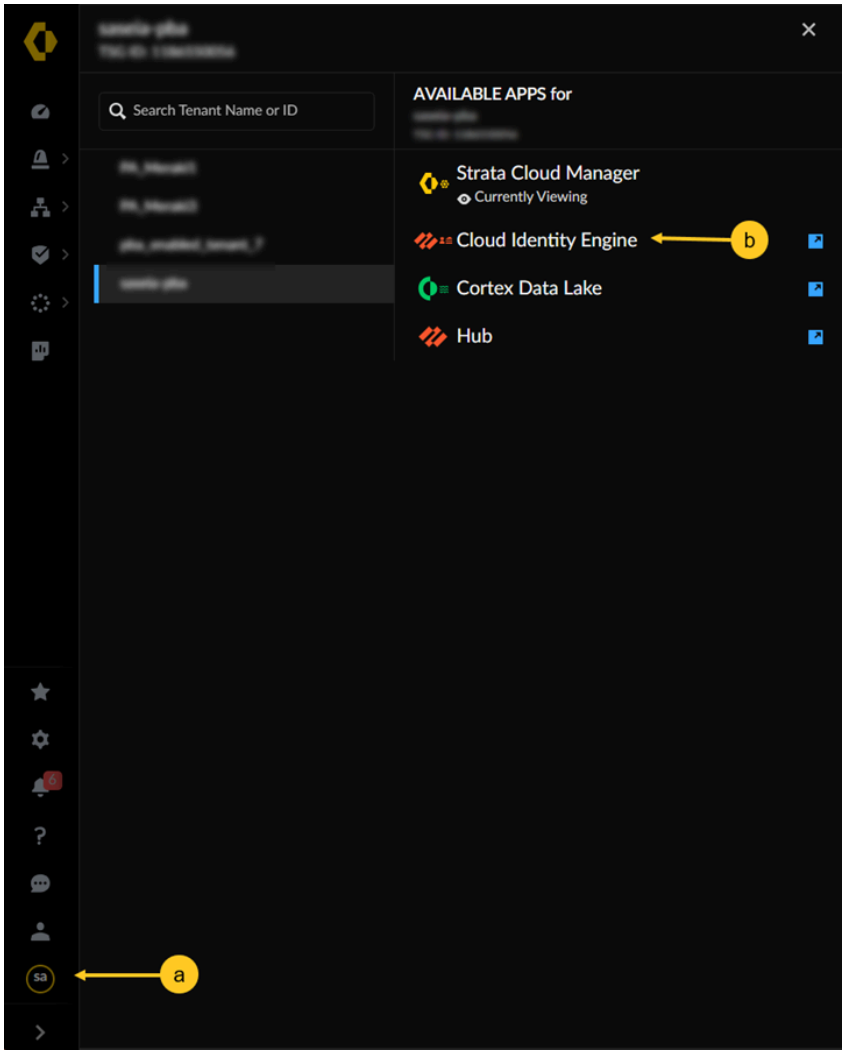
开始之前，请确保您已满足以下先决条件：

- 联系您的 Palo Alto Networks 客户代表以激活动态特权访问功能。
- 激活 Cloud Identity Engine 并创建您的第一个租户。
- 设置 Cloud Identity Engine。

在此工作流程中，我们使用 Azure 作为 IdP。您也可以使用 Okta 作为 IdP。

©2025 Palo Alto Networks, Inc.

STEP 1 | 从 Strata Cloud Manager 中，打开与您的租户关联的 Cloud Identity Engine 应用程序。



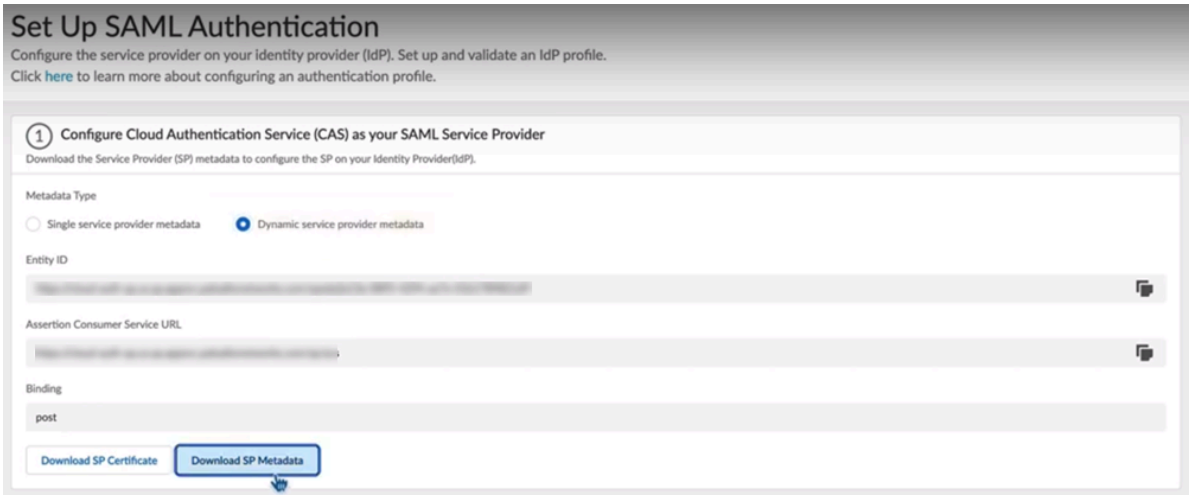
STEP 2 | 添加 Azure 目录或 Okta 目录 作为移动用户的 IdP。

©2025 Palo Alto Networks, Inc.

STEP 3 | 在 Cloud Identity Engine 应用程序中下载 SP 元数据。

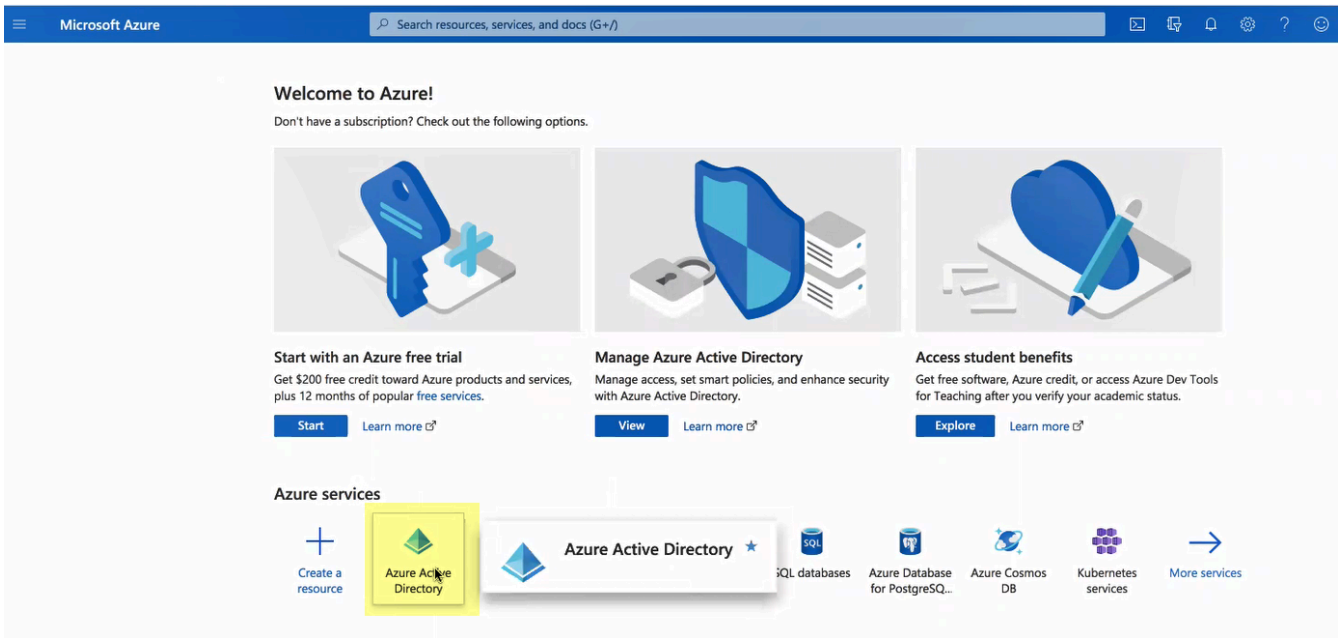
1. 转到 **Authentication**（身份验证） > **Authentication Types**（身份验证类型） > **Add New Authentication Type**（添加新的身份验证类型）。
2. **Set Up**（设置）SAML 2.0 身份验证类型。

   选择 **Dynamic service provider metadata**（动态服务提供商元数据）。
3. **Download SP Metadata**（下载 **SP** 元数据）。



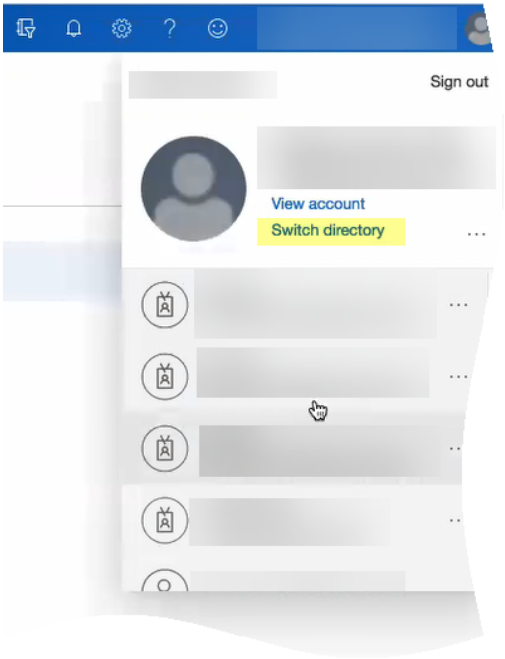
4. 登录到 Azure 门户并选择 **Azure Active Directory**。

   确保在 Azure 门户中完成所有必要的步骤。

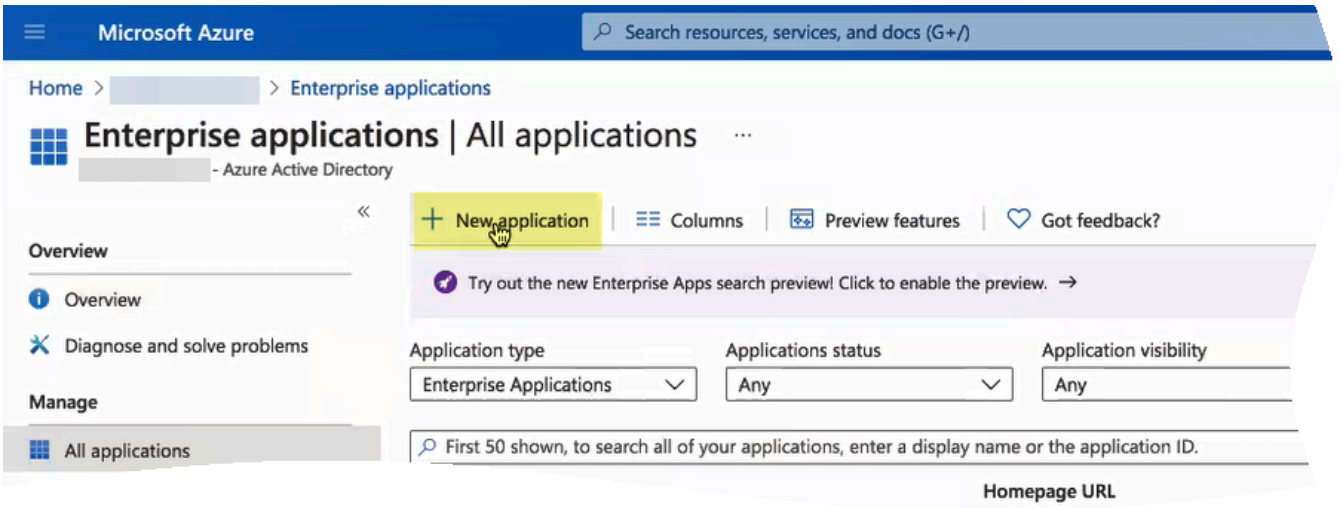


   如果您有多个目录，请 **Switch directory**（切换目录）以选择要用于 Cloud Identity Engine 的目录。

 ©2025 Palo Alto Networks, Inc.



5. 选择 **Enterprise Applications**（企业应用程序），单击 **New application**（新建应用程序）。



6. 搜索 **`Palo Alto Networks Cloud Identity Engine - Cloud Authentication Service`** 并创建 Azure Active Directory (AD) 单点登录集成。

   创建应用程序时，根据需要自定义应用程序名称。

7. 应用程序加载后，选择 **Users and groups**（用户和组），然后选择 **Add user/group**（添加用户/组）以将其 **Assign**（分配）给此应用程序。

   选择要在 Cloud Identity Engine 中使用 Azure IdP 进行身份验证的用户和组。

   请务必分配您正在使用的帐户，以便在配置完成后对其进行测试。添加帐户后，您可能需要刷新页面才能成功完成测试。

8. **Set up single sign-on**（设置单点登录），然后选择 **SAML**。

©2025 Palo Alto Networks, Inc.

9. 浏览到您在步骤 3.c 中从 Cloud Identity Engine 应用程序下载的元数据文件并单击 **Add**（添加），以便 **Upload Metadata File**（上传元数据文件）。
10. 元数据上传后，使用以下格式输入您的区域端点作为 **Sign-on URL**（登录 **URL**）：https://<RegionUrl>.paloaltonetworks.com/sp/acs（其中 <RegionUrl> 代表您的区域端点）。

    或者，将回复 URL 复制到登录 URL。
11. **Save**（保存）配置。

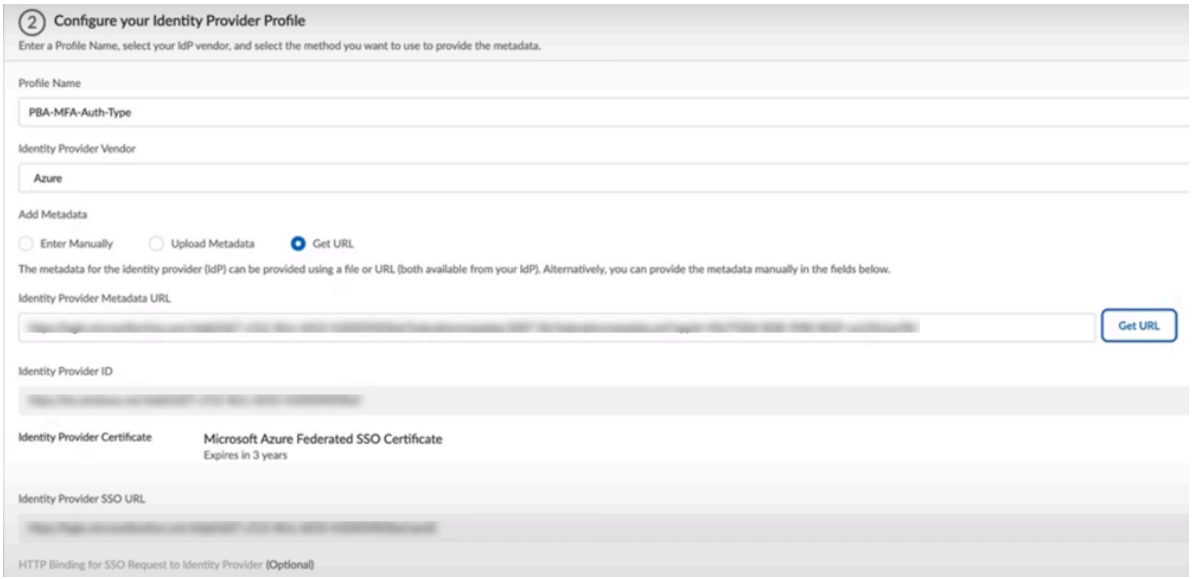
STEP 4 | 配置条件访问策略以对选定的用户组启用 MFA。

1. 转到应用程序的 **Overview**（概述） > **Conditional Access**（条件访问） > **Create a policy**（创建策略）。
2. 添加 **New Policy**（新建策略）。
3. 输入策略的名称。
4. 在 **Users**（用户）部分中，包括 **Select users and groups**（选择用户和组）并相应地选择您的项目组。
5. 验证 **Target resources**（目标资源）。
6. 选择触发策略的 **Conditions**（条件）。
7. 在 **Access Controls**（访问控制）中使用 **Require multifactor authentication**（需要多重因素身份验证）**Grant**（授予）访问权限。
8. 通过将选择器切换为 **On**（开）来启用策略，并 **Create**（创建）条件访问。

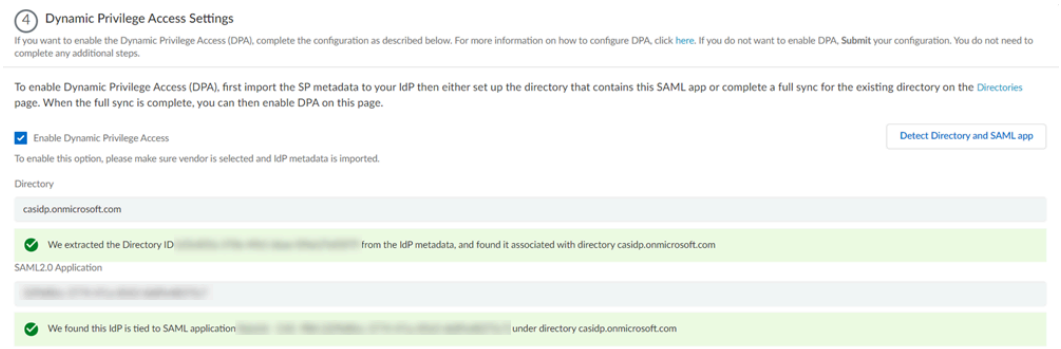
 ©2025 Palo Alto Networks, Inc.

STEP 5 | 添加您的 IdP 供应商作为身份验证类型。

1. 选择 **Single sign-on**（单点登录） > **SAML Certificates**（**SAML** 证书），并复制 **App Federation Metadata URL**（应用程序联合元数据 **URL**）。
2. 在 Cloud Identity Engine 应用程序中，选择 **Authentication**（身份验证） > **Authentication Types**（身份验证类型） > **Add New Authentication Type**（添加新的身份验证类型）。
3. **Set Up**（设置）SAML 2.0 身份验证类型。
4. 在 **Configure your Identity Provider Profile**（配置您的身份提供程序配置文件）下，输入 **Profile Name**（配置文件名称）。
5. 选择 **Azure** 作为您的 **IDP Vendor**（**IDP** 供应商）。
6. 选择 **Get URL**（获取 **URL**），粘贴步骤 5.a 中的 URL，然后选择 **Get URL**（获取 **URL**）以获取元数据。



7. 启用 **Multi-factor Authentication is Enabled on the Identity Provider**（在身份提供程序上启用多重因素身份验证）。
8. **Test SAML Setup**（测试 **SAML** 设置）以验证配置文件配置。
9. 选择您希望 Prisma Access 用于身份验证的 SAML 属性。
10. 启用 **Dynamic Privilege Access**（动态特权访问）。
    确保同步您在步骤 2 中添加的目录和 SAML 应用程序。



 ©2025 Palo Alto Networks, Inc.

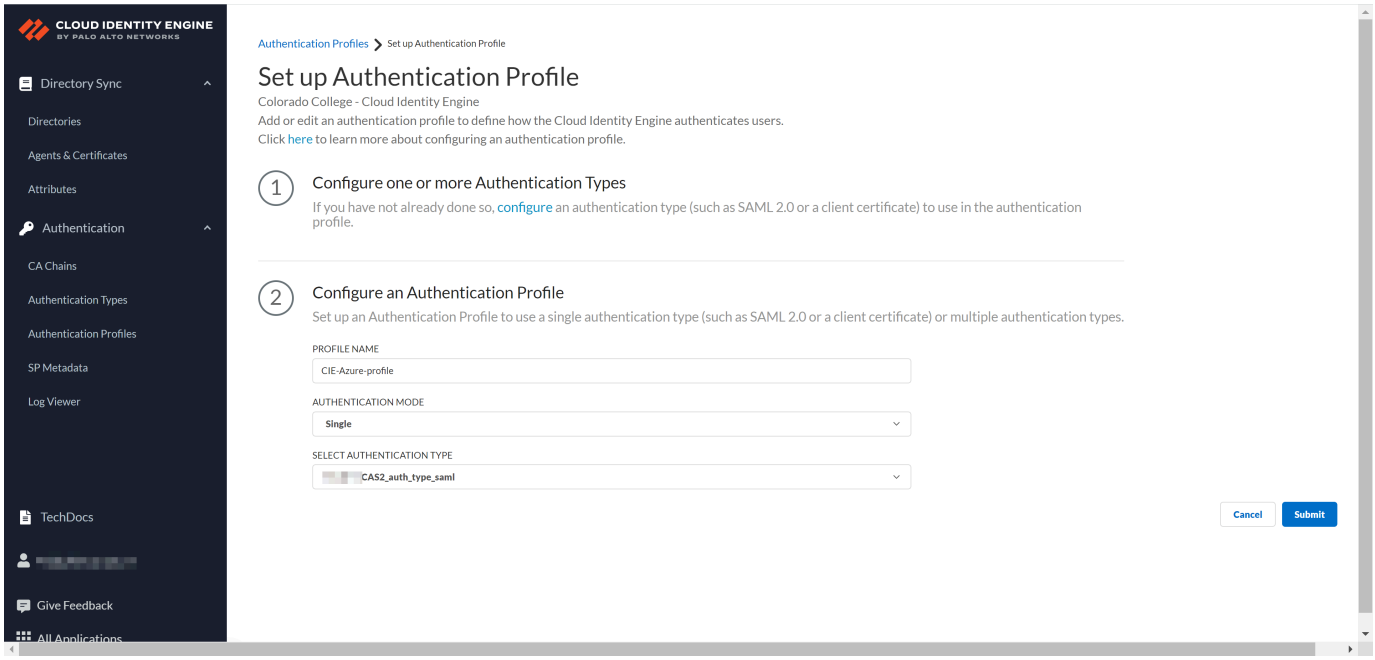
11. **Submit**（提交）IdP 配置文件。

STEP 6 | 重复步骤 3 到 5，为不需要 MFA 的用户组配置 SAML 应用程序。

对于不需要 *MFA* 的用户组，请勿在步骤 5.g 中启用 *MFA*。

STEP 7 | 为 MFA 用户组和非 MFA 用户组添加身份验证配置文件。

1. 选择 **Authentication**（身份验证） > **Authentication Profiles**（身份验证配置文件） > **Add Authentication Profile**（添加身份验证配置文件）。
2. 输入 **PROFILE NAME**（配置文件名称）。
3. 选择 **Authentication Mode**（身份验证模式）。
4. 根据需要 MFA 的用户组从步骤 5 或 6 中选择 **Authentication Type**（身份验证类型），然后选择 **Submit**（提交）。

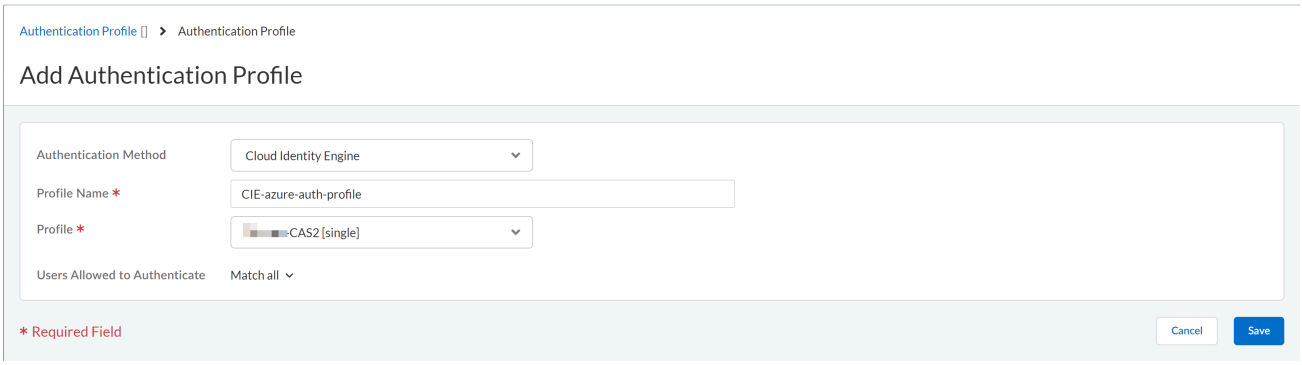


 ©2025 Palo Alto Networks, Inc.

STEP 8 | 将身份验证配置文件从 Cloud Identity Engine 添加到 Prisma Access。

1. 在 Strata Cloud Manager 中，选择 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Identity Services**（身份服务） > **Authentication**（身份验证） > **Authentication Profiles**（身份验证配置文件）。

   确保将配置范围设置为 **Access Agent** 移动用户容器。
2. 选择 **Add Profile**（添加配置文件）。
3. 选择 **Cloud Identity Engine** 作为您的 **Authentication Method**（身份验证方法）。
4. 输入 **Profile Name**（配置文件名称）。
5. 选择您在步骤 7 中添加到 Cloud Identity Engine 应用程序的 **Profile**（配置文件）。
6. **Save**（保存）更改。



STEP 9 | 将身份验证附加到移动用户。

1. 从 Strata Cloud Manager 启动 Prisma Access。
2. 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**）。
3. 将范围设置为您创建的项目代码段，然后导航到 **Security Services**（安全服务） > **Security Policy**（安全策略）。
4. 创建策略以仅允许来自特定项目 DHCP 范围和基于该项目的用户组的流量。

©2025 Palo Alto Networks, Inc.

启用访问客户端。

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 创新 ❑ macOS 12 或更高版本的桌面设备，或 Windows 10 版本 2024 或更高版本或 Windows 11 桌面设备 ❑ Prisma Access 许可证，且订阅了“移动用户” ❑ 角色：超级用户

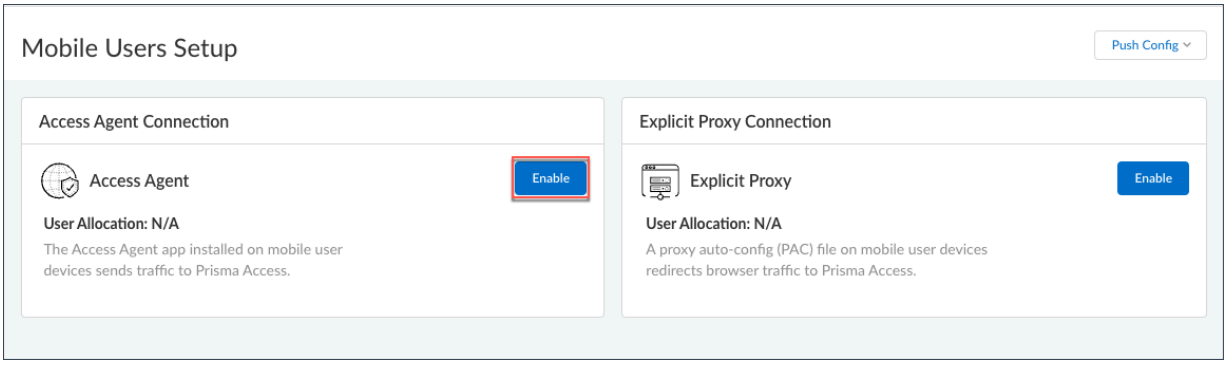
要想接入用户，必须先使用 Strata Cloud Manager 来启用访问代理并将其设置为移动用户连接类型。启用该连接类型后，安装在移动用户设备上的 Prisma Access Agents 将能够向 Prisma Access 发送流量。

开始启用 Prisma Access Agent 之前，请确保在 Cloud Identity Engine 中授权用户组映射进行动态特权访问。

STEP 1 | 选择 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Mobile Users**（移动用户）。

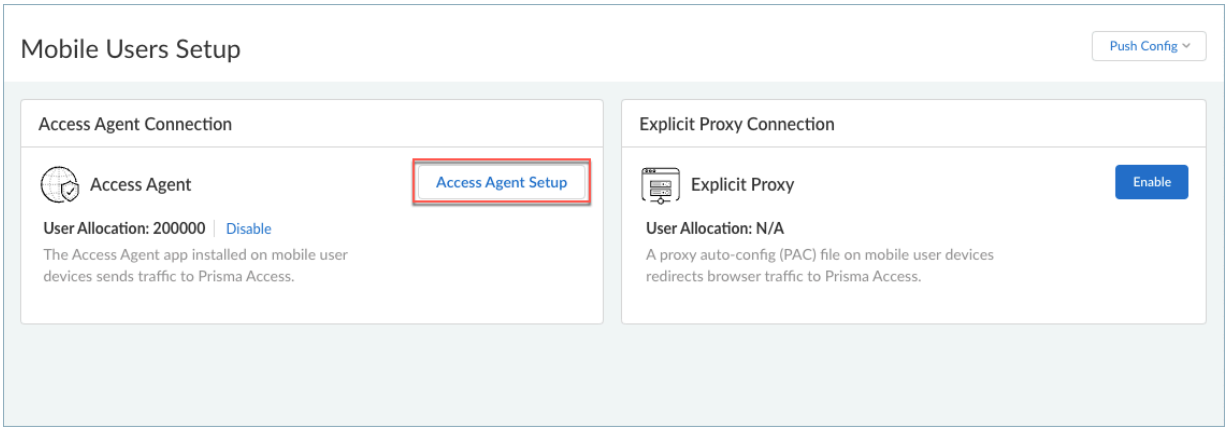
STEP 2 | 选择 **Enable**（启用）以启用访问代理。

Prisma Access Agent 不支持显式代理。

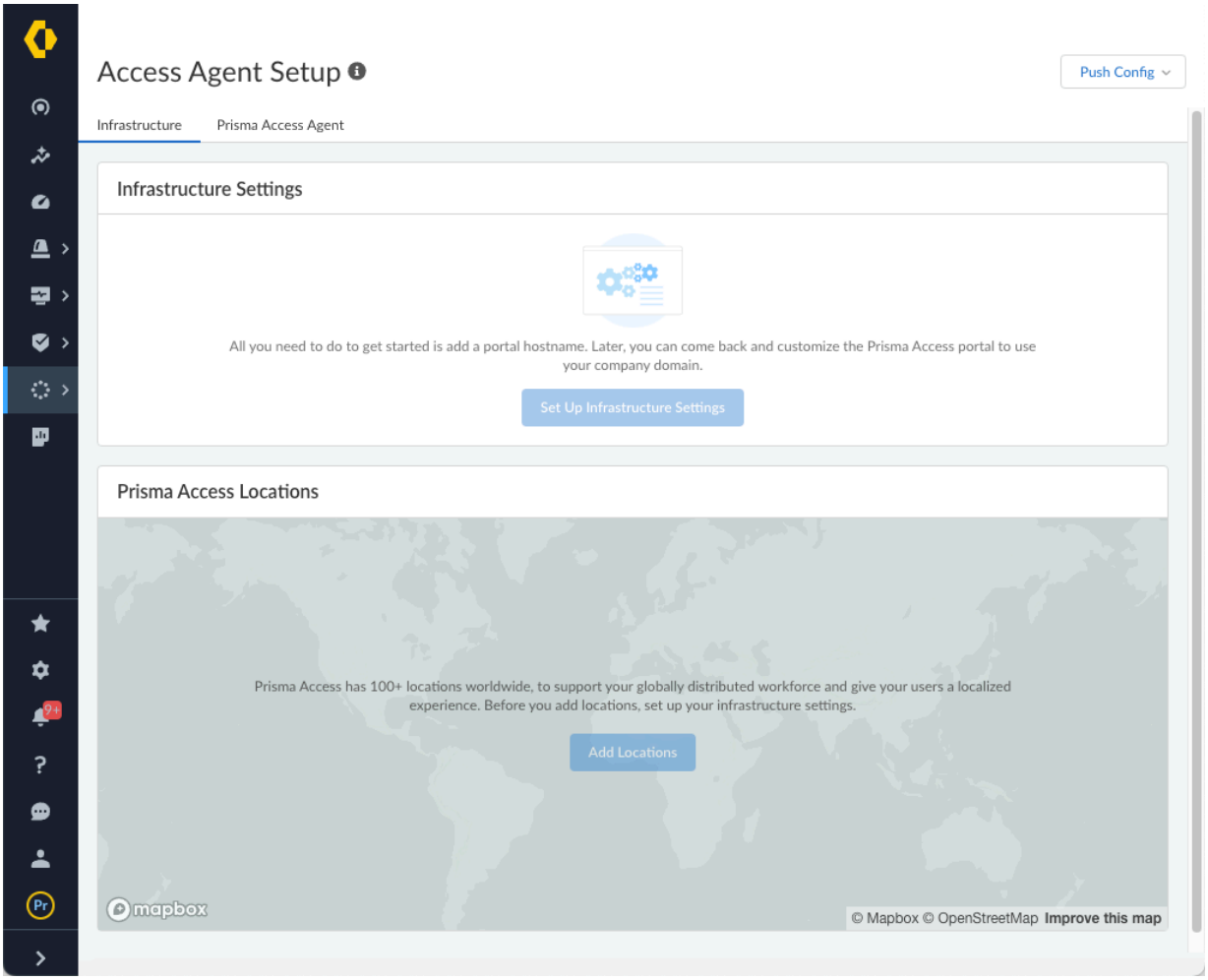


 ©2025 Palo Alto Networks, Inc.

STEP 3 | 单击 **Access Agent Setup**（访问代理设置）以开始载入您的移动用户。



此时将出现“Access Agent Setup（访问代理设置）”页面。



©2025 Palo Alto Networks, Inc.

为动态权限访问设置代理基础设施

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 创新 ❑ Prisma Access 许可证，且订阅了“移动用户” ❑ macOS 12 或更高版本的桌面设备，或 Windows 10 版本 2024 或更高版本或 Windows 11 桌面设备 ❑ 角色：超级用户

配置 Prisma Access Agent 的基础设施设置，以便 Prisma Access 能够为您的移动用户环境提供服务。然后，选择您的 Prisma Access Agent 用户将连接到的 Prisma Access 位置。

为动态权限访问启用 SC-NAT 支持为动态特权访问启用路由汇总如果您已创建服务连接以访问其数据中心或总部位置的私有应用程序，您还可以选择为动态特权访问启用 SC-NAT 支持，或者为动态特权访问启用路由汇总，以减少发送到网络的路由数量。

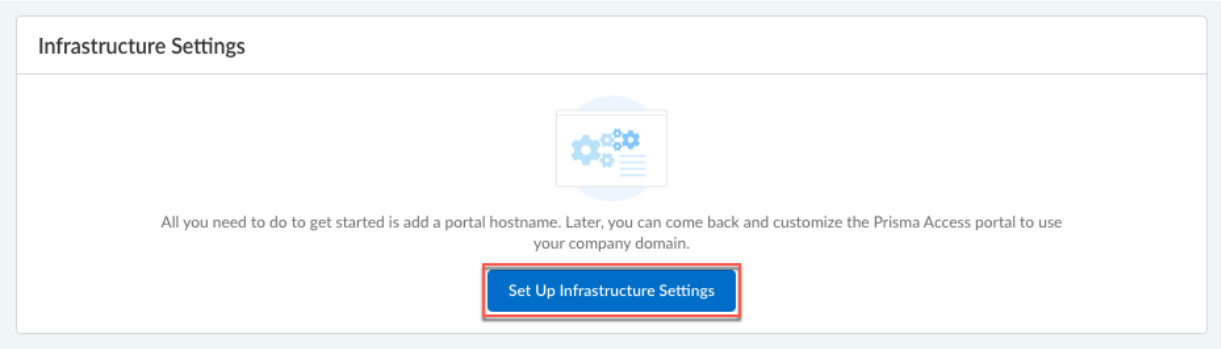
配置基础架构设置

Prisma AccessPrisma Access为了仅为用户启用互联网访问，提供了默认的IP地址池和云默认DNS服务器。Prisma AccessPrisma Accesshttps://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-cloud-managed-admin/prisma-access-service-infrastructure然而，如果您希望移动用户访问您总部、数据中心或您已接入的远程网络站点的内部资源，您必须分配客户端IP地址池。使用IP地址池为您的移动用户分配IP地址并建立Prisma Access服务基础设施。

在配置基础设施设置之前，请确保至少配置一个项目。否则，当您尝试提交和推送基础设施设置时，提交将失败。有关详细信息，请参阅创建项目。

STEP 1 | 在 Strata Cloud Manager 中，选择 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Access Agent**（访问代理） > **Infrastructure**（基础架构）。

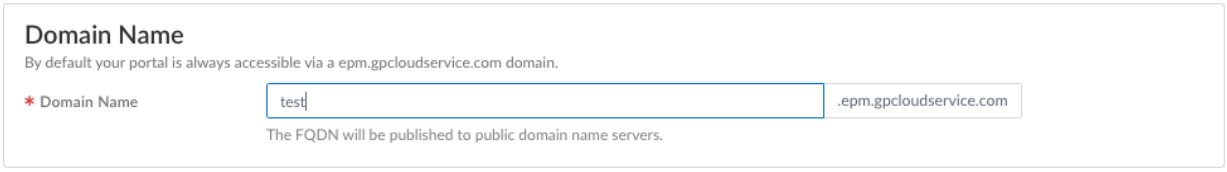
STEP 2 | 如果您是首次设置基础架构，请单击**Set Up Infrastructure Settings**（设置基础架构设置）。否则请编辑 **Infrastructure Settings**（基础架构设置）。



©2025 Palo Alto Networks, Inc.

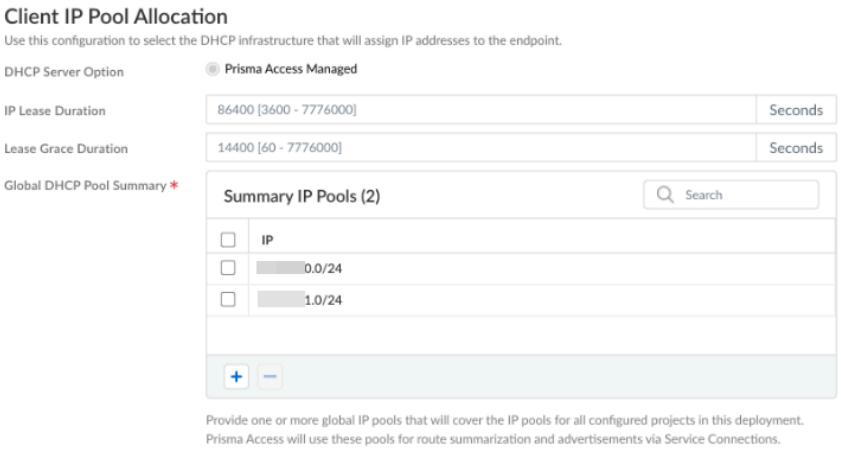
STEP 3 | 将主机名添加到 Prisma Access Agent 连接到的服务的 **Domain Name**（域名）中。

默认情况下，用户可以使用基于您的主机名和 **.epm.gpcloudservice.com** 域的 FQDN 来访问服务。



STEP 4 | Prisma Access在客户端IP池分配中，提供一个DHCP服务器，该服务器将管理IP地址分配给您的端点，以实现动态权限访问。

Prisma Access项目名称和位置组 ID 是 DHCP 请求的一部分。Prisma Access Agent每个连接到特定项目的设备都被分配一个来自该项目的IP子网的IP地址。Prisma Access Agent当用户切换到不同的项目时，将从项目的IP子网分配一个不同的IP地址。



您可以配置以下选项：

- Prisma Access AgentIP租赁持续时间—指定DHCP服务器为其分配网络地址的时间（以秒为单位）。默认的IP地址租赁持续时间为86400秒。
- Prisma Access Agent租约宽限期 - 指定在租约到期后，用户可以继续使用其IP地址租约的时间。默认租约宽限期为14,400秒。
- 为动态权限访问启用 SC-NAT 支持为动态特权访问启用路由汇总全局 DHCP 池摘要—选择您要启用 SC-NAT 的 IP 池，或配置并选择用于路由汇总的全局摘要 IP 池。

STEP 5 | 选择 **Save**（保存）以保存基础架构设置。

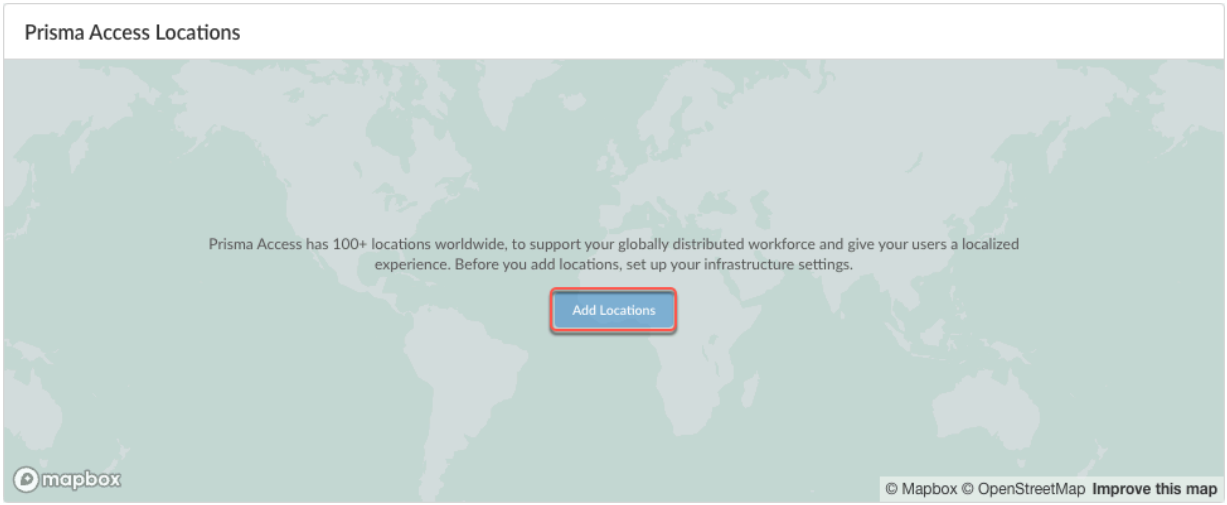
选择 Prisma Access 地点

选择要支持 Prisma Access Agent 用户的 Prisma Access 地点位置组用于动态特权访问。

STEP 1 | 在 Strata Cloud Manager 中，选择 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Access Agent**（访问代理） > **Infrastructure**（基础架构）。

 ©2025 Palo Alto Networks, Inc.

STEP 2 | 如果您是首次设置基础架构，请选择 **Add Locations**（添加位置）。否则请编辑 **Prisma Access Locations**（**Prisma Access** 位置）。



STEP 3 | 选择移动用户将连接到的 Prisma Access 位置。

根据您的许可协议，您可以选择本地或全球位置。该地图显示了您可以为用户部署 Prisma Access 的区域。此外，Prisma Access 还会在每个区域内提供多个位置，以确保您的用户能够连接到提供针对用户区域量身打造的用户体验的位置。要获得最佳性能，请全选。或者，在每

©2025 Palo Alto Networks, Inc.

个选定区域内选择用户需要访问的特定位置。通过将部署限制在单个区域，您可以更精细地控制已部署区域，并排除策略或行业法规要求的区域。

对于 *Prisma Access Agent*，您可以将 *Prisma Access* 部署到以下 *Strata* 日志记录服务区域：

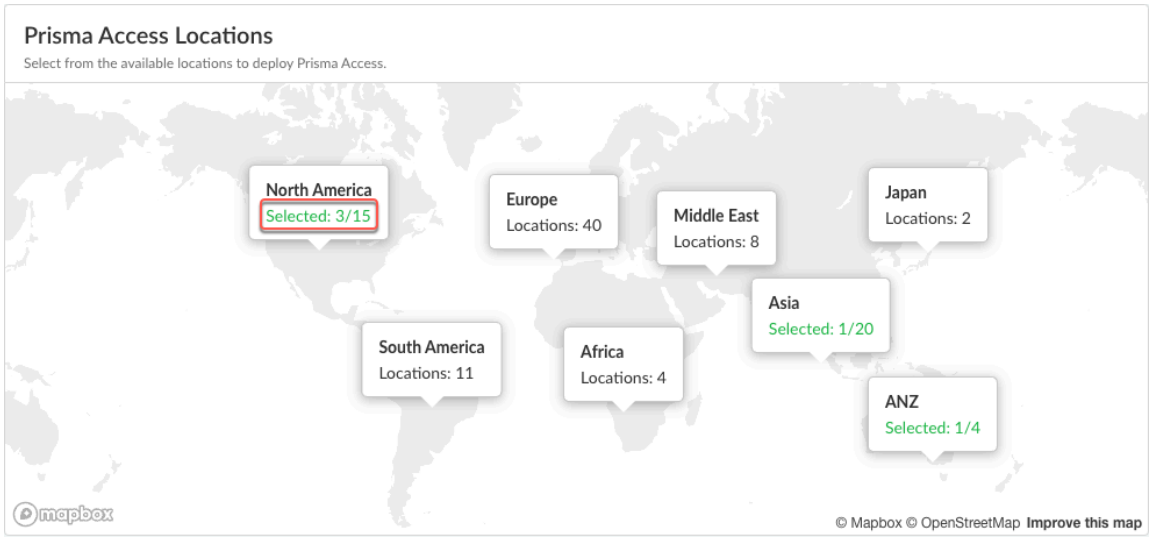
- 美国
- 德国
- 印度

此列表将随着更多区域可用而更新。

如果要限制位置数量，请选择离用户最近或与用户位于同一国家/地区的位置，以提供最佳用户体验。如果某个位置在您的移动用户居住的国家/地区不可用，请选择离用户最近的位置以提供最佳性能。

本节中的图片仅供参考。

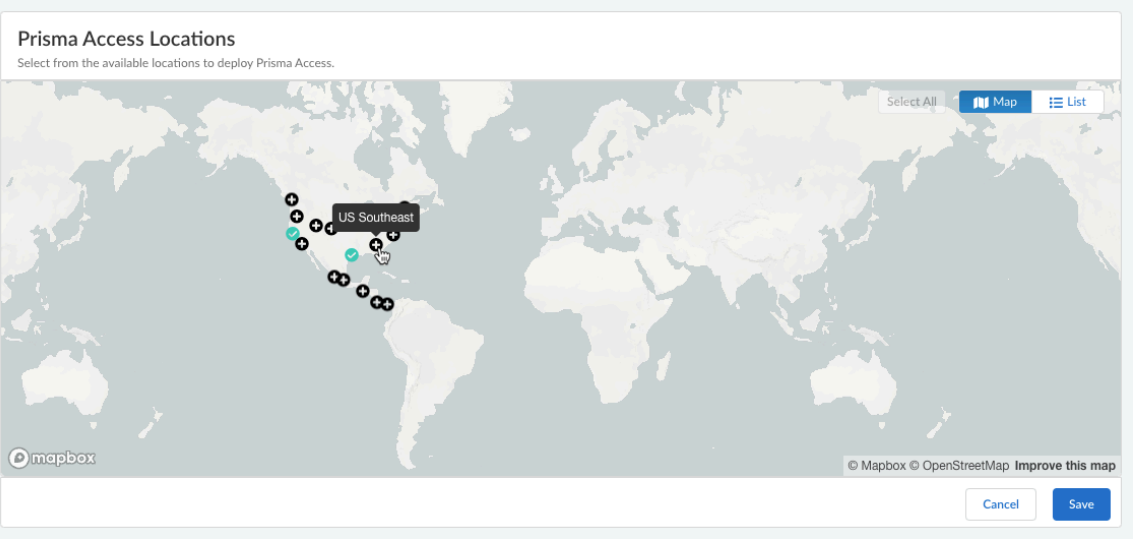
1. 在地图上选择一个可用的区域。



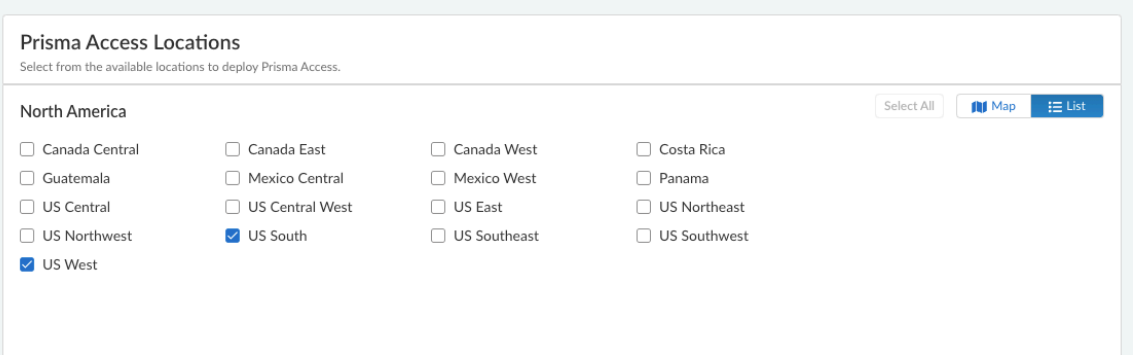
2. 在要添加的位置单击加号 **+**。

   可以在 **Map**（地图）视图和 **List**（列表）视图之间切换。您还可以选择 **Select All**（全选）以选择所有位置。

 ©2025 Palo Alto Networks, Inc.



在列表视图中，可以从可用位置列表中选择要部署 Prisma Access 的位置。您可以选择 **All**（所有）以选择区域内的所有站点。

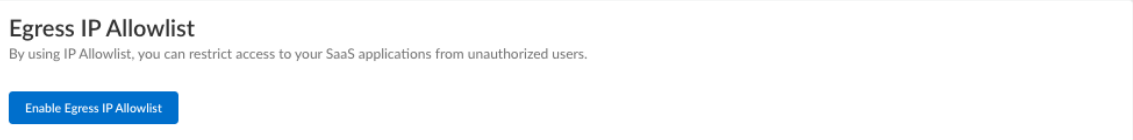


3. 选择 **Save**（保存）以保存您的 Prisma Access 位置设置。

STEP 4 | （可选）限制未经授权的用户访问您的 SaaS 应用程序。

您可以为现有移动用户部署以及在新用户载入期间启用出口 IP 允许列表。如果您为现有 Prisma Access 部署启用出口 IP 允许列表，Prisma Access 会将已为您的位置分配的所有出口 IP 地址迁移到出口 IP 允许列表中。对于新的 Prisma Access 部署，请在载入 Prisma Access Agent 移动用户时启用出口 IP 允许列表。每次您添加位置或发生自动缩放事件时，您都应该检索 Prisma Access 分配的新出口 IP 地址，并将其添加到 SaaS 应用程序中的允许列表。然后，您可以将配置推送到 Prisma Access 部署，以确认为您的位置分配的出口 IP 允许列表。

1. 选择 **Enable Egress IP Allowlist**（启用出口 **IP** 允许列表）将显示载入的 Prisma 访问位置的 IP 地址。



2. 复制分配的地址并添加到 SaaS 应用程序的允许列表中。
3. 选择 **Migrate**（迁移）以确认分配给 Prisma Access 中载入位置的 IP 地址。

 ©2025 Palo Alto Networks, Inc.

4. 针对新载入位置或在自动缩放事件期间检索 IP 地址。
   1. 选择 **Location**（位置）名称以查找分配给该位置的新出口 IP 地址。
   2. 在 Prisma Access 中确认这些 IP 地址之前，请将其添加到 SaaS 应用程序的允许列表中。
   3. 选择 **Save**（保存）以保存分配的出口 IP 地址。

为动态权限访问启用 SC-NAT 支持

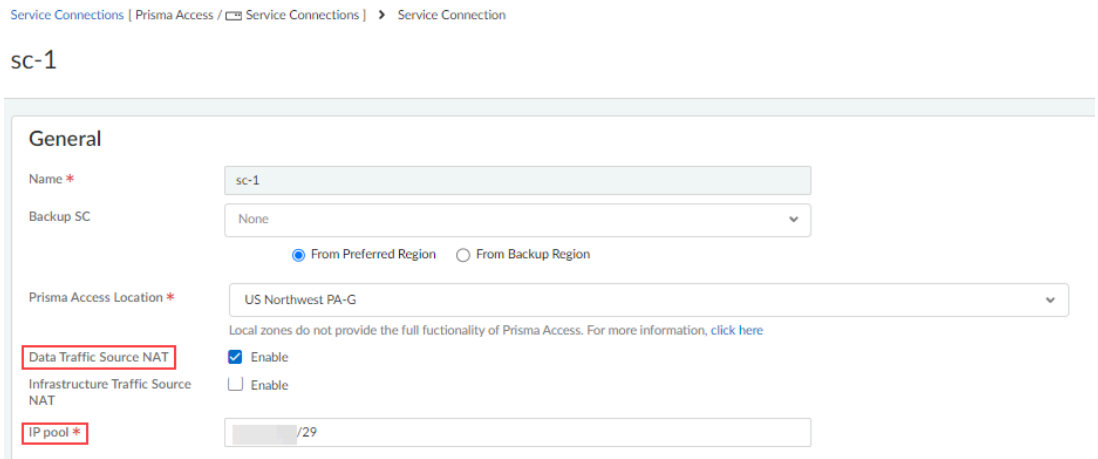
如果您使用动态权限访问 (DPA) 并已创建服务连接来访问数据中心或总部位置的专用应用程序，请使用 SC-NAT 支持。如果基础架构子网的 IP 地址重叠，DPA 环境中的多个项目可能会遇到 IP 地址耗尽的情况。为解决此问题，Prisma Access 可以为 IP 地址实施源 NAT (SNAT)，其作用是：

- 让 Prisma Access 为使用服务连接访问专用应用程序的移动用户映射单个 IP 地址
- 为您提供 SNAT 以简化路由
- 消除 IP 池重叠
- 消除 Prisma Access 和您的数据中心或总部位置之间的 IP 池 IPv4 耗尽问题

DPA客户可以通过服务连接将客户位置接入Prisma Access。然而，多个项目可能在多个数据中心拥有大量的IP池，这可能导致私有IP池的耗尽。要解决此问题，Prisma Access中的动态特权访问提供对具有定义池的SC-NAT的支持。客户可以选择使用 SC-NAT 而不是基础设施子网，以便划分 IP 池。如果您为服务连接企业接入节点（SC-CAN）启用 SC-NAT，则该服务连接将始终支持 SC-NAT。

启用DPA后，您可以根据项目开启（使用SC-NAT）或关闭（使用基础设施子网）SC-NAT。

1. 在 Strata Cloud Manager 中，选择 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Service Connections**（服务连接）。
2. 从服务连接表中选择一个服务连接。
3. 点击数据流量源NAT的复选框。
4. 在您点击数据流量源NAT复选框后，您会看到必填的IP池字段。输入您想要启用 SC-NAT 的子网。
5. **Save**（保存）更改。



 ©2025 Palo Alto Networks, Inc.

为动态特权访问启用路由汇总

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.2 Innovation ❑ Prisma Access 数据平面的最低版本：11.2.3 ❑ Prisma Access 许可证（包含移动用户订阅） ❑ 角色：超级用户

对于拥有有限容量的本地硬件的企业，例如只能容纳几百条路由的简单云路由器，Prisma Access 可以在向本地网络广告路由时对移动用户（MU）路由进行汇总。路由汇总通过保持在数据中心的路由容量内，最小化对这些设备的要求。

要启用路由汇总，请配置全局摘要池，该池包含可在多个项目中使用的大型 IP 池列表。当用户使用 Prisma Access Agent 连接到项目时，如果代理被分配了一个在全局摘要池范围内的 IP 地址，则 Prisma Access 服务连接会宣传全局摘要池，而不是较小的汇总路由。

- 为了帮助说明项目的路由汇总，考虑以下场景：您配置了一个全局摘要池 10.10.0.0/16，并在服务连接 SC-A 上启用了路由摘要选项。
- 用户-A连接到项目-A，该项目分配了IP项目池10.10.10.0/24。连接后，Prisma Access Agent 获取 10.10.10.10/32 IP 地址。
- 用户-B连接到项目-B，该项目分配了IP项目池10.10.11.0/24。连接后，Prisma Access Agent 获取 10.10.11.10/32 IP 地址。
- 在这种情况下，服务连接仅广告一个子网（*10.10.0.0/16* 的全局汇总池），而不是通过 *eBGP* 到本地网络的 */24* 聚合路由。
  - 项目中的*IP*池
  - *Prisma Access* 不会总结不属于项目的 *IP* 池。
  - 可以重叠，全球汇总*IP*
  - 池也可以重叠。

全球汇总池应该是大型IP池，包含与多个项目相关的项目IP池。

要在 Strata Cloud Manager 中启用项目的路由汇总：

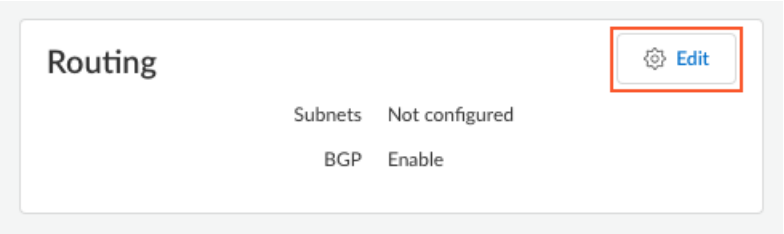
STEP 1 | 创建项目 > > **<Snippet>** > > > 在管理 NGFW 和 Prisma Access 对象动态权限访问项目的项目设置中配置项目 IP 池。

STEP 2 | 配置基础架构设置 > > > 在工作流 Prisma Access 设置访问代理基础设施设置中配置全局摘要 IP 池。

©2025 Palo Alto Networks, Inc.

STEP 3 | 在服务连接中启用路由汇总。

1. > > 前往工作流 Prisma Access 设置服务连接。
2. 从服务连接表中选择一个服务连接。
3. 编辑路由设置。



4. 选择**Summarize Mobile User Routes before advertising**（在通告之前汇总移动用户路由）。



STEP 4 | 保存路由设置。

STEP 5 | 保存服务连接设置。

STEP 6 | 推送 Prisma Access Agent 配置对Prisma Access执行所有管理员的推送配置。

©2025 Palo Alto Networks, Inc.

创建代码段

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 创新 ❑ Prisma Access 许可证，且订阅了“移动用户” ❑ 角色：超级用户

您可以创建代码段对 Prisma Access Agents 的配置进行分组，以便您可以快速将其推送到您的部署。代码段用于标准化一组基于项目的部署的通用基本配置，使您能够快速载入已知良好配置的新设备，并缩短载入新设备所需的时间。

创建代码段后，将代码段与范围关联，向该范围分配用户，并授予用户项目管理员角色。然后，用户可以项目管理员的身份登录，并使用代码段管理 Prisma Access Agent 的项目设置。项目管理员只能更改所分配代码段的 Prisma Access Agent 设置。

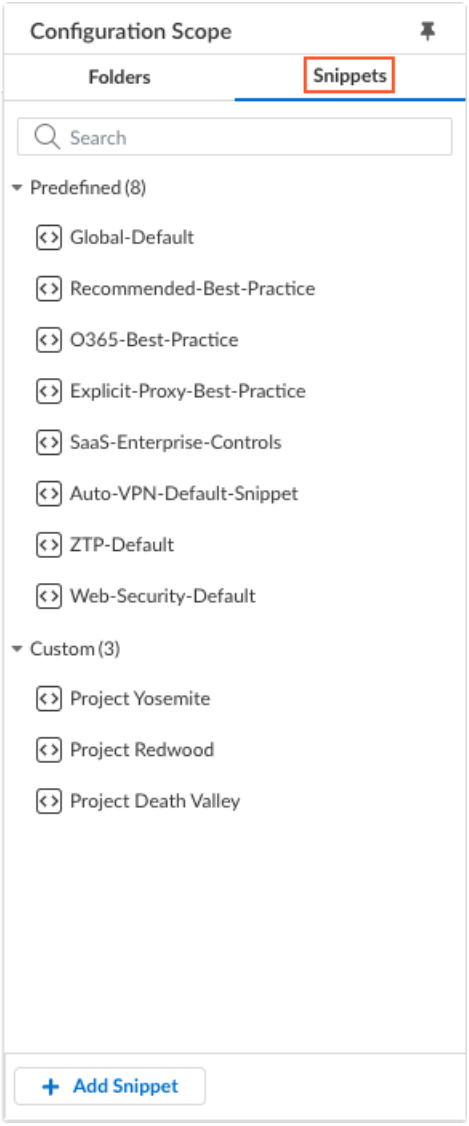
要创建代码段，请完成以下步骤：

STEP 1 | 以超级用户身份登录 Strata Cloud Manager。

STEP 2 | 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW** 和 **Prisma Access**。

©2025 Palo Alto Networks, Inc.

STEP 3 | 选择 **Overview**（概述），然后展开配置范围以查看 **Snippets**（代码段）。



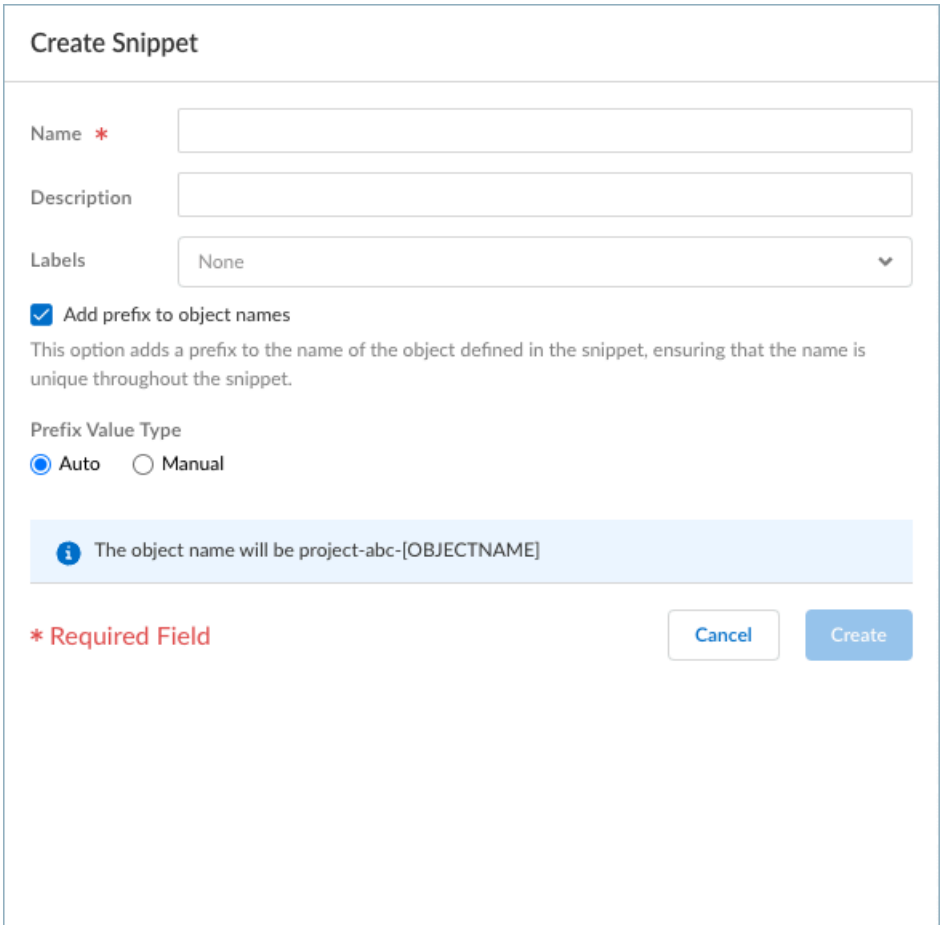
©2025 Palo Alto Networks, Inc.

STEP 4 | **Add Snippet**（添加代码段）并输入以下详细信息：

1. 输入代码段的 **Name**（名称）。
2. （可选）输入代码段的 **Description**（说明）。
3. （可选）分配一个或多个 **Labels**（标签）。

   您可以选择现有标签，也可以通过键入要创建的标签来创建新标签。
4. 为了确保对象名称在代码段中是唯一的，默认情况下启用 **Add prefix to object names**（为对象名称添加前缀）。

   选择是否 **Auto**（自动）生成随机前缀，或选择 **Manual**（手动）并添加您自己的 **Prefix Value**（前缀值）。前缀值可以是字母数字，最多包含六个字符。



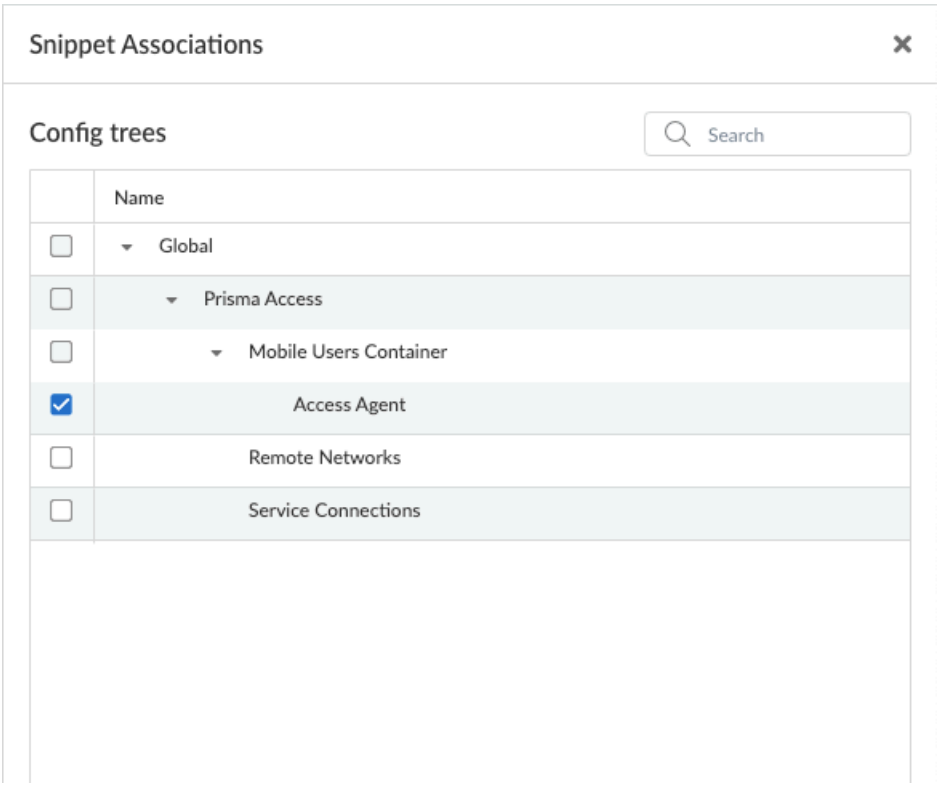
   前缀的格式为 **xxxxxx-**。添加对象时，Strata Cloud Manager 将使用前缀预填充对象名称。
5. **Create**（创建）代码段。

   创建代码段后，您将进入代码段的配置范围。您在代码段范围内创建的所有配置仅适用于代码段。

©2025 Palo Alto Networks, Inc.

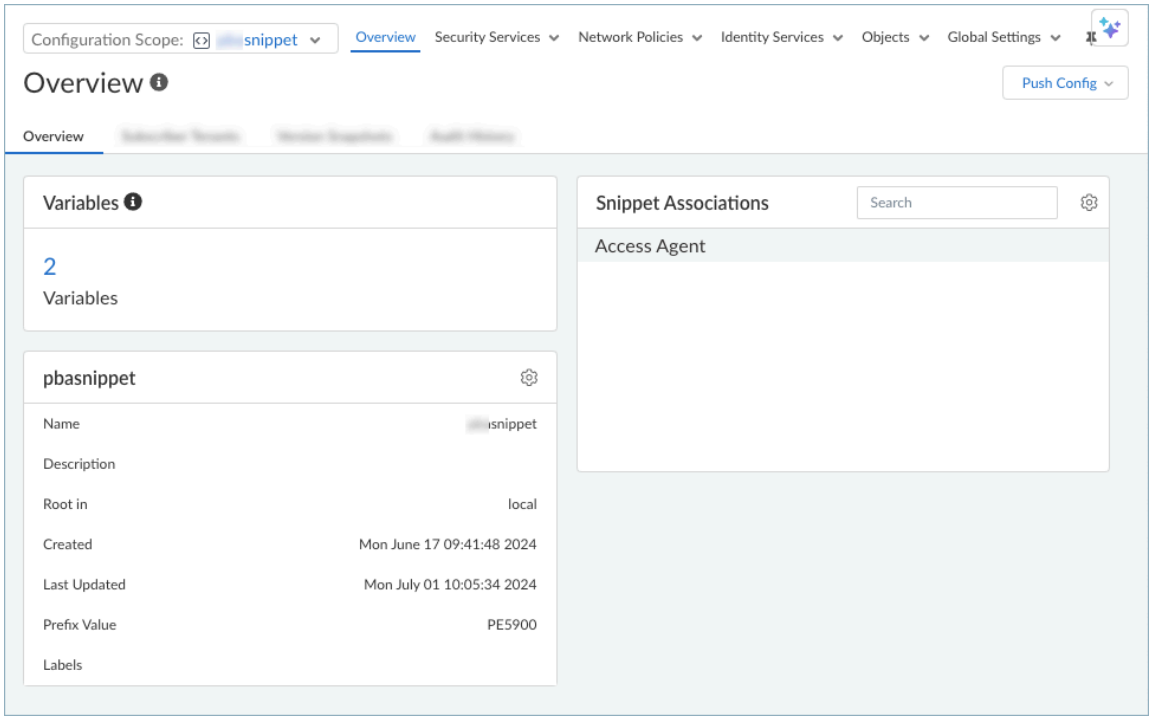
STEP 5 | 将代码段关联到 **Access Agent**（访问代理）文件夹。

1. 在代码段的“概述”页面中，选择 **Snippet Associations**（代码段关联）设置
2. 从 **Config trees**（配置树）中选择 **Access Agent**（访问代理）。



3. 单击 **X** 关闭代码段关联窗口。

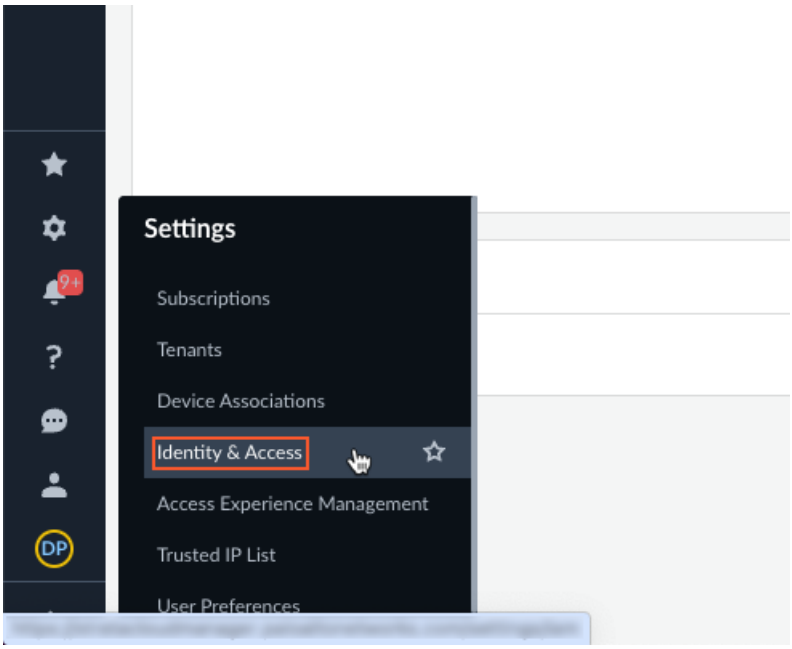
   Access Agent（访问代理）出现在代码段关联列表中。



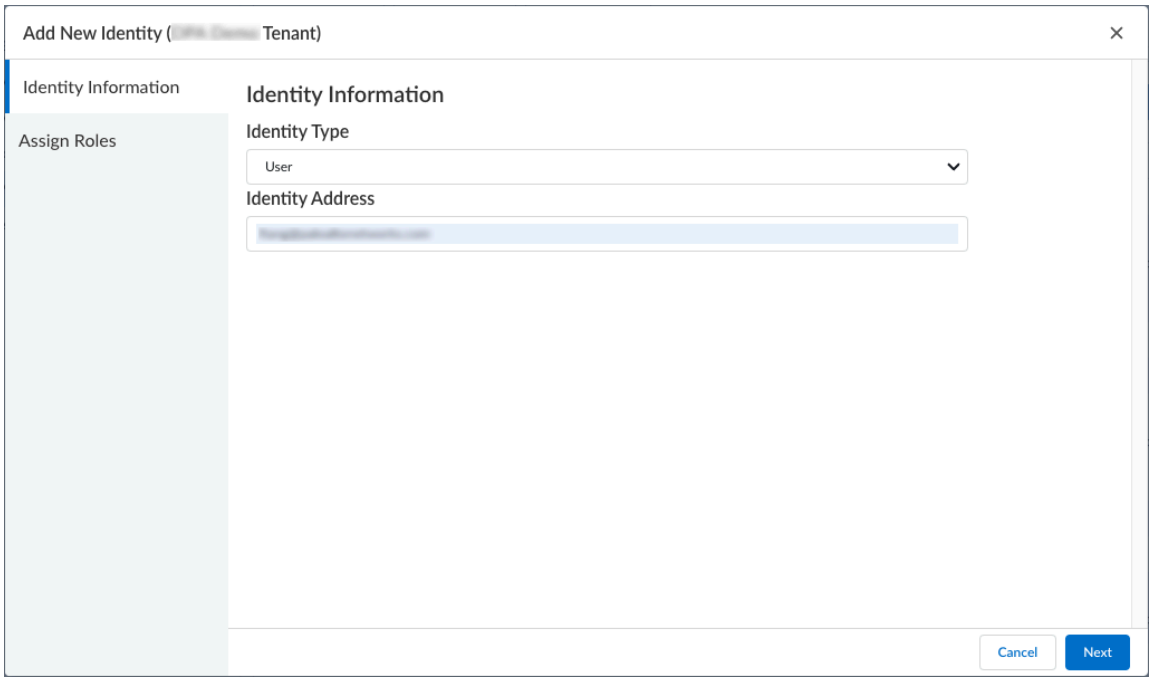
 ©2025 Palo Alto Networks, Inc.

STEP 6 | 如果您尚未这样做，请为将管理项目的用户创建身份，并为该用户分配项目管理员推送角色。

1. 在 Strata Cloud Manager 中，选择 **Settings**（设置） > **Identity & Access**（身份和访问）。

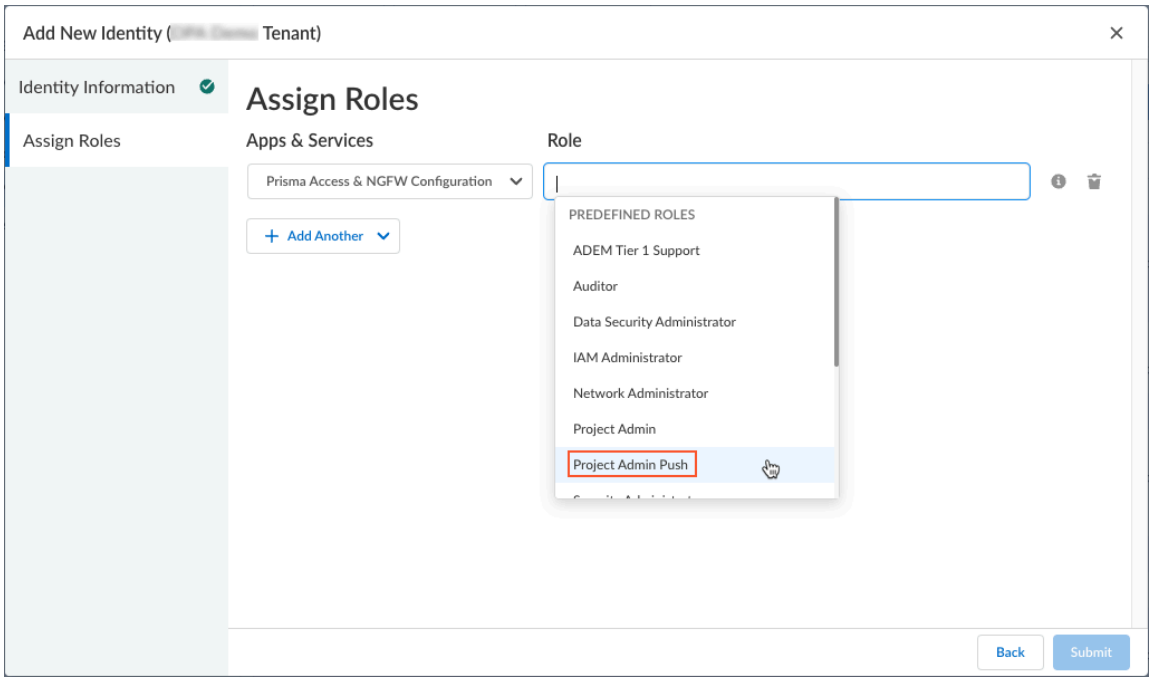


2. 选择 **Add Identity**（添加身份）。
3. 输入将成为项目管理员的用户的 **Identity Address**（身份地址），然后单击 **Next**（下一步）。



4. 选择 **Add Access**（添加访问） > **Prisma Access & NGFW Configuration**（**Prisma Access 和 NGFW** 配置），为该用户选择 **Project Admin Push**（项目管理员推送）。

©2025 Palo Alto Networks, Inc.



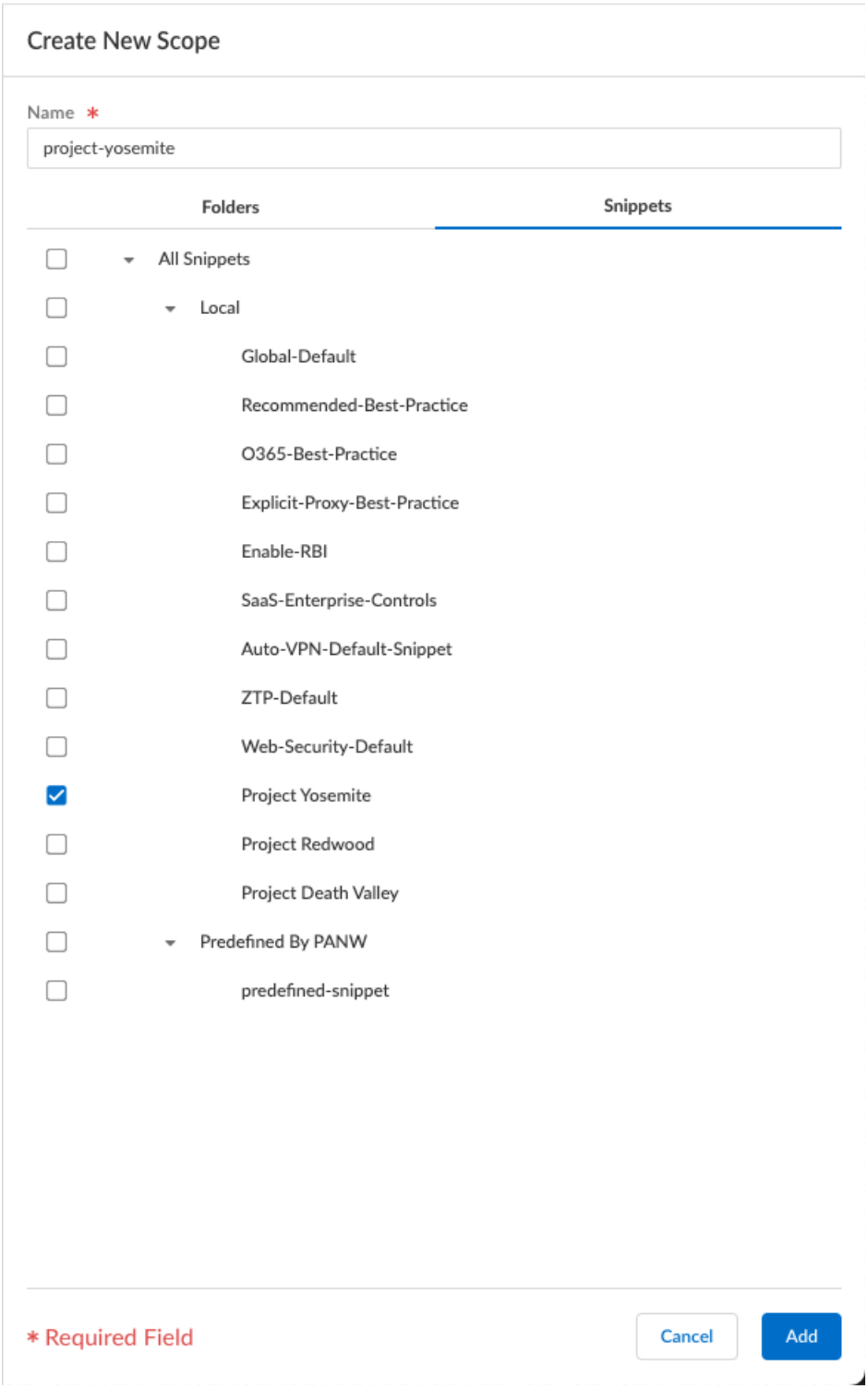
5. 单击 **Submit**（提交）。

©2025 Palo Alto Networks, Inc.

STEP 7 | 为代码段创建管理范围并向该范围分配用户。

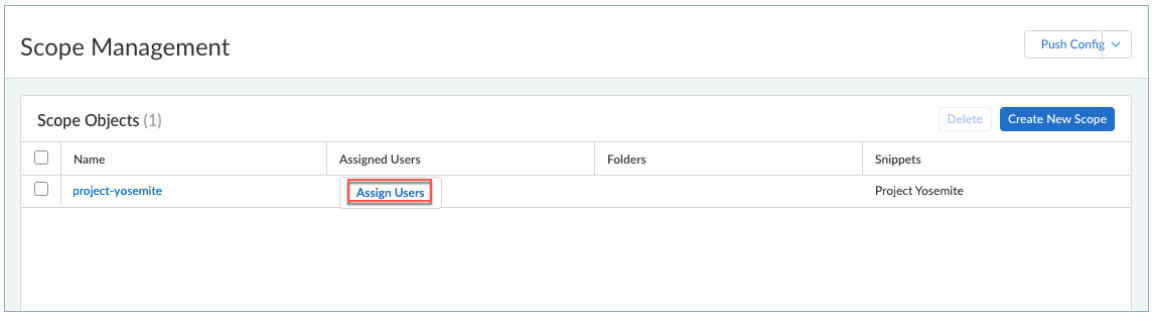
1. 选择 **Manage**（管理） > **Access Control**（访问控制） > **Scope Management**（范围管理）。
2. **Create New Scope**（创建新的范围）。
3. 输入范围的 **Name**（名称）并查看 **Snippets**（片段）。
4. 将代码段与范围关联。选择您创建的代码段并 **Add**（添加）该代码段。

 ©2025 Palo Alto Networks, Inc.

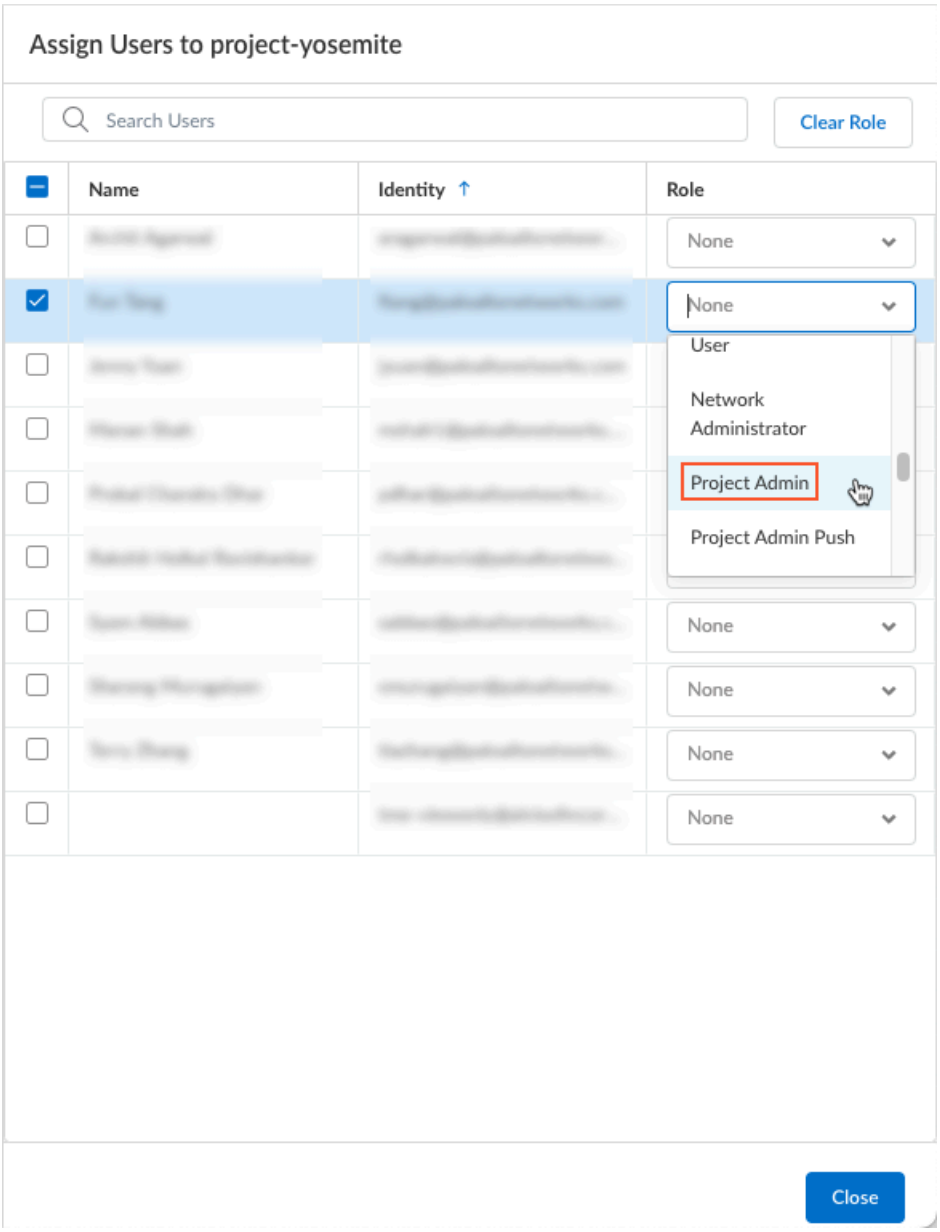


5. 在范围对象中，向您为代码段创建的范围 **Assign Users**（分配用户）。

©2025 Palo Alto Networks, Inc.



6. 通过从列表中选择一个用户并授予该用户 **Project Admin**（项目管理员）角色，将用户分配到该范围。



7. **Close**（关闭）窗口。
8. 推送配置。

©2025 Palo Alto Networks, Inc.

1. 选择 **Manage**（管理） > **Operations**（操作） > **Push Config**（推送配置）。
2. 选择 **All Admins**（所有管理员）管理员范围，然后选择 **Push Config**（推送配置） > **Push**（推送）。

推送配置操作完成后，将创建代码段，并将角色与该代码段关联。

分配的用户（项目管理员）现在可以登录 Strata Cloud Manager 并使用您创建的代码段配置项目特定的 Prisma Access Agent 设置。用户可以查看未分配的其他范围，但无法与之交互，例如更改任何配置。

©2025 Palo Alto Networks, Inc.

配置项目特定的 Prisma Access Agent 设置

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 创新 ❑ Prisma Access 许可证，且订阅了“移动用户” ❑ macOS 12 或更高版本的桌面设备，或 Windows 10 版本 2024 或更高版本或 Windows 11 桌面设备 ❑ 角色：项目管理员

在超级用户管理员设置基础架构、创建代码段并将该代码段分配给您之后，您可以项目管理员的身份登录，以便设置项目特定的 Prisma Access Agents 设置，例如专用 IP、拆分隧道和 DNS 信息，当他们使用 Prisma Access Agent 登录项目时会将这些信息分配给端点。

您可以为一个或多个 Prisma Access Agents 创建项目特定设置，也可以使用默认代理设置。您可以为您管理的每个项目使用不同的代理，或者多个项目共享一个代理。

配置转发配置文件以管理动态特权访问代理的代理流量

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 创新 ❑ Prisma Access 许可证，且订阅了“移动用户” ❑ macOS 12 或更高版本的桌面设备，或 Windows 10 版本 2024 或更高版本或 Windows 11 桌面设备 ❑ 角色：项目管理员

转发配置文件提供单一面板来配置和管理流量转发规则和流量实施，例如设置分割隧道设置和管理隧道连接之外的流量。转发配置文件改进了在使用其他移动访问代理时遇到的流量策略配置不连贯问题，并极大扩展了您可以配置的规则和条目数量。简化相关配置并且更加浅显易懂，可以让您更加专设置路由和实施端点流量的方式。

转发配置文件是一种配置文件类型，包含多个逻辑部分和有序部分。这些部分说明了在代理确定应如何控制连接之前，连接所经历的各个阶段。该组织结构会在每个部分中显示有序条目，从而帮助您了解为什么以某种方式路由流量。在每个部分中，您可以添加、编辑、移除或重新排序条目。

设置转发配置文件后，您可以在“Agent Settings（代理设置）”页面中将配置文件分配给用户或用户组。

 ©2025 Palo Alto Networks, Inc.

流量转发规则在转发配置文件中按照自上而下顺序应用。因此，请自上而下地配置转发模板，例如先配置最具体的规则，最后配置最模糊的规则。

转发规则

转发配置文件由一组流量转发规则组成，这些规则指定哪些源应用程序或目标域和目标 IP 地址流量经过隧道或绕过隧道，是否分割 DNS 流量，以及哪些流量实施有效。匹配规则的流量会根据流量转发规范而转发到 Prisma Access。转发规则中的规范分为以下部分：

- **Source Applications**（源应用程序） — 指定规则适用的专用应用程序或 SaaS 应用程序。当来自端点的流量与源应用程序匹配时，将根据转发规则路由流量。
- **Destinations**（目标） — 指定规则适用的域和 IP 地址。当流量与目标匹配（指定为 FQDN 或 IP 地址）时，将根据转发规则路由流量。

流量实施

每个转发配置文件还包含流量实施设置，可用于：

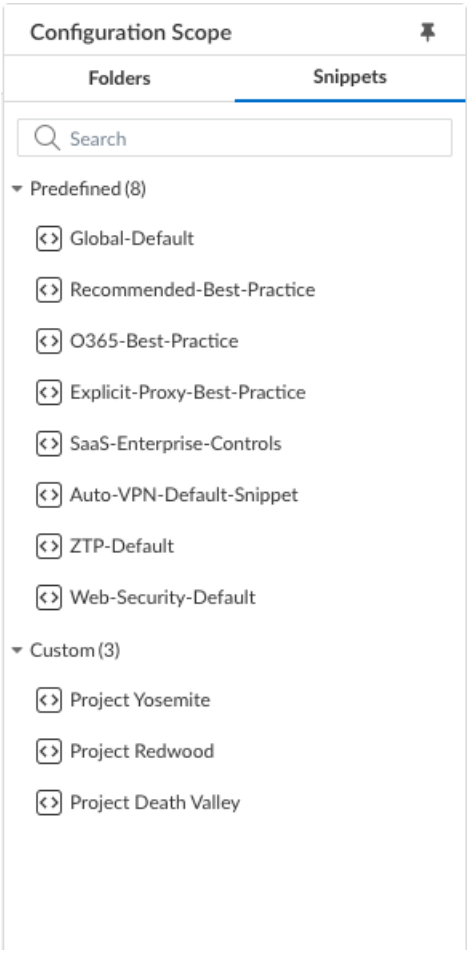
- 阻止所有不匹配任何转发规则的出站流量
- 当代理连接到隧道时阻止出站 LAN 访问
- 当代理连接到隧道时阻止入站访问

要配置转发配置文件，请完成以下步骤：

STEP 1 | 以项目管理员身份登录到 Strata Cloud Manager。

 ©2025 Palo Alto Networks, Inc.

STEP 2 | 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW** 和 **Prisma Access** > **Overview**（概览），然后展开配置范围以查看 **Snippets**（代码段）。

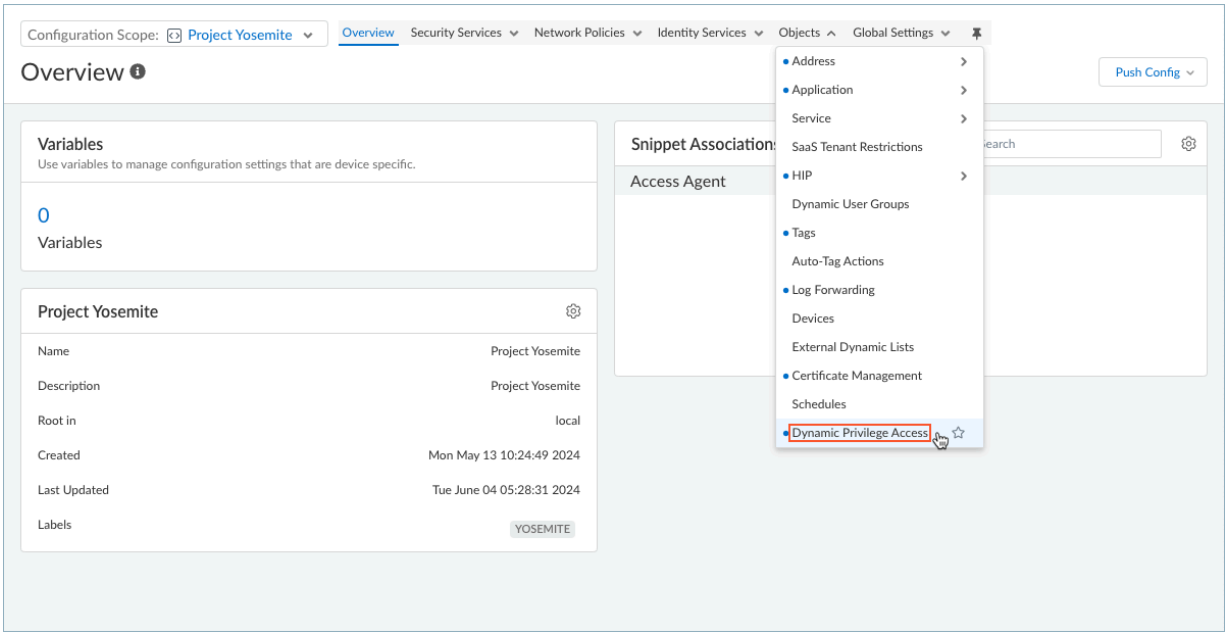


STEP 3 | 选择超级用户管理员分配给您的代码段。

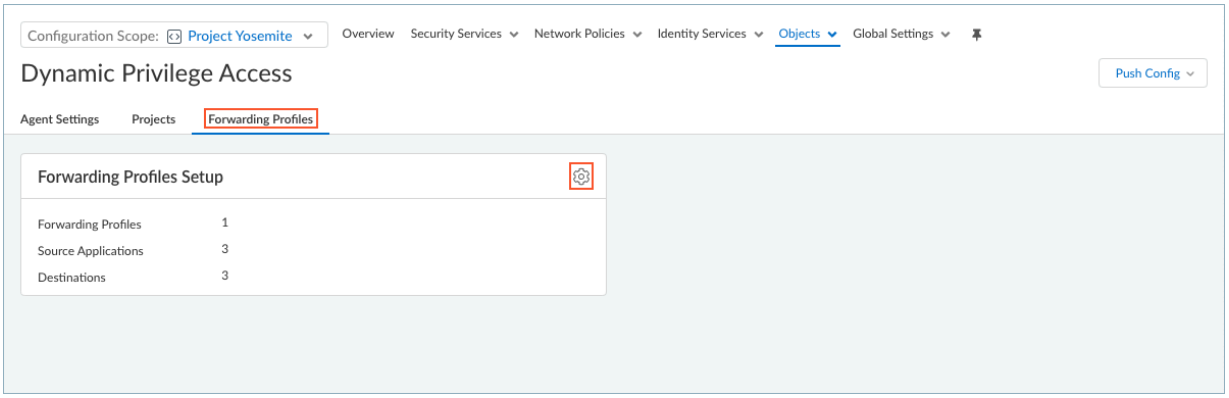
您还可以查看未分配给您的代码段，但您无法与之进行交互，例如更改配置。

 ©2025 Palo Alto Networks, Inc.

STEP 4 | 选择 **Objects**（对象） > **Dynamic Privilege Access**（动态特权访问）以打开动态特权访问设置。



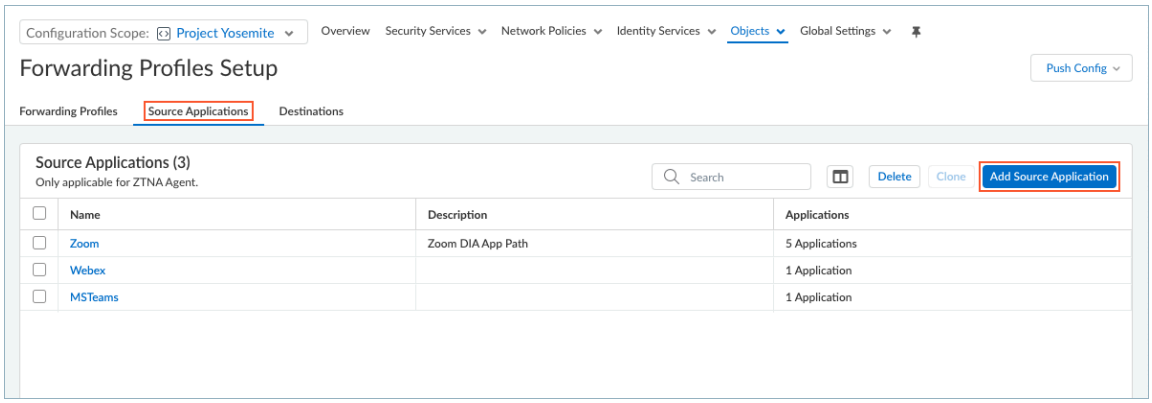
STEP 5 | 选择 **Forwarding Profiles**（转发配置文件）并编辑 **Forwarding Profiles Setup**（转发配置文件设置）。



©2025 Palo Alto Networks, Inc.

STEP 6 | 如果要根据 SaaS 或公共云应用程序名称创建拆分隧道，则设置 **Source Applications**（源应用程序）。

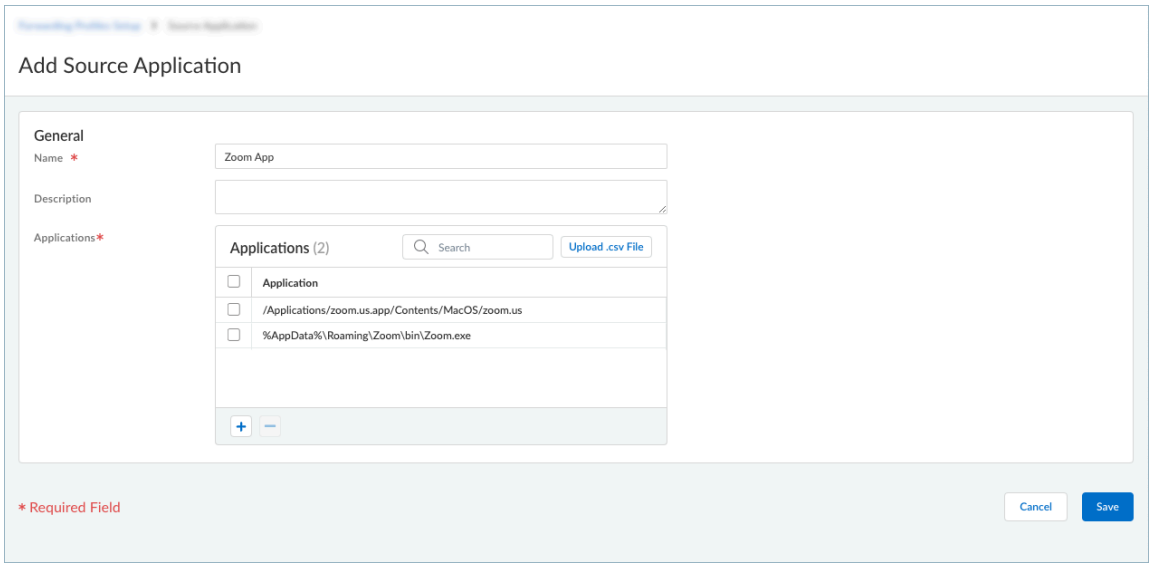
1. 在“Forwarding Profiles Setup（转发配置文件设置）”页面中，选择 **Source Applications**（源应用程序） > **Add Source Application**（添加源应用程序）。



2. 在 **Name**（名称）中，为您要添加的应用程序输入一个有意义名称。
3. 在 **Applications**（应用程序）表中单击 **+**，然后输入应用程序的完整路径。您可以添加一个或多个应用程序来管理是在隧道中排除还是包含应用程序流量。

   如果您选择排除应用程序流量（通过在转发规则中选择 **Direct**（直接）连接），则来自这些应用程序的流量将通过端点上的物理适配器发送，而不是通过隧道（虚拟适配器）发送。

   如果您选择包括应用程序流量（通过在转发规则中选择 **Tunnel**（隧道）连接），则来自这些应用程序的流量将被路由到 Prisma Access，即使它符合排除流量条件。



   例如，要管理来自 Zoom 应用程序的流量，请添加以下完整路径：

   - Windows 端点：**`%AppData%\Roaming\Zoom\bin\Zoom.exe`**
   - macOS endpoints: **`/Applications/zoom.us.app/Contents/MacOS/zoom.us`**

   如果您在逗号分隔值格式 (`.csv`) 的文本文件中列出了应用程序列表，则可以选择 **Upload .csv File**（上载 **.csv** 文件）。

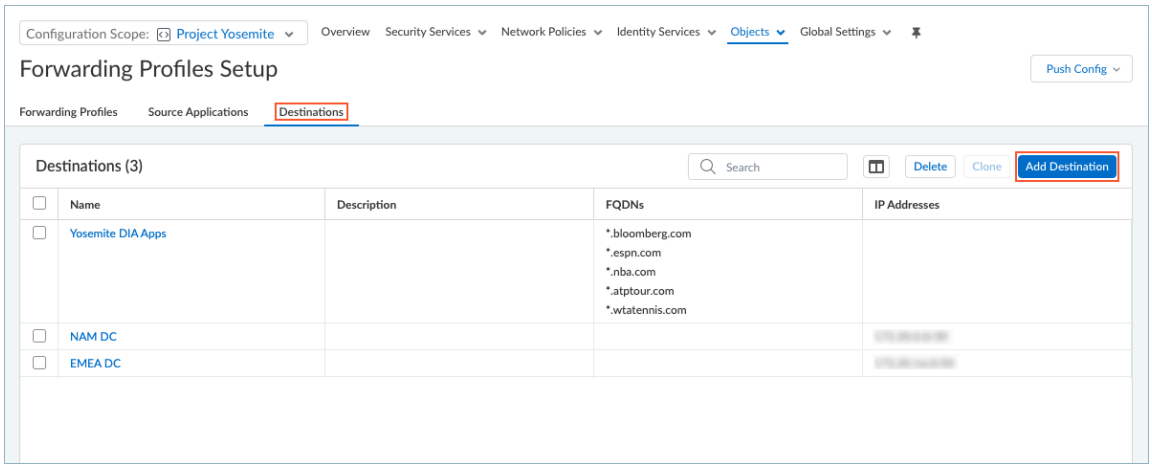
 ©2025 Palo Alto Networks, Inc.

4. 选择 **Save**（保存）以保存应用程序。
5. 重复这些步骤以添加更多源应用程序。

 ©2025 Palo Alto Networks, Inc.

STEP 7 | 如果要根据目标域或访问路由创建拆分隧道，请设置 **Destinations**（目标）。

1. 在“Forwarding Profiles Setup（转发配置文件设置）”页面中，选择 **Destinations**（目标） > **Add Destination**（添加目标）。

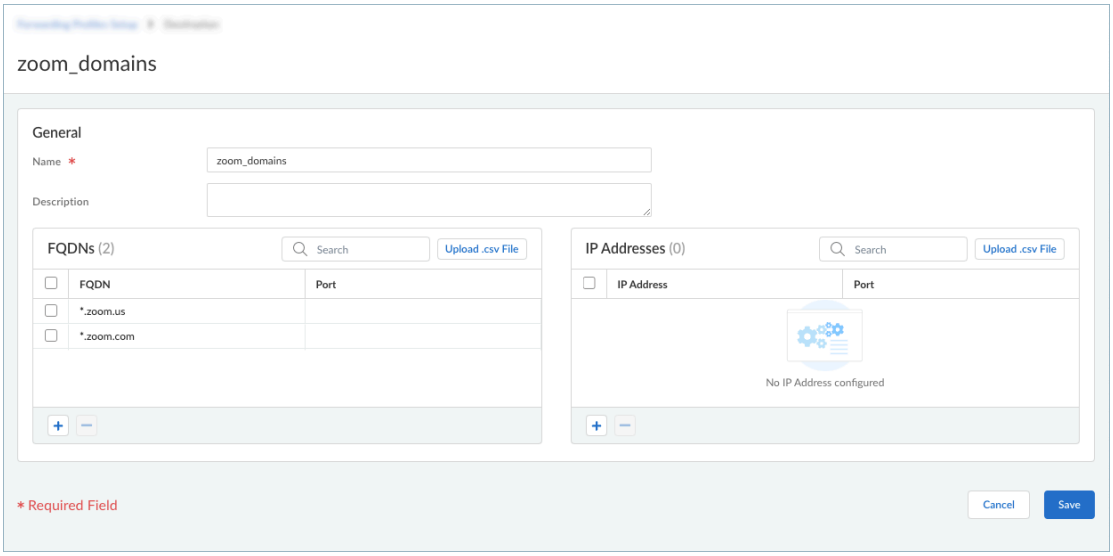


2. 在 **Name**（名称）中，为您要添加的目标输入一个有意义名称。
3. 通过指定域名和/或访问路由来添加目标。

   - 要添加目标域，请在 **FQDNs (FQDN)** 表中单击 **+**，然后输入目标域的 FQDN。您可以选择添加端口。如果不指定端口，则指定域的所有端口都适用转发规则。可以添加一个或多个域以进行流量管理。

     如果选择基于域名排除流量（通过在转发规则中选择 **Direct**（直接）连接），则来自该域的流量将通过端点上的物理适配器发送，而不是通过隧道（虚拟适配器）发送。

     如果选择基于域名包括流量（通过在转发规则中选择 **Tunnel**（隧道）连接），则来自该域的流量将始终路由到 Prisma Access，即使流量符合“排除通信量”条件。



   - 要添加访问路由，请在 **IP Addresses**（IP 地址）表中单击 **+**，然后输入目标子网。您可以添加一个或多个访问路由以进行流量管理。

     请勿在 IP 地址中包含通配符。转发配置文件不支持 IP 地址中的通配符。

©2025 Palo Alto Networks, Inc.

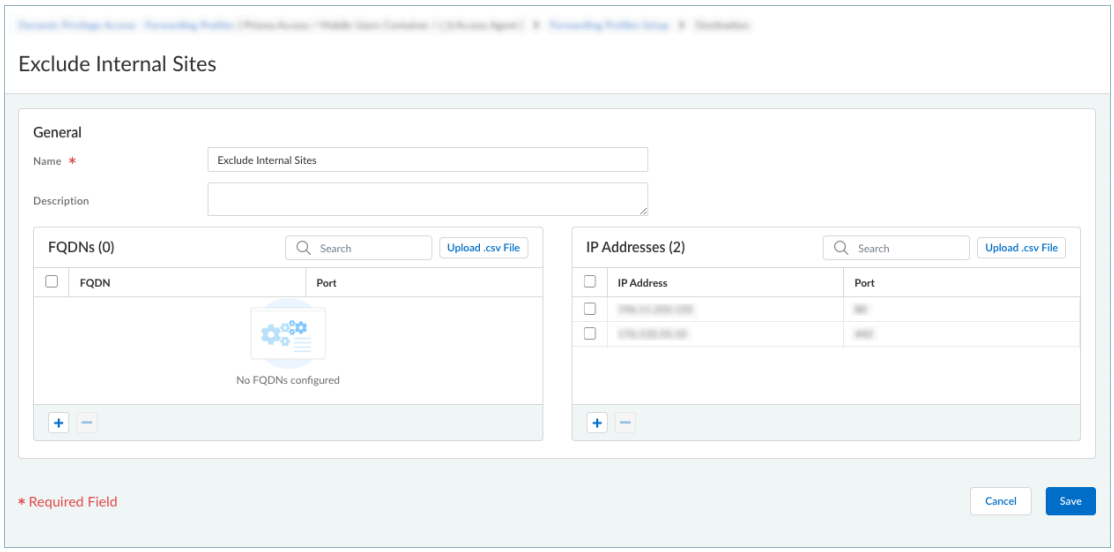
如果您不包含或排除路由或应用程序，则每个请求都通过隧道路由（没有分割隧道）。此外，每当用户连接到 Prisma Access 时，都会检查所有流量并强制执行策略。

定义拆分隧道通信以排除访问路由（通过在转发规则中选择 **Direct**（直接）连接）时，这些路由将通过端点上的物理适配器发送，而不是通过虚拟适配器（隧道）通过隧道发送。通过按访问路由排除分割隧道流量，您可以在隧道外发送延迟敏感型流量或高带宽流量，而所有其他流量则通过隧道进行路由，以由 Prisma Access 网关进行检查和执行策略。

将分割隧道流量定义为包括访问路由（通过在转发规则中选择 **Tunnel**（隧道）连接）时，Prisma Access 网关会将这些路由推送到远程用户的端点，以指定这些端点可以通过隧道发送的流量。

指定排除的路由时，需要比包括的路由更加具体；否则，您可能会排除比预期更多的流量。

如果您在文本文件中以 `.csv` 格式列出了 IP 地址列表，则可以选择 **Upload .csv File**（上传 **.csv** 文件）。

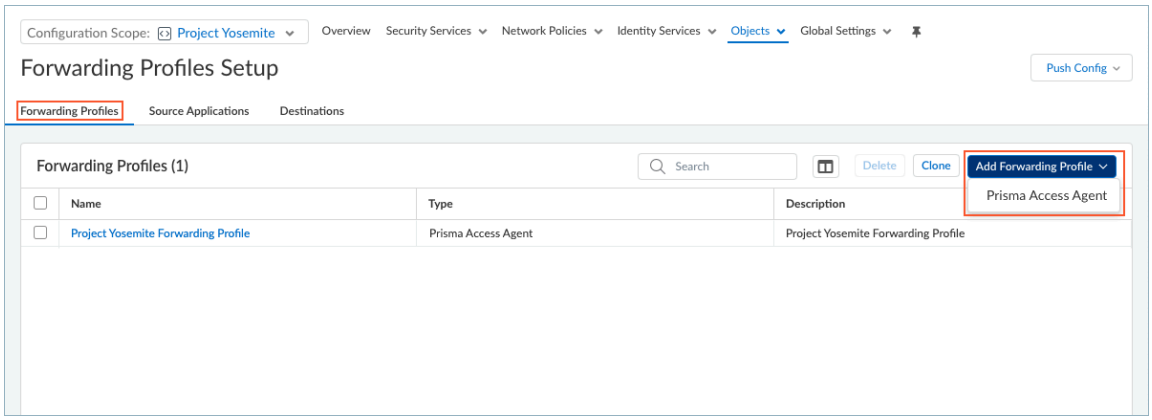


4. 选择 **Save**（保存）以保存目标。
5. 重复这些步骤以添加更多目标。

©2025 Palo Alto Networks, Inc.

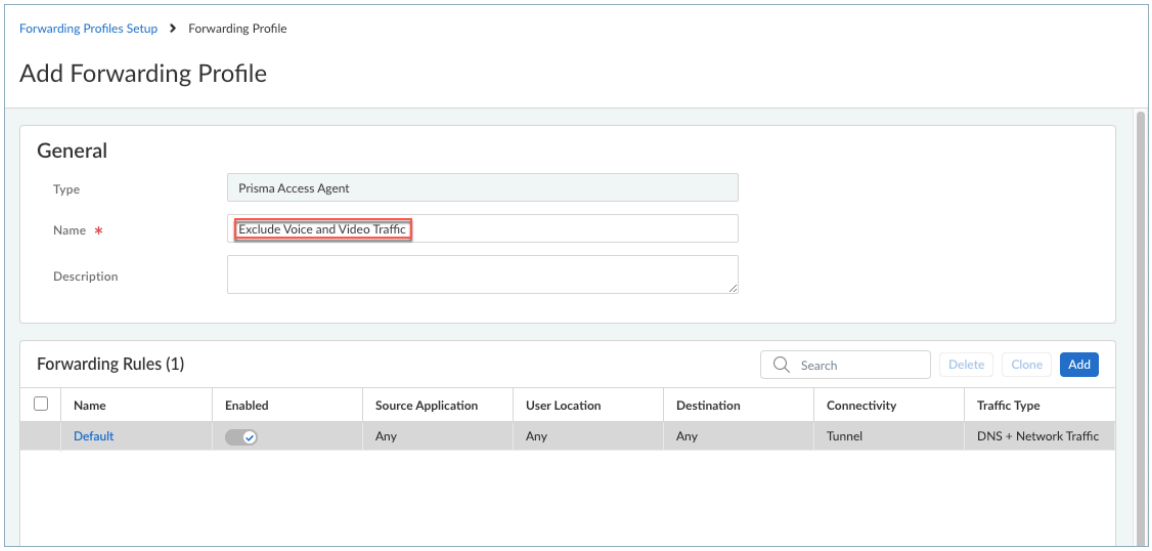
STEP 8 | 创建一个转发配置文件，根据您配置的源应用程序或目标来允许或排除流量。

1. 要添加转发配置文件，请选择 **Forwarding Profiles**（转发配置文件） > **Add Forwarding Profile**（添加转发配置文件） > **Prisma Access Agent**。



要编辑转发配置文件，请在“Forwarding Profiles（转发配置文件）”表中选择配置文件的名称。

2. 在 **Name**（名称）中，为转发配置文件输入一个有意义名称。
3. 选择 **Add**（添加）以添加转发规则。

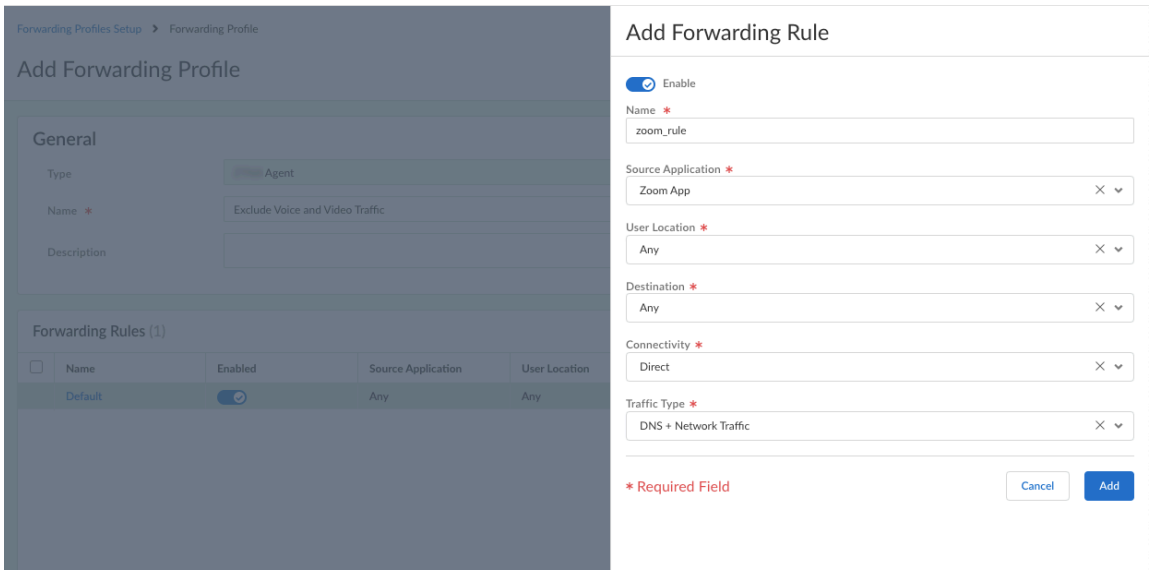


Forwarding Rules（转发规则）表显示构成转发配置文件的规则。所有转发配置文件都包含 **Default**（默认）转发规则，该规则通过隧道发送所有 DNS 和网络流量。您添加的

 ©2025 Palo Alto Networks, Inc.

任何新规则都将放置在默认规则的上方。无法删除或移动默认转发规则，但可以更改其 **Connectivity**（连接）设置。

4. 输入转发规则的规范。



1. **Enable**（启用）规则。
2. 输入规则的 **Name**（名称）。
3. 选择先前定义的 **Source Application**（源应用程序）。如果选择 **Any**（任意），则转发规则将应用于来自任何源应用程序的通讯。

   仅当连接是由指定的源应用程序建立时，规则才会匹配。
4. 选择 **User Location**（用户位置）。如果未设置用户位置，或者允许规则匹配任何用户位置，请选择 **Any**（任意）。（不适用于已启用 Dynamic Privilege Access（动态权限访问）的代理。

   仅当端点连接到您指定的用户位置时，该规则才会匹配。
5. 选择先前定义的 **Destination**（目标）。如果选择 **Any**（任意），转发规则将应用于来自任何目标域或 IP 地址的流量。

   仅当连接目标与指定的目标域或 IP 地址匹配时，规则才会匹配。
6. 选择 **Connectivity**（连接）：
   - **Direct**（直接） — 在隧道外部发送所有流量。所选应用程序或目标的所有流量都直接发送到端点上的物理适配器，不进行检查。
   - **Tunnel**（隧道） — 通过隧道发送流量。流向所选应用程序或目标的所有流量都通过隧道发送到 Prisma Access，以进行检查和执行策略。
7. 选择 **Traffic Type**（流量类型）：

   指定是否使用分割 DNS，以使用户除了网络流量外，还能够通过隧道或隧道外部来定向其对应用程序和资源的 DNS 查询。
   - **DNS + Network Traffic**（**DNS +** 网络流量） — 确保为包含项和排除项指定的基于目标域的拆分隧道将适用于该域的 DNS 流量或关联的网络应用程序流量。

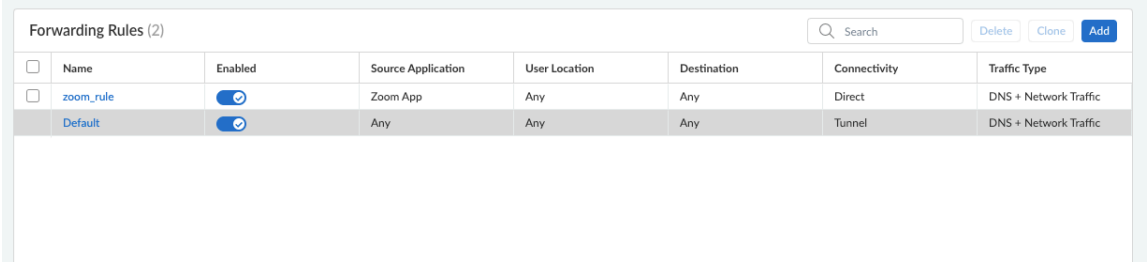
©2025 Palo Alto Networks, Inc.

- **Network Traffic**（网络流量） — 包含或排除仅适用于网络应用程序流量但不适用于 DNS 流量的规则。无论您是否为包含项和排除项指定了基于目标域的拆分隧道，所有 DNS 流量都会通过隧道。

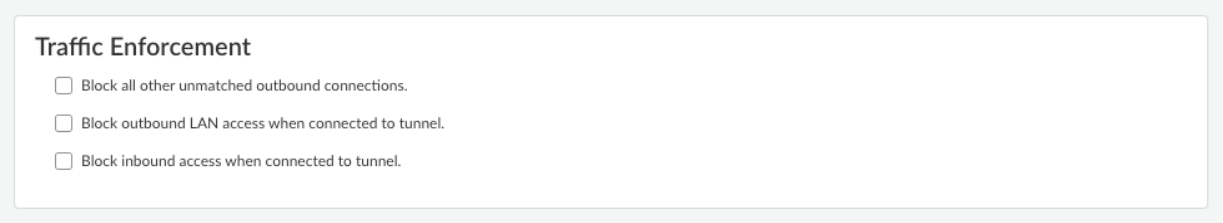
对于 *Windows* 代理，基于应用程序的分割隧道规则不支持分割隧道选项 ***DNS + Network Traffic***（***DNS +*** 网络流量）。如果您将分割隧道设置为根据应用程序名称而在隧道内包含或排除流量，并选择 ***DNS + Network Traffic***（***DNS +*** 网络流量），则排除和包含的应用的 *DNS* 查询数据包将不会遵守分割隧道规则。

5. 选择 **Add**（添加）以添加转发规则。

   该规则将添加到“Forwarding Rules（转发规则）”表中。可以向转发配置文件添加多个规则。



STEP 9 | 配置 **Traffic Enforcement**（流量执行）选项以确定如何强制执行流量。



请务必取消全选这些选项，因为不建议将这些选项用于动态特权访问。

- **Block all other unmatched outbound connections**（阻止所有其他不匹配的出站连接） — 启用该选项后，将阻止与任何转发规则都不匹配的所有连接。流量将不会通过隧道发送。
- **Block outbound LAN access when connected to the tunnel**（连接到隧道时阻止出站 **LAN** 访问） — 启用后，当代理连接到隧道时，将阻止对本地网络的直接访问。

  阻止访问本地网络会导致所有流量无法发送到本地适配器。此外，您的用户将无法访问本地子网上的资源，例如打印机。基于访问路由、目标域和应用程序的分割隧道流量仍可按预期工作。

  如果禁用该选项，则最终用户可以访问本地资源，无需先使用 Prisma Access 代理连接到 Prisma Access。
- **Block inbound access when connected to the tunnel**（连接到隧道时阻止入站访问） — 启用时，将阻止来自隧道的所有入站连接。

STEP 10 | 选择 **Save**（保存）以保存您的转发配置文件。

 ©2025 Palo Alto Networks, Inc.

STEP 11 | 通过选择 **Push Config**（推送配置） > **Push**（推送）来推送配置。此操作将使您的转发配置文件在“Agent Settings（代理设置）”页面中可供选择。

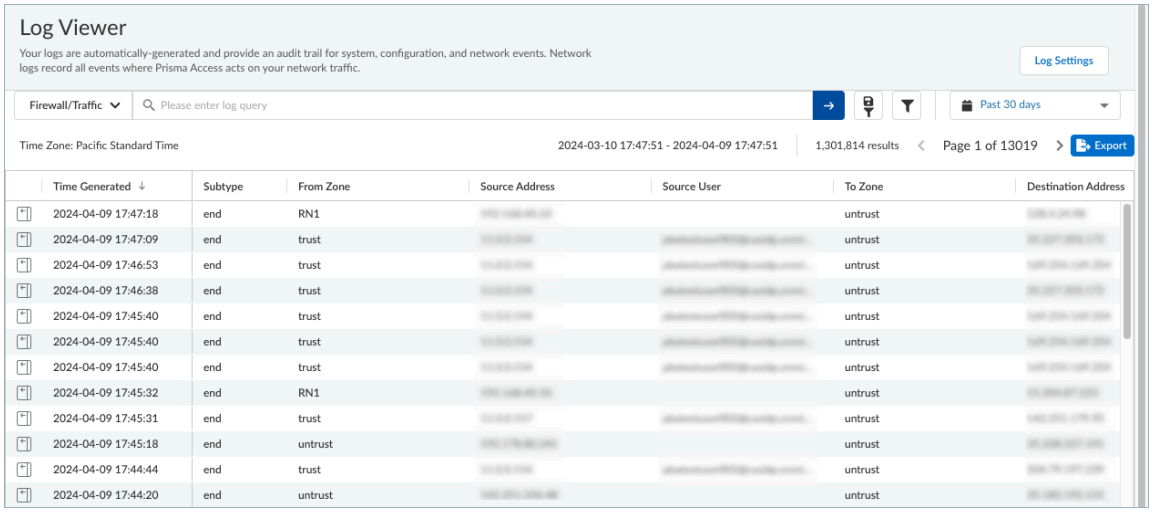
验证动态路由访问客户端的转发配置文件并排除故障

在何处可以使用？	需要提供什么？
• Prisma Access（由 Strata Cloud Manager 管理）	❑ Prisma Access 5.1 Preferred 或 Innovation ❑ Prisma Access 许可证，且订阅了“移动用户” ❑ macOS 12 或更高版本的桌面设备，或 Windows 10 版本 2024 或更高版本或 Windows 11 桌面设备 ❑ 角色：超级用户

配置转发配置文件后，您可以通过查看流量日志文件来验证流量是否按预期定向。可以在 Strata Cloud Manager 日志查看器中查看流量日志，也可以通过端点上的 Prisma Access 命令行工具 (PACli) 来查看。

要从 Strata Cloud Manager 日志查看器查看流量日志文件，请执行以下操作：

1. 选择 **Incidents & Alerts**（事件和警报） > **Log Viewer**（日志查看器）。
2. 查看 **Firewall/Traffic**（防火墙/流量）日志以了解更多详细信息。



 ©2025 Palo Alto Networks, Inc.

要查看端点上的流量日志文件，请执行以下操作：

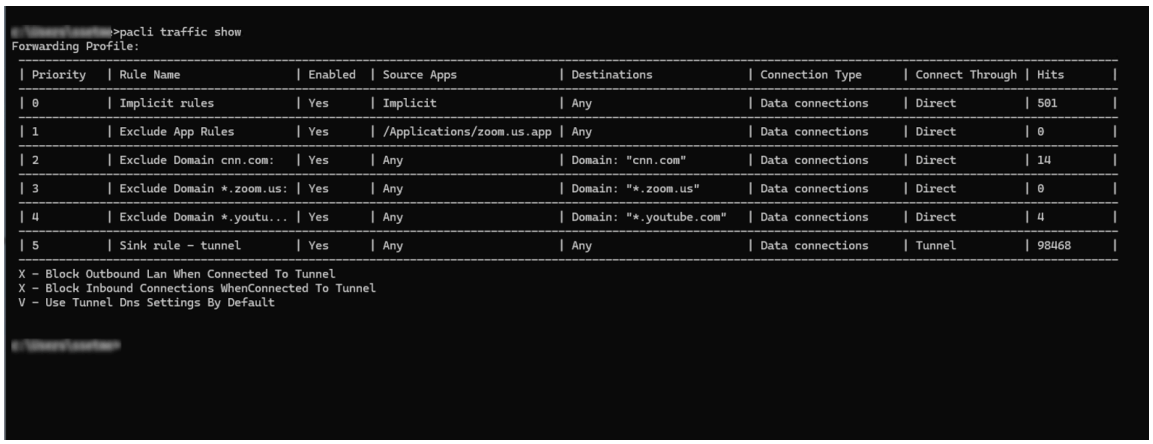
1. 在 **Manage**（管理） > **Prisma Access Agent** 中启动远程 shell，或在最终用户的设备上打开 Windows 命令提示符或 MacOS 终端窗口。
2. 要在转发配置文件中显示转发规则，请发出以下命令：
   - 在 Windows 上：

     ```
     "C:\Program Files\Palo Alto Networks\Prisma Access Agent
     \pacli" traffic show
     ```

   - 在 macOS 上：

     ```
     /Applications/Prisma\ Access\ Agent.app/Contents/Helpers/
     pacli traffic show
     ```

   如果您为 *PACli* 工具 *(`pacli`)* 设置了一个环境变量，则只需输入 ***`pacli traffic show`***。

   pacli 命令行示例输出会显示了一个表，其中包含在转发配置文件中生效的转发规则，包括转发规则的优先级。还会显示转发配置文件的流量强制选择。此表对应于您在转发配置文件中设置的转发规则。
3. 要显示转发规则的详细信息，请发出以下命令：

   ```
   pacli traffic show <number>
   ```

   其中 **<number>** 是 `Priority`（优先级）列中的数字，例如：

 ©2025 Palo Alto Networks, Inc.

```
[redacted]>pacli traffic show 1
Printing forwarding profile rule #1
Priority        : 1
Rule Name       : Exclude App Rules
Enabled         : Yes
Source Apps     : /Applications/zoom.us.app
Destinations    : Any
Connection Type : Data connections
Connect Through : Direct
Hits            : 0

[redacted]>pacli traffic show 2
Printing forwarding profile rule #2
Priority        : 2
Rule Name       : Exclude Domain cnn.com:
Enabled         : Yes
Source Apps     : Any
Destinations    : Domain: "cnn.com"
Connection Type : Data connections
Connect Through : Direct
Hits            : 25

[redacted]>
```

4. 要排除分割通道问题，您可能需要检查隧道内外的代理流量。为此，可以显示 Prisma Access Agent 连接日志。发出以下命令：

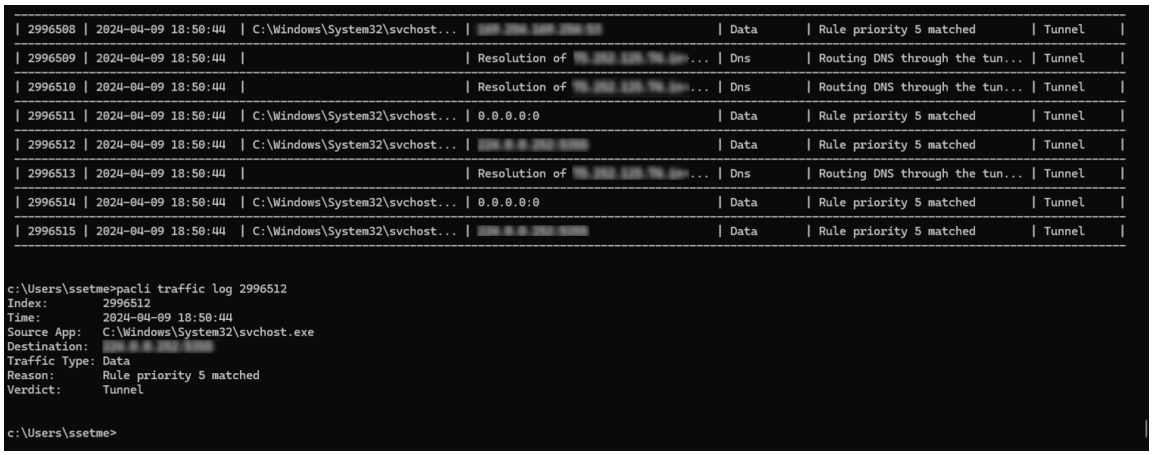
```
pacli traffic log
```

```
[redacted]>pacli traffic log
Network connection log:
 ------------------------------------------------------------------------------------------------------------------------------
 | Index   | Time                | Source App                  | Destination                  | Traffic... | Reason                      | Verdict   |
 ------------------------------------------------------------------------------------------------------------------------------
 | 2988329 | 2024-04-09 18:26:36 | C:\Windows\System32\svchost... | [redacted]                | Data       | Rule priority 5 matched     | Tunnel    |
 ------------------------------------------------------------------------------------------------------------------------------
 | 2988330 | 2024-04-09 18:26:37 | C:\Windows\System32\svchost... | 0.0.0.0:0                    | Data       | Rule priority 5 matched     | Tunnel    |
 ------------------------------------------------------------------------------------------------------------------------------
 | 2988331 | 2024-04-09 18:26:37 | C:\Windows\System32\svchost... | [redacted]                | Data       | Rule priority 5 matched     | Tunnel    |
 ------------------------------------------------------------------------------------------------------------------------------
 | 2988332 | 2024-04-09 18:26:37 |                              | Resolution of [redacted]... | Dns        | Routing DNS through the tun... | Tunnel    |
 ------------------------------------------------------------------------------------------------------------------------------
 | 2988333 | 2024-04-09 18:26:37 |                              | Resolution of [redacted]... | Dns        | Routing DNS through the tun... | Tunnel    |
 ------------------------------------------------------------------------------------------------------------------------------
 | 2988334 | 2024-04-09 18:26:37 | C:\Windows\System32\svchost... | 0.0.0.0:0                    | Data       | Rule priority 5 matched     | Tunnel    |
 ------------------------------------------------------------------------------------------------------------------------------
 | 2988335 | 2024-04-09 18:26:37 | C:\Windows\System32\svchost... | [redacted]                | Data       | Rule priority 5 matched     | Tunnel    |
 ------------------------------------------------------------------------------------------------------------------------------
 | 2988336 | 2024-04-09 18:26:37 |                              | Resolution of [redacted]... | Dns        | Routing DNS through the tun... | Tunnel    |
 ------------------------------------------------------------------------------------------------------------------------------
 | 2988337 | 2024-04-09 18:26:37 | C:\Windows\System32\svchost... | 0.0.0.0:0                    | Data       | Rule priority 5 matched     | Tunnel    |
 ------------------------------------------------------------------------------------------------------------------------------
 | 2988338 | 2024-04-09 18:26:37 | C:\Windows\System32\svchost... | [redacted]                | Data       | Rule priority 5 matched     | Tunnel    |
 ------------------------------------------------------------------------------------------------------------------------------
 | 2988339 | 2024-04-09 18:26:38 | C:\Windows\System32\svchost... | 0.0.0.0:0                    | Data       | Rule priority 5 matched     | Tunnel    |
 ------------------------------------------------------------------------------------------------------------------------------
 | 2988340 | 2024-04-09 18:26:38 | C:\Windows\System32\svchost... | [redacted]                | Data       | Rule priority 5 matched     | Tunnel    |
 ------------------------------------------------------------------------------------------------------------------------------
 | 2988341 | 2024-04-09 18:26:38 |                              | Resolution of [redacted]... | Dns        | Routing DNS through the tun... | Tunnel    |
```

要显示单个日志条目，请发出以下命令：

```
pacli traffic log <index>
```

其中 **<index>** 对应于条目的索引号。例如：



也可以将连接日志导出到文件中以便进一步分析，只需发出以下命令：

```
pacli traffic log export <filename>
```

为动态特权访问配置 Prisma Access Agent 应用程序设置

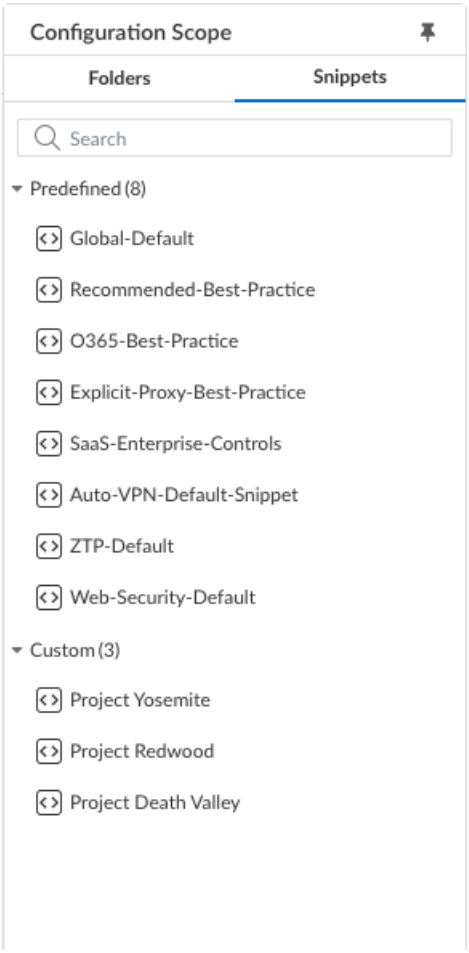
在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 创新 ❑ Prisma Access 许可证，且订阅了“移动用户” ❑ macOS 12 或更高版本的桌面设备，或 Windows 10 版本 2024 或更高版本或 Windows 11 桌面设备 ❑ 角色：项目管理员

Strata Cloud Manager 提供适用于所有项目中的所有用户组的默认 Prisma Access Agent 应用程序配置。您可以添加应用程序配置，以自定义项目中的最终用户与 Prisma Access Agent 交互的方式。

STEP 1 | 以项目管理员身份登录到 Strata Cloud Manager。

 ©2025 Palo Alto Networks, Inc.

STEP 2 | 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW** 和 **Prisma Access** > **Overview**（概览），然后展开配置范围以查看 **Snippets**（代码段）。

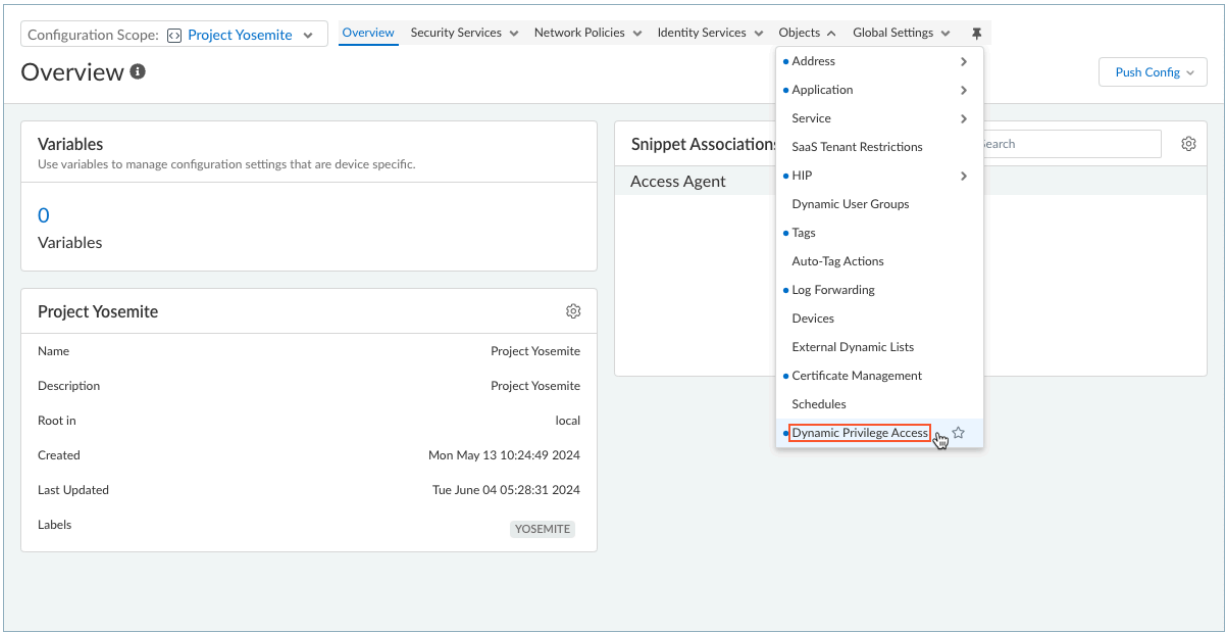


STEP 3 | 选择超级用户管理员分配给您的代码段。

您还可以查看未分配给您的代码段，但您无法与之进行交互，例如更改配置。

 ©2025 Palo Alto Networks, Inc.

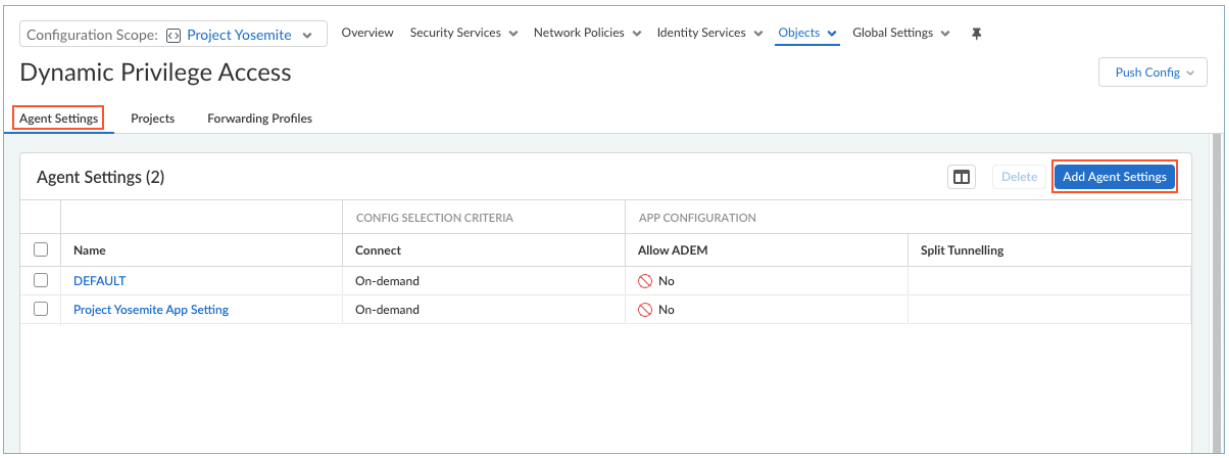
STEP 4 | 选择 **Objects**（对象） > **Dynamic Privilege Access**（动态特权访问）以打开动态特权访问设置。



STEP 5 | 选择 **Agent Settings**（代理设置）选项卡。

STEP 6 | Strata Cloud Manager 提供默认代理设置。如果您不想使用默认设置，选择 **Add Agent Settings**（添加代理设置）。

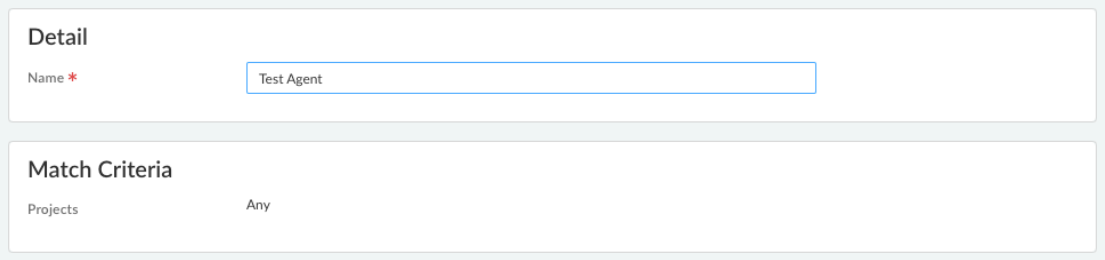
要编辑代理设置，请从表中选择一个代理名称。



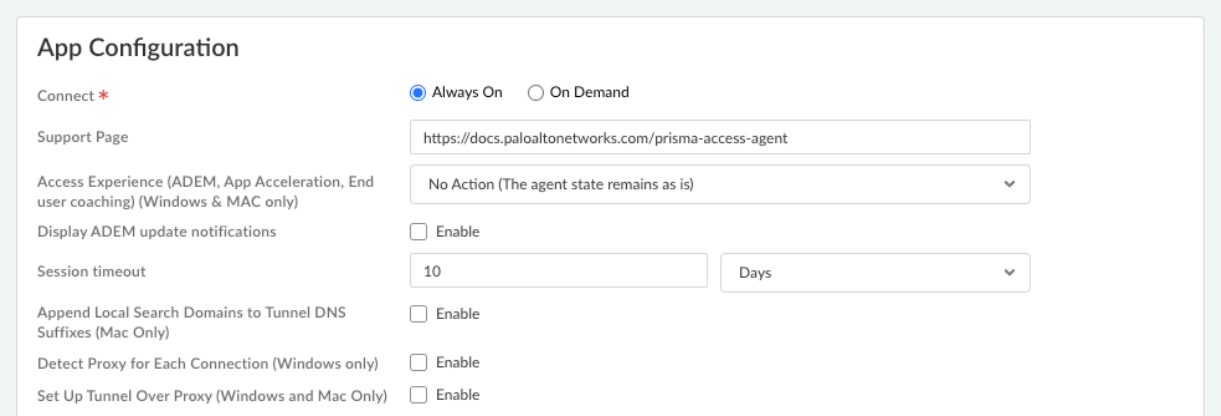
 ©2025 Palo Alto Networks, Inc.

STEP 7 | 创建应用配置规则。配置规则将一个或多个项目与特定于这些项目的某些设置相关联。

1. 输入规则的 **Name**（名称）。
2. 通过添加 **Projects**（项目）来指定 **Match Criteria**（匹配条件）。符合 **Project**（项目）条件的用户和组在使用 Prisma Access Agent 登录项目时将收到应用程序设置。
   - 要将配置部署到所有用户，请将 **Projects**（项目）设置为 **Any**（任意）。
   - 要将配置部署到登录特定项目的用户，请将 **Projects**（项目）设置为 **Add Projects**（添加项目）并从项目列表中进行选择。



STEP 8 | 配置 Prisma Access Agent 的应用设置。



- **Connect**（连接） — 指定 Prisma Access Agent 如何连接到 Prisma Access。该设置是必需的。
  - 选择 **Always on**（始终打开）可在每次用户登录端点时自动建立与 Prisma Access Agent 的连接。
  - 选择 **On demand**（按需）可仅在用户单击锁定按钮登录到 Prisma Access Agent 时才会连接到 Prisma Access Agent。
- **Support Page**（支持页面） — 输入用户在 Prisma Access Agent 中单击 **Support Resources**（支持资源）时可以访问以获得帮助的网站。

  默认支持页面是 Prisma Access Agent 文档的网站。
- **Access Experience (ADEM, App Acceleration, End user coaching) (Windows & MAC only)**（访问体验（**ADEM**、应用加速、最终用户辅导）（仅限 **Windows** 和 **MAC**）） — 指定在 Prisma Access Agent 应用安装期间是否安装自主 DEM (ADEM) 端点代理，并指定是否允许最终用户从该应用启用或禁用用户体验测试。
  - 安装代理
  - 卸载代理

 ©2025 Palo Alto Networks, Inc.

- **No action (The agent state remains as is)**（误操作（代理状态不变））（这是默认值）

有关在 Cloud 托管 Prisma Access 上开始使用 ADEM 的详细信息，请参阅自治 DEM 入门。

- **Display ADEM update notifications**（显示 **ADEM** 更新通知） — **Enable**（启用）该设置可在端点上有更新时显示来自 ADEM 的通知。
- **Session timeout**（会话超时） — 当用户连接到 Prisma Access 网关（位置）并成功进行身份验证时，将创建 Prisma Access Agent 用户会话。然后，会话被分配给特定网关，网关根据任何定义的分割隧道规则来确定要通过隧道传输的流量。Prisma Access 的最低数据平面版本必须为 11.2。

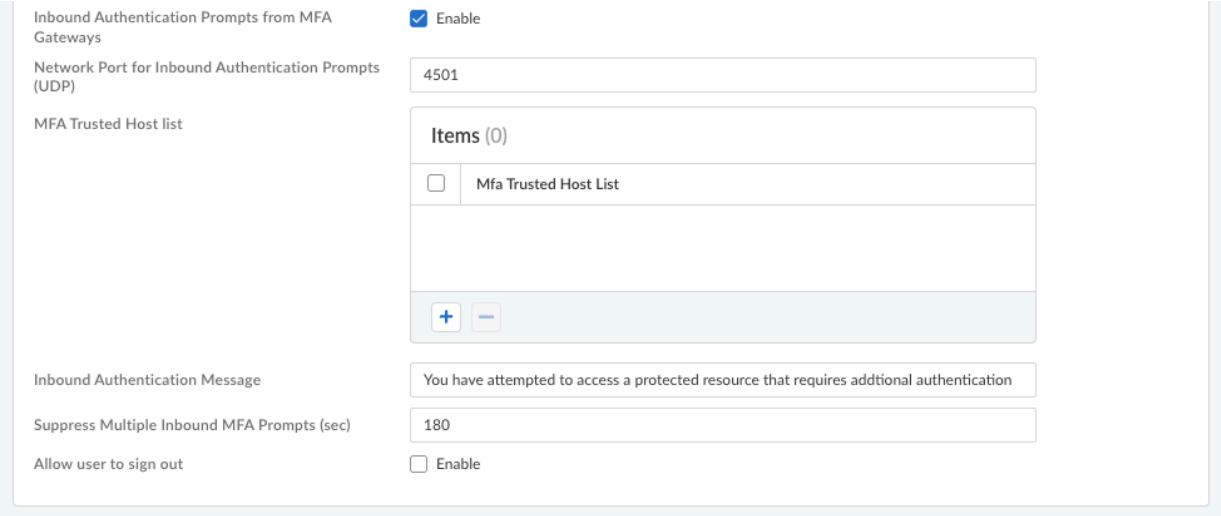
  指定会话在多久不活动之后就会导致会话超时。该设置是必需的。

  如果您在 *Prisma Access* 中使用 *Nebula (10.2)* 数据平面，则 ***Session timeout***（会话超时）值不可配置，默认值为 *7* 天。
- **Append Local Search Domains to Tunnel DNS Suffixes (Mac only)**（将本地搜索域附加到隧道 **DNS** 后缀（仅限 **MAC**）） — 选择 **Enable**（启用）可启用该设置，从而将隧道 DNS 搜索域附加到 MacOS 端点上的本地 DNS 搜索域。将隧道搜索域附加到端点的本地 DNS 搜索域后，用户无需输入完整地址即可快速访问他们经常访问的本地和远程公司网站和服务器。
- **Detect Proxy for Each Connection (Windows only)**（检测每个连接的代理（仅限 **Windows**）） — 选择 **Enable**（启用）可启用该设置，从而可在每次连接时自动检测代理。如果要自动检测网关连接的代理，并且后续使用该代理来进行 Prisma Access 连接，请禁用此设置。
- **Set Up Tunnel Over Proxy (Windows and Mac Only)**（设置代理隧道（仅限 **Windows** 和 **Mac**）） — 选择 **Enable**（启用）可启用该设置，从而基于 Prisma Access Agent 代理使用情况来配置网络流量行为。选择 **Enable**（启用）可要求 Prisma Access Agent 使用代理。如果希望要求 Prisma Access Agent 绕过代理，请禁用该设置。根据 Prisma Access Agent 代理使用情况、端点操作系统和隧道类型，网络流量的行为将有所不同。

  如果您禁用此选项，Prisma Access Agent 将绕过代理。匹配代理或 PAC 文件规则的 HTTP 或 HTTPS 流量都需要在到达预定目的地之前遍历 Prisma Access Agent 隧道。通过绕过代

 ©2025 Palo Alto Networks, Inc.

理，您可以防止用户设置个人代理来访问 Web 资源，而无需通过隧道进行检查和策略实施。



- **Optimized MTU**（优化 **MTU**） — 最大传输单元 (MTU) 是传输过程中可以在数据包中发送的最大数据包大小。单击 **Enable**（启用）可启用该选项，从而自动确定用于数据包传输的最佳 MTU。

  Prisma Access Agent 连接可以遍历多个 MTU 值低于标准 1500 字节的 ISP 和网络跃点。当静态代理 MTU 值低于 ISP 提供的值时，会产生过多的碎片和额外开销，导致吞吐量降低。如果 ISP 网络路径中数据包被丢弃，则还会触发重传，导致性能欠佳。

  启用 **Optimized MTU**（优化 **MTU**），可以帮助您避免手动确定和配置最佳 MTU 值的繁琐过程，并防止用户遇到影响工作效率的不良性能。

  默认情况下启用 **Optimized MTU**（优化 **MTU**）。如果禁用，您可以手动配置 MTU。**Configurable MTU (bytes)**（可配置 **MTU**（字节））范围为 256 到1420 字节。默认值为 1400 字节。
- **Inbound Authentication Prompts from MFA Gateways**（来自 **MFA** 网关的入站身份验证提示） — 要支持多因素身份验证 (MFA)，Prisma Access Agent 端点必须接收并确认来自网关的入站 UDP 提示。单击 **Enable**（启用）可启用该设置，从而允许 Prisma Access Agent 端点接收并确认 UDP 提示。此设置已默认启用。禁用此设置可阻止来自网关的 UDP 提示。
- **Network Port for Inbound Authentication Prompts (UDP)**（入站身份验证提示的网络端口 **(UDP)**） — 指定 Prisma Access Agent 端点用于从 MFA 网关接收入站身份验证提示的端口号。默认端口为 4501。要更改端口，请指定从 1 至 65535 之间的数字。
- **MFA Trusted Host list**（**MFA** 可信主机列表） — 单击 **Add**（添加）可为防火墙或身份验证网关添加主机，Prisma Access Agent 端点可以信任这些主机进行多因素身份验证。当端点在指定的网络端口上接收 UDP 消息时，Prisma Access Agent 仅在 UDP 提示来自受信任的网关时才会显示身份验证消息。
- **Inbound Authentication Messages**（入站身份验证消息） — 自定义当用户尝试访问需要执行额外身份验证的资源时要显示的通知消息。

  当用户尝试访问需要额外身份验证的资源时，Prisma Access Agent 会收到一个包含入站身份验证提示的 UDP 数据包，并显示上述通知消息。该 UDP 数据包还包含您在配置多因素

 ©2025 Palo Alto Networks, Inc.

身份验证时指定的身份验证门户页面的 URL。Prisma Access Agent 自动将 URL 附加到消息中。

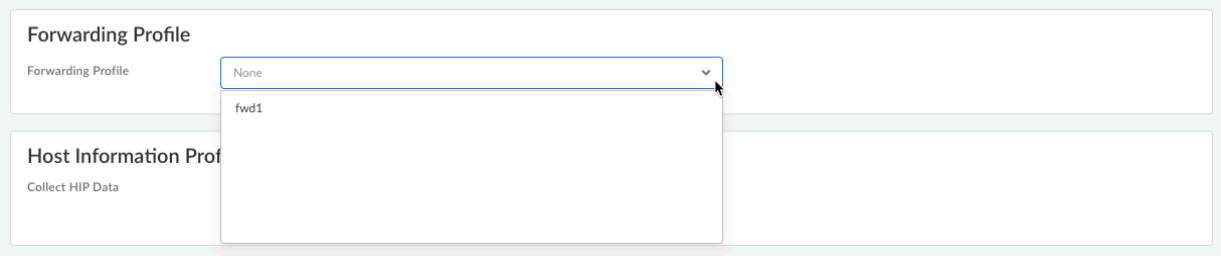
例如：

> 您试图访问需要附加身份验证的受保护资源。继续在

中进行身份验证 消息最多可以包含 255 个字符。

- **Suppress Multiple Inbound MFA Prompts (sec)**（禁止多个入站 **MFA** 提示（秒））— 指定等待的秒数，在超过该时间后，Prisma Access Agent 可以禁止多个入站 UDP 提示。默认值为 180 秒。
- 允许用户注销 — 选择 **Enable**（启用）可启用该设置，以允许用户注销 Prisma Access Agent。默认禁用该设置。

STEP 9 | 选择先前配置的 **Forwarding Profile**（转发配置文件），以管理代理与 Prisma Access 之间的流量流动方式。



STEP 10 | 为动态特权访问配置 DNS 设置

STEP 11 | 配置主机信息配置文件设置

STEP 12 | 完成 Prisma Access Agent 设置的设置后，单击 **Save**（保存）。

为动态特权访问配置 DNS 设置

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 创新 ❑ Prisma Access 许可证，且订阅了“移动用户” ❑ macOS 12 或更高版本的桌面设备，或 Windows 10 版本 2024 或更高版本或 Windows 11 桌面设备 ❑ 角色：项目管理员

您可以配置 DNS 服务器，以使 Prisma Access 能够解析您的内部域名。

STEP 1 | 在 Strata Cloud Manager 中，选择 **Manage**（管理） > **Configuration**（配置） > **NGFW** 和 **Prisma Access** > **Overview**（概览），然后展开配置范围以查看 **Snippets**（代码段）。

©2025 Palo Alto Networks, Inc.

STEP 2 | 选择超级用户管理员分配给您的代码段。

STEP 3 | 选择 **Objects**（对象） > **Dynamic Privilege Access**（动态特权访问）以打开动态特权访问设置。

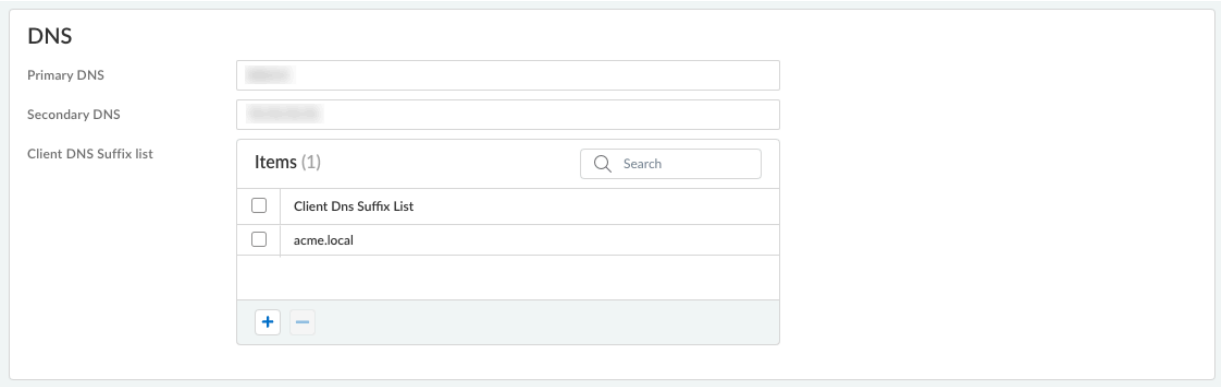
STEP 4 | 选择 **Agent Settings**（代理设置）选项卡。

STEP 5 | **Add Agent Settings**（添加代理设置）或从“代理设置”表中选择现有设置。

STEP 6 | 输入 Prisma Access 用于解析内部域名的 **Primary DNS**（主 **DNS**）服务器和 **Secondary DNS**（辅助 **DNS**）服务器。

STEP 7 | 您可以添加 **Client DNS Suffix List**（客户端 **DNS** 后缀列表），以指定当用户输入了客户端无法解析的不合格的主机名时客户端应在本地使用的后缀，例如 **`acme.local`**。

请勿在域名后缀前输入通配符 (*) 字符（例如 acme.com）。可以添加多个后缀。



为动态特权访问配置 HIP 数据收集设置

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 创新 ❑ macOS 12 或更高版本的桌面设备，或 Windows 10 版本 2024 或更高版本或 Windows 11 桌面设备 ❑ Prisma Access 许可证，且订阅了“移动用户” ❑ 角色：项目管理员

Prisma Access Agent 收集有关运行主机的信息，并在成功连接后将此主机信息提交给 Prisma Access 位置（网关）。网关将 Prisma Access Agent 提交的原始主机信息与您定义的任何主机信息配置文件 (HIP) 对象和 HIP 配置文件进行匹配。如果网关找到匹配，则将会在 HIP 匹配日志中生成一个条目。此外，如果网关在策略规则中找到 HIP 配置文件匹配，则将会实施相应的安全策略。

 ©2025 Palo Alto Networks, Inc.

在“Edit Global Agent Settings（编辑全局代理设置）”页面的 **HIP Notifications**（**HIP** 通知）选项卡中，您可以创建 HIP 通知、创建和管理 HIP 对象以及创建和管理适用于所有端点中的 Prisma Access Agent 的 HIP 配置文件。

在该选项卡中，您可以定义希望 Prisma Access Agent 收集或排除的自定义 HIP 数据。启用该选项后，Prisma Access Agent 将从运行 macOS 或 Windows 操作系统的设备收集数据。

例如，自定义检查可以让您知道某个应用程序是否在端点上安装或运行。您定义要在自定义检查中收集的数据包含在原始主机信息数据中，Prisma Access Agent 收集这些数据，然后在 Prisma Access Agent 连接时将其提交给 Prisma Access。

STEP 1 | 在 Strata Cloud Manager 中，选择 **Manage**（管理） > **Configuration**（配置） > **NGFW** 和 **Prisma Access** > **Overview**（概览），然后展开配置范围以查看 **Snippets**（代码段）。

STEP 2 | 选择超级用户管理员分配给您的代码段。

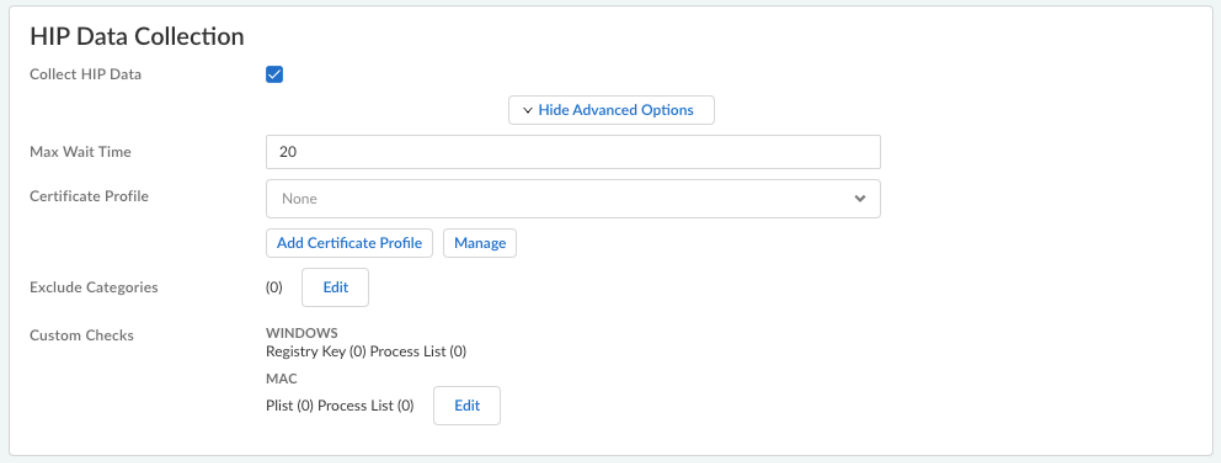
STEP 3 | 选择 **Objects**（对象） > **Dynamic Privilege Access**（动态特权访问）以打开动态特权访问设置。

STEP 4 | 选择 **Agent Settings**（代理设置）选项卡。

STEP 5 | **Add Agent Settings**（添加代理设置）或从“代理设置”表中选择现有配置。

STEP 6 | 在“Host Information Profile (HIP)（主机信息配置文件 (HIP)）”部分中，选择 **Collect HIP Data**（收集 **HIP** 数据）以在使用项目登录的端点上启用 HIP 数据收集。

STEP 7 | 选择 **Show Advanced Options**（显示高级选项）。



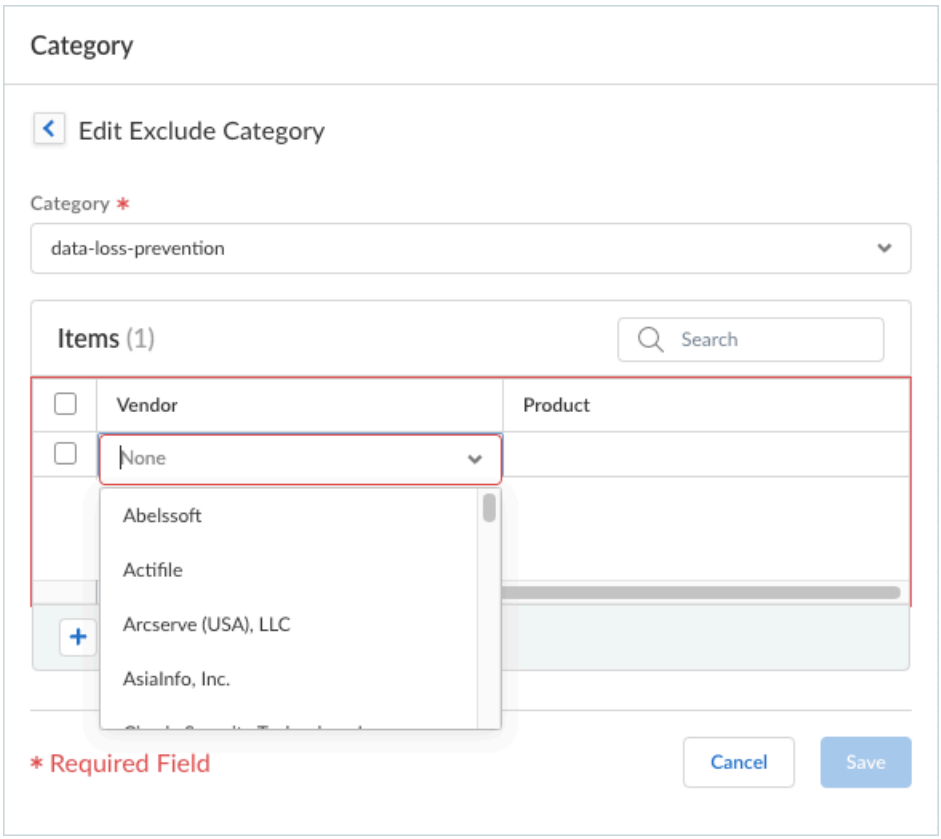
STEP 8 | 指定 **Max Wait Time**（最长等待时间）（以秒为单位），也就是 Prisma Access Agent 在提交可用数据之前应搜索 HIP 数据的时间。范围为 10 至 60 秒；默认为 20 秒。

STEP 9 | **Edit**（编辑）“Exclude Categories（排除类别）”可从 HIP 数据收集中排除特定类别或类别中的供应商、应用程序或版本。

选择要从 HIP 收集中排除的 **Category**（类别）（如 data loss prevention（数据丢失防护-DLP））。选择类别后，您可依次选择 **Add**（添加）、**Vendor**（供应商）来添加特定供应商，然后可再依次 **Add**（添加）、**Product**（产品）以添加来自供应商的产品，以根据需要进一步完

©2025 Palo Alto Networks, Inc.

善排除设置。您可以在排除列表中添加多个供应商和产品。选择 **Save**（保存）以保存每个对话框中的设置。



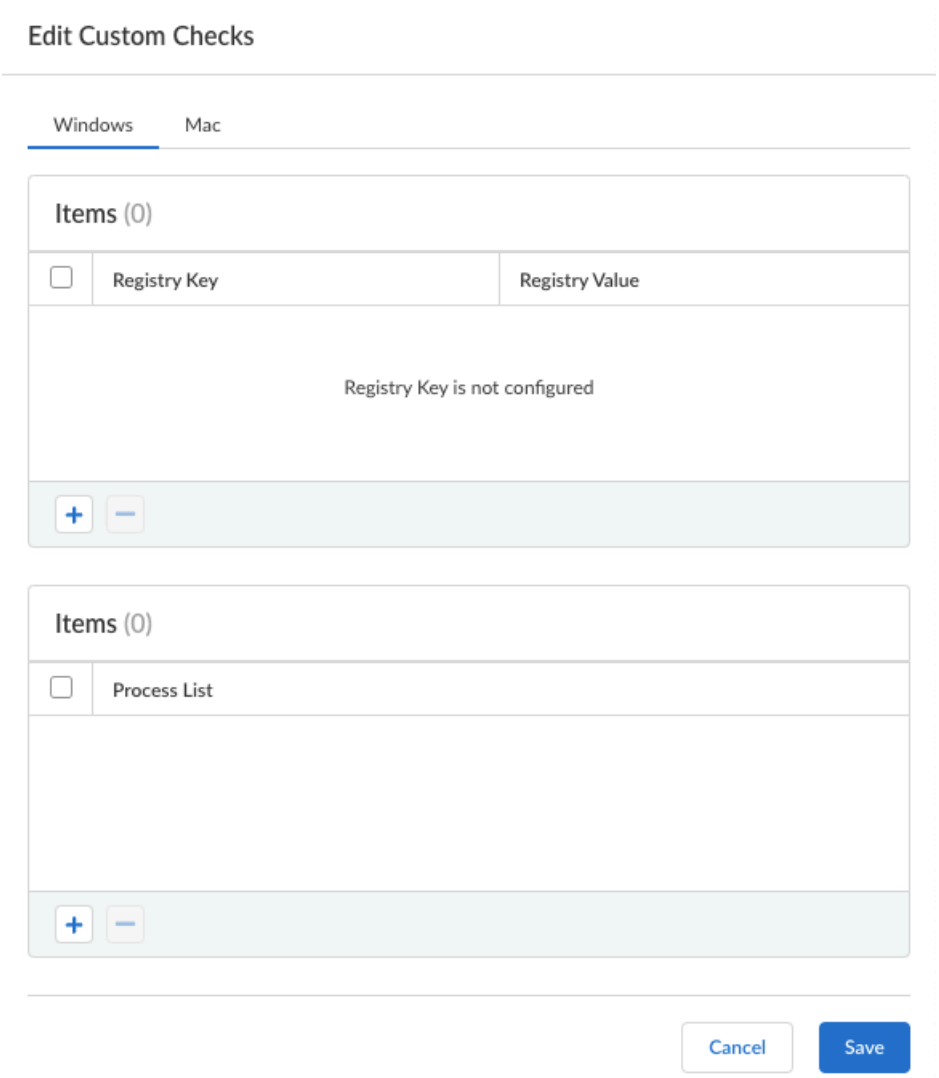
如果您不想排除整个供应商，则可以从供应商排除特定补丁。添加供应商后，您可以指定补丁名称或编号，还可以选择指定要从 HIP 报告中排除补丁更新的日期，格式如下：

```
Exclude: [kb-article-id1:MM/DD/YYYY], [kb-article-id2:MM/ DD/YYYY]
```

其中，**<kb-article-id>** 是属性中的名称或编号（例如 **<kb-article-id>2267602</kb-article-id>**），**MM/DD/YYYY** 指定从 HIP 报告中排除的修补程序日期。如果不设置日期，修补程序将无限期地从 HIP 报告中排除。如果选择设置日期，修补程序将排除到指定日期。

©2025 Palo Alto Networks, Inc.

STEP 10 | 选择 **Edit**（编辑） Custom Checks（自定义检查）以定义您要从正运行此配置的主机收集的自定义数据。



例如，如果您有任何必需应用程序未包含在用于创建 HIP 对象的供应商或产品列表中，则您可以创建自定义检查以确定是否已安装应用程序（如已安装，则具有对应的 Windows 注册表或 Mac plist 项），或者是否正在运行（具有对应的运行进程）：

- **Windows** — 选择 **Add**（添加）以添加对特定注册表项或注册表值的检查。要限制于收集特定注册表值的数据，请选择 **Add**（添加）并定义该特定注册表值。
- **Windows** — 选择 **Add**（添加）以添加对特定 **Plist** 项或键值的检查。要限制于收集特定表项值的数据，请选择 **Add**（添加）以添加键值。单击“OK（确定）”以保存设置。
- **Process List**（进程列表）— **Add**（添加）要在用户端上查看的进程，以确定其是否正在运行。例如，要确定某个软件应用程序是否正在运行，请将这个可执行文件的名称添加到进程列表中。您可以在 **Windows** 选项卡或 **Mac** 选项卡中添加进程，或同时在两个选项卡中添加。

完成后选择 **Save**（保存）以保存自定义检查设置。

©2025 Palo Alto Networks, Inc.

STEP 11 | 完成项目特定的 Prisma Access Agent 设置的配置后，选择 **Save**（保存）以保存配置。

 ©2025 Palo Alto Networks, Inc.

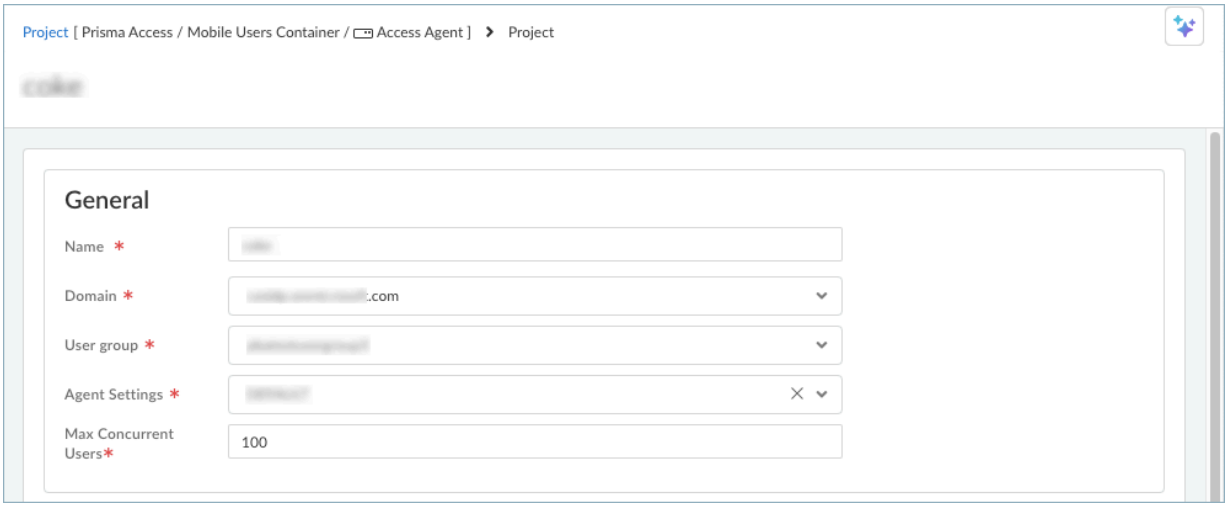
创建项目

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 许可证 ❑ 要求的最低 Prisma Access 版本：5.1 ❑ 角色：超级用户

使用 Prisma Access Agent 添加您希望用户访问的项目。只有项目管理员可以创建和管理项目定义。

STEP 1 | 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**）。

STEP 2 | 将范围设置为您创建的项目代码段，然后导航到 **Objects**（对象） > **Dynamic Privilege Access**（动态权限访问） > **Projects**（项目） > **Add Project**（添加项目）。

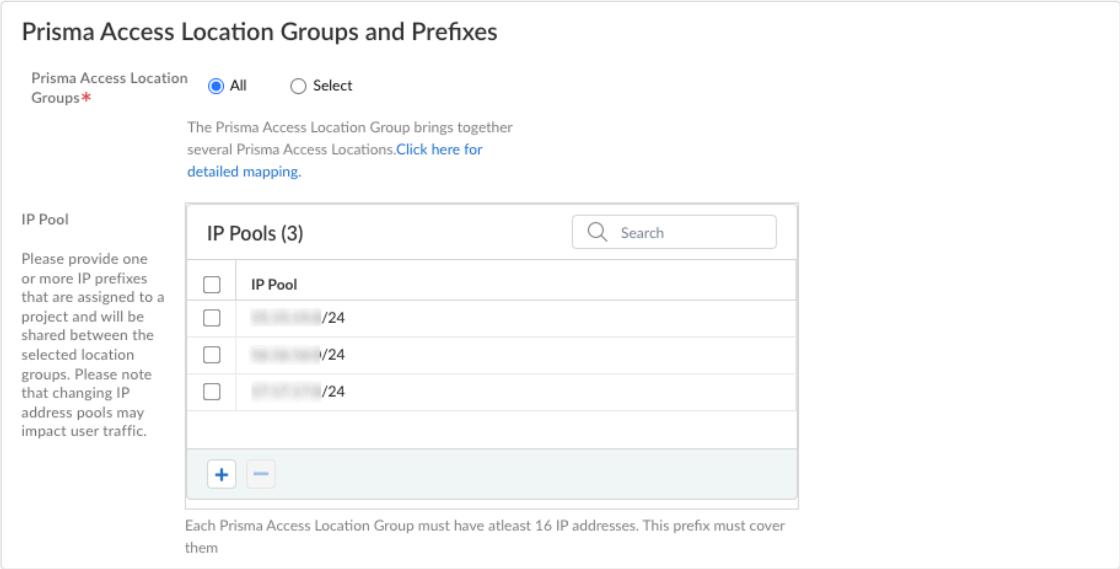


1. 输入项目 **Name**（名称）。
2. 选择您在云身份引擎中添加的 **Domain**（域），以及映射到该目录的 **User Group**（用户组）。
3. 选择您之前添加的 **Agent Settings**（代理设置），以及项目的 **Max Concurrent Users**（最大并发用户数）。
4. 选择 **Prisma Access Location Groups**（**Prisma Access** 地点组）。根据您添加 GlobalProtect 网关的地点来填充地点组列表。

   您正在创建的项目与 IP 池和地点组相关联。用户将根据他们使用 Prisma Access Agent 连接到的项目和 Prisma Access 计算地点获取 IP 地址。项目只能连接到与该项目关联

©2025 Palo Alto Networks, Inc.

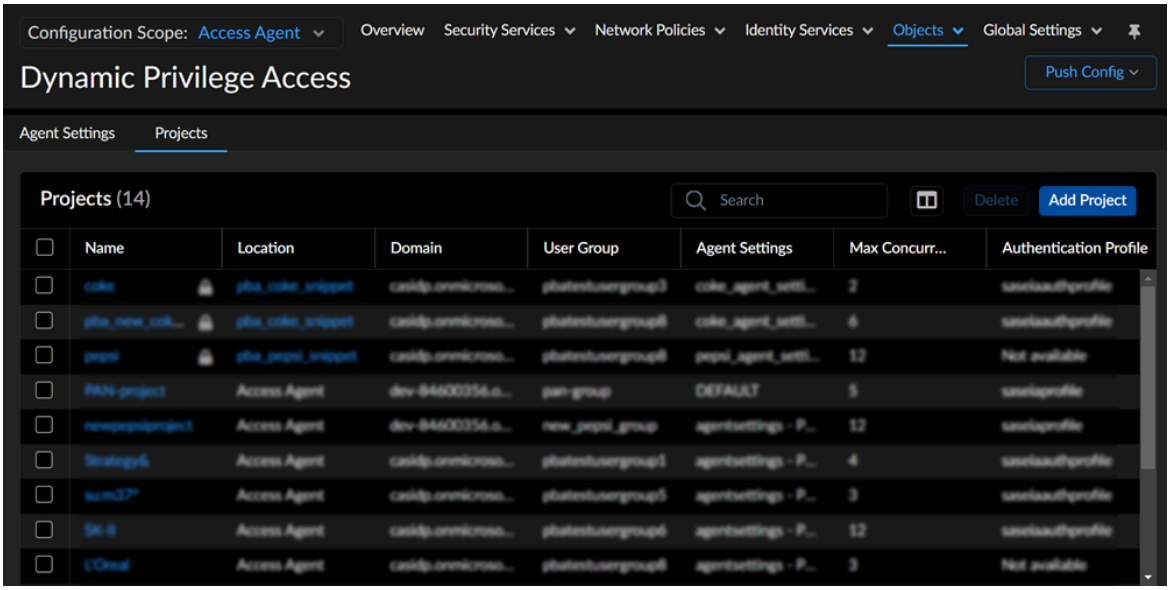
的地点组中的地点。您可以选择 **Click here for detailed mapping**（单击此处查看详细映射），以查看 Prisma Access 地点组和 Prisma Access 计算地点之间的映射。



5. 为项目添加或选择 **IP Pools**（**IP** 池）。IP 前缀分配给您的项目，将在您选择的 Prisma Access 地点组之间共享。

   可以汇总这些项目 IP 池以减少发送到网络的路由数量。

6. **Save**（保存）项目设置。



 ©2025 Palo Alto Networks, Inc.

- 在配置范围中选择项目代码段时，您只能访问与该特定项目相关的设置和详细信息。
- 当您以项目管理员或项目推送管理员身份登录到 *Strata Cloud Manager* 时，只能查看您有权访问的项目详细信息。如果选择其他项目代码段的配置范围，则无法访问其他项目的设置和详细信息。
- 要在项目之间进行切换，必须使用不同项目的凭据以其他项目管理员或项目推送管理员的身份重新登录 *Strata Cloud Manager*。

STEP 3 | **Push**（推送）您的更改。

在 Prisma Access 中创建项目后，用户最多需要 15 分钟才能使用 Prisma Access Agent 对该项目进行身份验证。

 ©2025 Palo Alto Networks, Inc.

动态特权访问的流量控制

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 许可证 ❑ 要求的最低 Prisma Access 版本：5.1 ❑ 角色：项目管理员

使用流量控制将项目的流量转发到服务连接和特定于项目的路由。

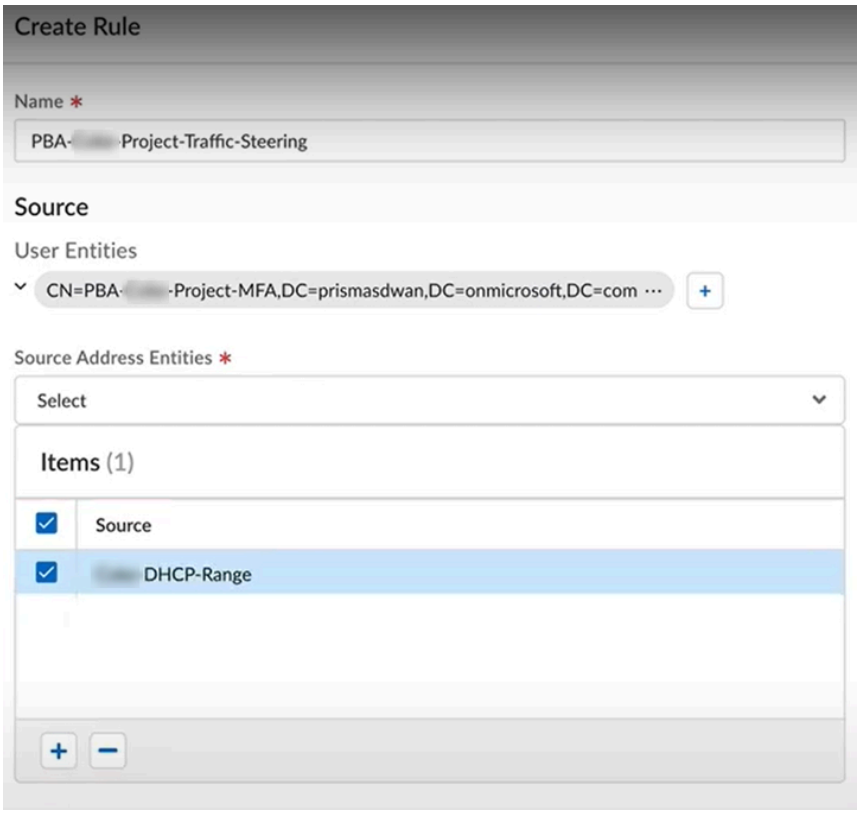
STEP 1 | 选择 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Service Connections**（服务连接）。

STEP 2 | 添加服务连接。

STEP 3 | 编辑 **Advanced Settings**（高级设置）以路由流量。

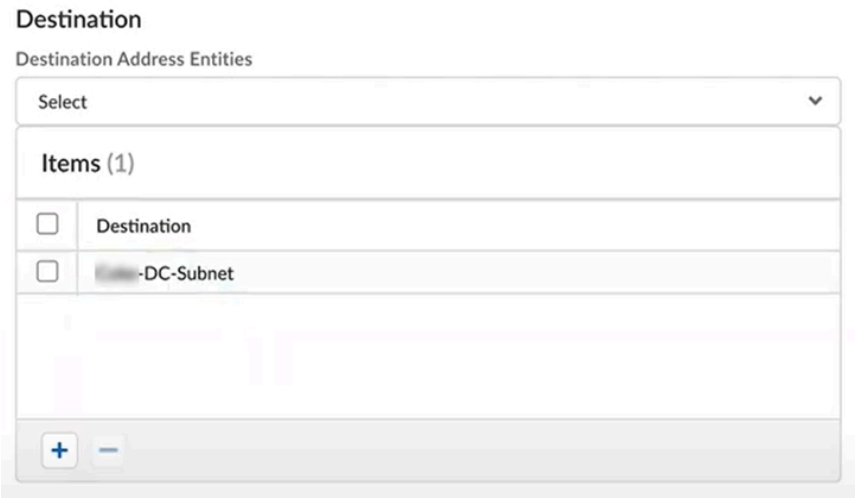
STEP 4 | 在项目的 **Traffic Steering**（流量控制）下面选择 **Add Rule**（添加规则）。

STEP 5 | 将 **Source**（源）与用户匹配，并将项目 DHCP 范围添加为 **Source Address Entities**（源地址实体）。

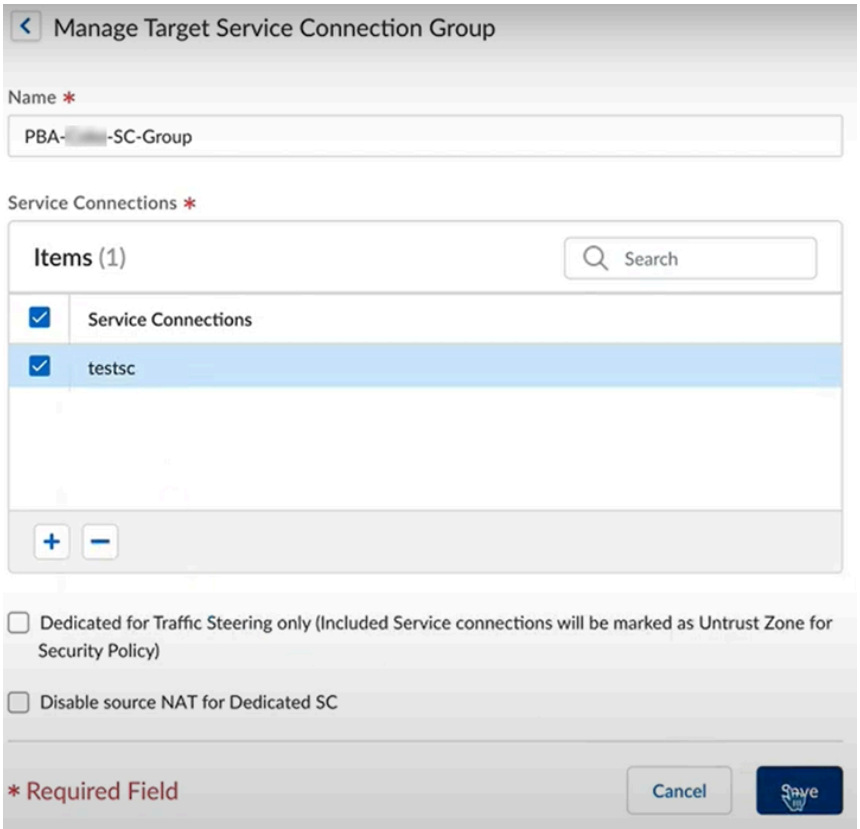


 ©2025 Palo Alto Networks, Inc.

STEP 6 | 匹配 **Destination**（目标）地址实体。



STEP 7 | 选择服务和操作。



STEP 8 | 保存并推送更改。

©2025 Palo Alto Networks, Inc.

为动态特权访问设置 Prisma Access Agent

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 创新 ❑ Prisma Access 许可证，且订阅了“移动用户” ❑ macOS 12 或更高版本的桌面设备，或 Windows 10 版本 2024 或更高版本或 Windows 11 桌面设备 ❑ 角色：超级用户

您的最终用户将使用 Prisma Access Agent 根据您的用户被分配到的客户项目访问您组织的网络。

设置 项目特定的代理设置 并 创建项目后，您可以配置其他 Prisma Access Agent 分阶段推出和全局代理设置等设置。

您可以配置以下 Prisma Access Agent 设置：

- 为 Prisma Access Agent 配置分阶段推出
- 配置 Prisma Access Agent 的常规全局设置
- 配置 Prisma Access Agent 的 HIP 通知

为 Prisma Access Agent 配置分阶段推出

在何处可以使用？	需要提供什么？
• Prisma Access（由 Strata Cloud Manager 管理）	❑ Prisma Access 5.1 Preferred 或 Innovation ❑ Prisma Access 许可证，且订阅了“移动用户” ❑ macOS 12 或更高版本的桌面设备，或 Windows 10 版本 2024 或更高版本或 Windows 11 桌面设备 ❑ 角色：超级用户

Prisma Access Agent 分阶段升级功能为管理员提供了一种按特定顺序升级设备组的方法。通过分阶段升级，您不必再依赖移动设备管理 (MDM) 软件（如 Jamf Pro 和 Microsoft Intune）来升级 Prisma Access Agent。

只有在最终用户的设备上初始部署或安装 *Prisma Access Agent* 后，才能进行分阶段升级。

©2025 Palo Alto Networks, Inc.

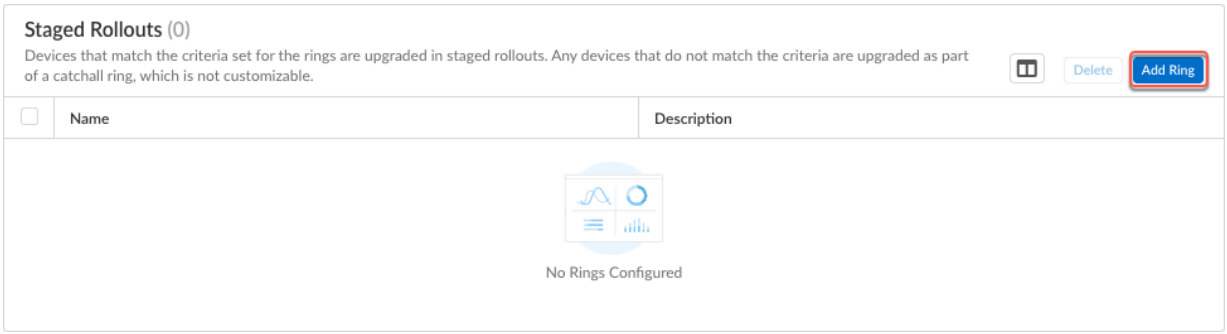
要分阶段进行 Prisma Access Agent 升级，您可以根据用户、组和操作系统配置具有匹配条件的升级环。符合条件的设备将按照升级环的顺序进行升级（0 环到 4 环，默认环）。

使用 Prisma Access Agent 的“Access Agent Setup（访问代理设置）”页面载入移动用户时，您可以选择定义升级环。如果在初始代理配置期间未选择定义升级环，则所有设备都将置于默认环中。可以稍后返回到 Prisma Access Agent Setup（Prisma Access Agent 设置）页面，以定义升级环，并将配置推送到 Prisma Access。这些更改将在下一个分阶段进行期间生效，或者在您停止并启动阶段进行之后生效。

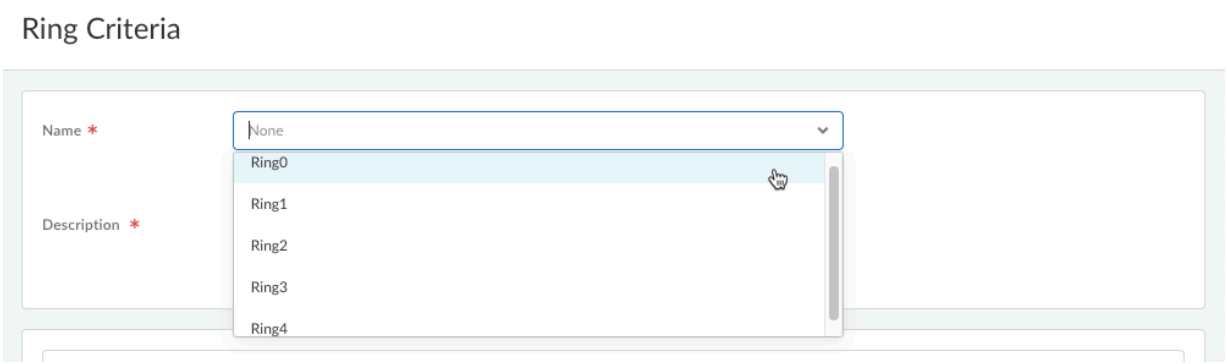
要配置升级环：

STEP 1 | 在 Strata Cloud Manager 中，选择 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Access Agent**（访问代理） > **Prisma Access Agent**。

STEP 2 | 在 **Staged Rollouts**（分阶段推出）部分中，单击 **Add Ring**（添加环）。



STEP 3 | 在 **Name**（名称）中，选择环的预定义名称。可以选择从 **Ring0** 到 **Ring4**。您要添加的第一个环是 **Ring0**。

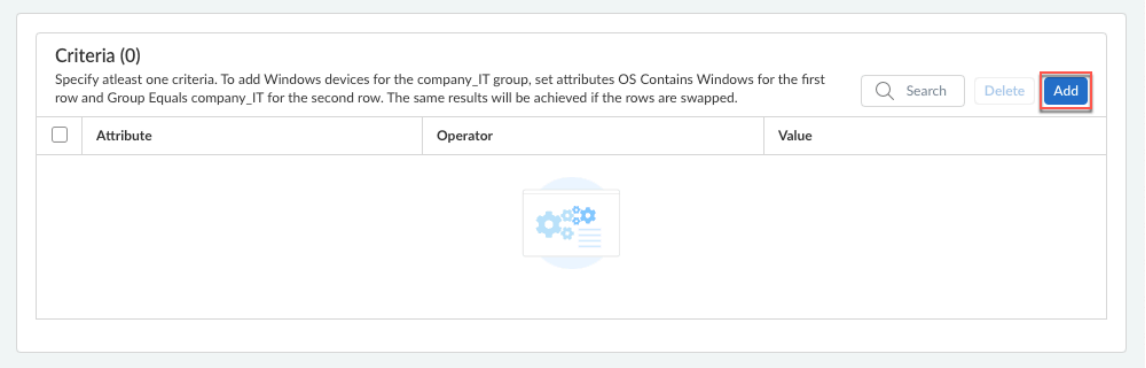


STEP 4 | 在 **Description**（说明）中，为环输入一个有意义的说明。

 ©2025 Palo Alto Networks, Inc.

STEP 5 | 根据 **User**（用户）、**Groups**（组）或**Device OS**（设备操作系统）属性指定环的条件。

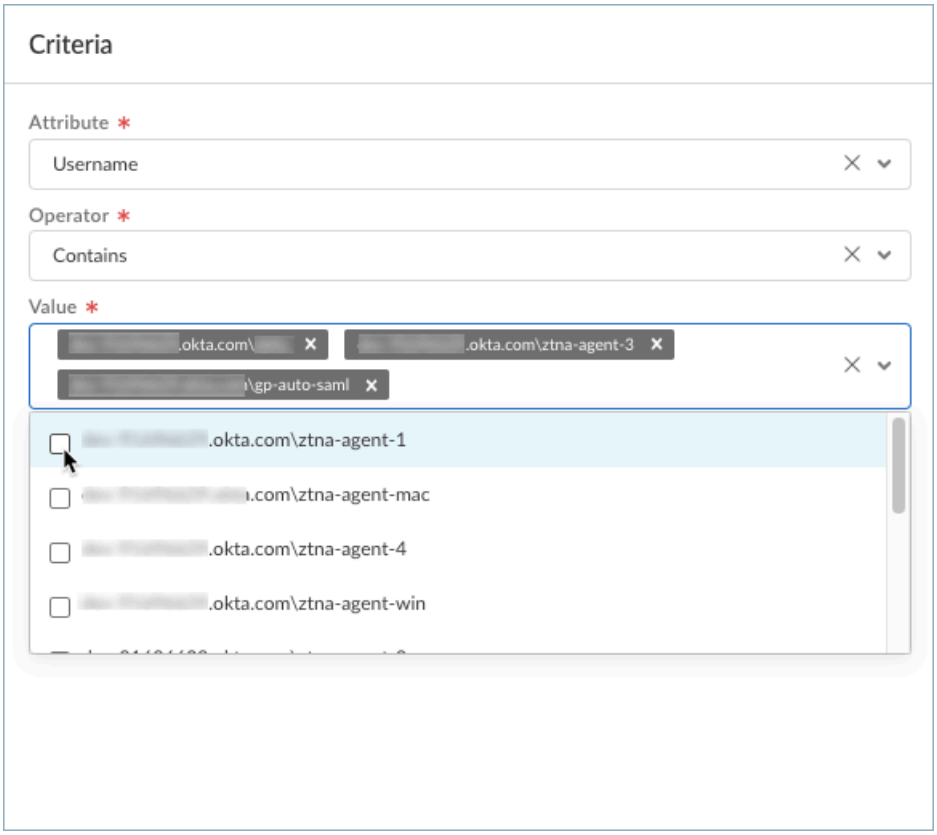
1. 选择 **Add**（添加）以添加条件。



2. 对于每个条件，请选择 **Attribute**（属性）、**Operator**（运算符）、**Value**（值），然后单击 **Add**（添加）。对于每个条件，您只能选择一个属性和一个运算符。值取决于您为属性和运算符选择的内容：

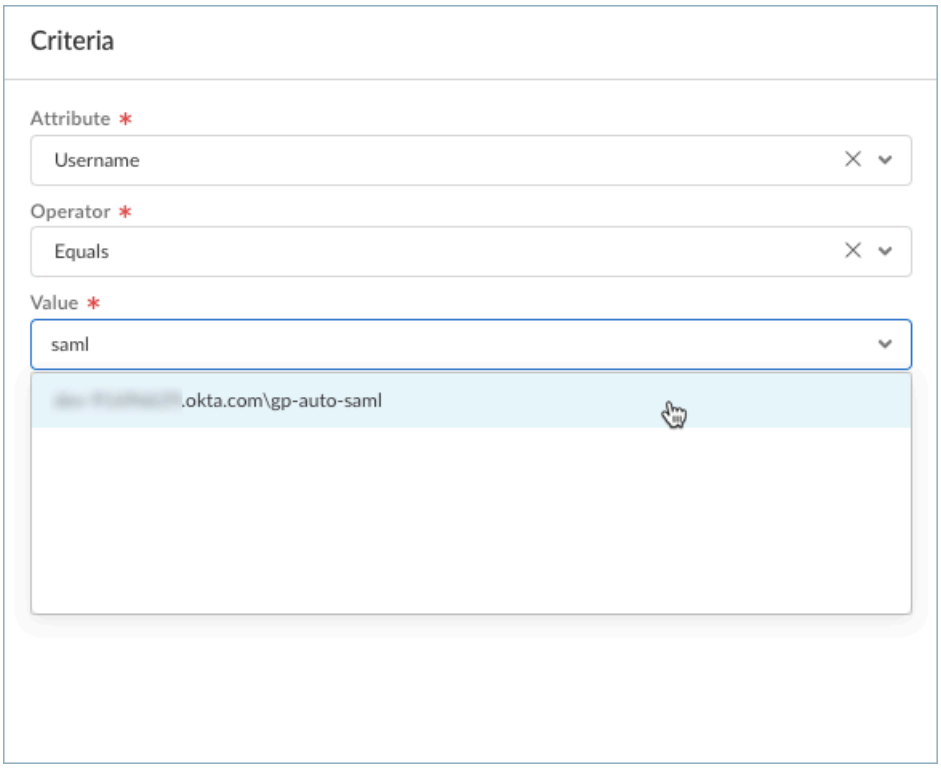
   - 对于 **Username**（用户名）属性：

     - 如果选择 **Operator**（运算符） > **Contains**（包含），请从 **Value**（值）列表中选择或搜索用户名。要开始搜索，请开始键入用户名。您可以从列表中选择一个或多个用户名。

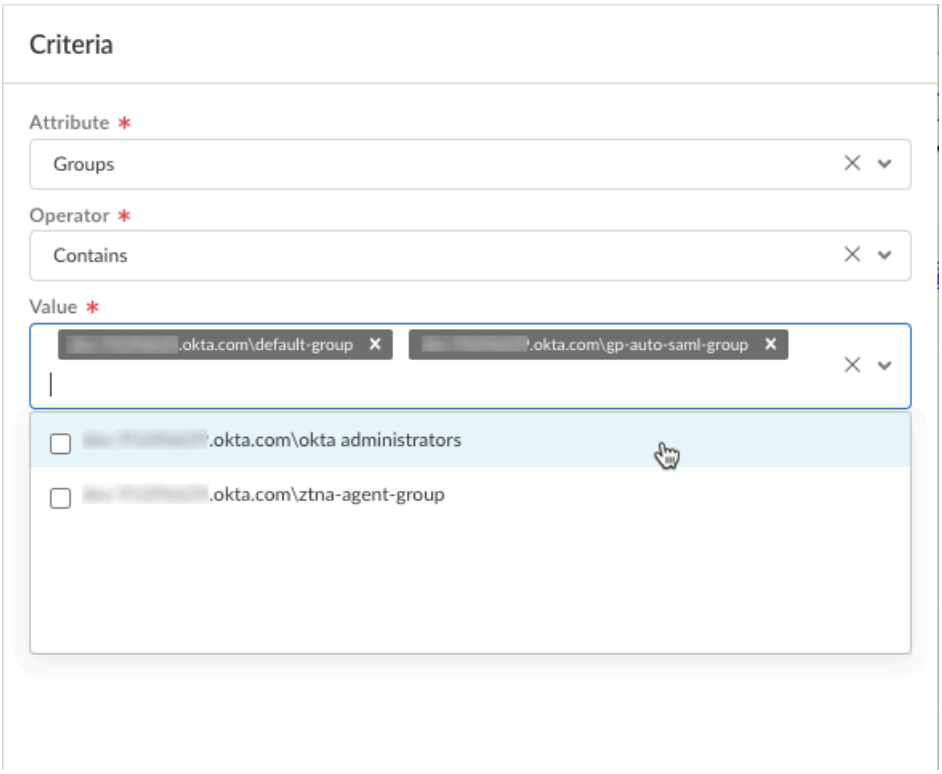


     - 如果选择 **Operator**（运算符） > **Equals**（等于），则从 **Value**（值）列表中选择或搜索用户名。要开始搜索，请开始键入用户名。可以从列表中选择一个用户名。

 ©2025 Palo Alto Networks, Inc.

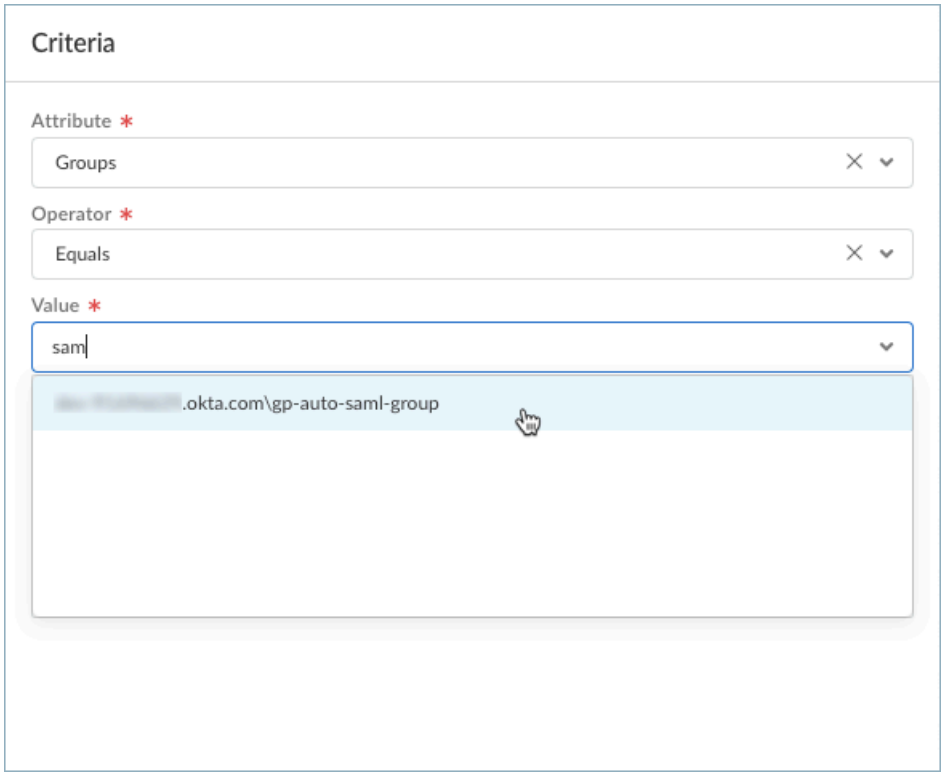


- 对于 **Groups**（组）属性：
  - 如果选择 **Operator**（运算符） > **Contains**（包含），则从 **Value**（值）列表中选择或搜索组。要开始搜索，请开始键入组名称。可以从列表中选择一个或多个组。



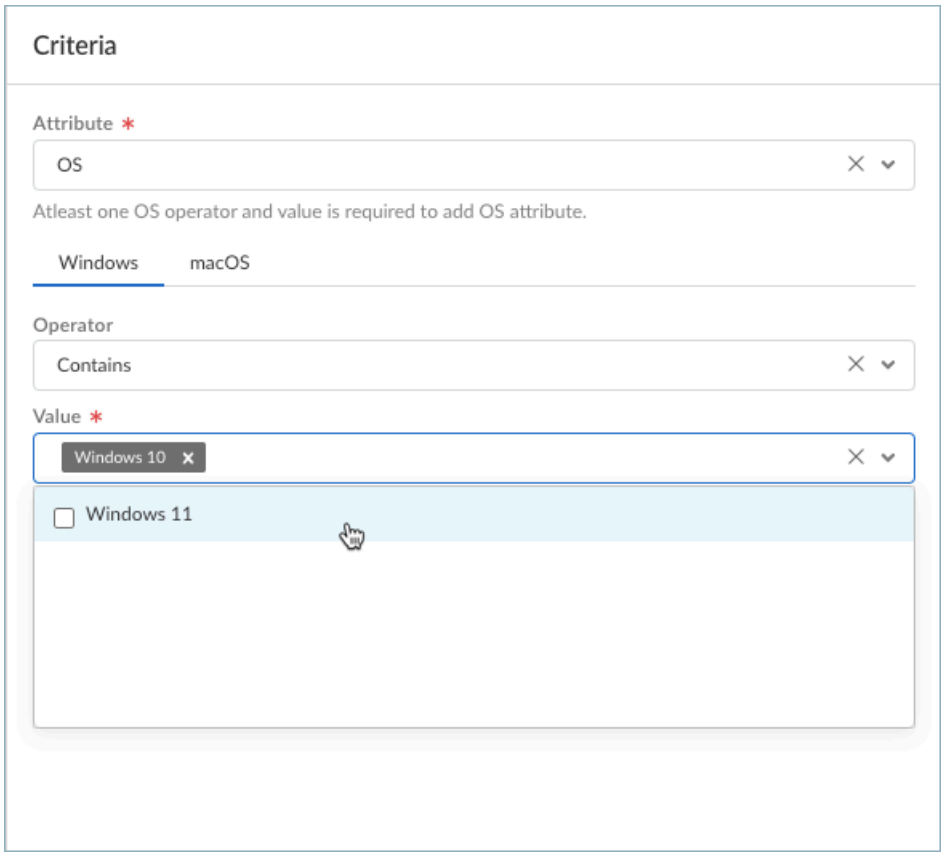
 ©2025 Palo Alto Networks, Inc.

- 如果选择 **Operator**（运算符） > **Equals**（等于），则从 **Value**（值）列表中选择或搜索组。要开始搜索，请开始键入组名称。可以从列表中选择一个组。



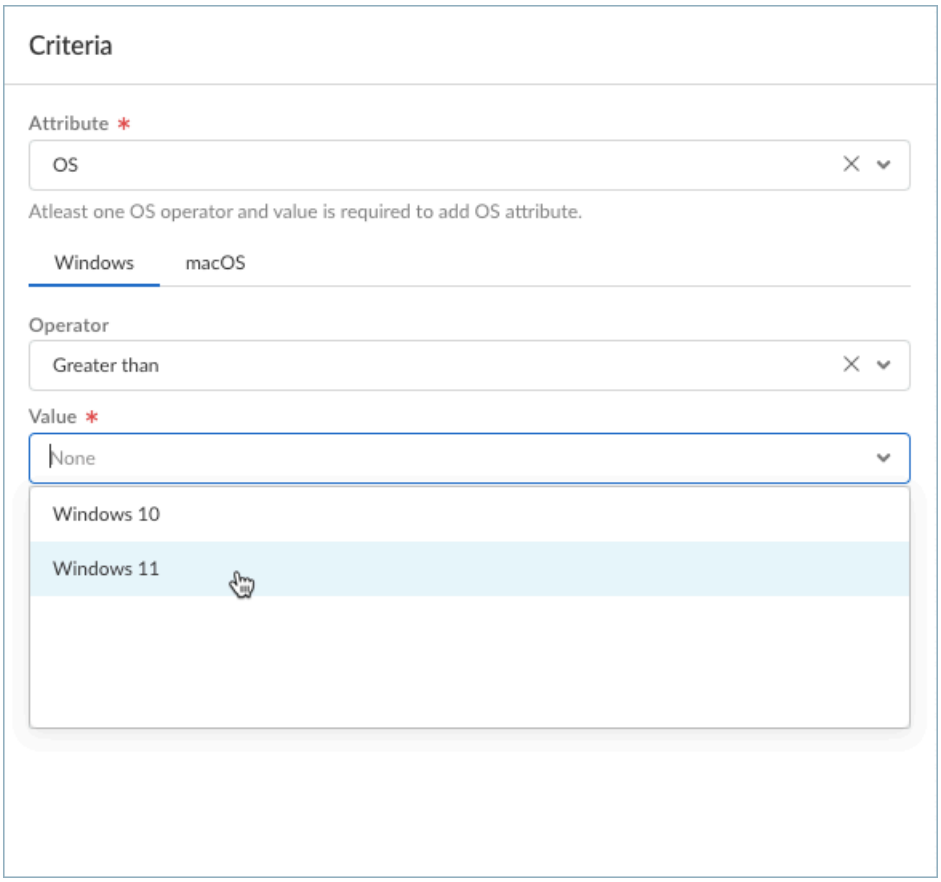
- 在 **OS**（操作系统）属性中，选择操作系统类型（**Windows** 或 **macOS**）。那么：
  - 如果选择 **Operator**（运算符） > **Contains**（包含），请从 **Value**（值）列表中搜索或选择一个或多个操作系统版本。要开始搜索，请开始键入操作系统和版本。可以从列表中选择一个或多个操作系统版本。

©2025 Palo Alto Networks, Inc.



- 如果选择 **Greater than**（大于）或 **Less than**（小于）运算符，则从 **Value**（值）列表中搜索或选择操作系统版本。要开始搜索，请开始键入操作系统和版本。可以从列表中选择一个操作系统版本。

©2025 Palo Alto Networks, Inc.

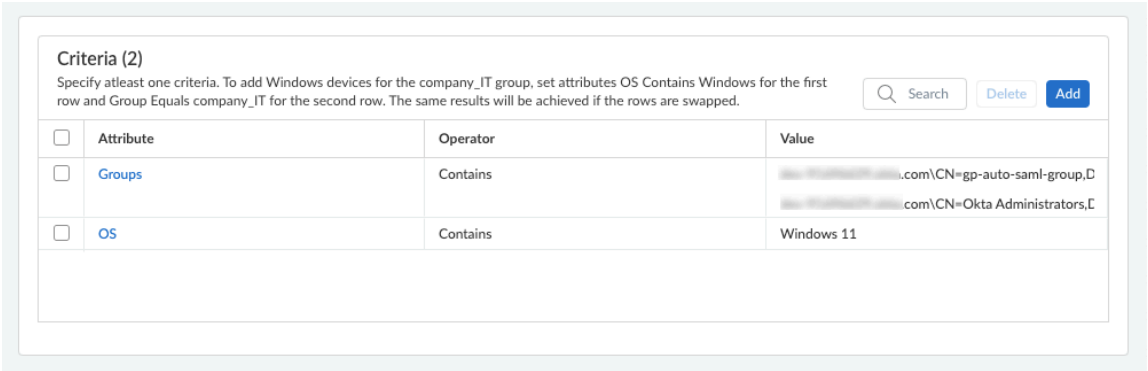


3. 如果需要，可以选择 **Add**（添加）以添加更多条件。每个环最多可指定三个条件。

   每个环只能使用一次属性。使用属性添加条件后，该属性将不再显示在 **Attribute**（属性）下拉列表中。

   添加标准后，条件将显示在“Ring Criteria（环条件）”页面中的 **Criteria**（条件）表中。Prisma Access 在计算条件时，使用逻辑 OR（或）运算符来计算同一单元格中列出的值，使用逻辑 AND（与）运算符来计算行之间的属性和值。

   例如，下图中的条件将匹配属于 **gp-auto-saml-group** 或 **Okta Administrators** 组并运行 Windows 11 操作系统的设备。



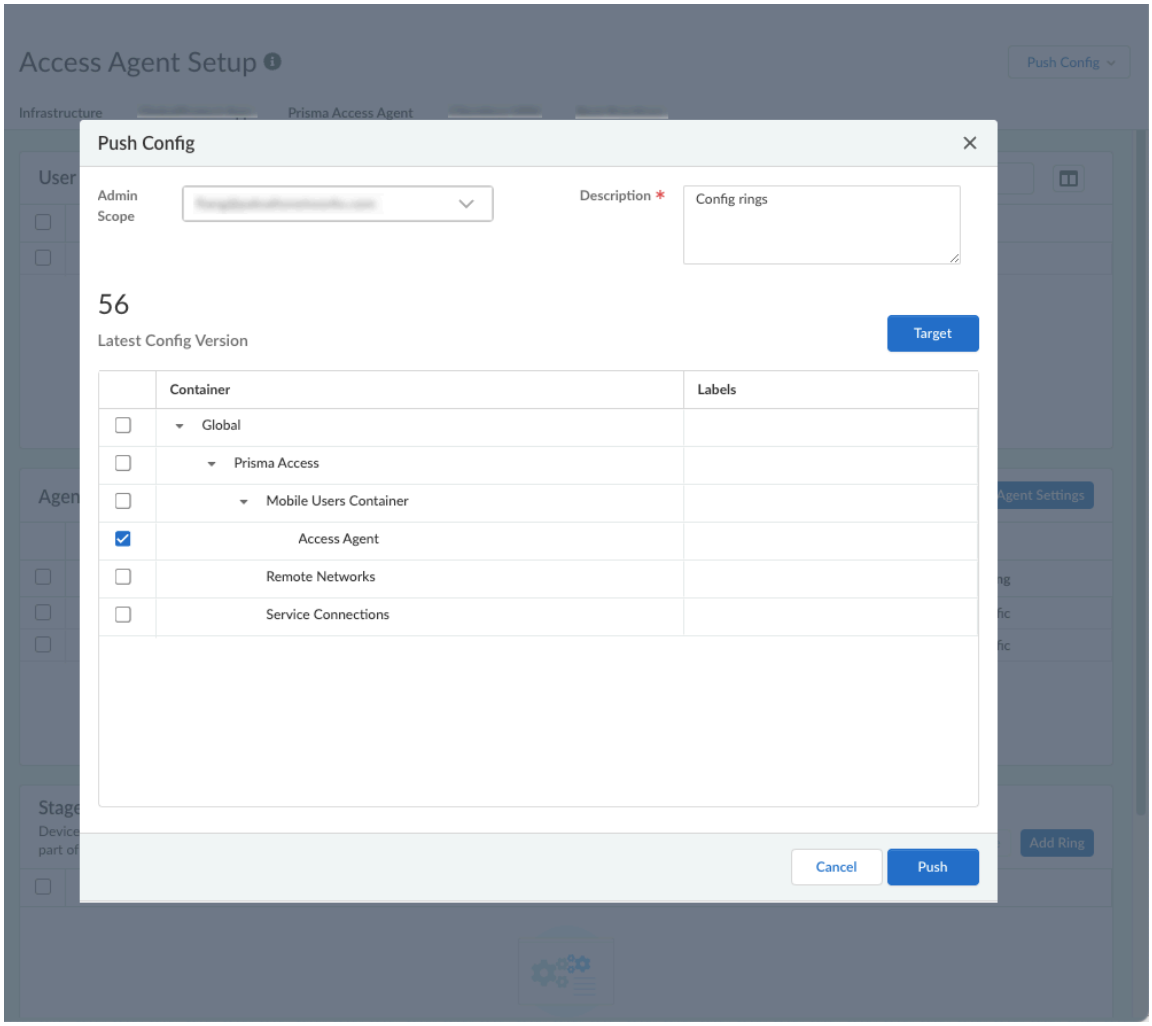
4. 选择 **Save**（保存）以保存环条件。

STEP 6 | 要创建更多环，请重复步骤 2 到 5。总共可以创建五个环（0 环到 4 环）。

 ©2025 Palo Alto Networks, Inc.

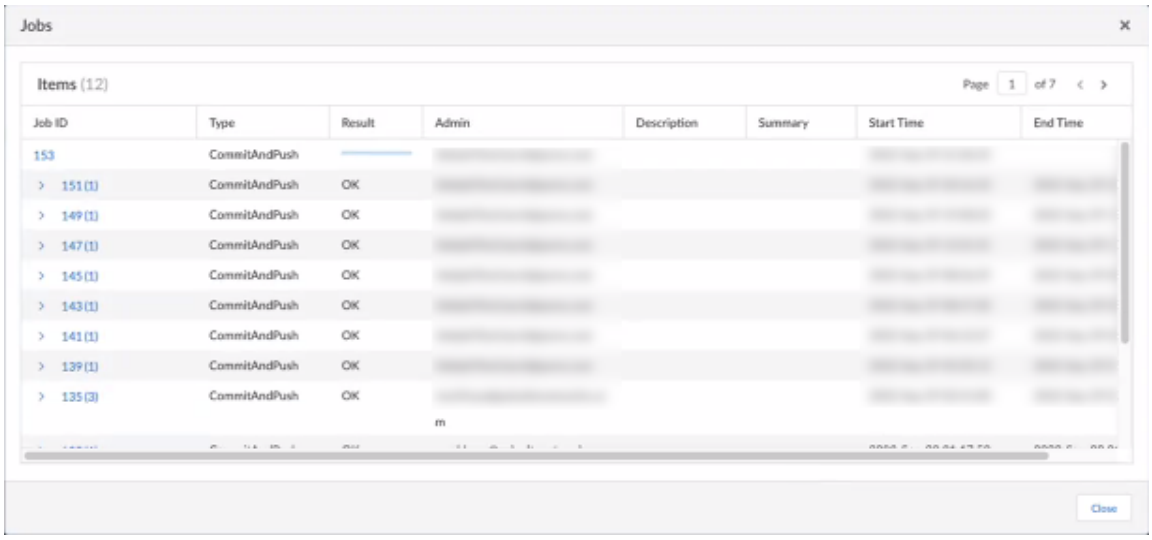
STEP 7 | 将配置推送到 Prisma Access。

1. 选择 **Push Config**（推送配置） > **Push**（推送）。
2. 在 **Description**（说明）中输入作业的说明。
3. 选择 **Global**（全局） > **Prisma Access** > **Mobile Users**（移动用户） > **Access Agent**（访问代理）容器，然后单击 **Push**（推送）。



4. 等待作业完成，然后选择 **Close**（关闭）以关闭“Jobs（作业）”对话框。

©2025 Palo Alto Networks, Inc.



STEP 8 | 可以在 Strata Cloud Manager 中的 **Manage**（管理） > **Prisma Access Agent** 中监视分阶段推出 。

配置 Prisma Access Agents 的常规全局设置

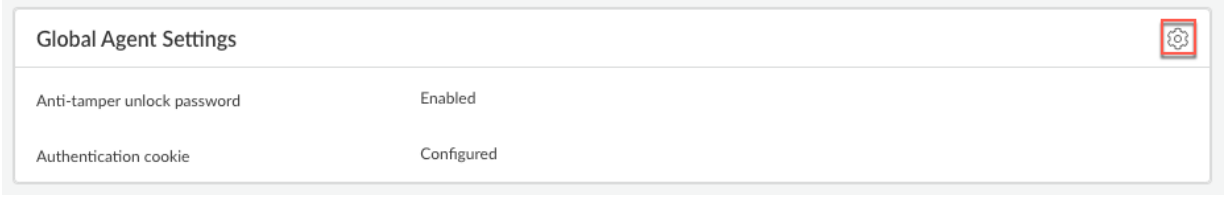
在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 创新 ❑ Prisma Access 许可证，且订阅了“移动用户” ❑ macOS 12 或更高版本的桌面设备，或 Windows 10 版本 2024 或更高版本或 Windows 11 桌面设备 ❑ 角色：超级用户

您可以自定义适用于所有端点上的 Prisma Access Agent 的全局代理设置。

常规全局代理设置包括设置防篡改功能，该功能可防止用户篡改 Prisma Access Agent，例如从最终用户的设备上将其卸载。此外，您还可以配置身份验证覆盖设置、非活动超时设置以及阻止被隔离设备的登录。

STEP 1 | 从 Strata Cloud Manager 中，选择 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Access Agent**（访问代理） > **Prisma Access Agent**。

STEP 2 | 编辑 **Global Agent Settings**（全局代理设置）。



 ©2025 Palo Alto Networks, Inc.

STEP 3 | 选择 **General**（常规）。

STEP 4 | 配置防篡改解锁密码。

可以通过启用防篡改功能来保护 Prisma Access Agent，该功能可防止任何未经授权的用户篡改 Prisma Access Agent。防篡改功能可以保护端点上的以下 Prisma Access Agent 资源：Prisma Access Agent 文件夹和文件 — 未经授权的用户无法删除或重命名任何与 Prisma Access Agent 相关的文件和文件夹。Prisma Access Agent 服务和主机信息配置文件 (HIP) 进程 — 未经授权的用户无法停止任何与 Prisma Access Agent 相关的服务和 HIP 进程。HIP 进程收集有关运行 Prisma Access Agent 的主机的信息，并将主机信息提交给 Prisma Access 进行检查。如果用户试图停止进程，则必须提供防篡改解锁密码。Prisma Access Agent 注册表项（在 Windows 上）或 .plist 文件（在 MacOS 上） — 未经授权的用户无法删除或更新 Windows 注册表项或 Prisma Access Agent 的 .plist 文件。PACli 命令行界面 — 未经授权的用户无法使用 PACli 命令行界面禁用 Prisma Access Agent 或防篡改功能。需要在命令行上执行某些操作以进行故障排除的管理员和授权用户必须在出现提示时提供防篡改解锁（主管）密码。

要解锁防篡改功能以排除 Prisma Access Agent 故障，您需要设置防篡改解锁密码（也称为主管密码）。

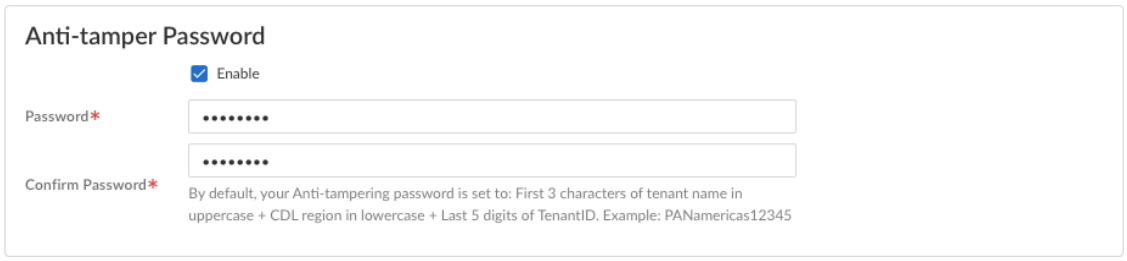
1. 防篡改解锁密码

   如果不启用防篡改密码，则不会分配密码，用户可以在 Prisma Access Agent 命令行提示时输入任何密码（包括空密码）。

   如果在启用防篡改密码后将其禁用，则用户可以在代理上运行某些 PACli 命令，如 **`pacli disable`**、**`pacli hip status`**、**`pacli protect disable`** 和 **`pacli switchto GlobalProtect`** 命令，而无需提供主管密码。在系统提示输入密码时，用户只需要按 **Enter** 键。

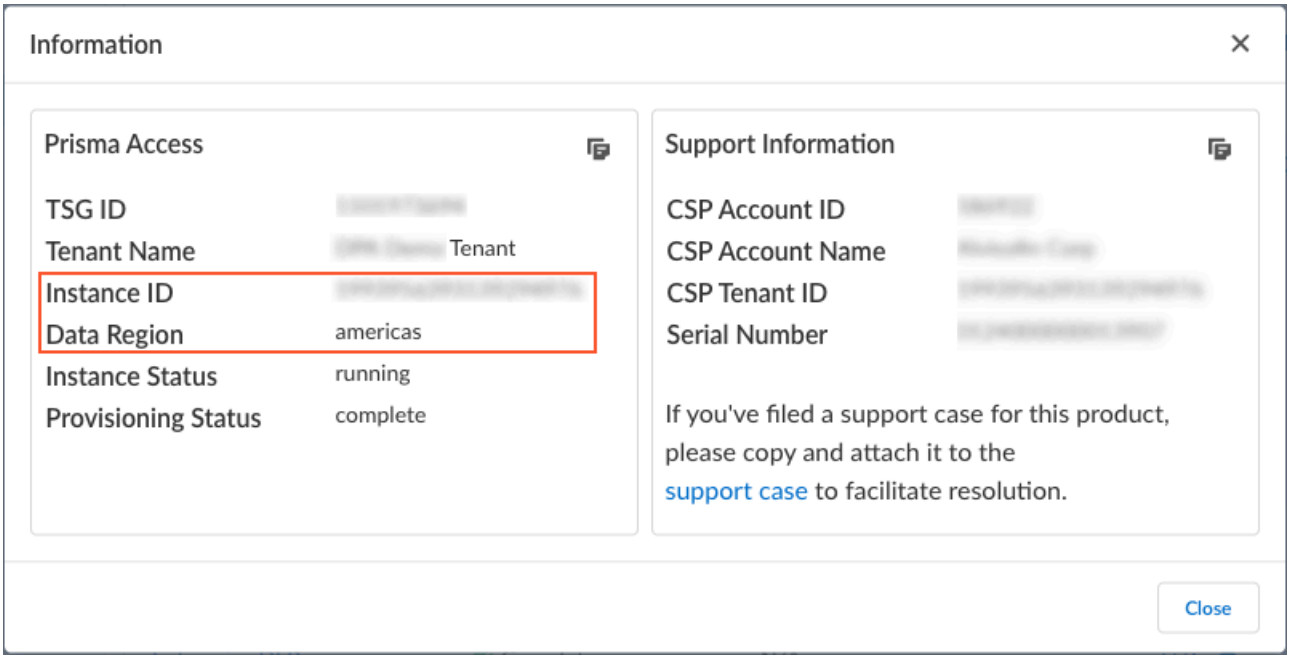
 ©2025 Palo Alto Networks, Inc.

2. 在 **Password**（密码）中输入密码，然后在 **Confirm Password**（确认密码）中重新输入密码以确认密码。密码必须至少包含八个字母数字字符。



如果您不提供密码，则将使用默认密码。默认情况下，防篡改密码设置为 Prisma Access 租户名称的前三个字符（大写）、Prisma Access 数据区域的前三个字符（小写）以及 Prisma Access 实例 **ID** 的后五位数字，例如：**PANamericas56789**。

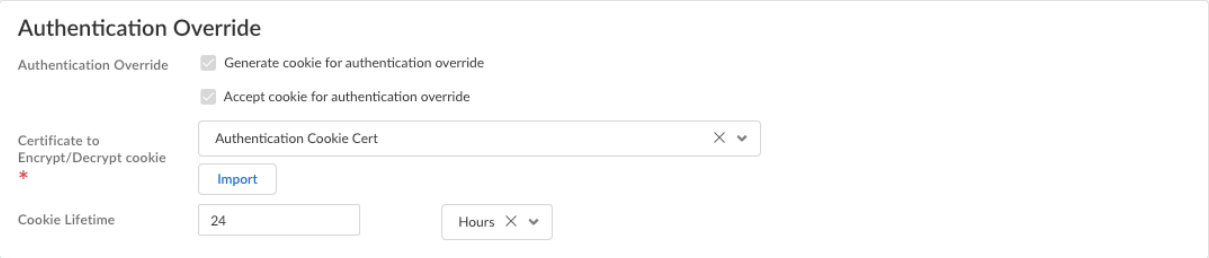
还可以通过以下方式来获取 Prisma Access 实例 **ID** 和数据区域：选择 **Settings**（设置）> **Tenants**（租户）> **<your_tenant>**，然后选择 Prisma Access 序列号旁边的 **View Support Info**（查看支持信息）工具提示。



要为代理提供更高级别的安全性，请设置新的防篡改解锁密码以覆盖默认密码，因为默认密码可能不是最安全的。

©2025 Palo Alto Networks, Inc.

STEP 5 | 配置 **Authentication Override**（身份验证覆盖）设置，以允许 Prisma Access 生成和接受安全加密的 Cookie 对用户进行身份验证。身份验证替代允许用户在指定的 **Cookie Lifetime**（**Cookie** 生存期）内仅提供一次登录凭据。



- **Generate cookie for authentication override**（生成用于身份验证覆盖的 **Cookie**） — 允许 Prisma Access 生成加密的特定端点 Cookie 并将身份验证 Cookie 颁发至端点。
- **Accept cookie for authentication override**（接受用于身份验证覆盖的 **Cookie**） — 允许 Prisma Access 使用有效的加密 Cookie 对用户进行身份验证。应用程序出示有效 Cookie 后，Prisma Access 将验证此 Cookie 是否最初已经过 Prisma Access 加密，再对其进行解密，然后对用户进行身份验证。
- **Certificate to Encrypt/Decrypt Cookie**（加密/解密 **Cookie** 的证书） — 选择对 Cookie 进行加密和解密时所使用的 RSA 证书。
- **Cookie Lifetime**（**Cookie** 生命周期）— 指定 Cookie 有效的小时数、天数或周数（默认为 24 小时）。小时的范围是 1 至 72；周的范围是 1 至 52；天数的范围是 1 至 365。Cookie 过期后，用户必须重新输入其登录凭据。然后，Prisma Access 加密新的 Cookie 以发送给代理。该值可与配置的 Cookie 生命周期相同或不同。

STEP 6 | 为 **Inactivity Logout**（非活动注销） 输入分钟数，以指定空闲用户在多长时间之后将从 Prisma Access Agent 注销。

您可以使用非活动注销周期来实施安全策略，以在连接到 Prisma Access 时监控来自端点的流量，并快速注销非活动的 Prisma Access Agent 会话。您可以实施更短的非活动注销期间。如果 Prisma Access Agent 未通过隧道路由流量，或者网关在配置的时间段内未收到来自端点的 HIP 检查，则用户将被注销。

STEP 7 | **Block Login for Quarantined Devices**（阻止隔离设备登录），可防止 Prisma Access Agent 用户从隔离的设备登录。

启用此设置后，如果用户尝试从隔离的设备登录，则 Prisma Access Agent 会通知用户该设备已被隔离，用户无法从该设备登录。如果未启用此设置，用户将收到通知，但是仍能从隔离设备登录。

STEP 8 | **Save**（保存）您的设置。

为动态特权访问 Prisma Access Agent 配置 HIP 通知

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 创新

 ©2025 Palo Alto Networks, Inc.

在何处可以使用？	需要提供什么？
	❑ Prisma Access 许可证，且订阅了“移动用户” ❑ macOS 12 或更高版本的桌面设备，或 Windows 10 版本 2024 或更高版本或 Windows 11 桌面设备 ❑ 角色：超级用户

在“Edit Global Agent Settings（编辑全局代理设置）”页面的 **HIP Notifications**（**HIP** 通知）选项卡中，您可以创建主机信息配置文件通知、创建和管理 HIP 对象以及创建和管理适用于所有端点中的 Prisma Access Agent 的 HIP 配置文件。

Prisma Access Agent 收集有关运行主机的信息，并在成功连接后将此主机信息提交给 Prisma Access 位置（网关）。网关将 Prisma Access Agent 提交的原始主机信息与您定义的任何 HIP 对象和 HIP 配置文件进行匹配。如果网关找到匹配，则将会在 HIP 匹配日志中生成一个条目。此外，如果网关在策略规则中找到 HIP 配置文件匹配，则将会实施相应的安全策略。

HIP 检查在应用程序连接到网关时执行，且在连接到 Prisma Access Agent 后，每小时执行一次后续检查。一旦之前的 HIP 检查发生变化，Prisma Access Agent 代理会请求获取更新后的 HIP 报告。网关上每个端点都只保留最新 HIP 报告。

使用策略实施的主机信息配置文件可启用粒度安全功能，确保远程主机能够访问得到充分维护的关键资源，并且保证遵循安全标准之后才允许访问网络资源。例如，在允许访问最敏感的数据系统前，您可能要确保主机访问在其硬盘驱动器上已启用加密功能的数据。如果端点系统已启用加密功能，则您可以通过创建安全规则实施此策略只允许访问应用程序。

此外，对于不符合此规则的端点，您可以创建通知消息，提醒用户他们被拒绝访问的原因。您还可以提供一个指向特定位置的链接，用户可以从该位置访问缺失加密软件的安装程序。为了允许用户访问该文件共享，您必须创建相应的安全规则，允许访问与特定 HIP 配置文件匹配的主机的特定共享。

可以完成以下任务：

- 为动态特权访问 Prisma Access Agent 创建 HIP 通知
- 为动态特权访问 Prisma Access Agent 创建和管理 HIP 对象
- 为动态特权访问 Prisma Access Agent 创建和管理 HIP 配置文件

为动态特权访问 **Prisma Access Agent** 创建 **HIP** 通知

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 创新 ❑ Prisma Access 许可证，且订阅了“移动用户” ❑ macOS 12 或更高版本的桌面设备，或 Windows 10 版本 2024 或更高版本或 Windows 11 桌面设备

 ©2025 Palo Alto Networks, Inc.

在何处可以使用？	需要提供什么？
	❑ 角色：超级用户

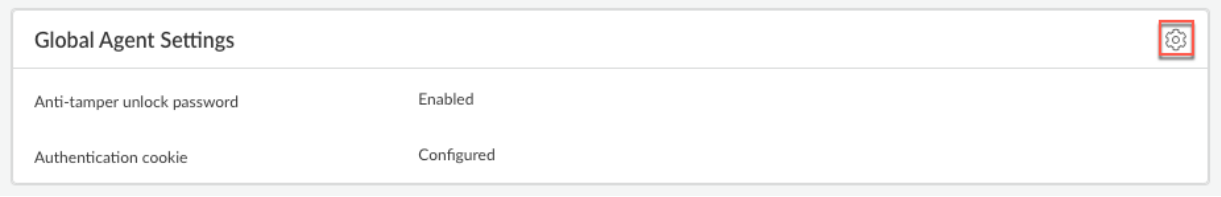
您可以定义在实施含有 HIP 配置文件的安全规则时最终用户可以看到的通知消息。

在用户的配置与策略中的 HIP 配置文件匹配或不匹配的情况下，决定是否显示通知消息很大程度上取决于您的策略以及 HIP 匹配（或不匹配）对用户的意义。也就是说，匹配是否意味着他们被授予对您的网络资源的完全访问权限，或者是否意味着他们由于不合规问题而具有受限的访问权限？

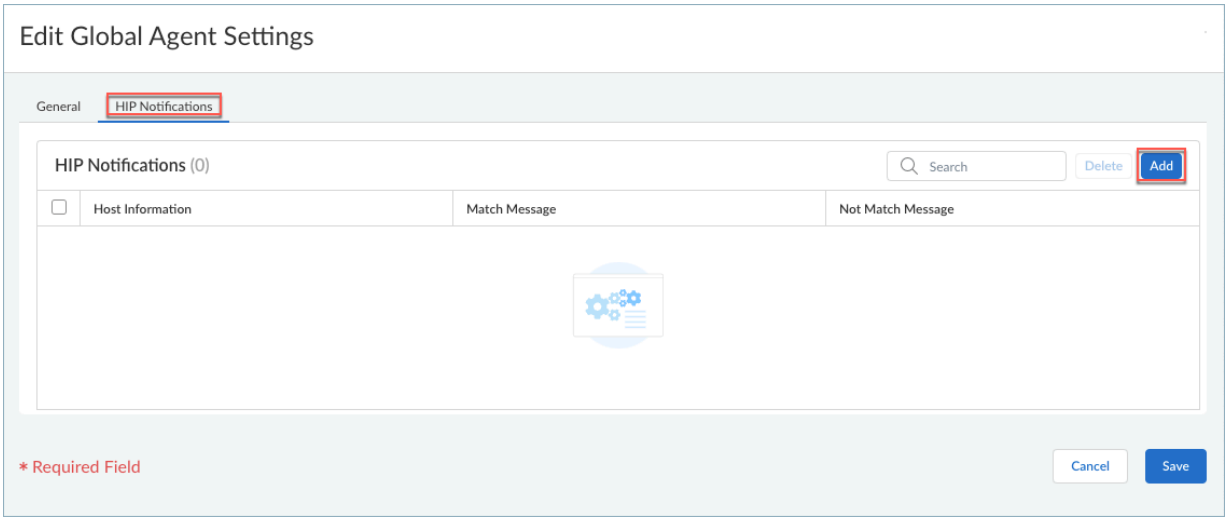
例如，如果尚未安装所需的企业防病毒和反间谍软件包，则假设您可以创建 HIP 配置文件进行匹配。您可能要为匹配 HIP 配置文件的用户创建 HIP 通知消息告知他们需要安装软件。或者，如果您的 HIP 配置文件已匹配（如果已安装相同的应用程序），则您可能要为不匹配配置文件的用户创建消息。

STEP 1 | 从 Strata Cloud Manager 中，选择 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Access Agent**（访问代理） > **Prisma Access Agent**。

STEP 2 | 依次点击 **Edit**（编辑）、**Global Agent Settings**（全局代理设置）以编辑全局代理设置。

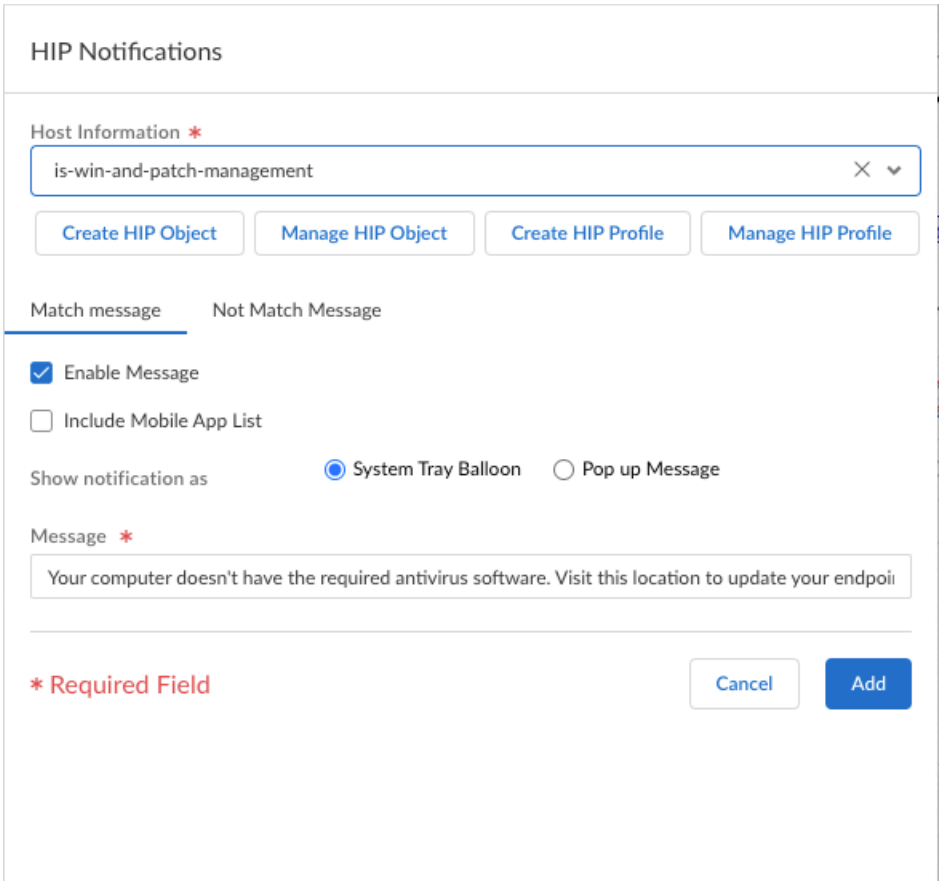


STEP 3 | 选择 **HIP Notifications**（**HIP** 通知），然后单击 **Add**（添加）。



 ©2025 Palo Alto Networks, Inc.

STEP 4 | 从 **Host Information**（主机信息）下拉列表中选择此消息应用到的 HIP 配置文件。



如果没有 HIP 配置文件，则需要创建 HIP 配置文件。

STEP 5 | 根据您是否希望匹配相应的 HIP 配置文件时，或是在不匹配时显示消息，选择 **Match Message**（匹配消息）或 **Not Match Message**（不匹配消息）。在某些情况下，您可能要为匹配和不匹配创建消息，取决于匹配的对象和策略的目标。

STEP 6 | 选择 **Enable Message**（启用消息），然后选择是否要将消息显示为 **System Tray Balloon**（系统托盘气球）或 **Pop Up Message**（弹出消息）。

STEP 7 | 在 **Message**（消息）中输入您的消息文本，然后单击 **Add**（添加）。

STEP 8 | 为您要定义的每个消息重复执行此程序。

为动态特权访问 Prisma Access Agent 创建和管理 HIP 对象

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	☐ Prisma Access 5.1 创新 ☐ Prisma Access 许可证，且订阅了“移动用户”

 ©2025 Palo Alto Networks, Inc.

在何处可以使用？	需要提供什么？
	❑ macOS 12 或更高版本的桌面设备，或 Windows 10 版本 2024 或更高版本或 Windows 11 桌面设备 ❑ 角色：超级用户

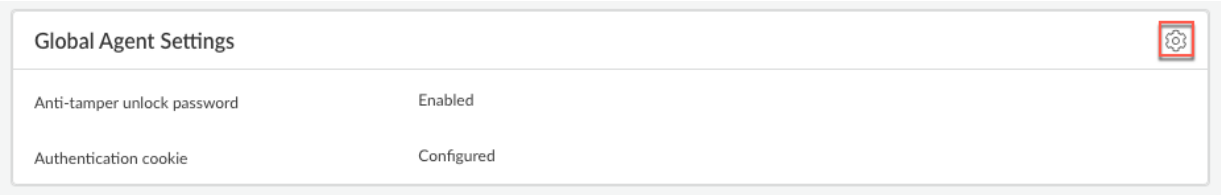
通过在 Prisma Access 网关上创建 HIP 对象和 HIP 配置文件，可以定义要监视或用于策略实施的主机属性。

HIP 对象由匹配条件组成，这些匹配条件用于筛选出您需要使用的主机信息，从而通过 Prisma Access Agent 报告的原始数据实施策略。例如，尽管原始主机数据可能包括有关端点上安装的若干防病毒软件包的信息，但是您可能仅某个特定应用程序感兴趣。在这种情况下，您将创建 HIP 对象以匹配您有兴趣实施的特定应用程序。

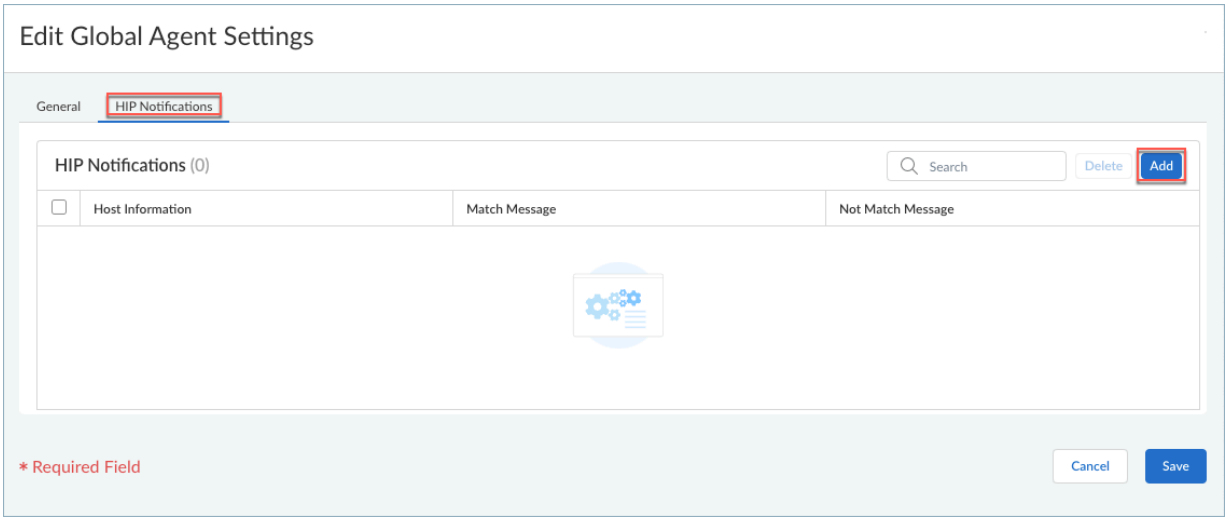
确定您需要的 HIP 对象的最佳方式是确定您将如何使用所收集的主机信息来实施策略。请记住，HIP 对象自身仅仅是构建块，使您可以创建在安全策略中使用的 HIP 配置文件。因此，请尽量保持对象简化，方法是与一个项目匹配，例如，是否存在特定类型的必需软件、特定域中的成员身份或者特定操作系统。如此，您将能够灵活创建非常精细的 HIP 扩充策略。

STEP 1 | 从 Strata Cloud Manager 中，选择 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Access Agent**（访问代理） > **Prisma Access Agent**。

STEP 2 | 依次点击 **Edit**（编辑）、**Global Agent Settings**（全局代理设置）以编辑全局代理设置。

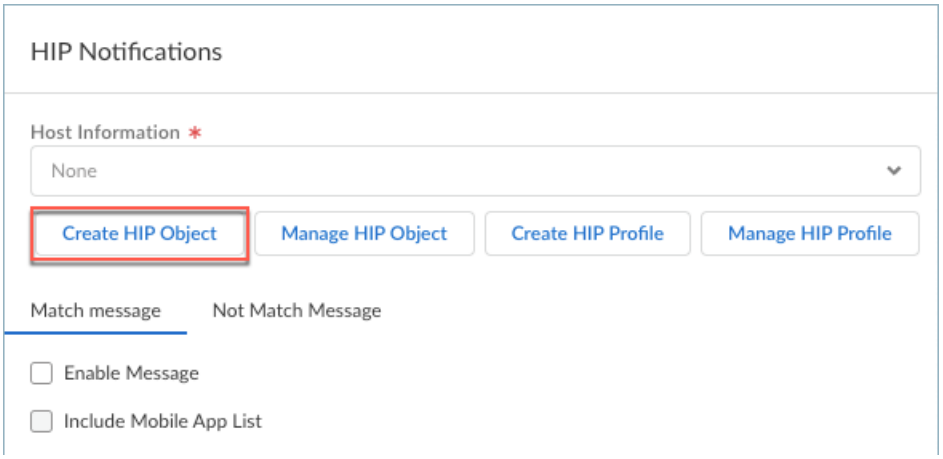


STEP 3 | 选择 **HIP Notifications**（**HIP** 通知），然后单击 **Add**（添加）。



 ©2025 Palo Alto Networks, Inc.

STEP 4 | 单击 **Create HIP Object**（创建 **HIP** 对象）。



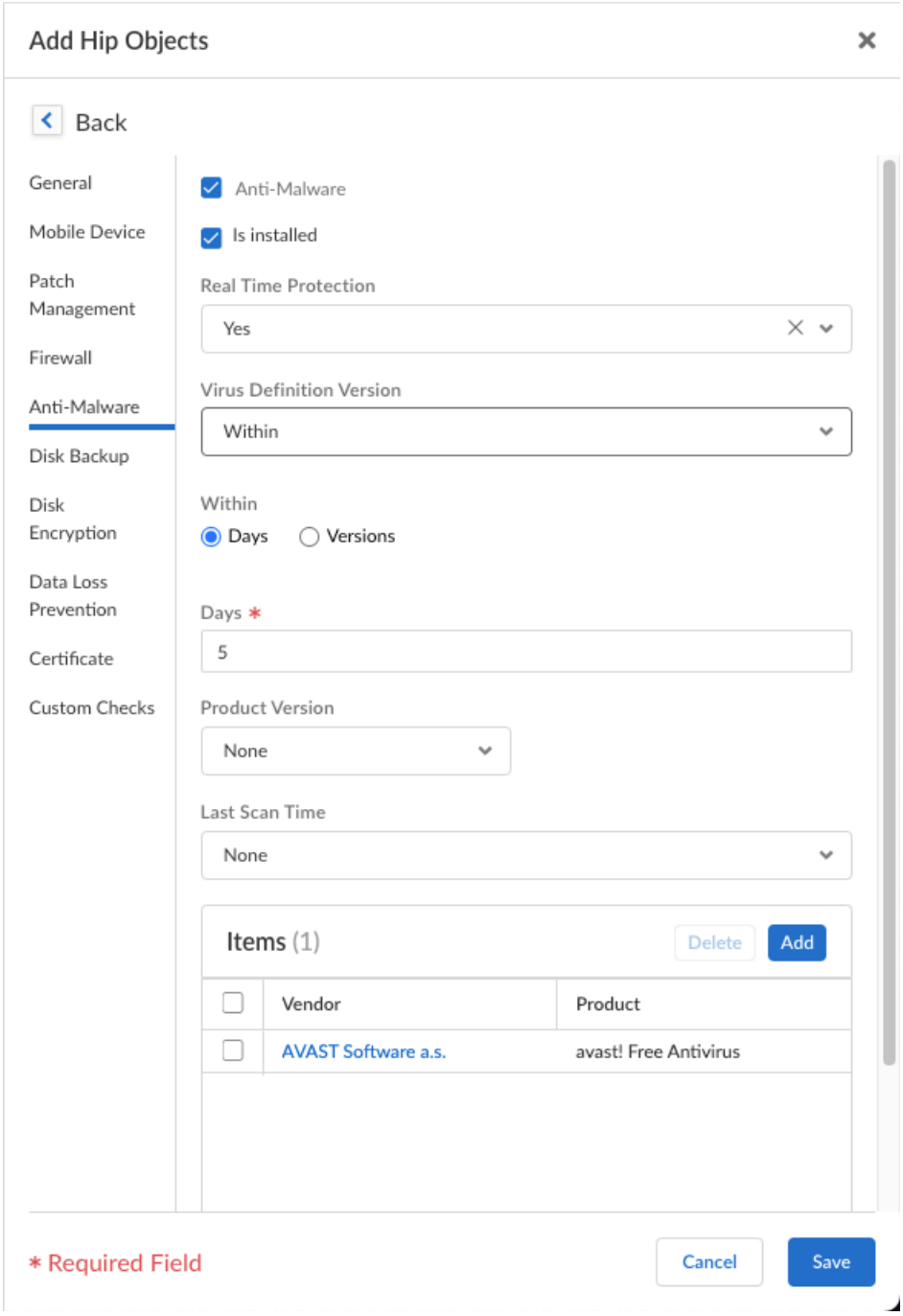
STEP 5 | 输入对象的 **Name**（名称）和 **Description**（说明）。

©2025 Palo Alto Networks, Inc.

STEP 6 | 选择与您感兴趣匹配的主机信息类别相对应的选项卡，然后选中该复选框启用根据类别匹配的对象。

例如，要创建对象查找有关防病毒软件或防间谍软件的信息，可以选择 **Antivirus**（防病毒）选项卡，然后选中 **Antivirus**（防病毒）复选框以启用相应的字段。填写完成下列字段以定义所需的匹配条件。

例如，下面的图像显示了如何创建是否与所安装的 AVAST 免费防病毒软件应用程序匹配、已经启用 **Real Time Protection**（实时保护）和拥有在最近 5 天内更新的恶意软件定义的 HIP 对象。



 ©2025 Palo Alto Networks, Inc.

对于您要根据该对象匹配的每个类别，请重复此步骤。有关详细信息，请参阅表：数据收集类别。

STEP 7 | 依次选择 **Save**（保存）和 **Add**（添加）以保存并添加 HIP 对象。

STEP 8 | 要管理您的 HIP 对象，您可以从 HIP 通知表中选择一个现有对象，或者单击“Edit Global Agent Settings（编辑全局代理设置）”页面中的 **Add**（添加）以打开 HIP 通知窗口。

从该窗口中，单击 **Manage HIP Object**（管理 **HIP** 对象）以查看您配置的 HIP 对象列表。您可以选择一个 HIP 对象，然后选择 **Delete**（删除）、**Clone**（克隆）或 **Move**（移动）以执行对应操作。

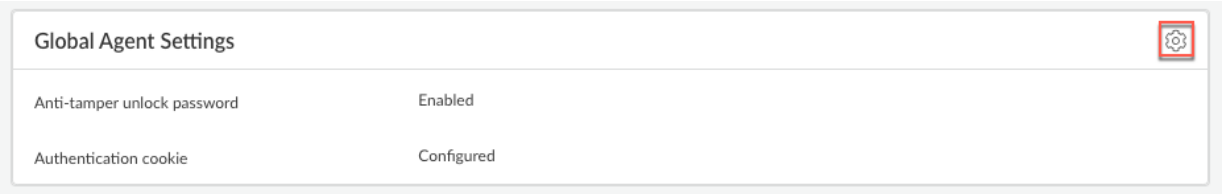
为动态特权访问 Prisma Access Agent 创建和管理 HIP 配置文件

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 创新 ❑ Prisma Access 许可证，且订阅了“移动用户” ❑ macOS 12 或更高版本的桌面设备，或 Windows 10 版本 2024 或更高版本或 Windows 11 桌面设备 ❑ 角色：超级用户

HIP 配置文件是主机信息配置文件对象的集合，将同时评估这些对象，以用于监控或安全策略实施。创建 HIP 配置文件时，可以使用布尔逻辑来合并现在的 HIP 对象和先前创建的 HIP 对象，例如，当按照生成的 HIP 配置文件对通信流进行评估时，可能匹配，也可能不匹配。如果存在匹配项，那么将执行对应的策略规则。如果没有匹配项，将按照下一个规则来对通信流进行评估（与任何其他策略匹配条件一样）。

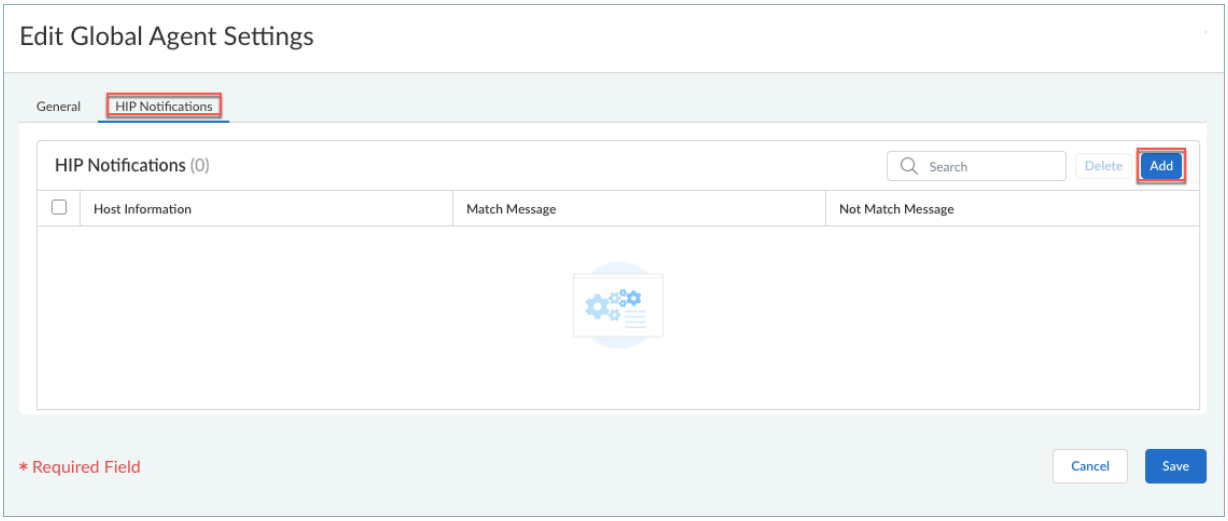
STEP 1 | 从 Strata Cloud Manager 中，选择 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Access Agent**（访问代理） > **Prisma Access Agent**。

STEP 2 | 依次点击 **Edit**（编辑）、**Global Agent Settings**（全局代理设置）以编辑全局代理设置。

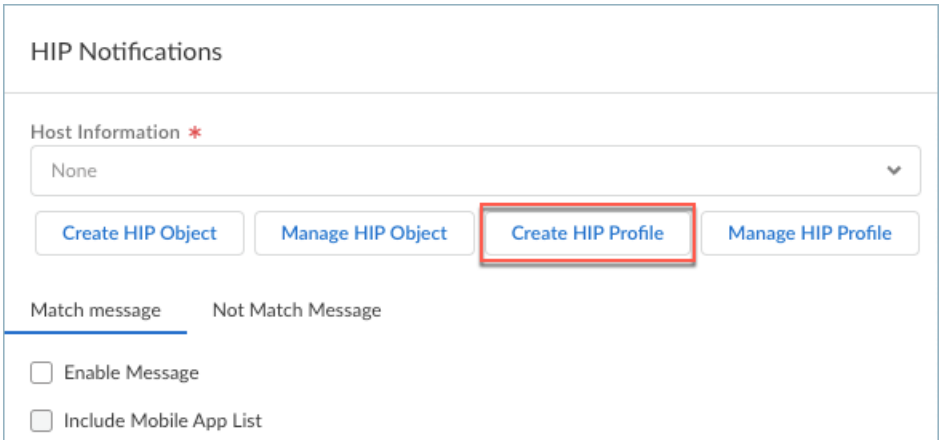


 ©2025 Palo Alto Networks, Inc.

STEP 3 | 选择 **HIP Notifications**（**HIP** 通知），然后单击 **Add**（添加）。



STEP 4 | 单击 **Create HIP Profile**（创建 **HIP** 配置文件）。



STEP 5 | 输入 **Name**（名称）和 **Description**（说明）以标识配置文件。

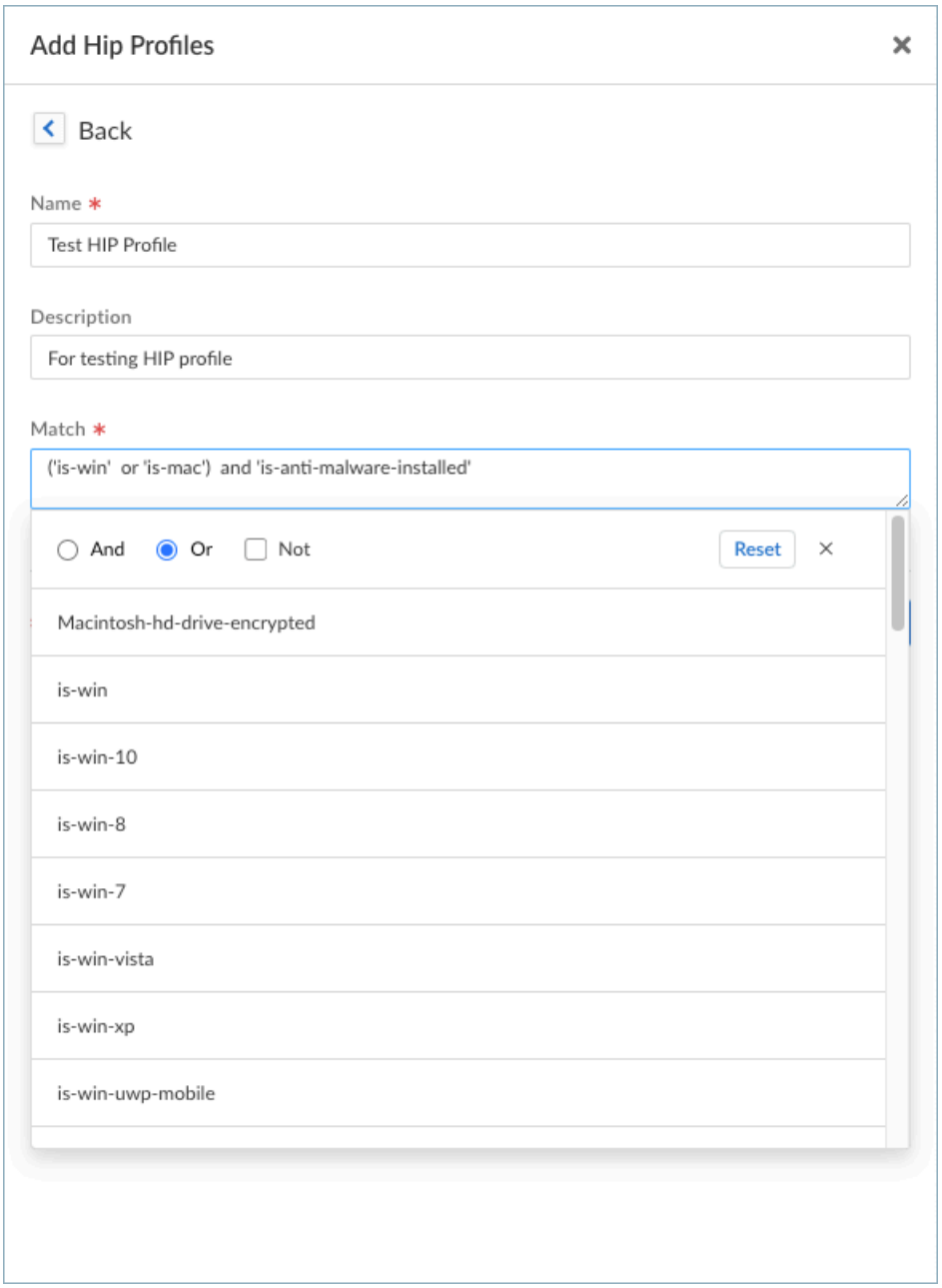
STEP 6 | 单击 **Match**（匹配）字段即可打开 HIP 配置文件生成器。

1. 从列表中选择要用作匹配条件的 HIP 对象或配置文件。
2. 选择一个布尔运算符 **(And, And)**。如果您希望仅当对象中的条件对于流不成立时，HIP 配置文件才作为匹配项评估对象，请在添加对象之前选中 **Not**（非）复选框。
3. 选择另一个 HIP 对象或配置文件以作为第一个对象的评估依据。

STEP 7 | 继续为您在生成的配置文件添加匹配条件，确保在每个加法之间选中相应的布尔运算符单选按钮（**And**（与）或 **And**（与））（如果适用，请使用 **NOT**（非）复选框）。HIP 配置文件最多可包含 2048 个字符。

©2025 Palo Alto Networks, Inc.

STEP 8 | 在创建复杂的布尔表达式时，必须手动在匹配文本框中的适当位置中添加圆括号，以确保使用需要的逻辑来对 HIP 配置文件进行求值。



STEP 9 | 依次选择 **Save**（保存）和 **Add**（添加）以保存并添加 HIP 配置文件。

STEP 10 | 要管理您的 HIP 配置文件，您可以从 HIP 通知表中选择一个现有配置文件，或者单击“Edit Global Agent Settings（编辑全局代理设置）”页面中的 **Add**（添加）以打开 HIP 通知窗口。

从该窗口中，单击 **Manage HIP Profile**（管理 **HIP** 配置文件）以查看您配置的 HIP 配置文件列表。您可以选择一个 HIP 配置，然后选择 **Delete**（删除）、**Clone**（克隆）或 **Move**（移动）以执行对应操作。您还可以从选择 **Add**（添加）以添加 HIP 配置文件。

©2025 Palo Alto Networks, Inc.

推送 Prisma Access Agent 配置

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 创新 ❑ Prisma Access 许可证，且订阅了“移动用户” ❑ macOS 12 或更高版本的桌面设备，或 Windows 10 版本 2024 或更高版本或 Windows 11 桌面设备 ❑ 角色：超级用户

完成 Prisma Access Agent 配置或更新配置后，必须将配置推送到 Prisma Access。

请至少创建一个项目，然后才能推送提交，否则提交将失败。

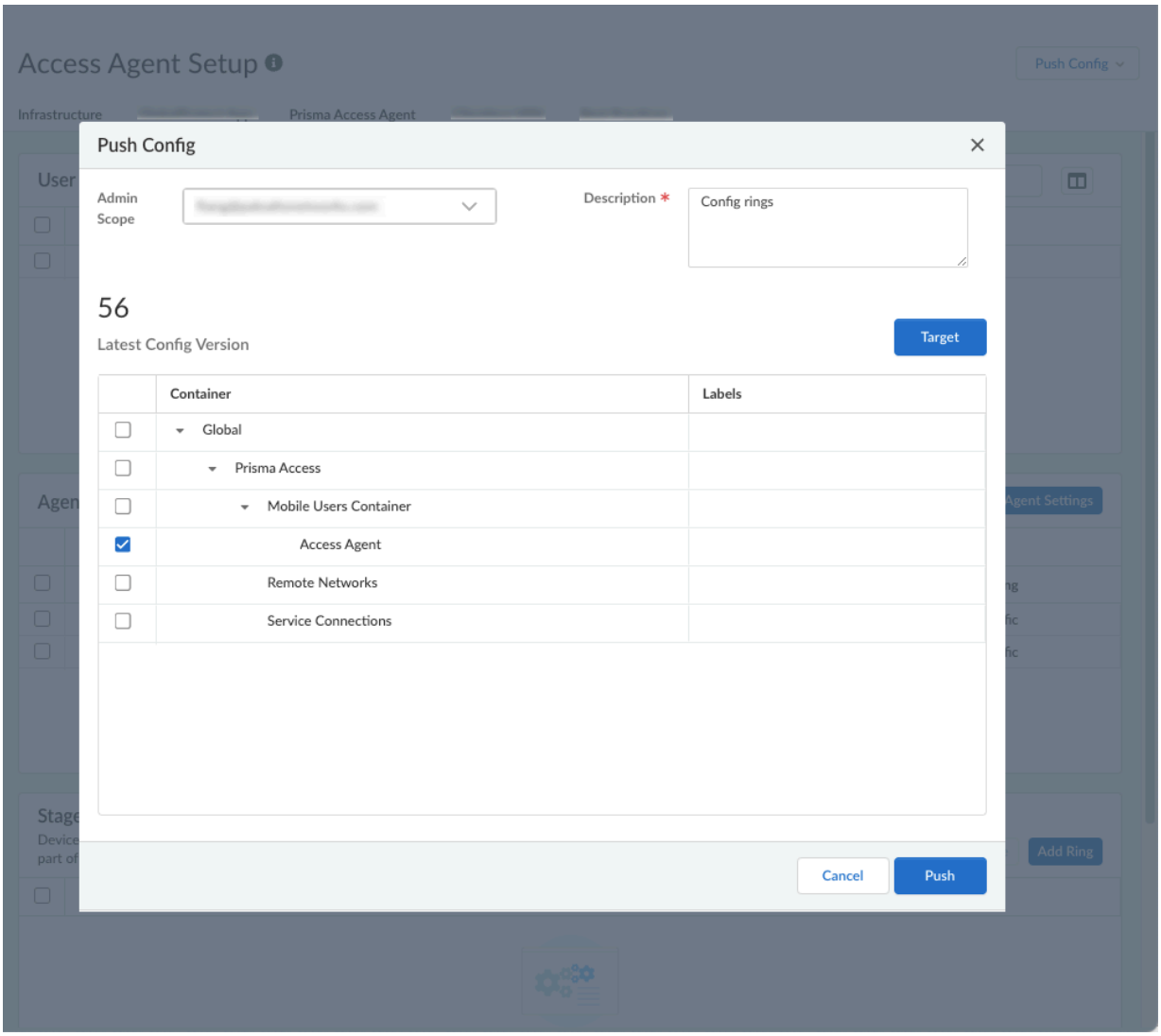
STEP 1 | 选择 **Workflows**（工作流） > **Prisma Access** 设置 > **Access Agent**（访问代理）。

STEP 2 | 选择 **Push Config**（推送配置） > **Push**（推送）。

STEP 3 | 在 **Description**（说明）中输入作业的说明。

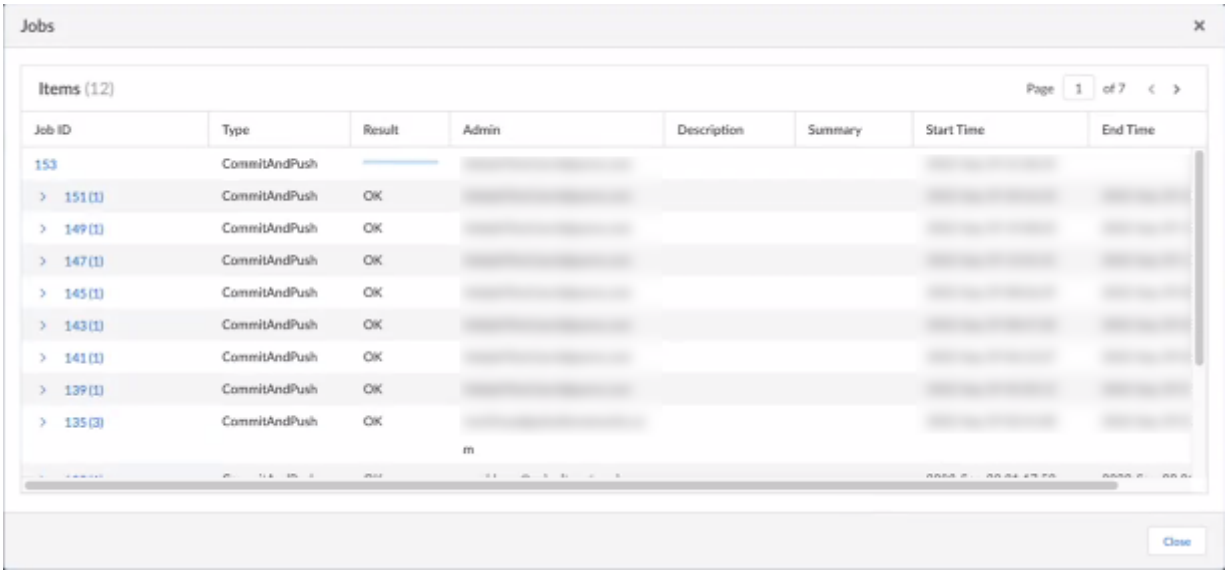
©2025 Palo Alto Networks, Inc.

STEP 4 | 选择 **Global**（全局） > **Prisma Access** > **Mobile Users**（移动用户） > **Access Agent**（访问代理）容器，然后单击 **Push**（推送）。



 ©2025 Palo Alto Networks, Inc.

STEP 5 | 等待作业完成，然后选择 **Close**（关闭）以关闭“Jobs（作业）”对话框。



 ©2025 Palo Alto Networks, Inc.

下载启用动态权限访问的 Prisma Access Agent 软件包

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.1 创新 ❑ Prisma Access 许可证，且订阅了“移动用户” ❑ 角色：超级用户

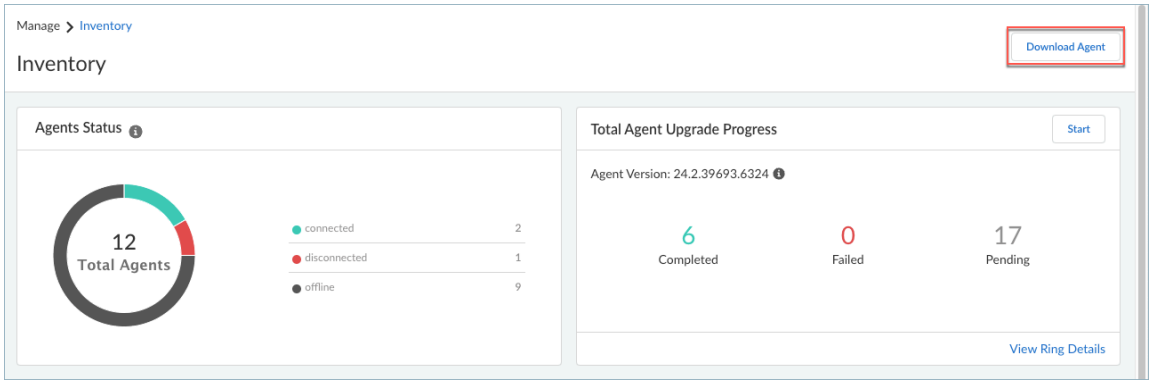
在配置了 Prisma Access Agent 和特定于项目的 Prisma Access Agent 设置之后，可以下载 Prisma Access Agent 软件包，以便最终用户可以下载和安装该软件包。

此外，请确保您下载了配置文件。您的客户端和特定于项目的客户端配置以及 Prisma Access 问租户 ID 和服务器域将保存到 Prisma Access Agent 配置文件中。将在安装和注册 Prisma Access Agent 的过程中使用该配置文件。

©2025 Palo Alto Networks, Inc.

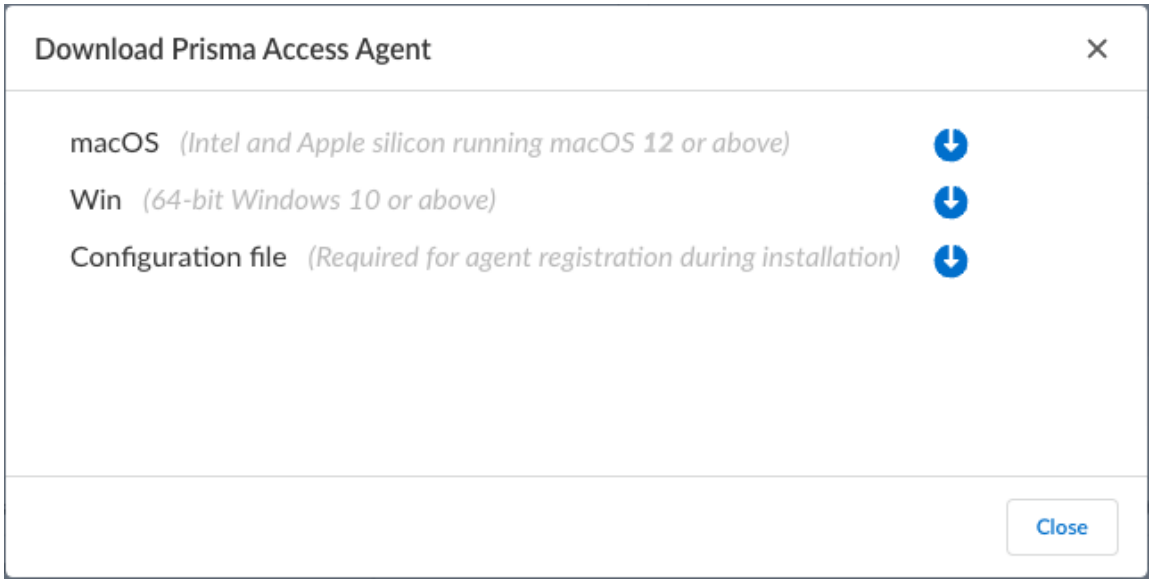
STEP 1 | 下载 Prisma Access Agent 软件包和配置文件。

1. 选择 **Manage**（管理） > **Prisma Access Agent** > **Inventory**（清单）。
2. 单击 **Download Agent**（下载客户端）。



3. 单击与要下载的项目对应的向下箭头。

   请务必下载配置文件，因为在安装和注册 Prisma Access Agent 的过程中将使用该文件。



4. 将软件包保存到系统上的某个位置，然后单击 **Close**（关闭）以关闭“Download Agent（下载客户端）”对话框。

STEP 2 | 将软件包上载到组织网络中的中心位置或分发软件包，以便最终用户可以下载并安装 Prisma Access Agent。

©2025 Palo Alto Networks, Inc.

使用 Prisma Access Agent 访问您的项目

在何处可以使用？	需要提供什么？
• Prisma Access Agent	❑ macOS 12 或更高版本的桌面设备，或 Windows 10 版本 2024 或更高版本或 Windows 11 桌面设备 ❑ 允许访问 Internet

如果您的组织是一家 IT 或 IT 支持服务 (ITES) 公司，需要控制哪些用户有权访问其客户项目，则动态特权访问可为您提供一种无缝、安全且分隔的方式，让您仅访问分配给您的项目。

如果您的管理员已设置 Prisma Access 和 Prisma Access Agent 对于动态特权访问，您可以使用 Prisma Access Agent 访问并处理您被分配到的项目。

登录项目后，您可以访问组织的网络、网络中的资源或特定于项目的软件即服务应用程序。了解如何：

- 登录到启用了动态特权访问的 Prisma Access Agent
- 查看连接状态
- 更改启用了动态特权访问的 Prisma Access Agent 的首选项
- 连接到其他 Prisma Access 位置
- 查看应用程序通知

此外，如果您被分配到不同的项目工作，您可以 切换到不同的项目 或 将 Prisma Access Agent 连接到不同的服务器。

安装 Prisma Access Agent

在何处可以使用？	需要提供什么？
• Prisma Access Agent	❑ macOS 12 或更高版本的桌面设备，或 Windows 10 版本 2024 或更高版本或 Windows 11 桌面设备（具有管理员特权） ❑ 允许访问 Internet

如果管理员未将 Prisma Access Agent 推送到您的设备，您可以在 MacOS 或 Windows 设备上手动安装 Prisma Access Agent。

Prisma Access Agent 和 *GlobalProtect* 应用程序在同一设备上共存，但只有其中一个应用程序可以连接到 *Prisma Access*。如果您的设备上还安装并启用了 *GlobalProtect* 应用程序，则 *Prisma Access Agent* 安装将自动禁用 *GlobalProtect* 应用程序。要在安装 *Prisma Access Agent* 后使用 *GlobalProtect* 应用程序，您需要切换到 GlobalProtect 应用程序。

©2025 Palo Alto Networks, Inc.

- macOS
- Windows

安装 Prisma Access Agent (macOS)

要在 macOS 设备上手动安装 Prisma Access Agent，请执行以下操作：

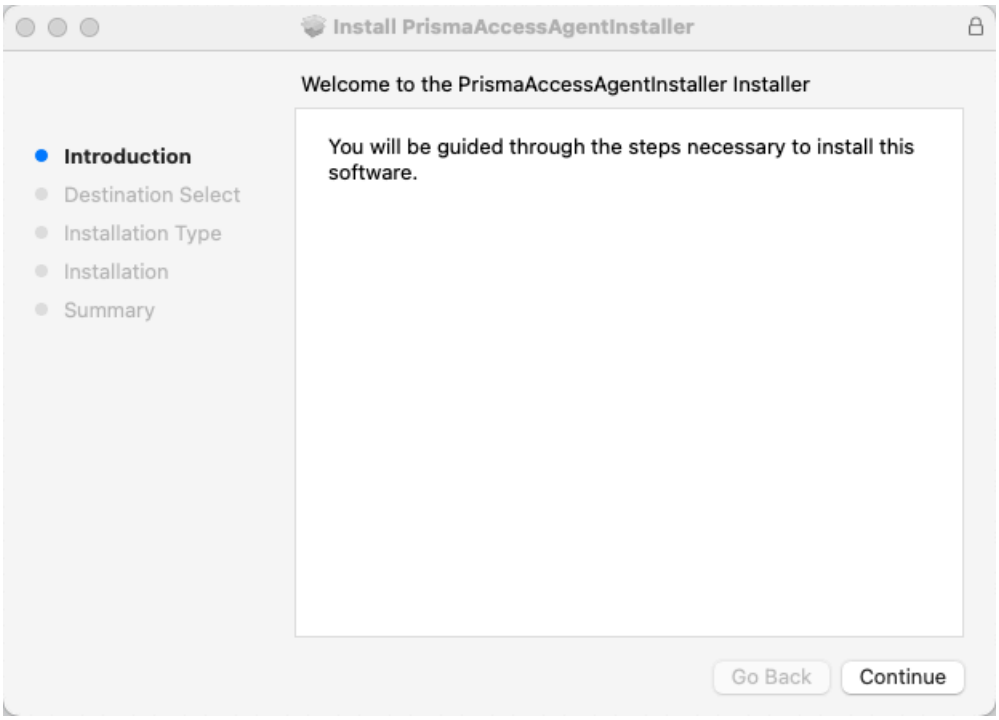
STEP 1 | 获取管理员提供给您的 Prisma Access Agent 软件包。软件包名称的格式如下：

`PrismaAccessAgentInstaller_<version>.pkg`

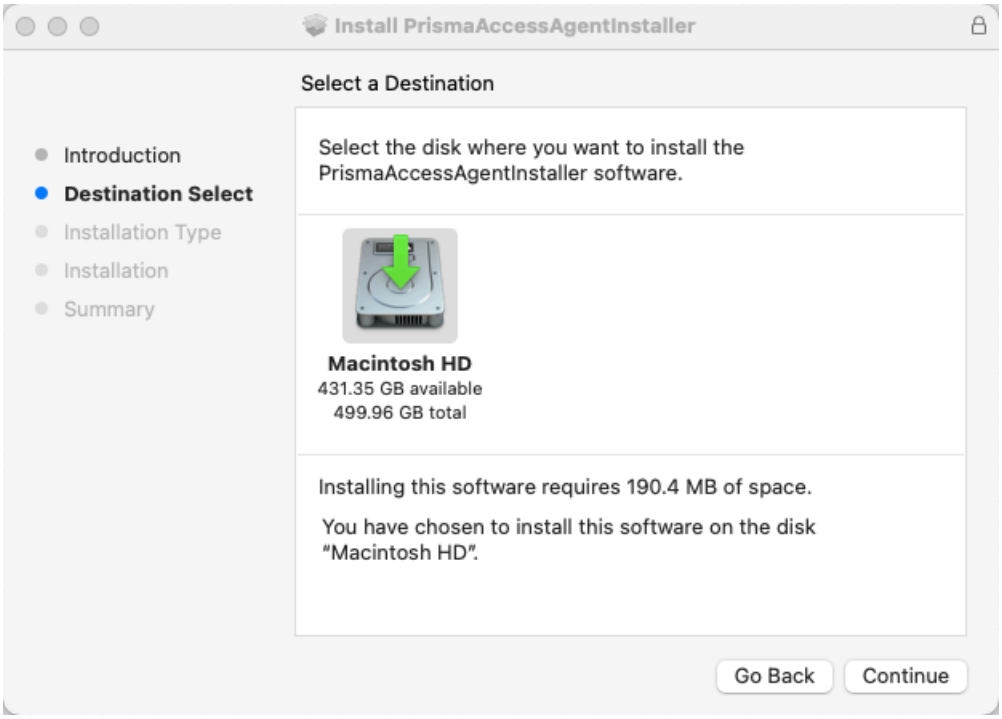
©2025 Palo Alto Networks, Inc.

STEP 2 | 在您的 Downloads（下载）文件夹中（或您放置安装包的位置），打开安装包并按照提示安装 Prisma Access Agent。

1. 在安装程序中，单击 **Continue**（继续）。

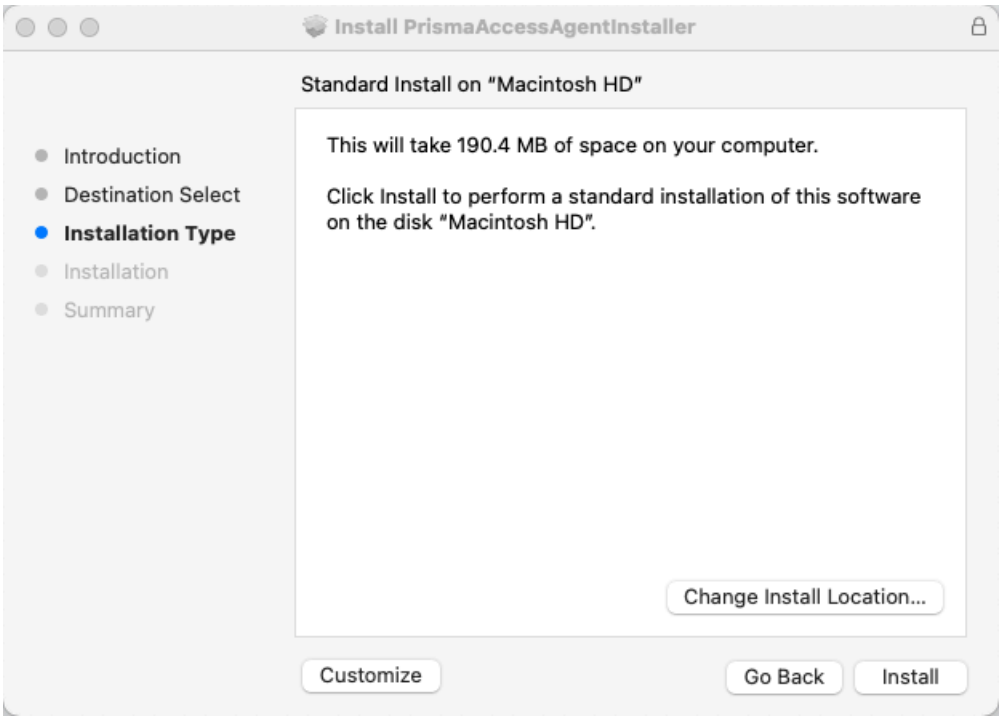


2. 选择用于安装 Prisma Access Agent 的文件夹，然后单击 **Continue**（继续）。



3. 查看“Installation Type（安装类型）”页面中的信息，然后单击 **Install**（安装）。

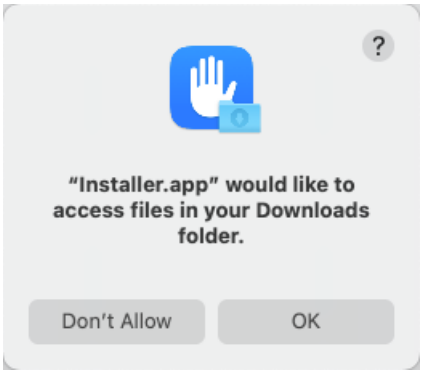
©2025 Palo Alto Networks, Inc.



4. 出现提示时，在 **User Name**（用户名）和 **Password**（密码）中输入用户名和密码，然后单击 **Install Software**（安装软件）以开始安装。

   也可以使用 Touch ID（如果已启用）来完成此步骤。

5. 当系统提示是否允许安装程序访问您下载安装程序包的文件夹中的文件时，单击 **OK**（确定）。



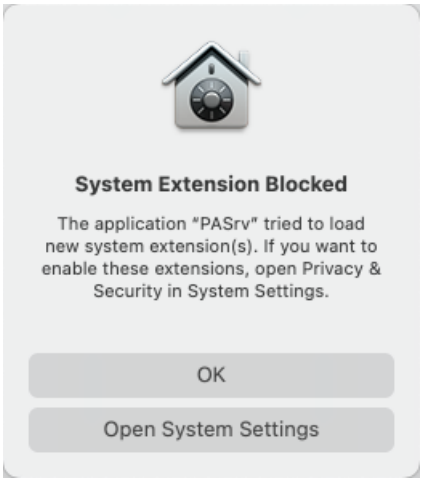
6. 默认情况下，macOS 会阻止 Prisma Access Agent 系统扩展。如果管理员为 Prisma Access Agent 配置了以下流量转发规则，则会显示系统或网络扩展：

   - 分割隧道 — 通过 Prisma Access 连接或在 Prisma Access 连接之外引导网络流量。
   - 分割 DNS — 除了网络流量之外，还通过 Prisma Access 或在 Prisma Access 之外引导对应用程序和资源的 DNS 查询。

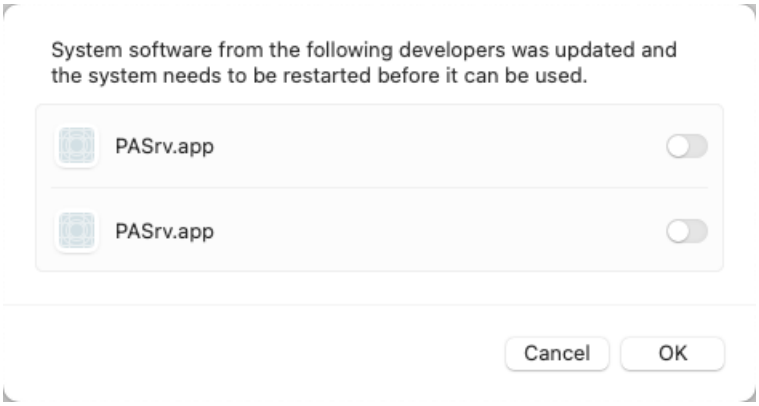
   要使 Prisma Access Agent 工作，您需要启用系统扩展：

   1. 单击 **Open System Settings**（打开系统设置）。

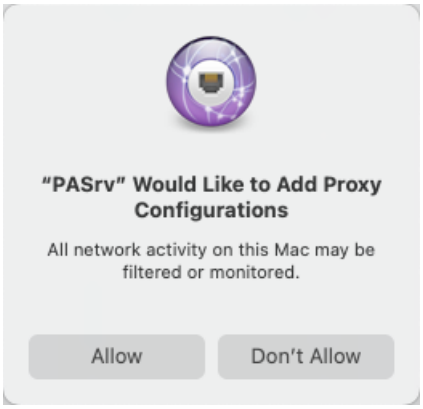
 ©2025 Palo Alto Networks, Inc.



2. 在“Privacy & Security（隐私和安全）”窗口中，在 **Some system software requires your attention before it can be used**（某些系统软件需要您的注意才能使用）中单击 **Details**（详细信息）。
3. 启用两个 **PASrv.app** 应用，然后单击 **OK**（确定）。



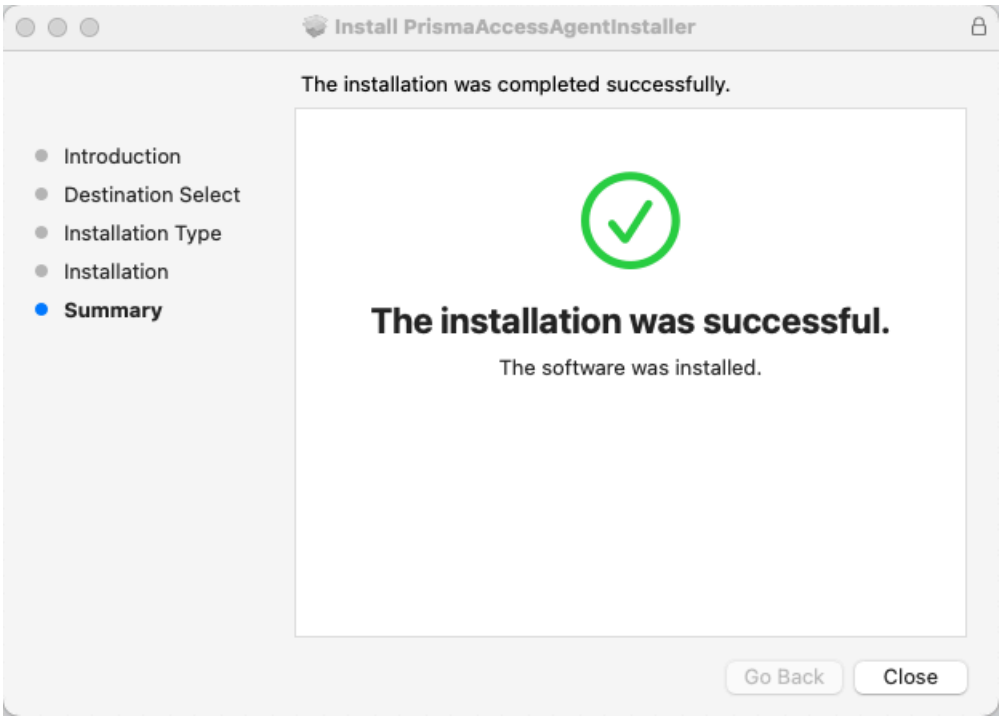
7. 如果您的管理员启用了该功能以强制使用 Prisma Access 连接进行网络访问，则系统将提示您添加配置以过滤网络内容。要继续，请单击 **Allow**（允许）。



允许此操作后，Prisma Access Agent将出于安全目的过滤和监视您的网络连接。

8. 安装完成后，选择 **Close**（关闭）以关闭安装程序。

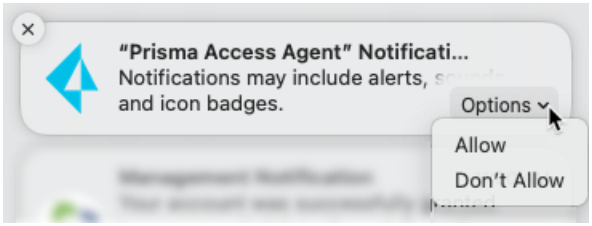
 ©2025 Palo Alto Networks, Inc.



9. 如果管理员将代理配置为安装 Autonomous DEM代理和 Prisma Access Agent，请单击 **OK**（确定），这样就不会再次出现提示。
10. 单击“Prisma Access Agent Notifications（Prisma Access Agent 通知）”弹出窗口以打开“Notifications preferences（通知首选项）”窗口。

STEP 3 | 如果出现提示，请启用 Prisma Access Agent 通知。

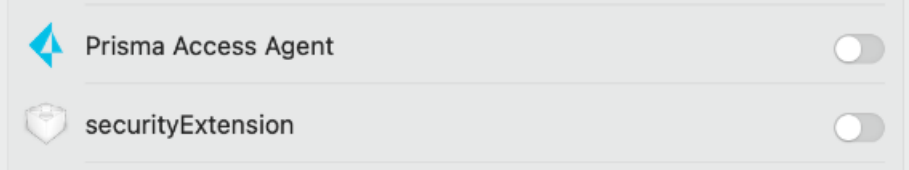
桌面上出现 Prisma Access Agent 通知弹出窗口时，将光标移到弹出窗口上，然后选择 选项（**Options**） > **Allow**（允许）。



 ©2025 Palo Alto Networks, Inc.

STEP 4 | 要使 Prisma Access Agent 在 Safari 浏览器中访问数据，必须向 Security Extension 和 Prisma Access Agent 授予完整磁盘访问权限。

1. 从 macOS 中，选择 **System Settings**（系统设置） > **Privacy & Security**（隐私与安全） > **Full Disk Access**（完整磁盘访问权限）。从应用列表中启用 **Prisma Access Agent** 和 **securityExtension**。



2. 出现提示时，选择 **Quit & Reopen**（退出并重新打开）退出并重新打开 Prisma Access Agent，以使更改生效。

安装 Prisma Access Agent (macOS)

如果不再需要使用Prisma Access Agent，可以手动卸载它。请记住，通过卸载代理，您将不再能够访问公司网络，并且您的端点将不受组织安全策略的保护。

在开始之前，如果管理员为Prisma Access Agent启用了防篡改功能，则必须从管理员处获取防篡改解锁密码。要卸载代理，您必须具有提升的管理权限。

完成以下步骤，从命令行界面卸载Prisma Access Agent。

STEP 1 | 在 macOS 设备上，打开终端窗口并发出以下命令：

```
sudo /Applications/Prisma\ Access\Agent.app/Contents/Helpers/
uninstaller
```

STEP 2 | 出现提示时输入管理员密码。

STEP 3 | 如果提示输入管理员密码，请输入防篡改解锁密码。否则，按Enter开始卸载。

Prisma Access Agent及其扩展将被删除。

安装 Prisma Access Agent (Windows)

在 Windows 设备上手动安装 Prisma Access Agent。

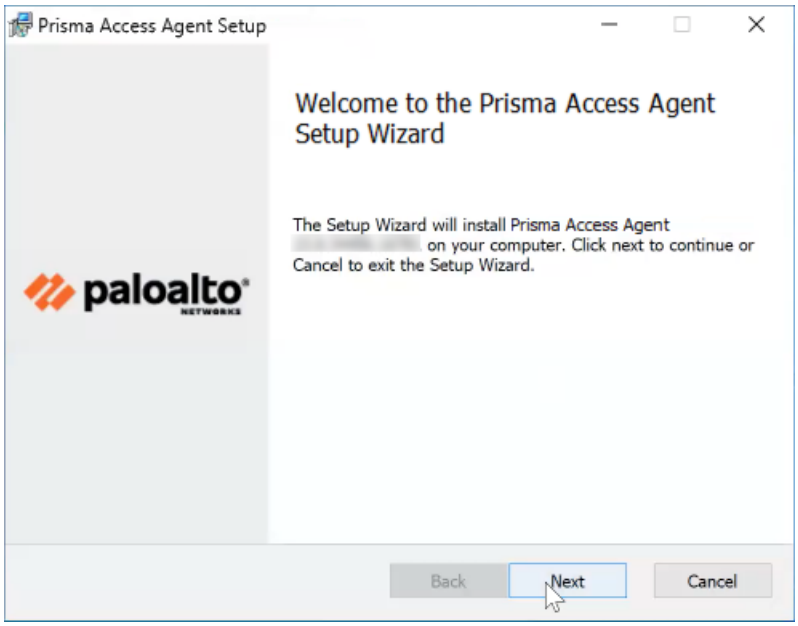
STEP 1 | 获取管理员提供给您的 Prisma Access Agent 软件包。软件包名称的格式如下：

`PrismaAccessAgent_x64_<version>.msi`

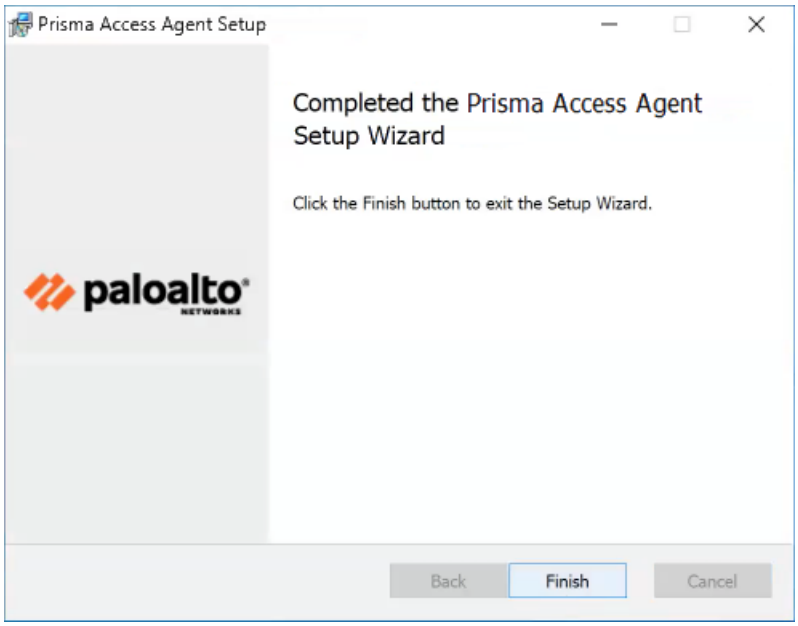
 ©2025 Palo Alto Networks, Inc.

STEP 2 | 在您的 Downloads（下载）文件夹中（或您放置安装包的位置），双击安装包图标并按照提示安装 Prisma Access Agent。

1. 出现安装向导时，单击 **Next**（下一步）继续。



2. 查看最终用户许可协议，选择 **I accept the terms in the License Agreement**（我接受许可协议中的条款），然后单击 **Next**（下一步）。
3. 单击 **Install**（安装）以开始安装。
4. 当系统出现提示 **allow this app to make changes to your device**（允许此应用对您的设备进行更改）时，请单击 **Yes**（是）。
5. 安装完成后，单击 **Finish**（完成）。



6. 如果管理员将代理配置为安装 Autonomous DEM代理和 Prisma Access Agent，请单击 **OK**（确定），这样就不会再次出现提示。

©2025 Palo Alto Networks, Inc.

安装 **Prisma Access Agent (Windows)**

如果不再需要使用Prisma Access Agent，可以手动卸载它。请记住，通过卸载代理，您将不再能够访问公司网络，并且您的端点将不受组织安全策略的保护。

开始之前，如果已为Prisma Access Agent启用防篡改功能，则必须从管理员处获取防篡改解锁密码。要卸载代理，您必须具有管理员权限。

完成以下步骤以卸载Prisma Access Agent：

STEP 1 | 启用 Prisma Access Agent

1. 在命令提示符窗口中运行以下命令：

```
"C:\Program Files\Palo Alto Networks\Prisma Access Agent
\pacli" traffic show
```

2. 如果提示输入管理员密码，请输入防篡改解锁密码。

STEP 2 | 从“设置”中禁用Prisma Access Agent。

- 在 Windows 上：
  1. 打开开始菜单
  2. 选择设 > 置 > 应用程序已安装的应用 > 程序。
  3. 滚动到**Prisma Access Agent**。
  4. 选 择更多选 > 项。
  5. 当系统提示您继续卸载时，单击“是”。
- 在 Windows 上：
  1. 打开开始菜单
  2. 选择 > 设 > 置应用程序应用程序和功能。
  3. 滚动到**Prisma Access Agent**。
  4. 选择 > 更多选项。
  5. 当系统提示您继续卸载时，单击“是”。

登录到已启用动态特权访问的 Prisma Access Agent

在何处可以使用？	需要提供什么？
• Prisma Access Agent	❑ macOS 12 或更高版本的桌面设备，或 Windows 10 版本 2024 或更高版本或 Windows 11 桌面设备 ❑ 允许访问 Internet

要访问组织的网络、资源、SaaS 应用程序或互联网，请使用登录凭据登录 Prisma Access Agent。

 ©2025 Palo Alto Networks, Inc.

登录到 Prisma Access Agent 后，您将使用 Prisma Access 最佳位置（有时称为网关）自动连接到网络。会自动选择最佳位置以提供最佳性能，从而获得更好的体验，例如以本地语言查看网站。当您的设备位于组织网络之外时，代理会查找最佳位置，以便在连接到网络时为您提供最佳性能。

开始之前，必须在设备上安装了 Prisma Access Agent。通常，您的管理员会将 Prisma Access Agent 部署到您用来访问组织网络、资源和应用程序的设备。将根据管理员定义的策略规则来配置代理，并部署到设备上。但如果您的管理员未将 Prisma Access Agent 部署到您的设备，则需要手动安装 Prisma Access Agent。

根据组织中 Prisma Access 的设置方式，管理员应向您提供以下登录信息：

- 承载管理 Prisma Access Agent 的服务的 Prisma Access 服务器的名称。可以有多个服务器，具体取决于 Prisma Access 设置。
- 如果您的组织使用动态特权访问，则为您处理的项目的名称。动态特权访问使您能够根据您被分配到的项目访问组织的网络和资源，以免意外访问其他项目的资源。如果您被分配负责多个项目，便可以轻松切换项目。

根据您的操作系统设置，应用图标和应用界面可以使用深色模式或浅色模式显示。

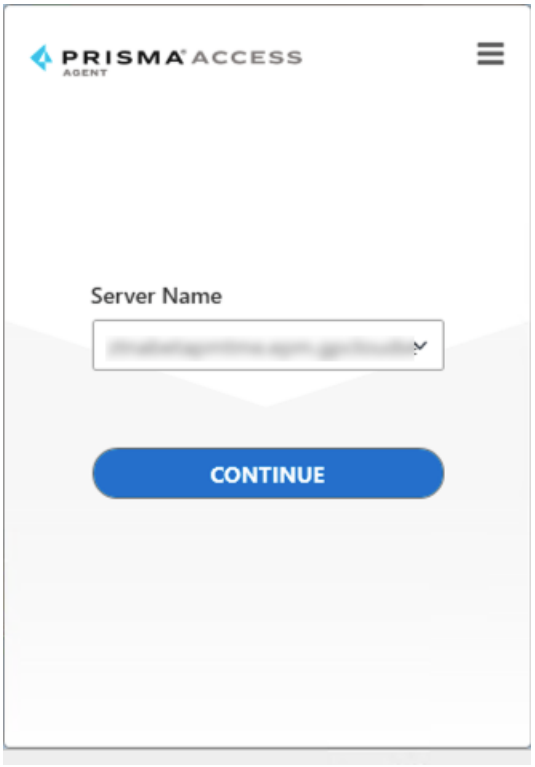
完成以下步骤以登录 Prisma Access Agent：

STEP 1 | 通过单击 macOS 菜单栏或 Windows 任务栏中的 Prisma Access Agent 图标 来启动 Prisma Access Agent。

 ©2025 Palo Alto Networks, Inc.

STEP 2 | 如果出现提示，则在 **Server Name**（服务器名称）中，输入或选择管理员提供的 Prisma Access 服务器的服务器名称，然后选择 **Continue**（继续）。

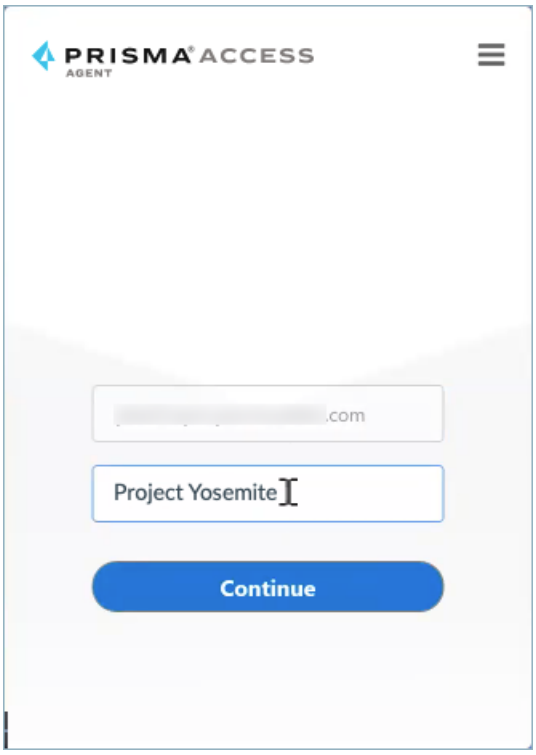
服务器名称的格式为 **<example.domain.com>**（无 **https://** 协议）。服务器名称的最大长度为 256 个字符。



 ©2025 Palo Alto Networks, Inc.

STEP 3 | 输入管理员发送给您的项目名称，然后单击 **Continue**（继续）。

项目名称的最大长度为 32 个字符。



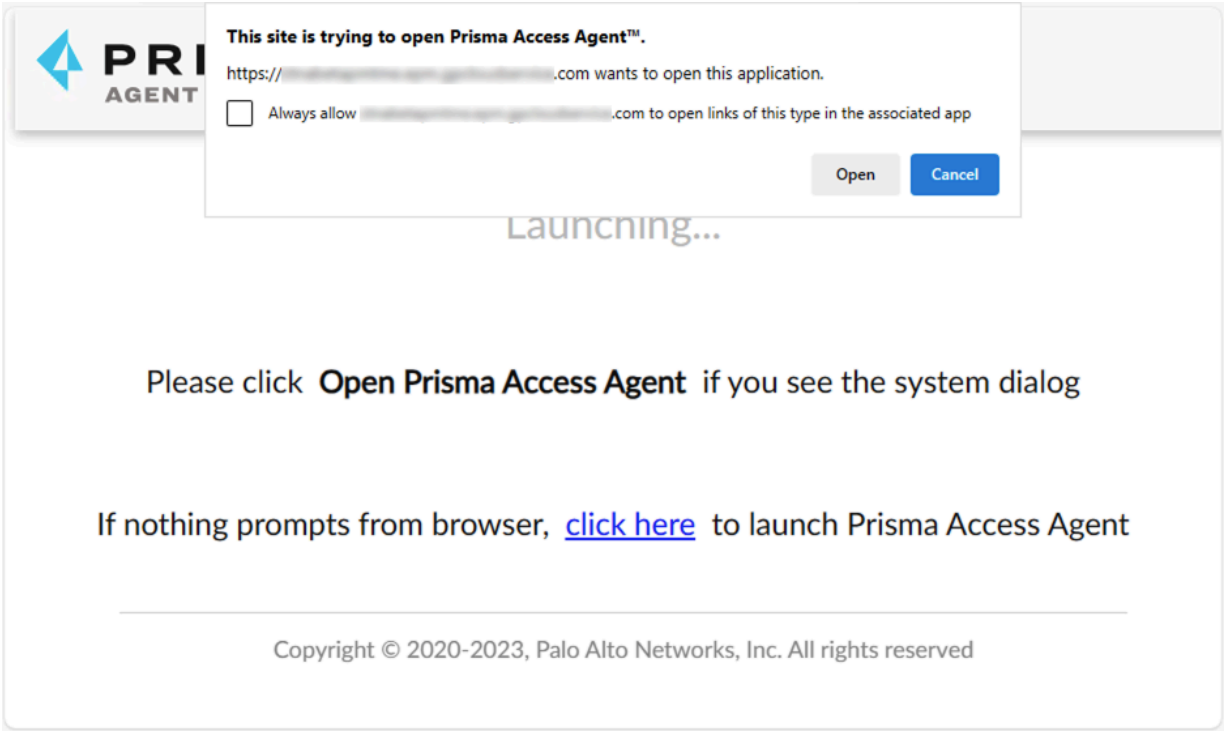
STEP 4 | 在默认 Web 浏览器中显示的登录页面中，通过输入组织的登录凭据来登录到组织的单点登录 (SSO) 应用，如 Okta 或 Azure Active Directory (AD)。

如果您的管理员启用了多因素身份验证 (MFA)，则您需要在登录时在浏览器中完成其他验证。

©2025 Palo Alto Networks, Inc.

STEP 5 | 当 Web 浏览器提示您时，单击 **Open**（打开）。

如果您不希望浏览器在下次登录时提示您，请选择 **Always allow**（始终允许）**<site>**以在关联应用中打开这些类型的链接，然后单击 **Open**（打开）（如果默认 Web 浏览器支持）。

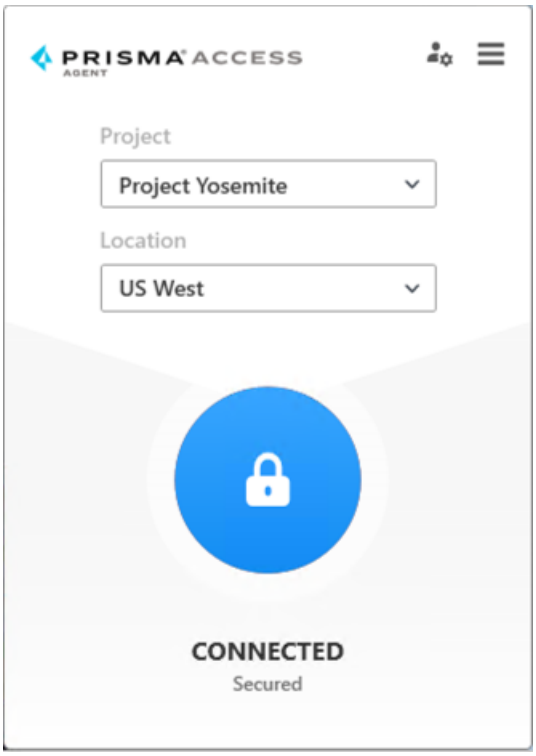


STEP 6 | 请等待 Prisma Access 代理连接到 Prisma Access。



 ©2025 Palo Alto Networks, Inc.

STEP 7 | 成功登录后，您将自动连接到最佳可用 Prisma Access 位置。如果您使用项目登录，则会连接到项目的最佳可用位置。



您现在可以访问组织的资源和 SaaS 应用程序，还可以安全访问互联网。

如果管理员为 *Prisma Access Agent* 启用了 ***Always On***（始终打开）模式，则由于组织的策略，您无法断开与 *Prisma Access* 的连接。不过仍然可以更改 *Prisma Access* 位置。

如果您的管理员为 *Prisma Access Agent* 启用了 ***On Demand***（按需）模式，则必须单击锁图标才能连接到 *Prisma Access*。

更改启用动态特权访问的 Prisma Access Agent 的首选项

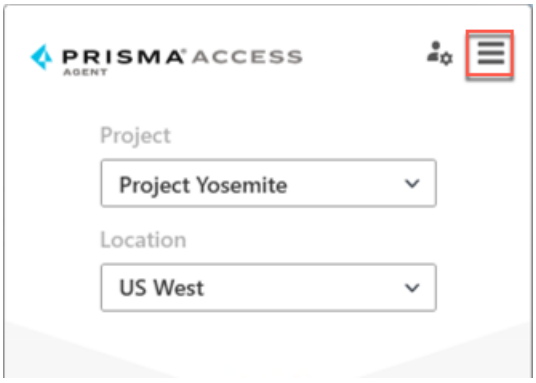
在何处可以使用？	需要提供什么？
• Prisma Access Agent	❑ macOS 12 或更高版本的桌面设备，或 Windows 10 版本 2024 或更高版本或 Windows 11 桌面设备 ❑ 允许访问 Internet

使用 Prisma Access Agent 首选项窗口可查看有关设备的信息和更改代理的选项，例如启用桌面通知 。

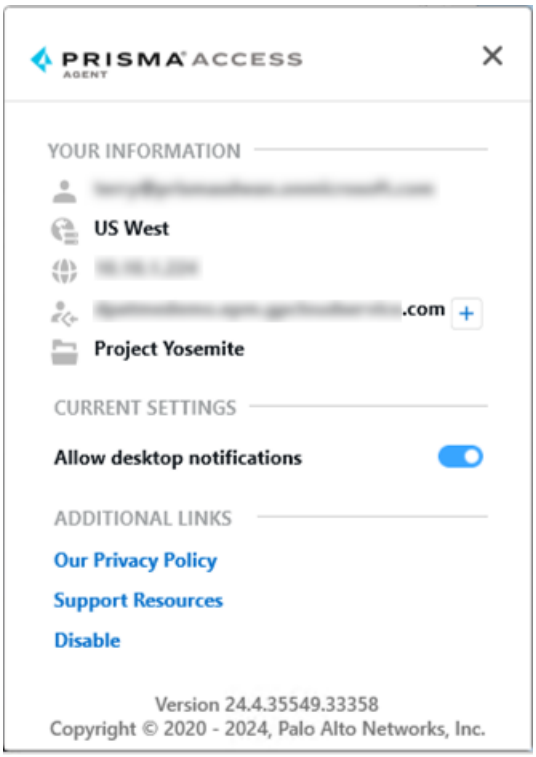
STEP 1 | 通过单击 macOS 菜单栏或 Windows 任务栏中的 Prisma Access Agent 图标 来启动 Prisma Access Agent。

©2025 Palo Alto Networks, Inc.

STEP 2 | 单击汉堡菜单以打开首选项窗口。



STEP 3 | 在首选项窗口中，您可以查看以下信息：



图标	说明
	您的用户 ID。
	您的设备连接的 Prisma Access 地点。
	Prisma Access 地点的 IP 地址。
	您连接的管理接口（服务器）的主机名或 IP 地址。您可以单击加号 (+) 图标连接到其他服务器。

©2025 Palo Alto Networks, Inc.

图标	说明
	您登录的项目。

STEP 4 | 要在菜单栏（macOS 上）或任务栏（Windows 上）中接收 Prisma Access Agent 通知，请选择 **Allow desktop notifications**（允许桌面通知）。此设置已默认启用。

桌面通知是否显示取决于安装时设置的“请勿打扰”设置。操作系统将在安装时提示您允许接收来自 Prisma Access Agent 的通知。

STEP 5 | 要了解 Prisma Access Agent 收集哪些数据以及如何使用这些信息，请查看**Our Privacy Policy**（我们的隐私政策）。

STEP 6 | 要获得有关您在使用 Prisma Access Agent 时可能遇到的问题的协助，请单击 **Support Resources**（支持资源）。

STEP 7 | 如果管理员允许，您可以 **Sign Out**（注销）Prisma Access Agent。

STEP 8 | 如果管理员启用了该功能，您可以 **Disable**（禁用）Prisma Access Agent，以便您可以切换到 GlobalProtect 应用程序（如果您的设备上安装了该应用程序）。

STEP 9 | 查看 Prisma Access Agent 的版本。

STEP 10 | 要关闭该窗口，请单击 **X**。

将启用动态特权访问的 Prisma Access Agent 连接到不同的地点

在何处可以使用？	需要提供什么？
• Prisma Access Agent	❑ macOS 12 或更高版本的桌面设备，或 Windows 10 版本 2024 或更高版本或 Windows 11 桌面设备 ❑ 允许访问 Internet

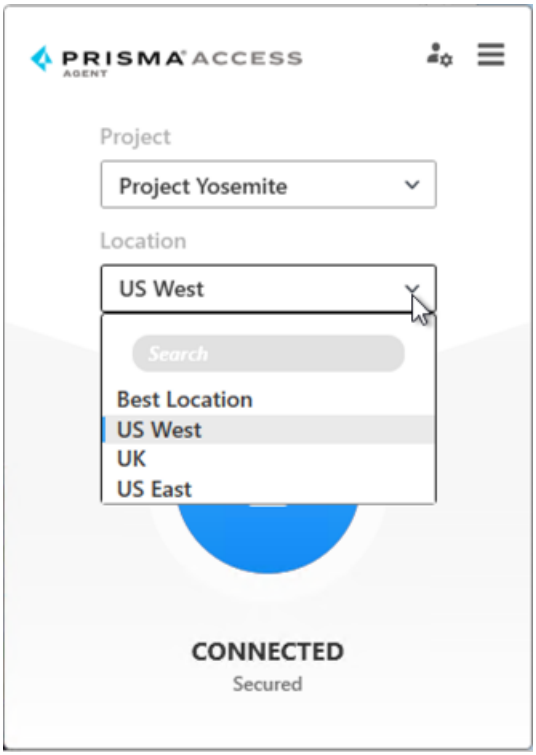
登录 Prisma Access Agent 后，您将自动连接到最佳可用的 Prisma Access 地点。如果要更改地点，可以使用 **Location**（地点）下拉列表进行更改。

STEP 1 | 通过单击 macOS 菜单栏或 Windows 任务栏中的 Prisma Access Agent 图标 来启动 Prisma Access Agent。

 ©2025 Palo Alto Networks, Inc.

STEP 2 | 选择不同的 **Location**（地点）。您可以 **Search**（搜索）某个地点或从列表中选择一个地点。

根据响应时间、可用性和其他因素，可用地点列表按照最佳体验进行排序。提供最佳体验的地点将被列为 **Best Location**（最佳地点）。



STEP 3 | 如果您的管理员为 Prisma Access Agent 启用了 **On Demand**（按需）模式，请单击锁定图标连接到新选择的地点。否则，Prisma Access Agent 会继续更改地点。

切换到不同的项目

在何处可以使用？	需要提供什么？
• Prisma Access Agent	☐ macOS 12 或更高版本的桌面设备，或 Windows 10 版本 2024 或更高版本或 Windows 11 桌面设备 ☐ 允许访问 Internet

如果您在组织中被分配到多个项目，您可以切换到另一个项目以访问与该项目相关的网络和资源。

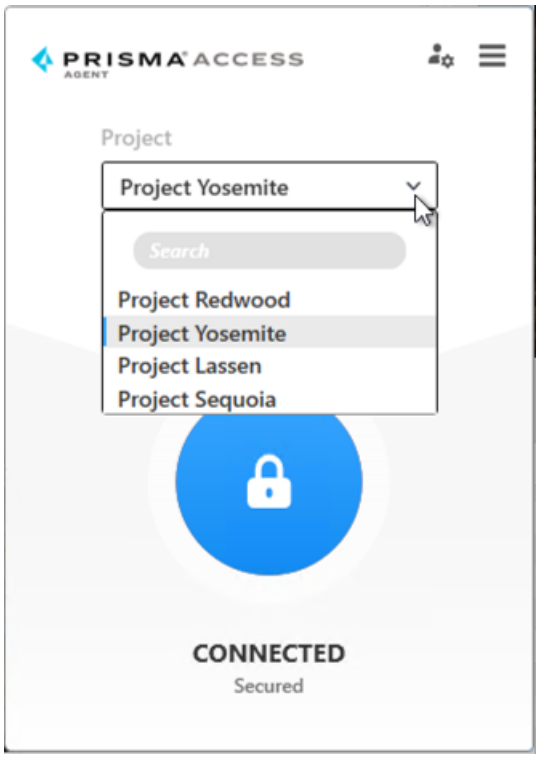
如果您尝试切换的项目可以从不同的服务器访问，您需要先切换到该服务器。

STEP 1 | 通过点击macOS菜单栏Windows任务栏中的 Prisma Access Agent 图标 来启动 Prisma Access Agent

©2025 Palo Alto Networks, Inc.

STEP 2 | 选择其他 **Project**（项目）。您可以搜索一个位置或从列表中选择一个位置。

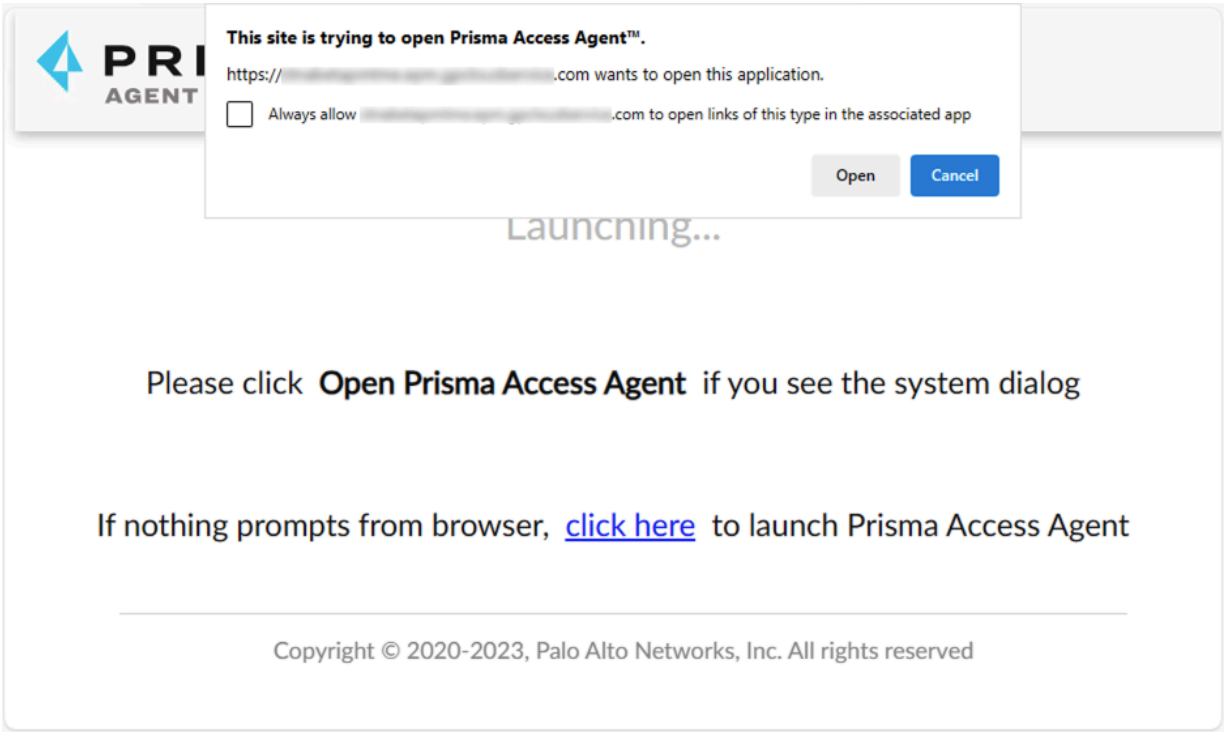
您必须被分配到您要切换到的项目。



STEP 3 | 如果您的管理员已为 Prisma Access Agent 启用 **On Demand**（按需模式），请单击锁定图标以切换项目。否则，Prisma Access Agent 会继续切换项目。

©2025 Palo Alto Networks, Inc.

STEP 4 | 每次切换项目时，Prisma Access Agent 都会断开与当前项目的连接，并连接到新选择的项目。您可能会被提示再次打开 Prisma Access Agent。



将启用动态特权访问的 Prisma Access Agent 连接到不同的服务器

在何处可以使用？	需要提供什么？
• Prisma Access Agent	❑ macOS 12 或更高版本的桌面设备，或 Windows 10 版本 2024 或更高版本或 Windows 11 桌面设备 ❑ 允许访问 Internet

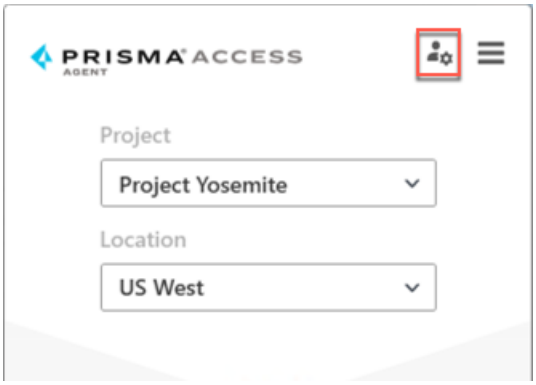
Prisma Access 服务器的实例也称为租户。如果您的管理员设置了多个 Prisma Access 服务器，您可以连接到不同的服务器以通过该服务器访问网络或资源。

例如，您需要处理另一个项目，但只能在另一台服务器上访问该项目。您需要先连接到该服务器，然后才能切换到该项目。

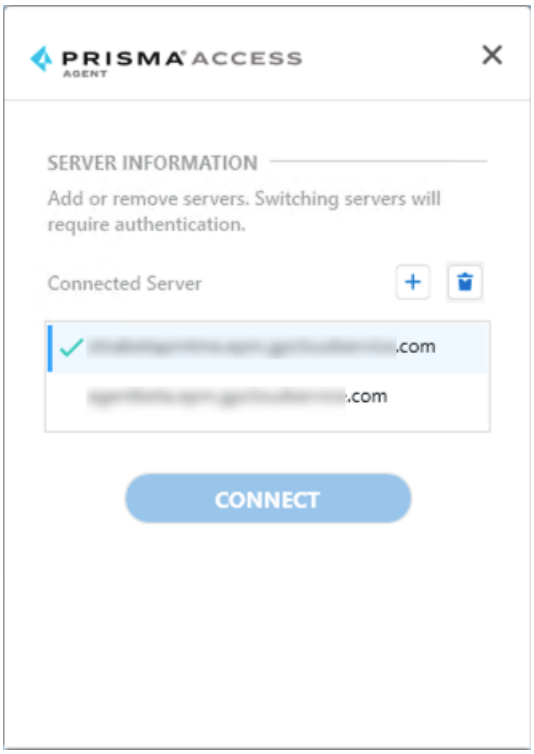
STEP 1 | 通过单击 macOS 菜单栏或 Windows 任务栏中的 Prisma Access Agent 图标 来启动 Prisma Access Agent。

 ©2025 Palo Alto Networks, Inc.

STEP 2 | 通过选择服务器管理图标来编辑服务器设置。



STEP 3 | 服务器信息窗口显示您所连接的服务器。如果列出了其他服务器，您可以选择一个服务器，然后选择 **Connect**（连接）以进行连接。

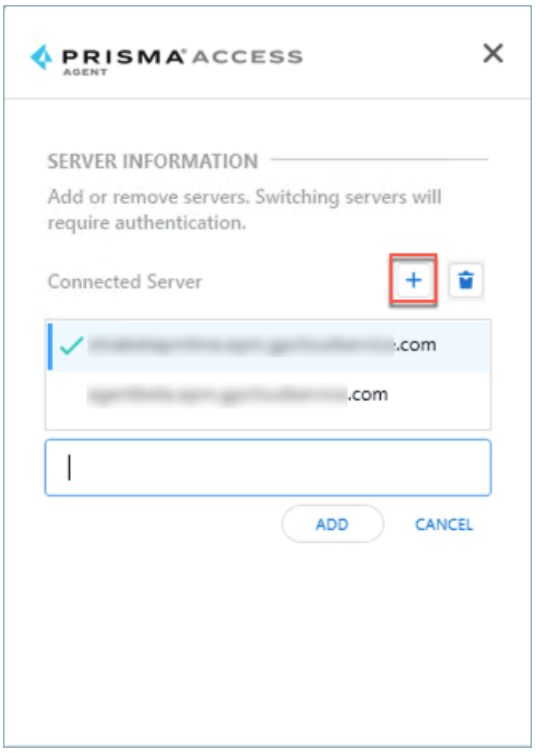


 ©2025 Palo Alto Networks, Inc.

STEP 4 | 如果需要添加服务器，请完成以下步骤：

1. 单击 **+** 符号。
2. 输入新的服务器名称（由您的管理员提供），然后选择 **Add**（添加）以添加。

   服务器名称的格式为 **<example.domain.com>**（无 **https://**）。服务器名称的最大长度为 256 个字符。此页面允许的最大服务器数量为 20。



3. 添加服务器后，选择该服务器并单击 **Connect**（连接）。

STEP 5 | 出现确认窗口时，单击 **Yes**（是）以断开与当前服务器的连接并连接到其他服务器。您将需要再次提供您的单点登录凭证。

STEP 6 | 出现提示时，通过提供项目名称（如果适用）登录到新服务器。

在 GlobalProtect 应用程序和 Prisma Access Agent 之间切换

在何处可以使用？	需要提供什么？
• Prisma Access Agent	❑ macOS 12 或更高版本的桌面设备，或 Windows 10 版本 2024 或更高版本或 Windows 11 桌面设备 ❑ 允许访问 Internet

在某些组织中，Prisma Access Agent 安装在已安装 GlobalProtect 应用程序的用户设备上。安装 Prisma Access Agent 后，您可以根据需要在 Prisma Access Agent 和GlobalProtect应用程序之间切换。

©2025 Palo Alto Networks, Inc.

在切换到 GlobalProtect 应用程序后，Prisma Access 代理处于禁用状态。在禁用状态下：

- 所有对 Prisma Access 位置的流量均已禁用，且多因素身份验证 (MFA) 已禁用。

  Prisma Access Agent 和 GlobalProtect 都使用相同的 GlobalProtect 端口来监听 MFA 请求（用于某些应用程序的额外身份验证），但一次只能有一个代理使用该端口。当您禁用 Prisma Access 代理时，端口将被释放以供 GlobalProtect 使用。
- 与服务器的通信持续进行，以便代理可以继续接收分阶段的升级、ADEM通知、来自管理员的远程Shell请求，并执行HIP检查。
- 如果由管理员配置，防篡改功能将继续运行，以保护代理免受未经授权的篡改。
- 在 macOS 设备上，Prisma Access Agent 的系统和网络扩展将继续处于活动状态，内容过滤器也将继续处于活动状态。
- 如果您切换到另一个服务器，Prisma Access Agent 将会自动重新启用。如果您尝试在代理被禁用时连接到 Prisma Access 位置，代理将连接到最佳位置。

您可以使用 Prisma Access Agent 应用程序或 Prisma Access 命令行工具 (PACli) 在两个应用程序之间切换。

- Prisma Access Agent 应用程序
- Prisma Access 命令行 (PACli)

在 Prisma Access Agent 与 GlobalProtect 应用程序（使用 Prisma Access 客户端应用程序）之间切换

在切换到 GlobalProtect™ 应用程序之前，您需要禁用 Prisma Access Agent。如果您的管理员配置了该功能以允许用户禁用 Prisma Access Agent，则您可以使用该应用程序禁用 Prisma Access Agent。禁用 Prisma Access Agent 后，您可以启动 GlobalProtect 应用程序。

您的管理员必须联系 *Palo Alto Networks* 团队才能启用此租户级功能。它不作为代理设置 。

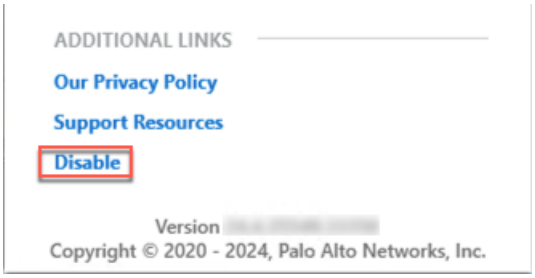
©2025 Palo Alto Networks, Inc.

要从 Prisma Access Agent 切换到 GlobalProtect 应用，请执行以下操作：

1. 启用 Prisma Access Agent

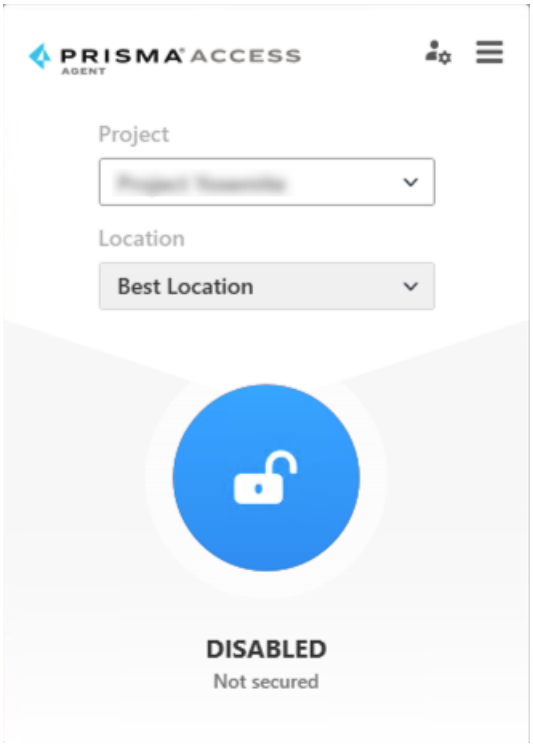
   如果您是第一次禁用代理，请打开 Prisma Access Agent 应用程序并退出 Prisma Access Agent。

   1. 选择汉堡菜单并选择“退出”。
   2. 再次登录 Prisma Access Agent 应用程序，使“禁用”链接出现在首选项窗口中。
2. 单击汉堡菜单以打开首选项窗口。
3. 启用 Prisma Access Agent



4. 单击 **X**关闭首选项窗口。

   Prisma Access Agent 已禁用。



5. 启动 GlobalProtect 应用程序并 连接 到 GlobalProtect。

©2025 Palo Alto Networks, Inc.

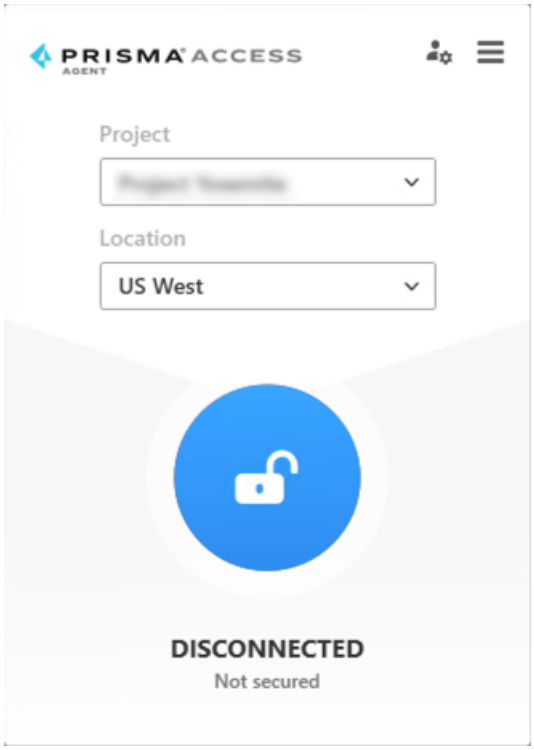
要从 Prisma Access Agent 切换到 GlobalProtect 应用，请执行以下操作：

1. 打开 GlobalProtect 应用程序。
2. 单击选项菜单并选择 断开连接。
3. 登录到 Prisma Access Agent
4. 单击汉堡菜单以打开首选项窗口。
5. 启用 Prisma Access Agent



6. 单击 **X**关闭首选项窗口。
7. 如果代理处于始终开启模式，则代理将启用并连接到最佳位置。

   如果代理处于按需模式，则 Prisma Access Agent 已启用但仍处于断开连接状态。单击锁定图标即可连接到 Prisma Access 位置。



在 Prisma Access Agent 和 GlobalProtect 应用程序之间切换（使用 PACli 工具）

要在 Prisma Access Agent 和 GlobalProtect 应用之间切换，请运行 Prisma Access 命令行工具 (PACli)。切换到 GlobalProtect 应用程序时，如果管理员在 Prisma Access Agent 入职期间设置了

©2025 Palo Alto Networks, Inc.

防篡改解锁密码，PACli 工具将提示您输入防篡改解锁密码。切换到所需的应用将禁用您一直在使用的当前应用。

STEP 1 | 要从 Prisma Access Agent 切换到 GlobalProtect 应用，请执行以下操作：

1. 运行 **switchto** 命令切换代理：
   - 在 macOS 设备上，打开终端窗口并发出以下命令：

     ```
     sudo /Applications/Prisma\ Access\ Agent.app/Contents/
     Helpers/pacli switchto GlobalProtect
     ```

   - 在 Windows 设备上，打开命令提示符窗口并发出以下命令：

     ```
     "C:\Program Files\Palo Alto Networks\Prisma Access Agent
     \pacli" switchto GlobalProtect
     ```

2. （macOS）出现提示时输入管理员密码。
3. 如果出现提示，请输入 **Y** 以切换到 GlobalProtect 应用。
4. 如果提示输入管理员密码，请输入防篡改解锁密码。

   以下文本显示了在 macOS 设备上从 Prisma Access Agent 切换到 GlobalProtect 的示例：

   ```
   <username@hostname>~#cd /应用程序/Prisma \ Access \ Agent.app/
   Contents/Helpers <username@hostname> 助手#sudo./pacli switchto
    GlobalProtect输入管理员密码：已禁用 Prisma Access Agent。启动
    GlobalProtect 服务。这可能需要最多 15 分钟。成功启动 GlobalProtect。
   切换完成。<username@hostname> 助手 %
   ```

   此操作将停止 GlobalProtect 服务并启动 Prisma Access Agent 服务以及防篡改功能。向 Prisma Access Agent 日志中写入一条条目，表明 Prisma Access Agent 已被禁用。例如，记录以下事件：

   ```
   <username@hostname>~#cd /应用程序/Prisma \ Access \ Agent.app/
   Contents/Helpers <username@hostname> 助手 %./pacli 事件..740
    2024-12-11 23:20:57 篡改检测代理已禁用 741 2024-12-11 23:20:57 代
   理隧道已断开连接。
   ```

5. （可选）通过运行 **pacli switchto status** 命令显示 **switchto** 命令的状态。

   以下文本显示了在 macOS 上检查 **switchto** 命令状态的示例：

   ```
   <username@hostname>~#cd /应用程序/Prisma \ Access \ Agent.app/
   Contents/Helpers <username@hostname> 助手#sudo./pacli switchto
    status Prisma Access Agent：已禁用 GlobalProtect：已启用
    <username@hostname> 助手 %
   ```

 ©2025 Palo Alto Networks, Inc.

STEP 2 | 要切换回 Prisma Access Agent，请执行以下操作：

1. 运行 **switchto** 命令切换代理：
   - 在 macOS 设备上，打开终端窗口并发出以下命令：

     ```
     sudo /Applications/Prisma\ Access\ Agent.app/Contents/
     Helpers/pacli switchto PrismaAccessAgent
     ```

   - 在 Windows 设备上，打开命令提示符窗口并发出以下命令：

     ```
     "C:\Program Files\Palo Alto Networks\Prisma Access Agent
     \pacli" switchto PrismaAccessAgent
     ```

2. （macOS）出现提示时输入管理员密码。
3. 如果出现提示，请输入 **Y** 以切换到 Prisma Access Agent。
4. 如果提示输入管理员密码，请输入防篡改解锁密码。

   以下文本显示了在 macOS 设备上从 GlobalProtect 应用程序切换到 Prisma Access Agent 的示例：

   ```
   <username@hostname>~#cd /应用程序/Prisma \ Access \ Agent.app/
   Contents/Helpers <username@hostname> 助手#sudo./pacli switchto
    PrismaAccessAgent 密码：输入管理员密码：停止 GlobalProtect 服务。
   这可能需要最多 15 分钟。已禁用 GlobalProtect。成功启动 Prisma Access
    Agent。切换完成。<username@hostname> 助手 %
   ```

   此操作将停止 GlobalProtect 服务并启动 Prisma Access Agent 服务以及防篡改功能。向 Prisma Access Agent 日志中写入一条条目，表明 Prisma Access Agent 已启用。例如，记录以下事件：

   ```
   <username@hostname>~#cd /应用程序/Prisma \ Access \ Agent.app/
   Contents/Helpers <username@hostname> 助手 %./pacli 事件..742
    2024-12-11 23:21:05 篡改检测代理已启用 743 2024-12-11 23:21:21 代
   理隧道 隧道已连接..
   ```

   切换回 Prisma Access Agent 后，如果代理处于 Always On 模式，则代理将被启用并连接到最佳位置。如果代理处于按需模式，则代理将被启用但断开连接。
5. （可选）通过运行 **pacli switchto status** 命令显示 **switchto** 命令的状态。

   以下文本显示了在 macOS 上检查 **switchto** 命令状态的示例：

   ```
   <username@hostname>~#cd /应用程序/Prisma \ Access \ Agent.app/
   Contents/Helpers <username@hostname> 助手#sudo./pacli switchto
    status Prisma Access Agent：已启用 GlobalProtect：已禁用
    <username@hostname> 助手 %
   ```

 ©2025 Palo Alto Networks, Inc.

查看和监控动态权限访问用户

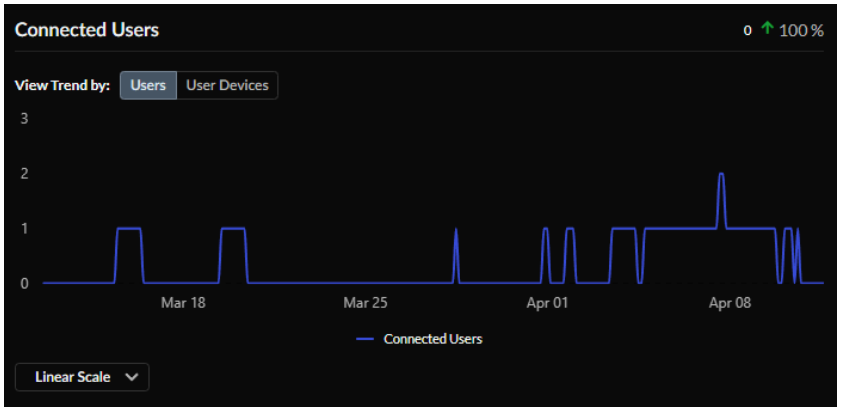
在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 许可证

动态权限访问允许 Prisma Access 根据用户正在处理的项目将不同的网络和安全策略规则应用于移动用户流。在 Strata Cloud Manager 命令中心转到 **Insights**（见解） > 用户，查看环境中基于用户的访问信息。

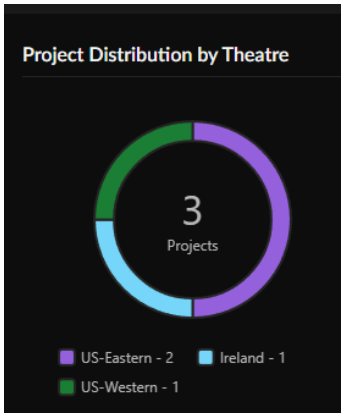
已连接用户

查看 **Connected Users**（连接的用户）以查看当前连接的用户或连接的用户设备。向上或向下箭头将此时间范围与之前的时间范围进行比较，以确定连接的用户或设备数量的百分比差异。

选择按用户查看趋势以查看当前连接到 Prisma Access Agent 的用户数量，然后单击按用户设备查看趋势以查看当前连接到 Prisma Access Agent 的用户设备数量。

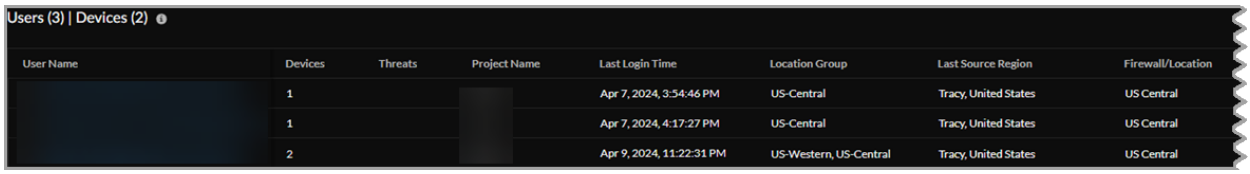


查看按大区划分的项目分布情况，按地点或大区查看项目数量。



用户 | 设备表显示与每个用户和设备关联的项目名称。您还可以查看用户连接了多少设备、上次登录时间、上次访问源位置、上次连接的 Prisma Access 位置、源互联网协议以及操作系统系列和版本。

©2025 Palo Alto Networks, Inc.

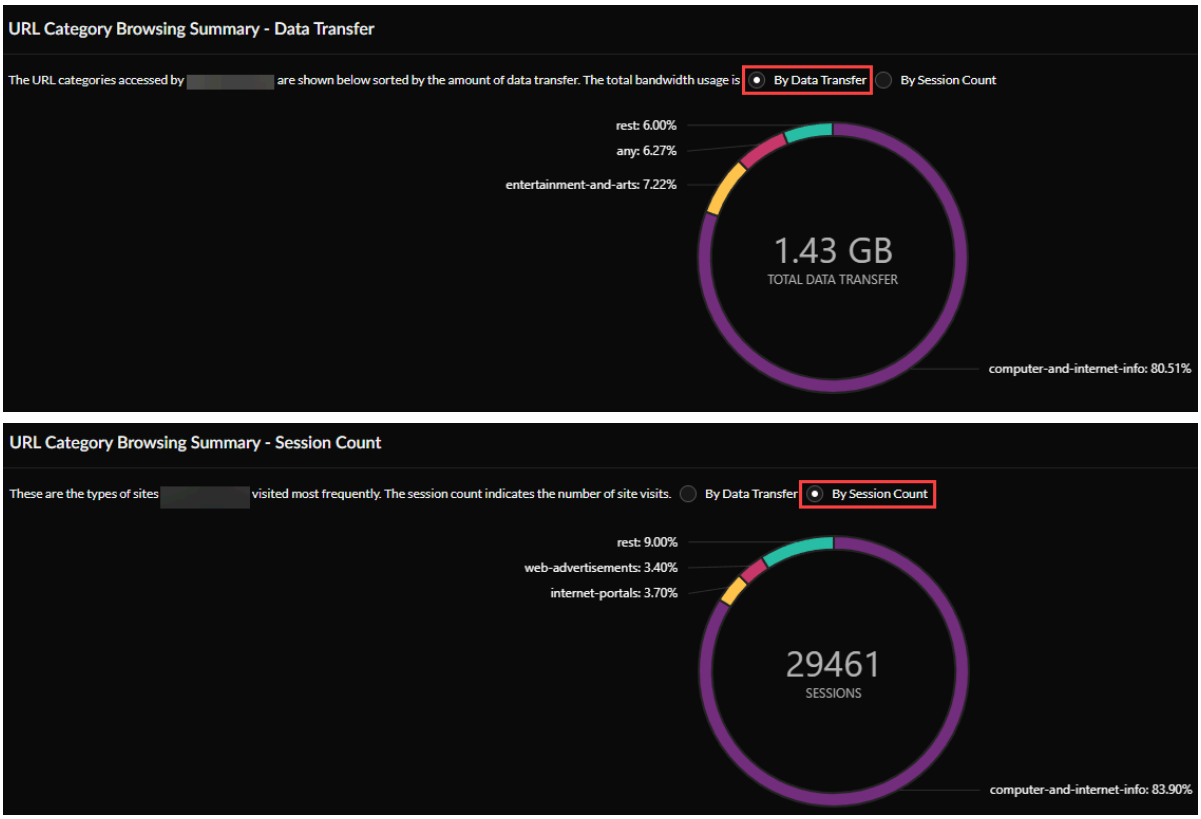


选择任意项目名称以转到项目页面。

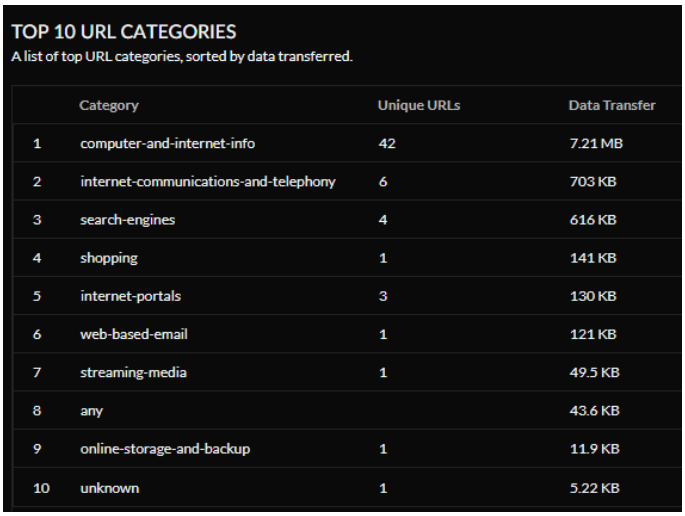
选择任何用户名以查看用户详细信息，例如活动和连接。

活动

URL 浏览类别摘要 — 数据传输 —按数据传输或按会话计数查看您的浏览类别数据传输摘要。您还可以查看按传输的数据排序的前 **10** 个 **URL** 类别的列表。



 ©2025 Palo Alto Networks, Inc.

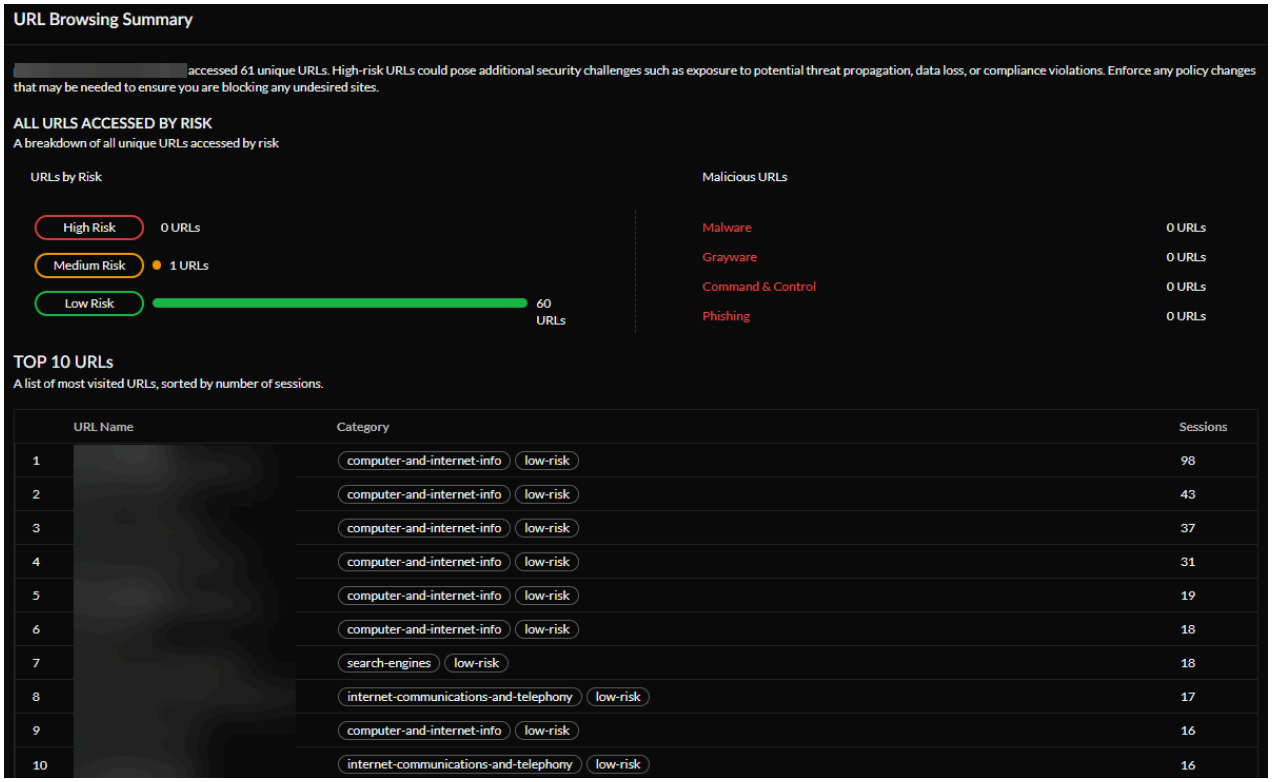


TOP 10 URL CATEGORIES

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

网址浏览摘要 — 查看您的 URL 浏览摘要，包括风险访问的所有网址。您可以查看按风险（高、中或低）划分的网址，并查看访问了多少恶意 URL。您还可以查看访问过的前 **10** 个 **URL** 的列表，以及您访问每个网址的次数。



URL Browsing Summary

[redacted] accessed 61 unique URLs. High-risk URLs could pose additional security challenges such as exposure to potential threat propagation, data loss, or compliance violations. Enforce any policy changes that may be needed to ensure you are blocking any undesired sites.

ALL URLS ACCESSED BY RISK

A breakdown of all unique URLs accessed by risk

URLs by Risk

High Risk 0 URLs

Medium Risk 1 URLs

Low Risk 60 URLs

Malicious URLs

Malware 0 URLs

Grayware 0 URLs

Command & Control 0 URLs

Phishing 0 URLs

TOP 10 URLs

A list of most visited URLs, sorted by number of sessions.

	URL Name	Category	Sessions
1	[redacted]	computer-and-internet-info low-risk	98
2		computer-and-internet-info low-risk	43
3		computer-and-internet-info low-risk	37
4		computer-and-internet-info low-risk	31
5		computer-and-internet-info low-risk	19
6		computer-and-internet-info low-risk	18
7		search-engines low-risk	18
8		internet-communications-and-telephony low-risk	17
9		computer-and-internet-info low-risk	16
10		internet-communications-and-telephony low-risk	16

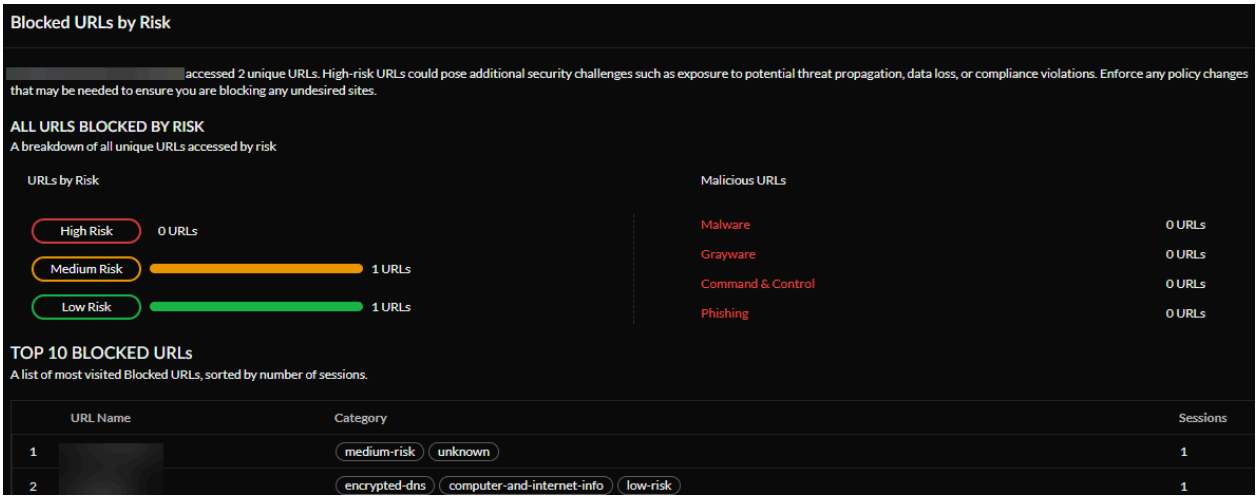
查看 **URL** 过滤日志 — 选择查看 **URL** 过滤日志以查看有关传输总数据的详细信息。日志提供系统、配置和网络事件的审计跟踪。网络日志记录 Prisma Access 在网络上进行操作的所有事件。

- 查看所有日志数据，或使用下拉列表按防火墙/**URL**、通用或终端进行筛选。这些过滤器中的每一个都有几个子过滤器可供选择。
- 输入日志查询。单击此字段可查看从一开始就选择的查询，然后生成您的查询。
- 选择一个时间范围。默认值为过去 60 分钟。

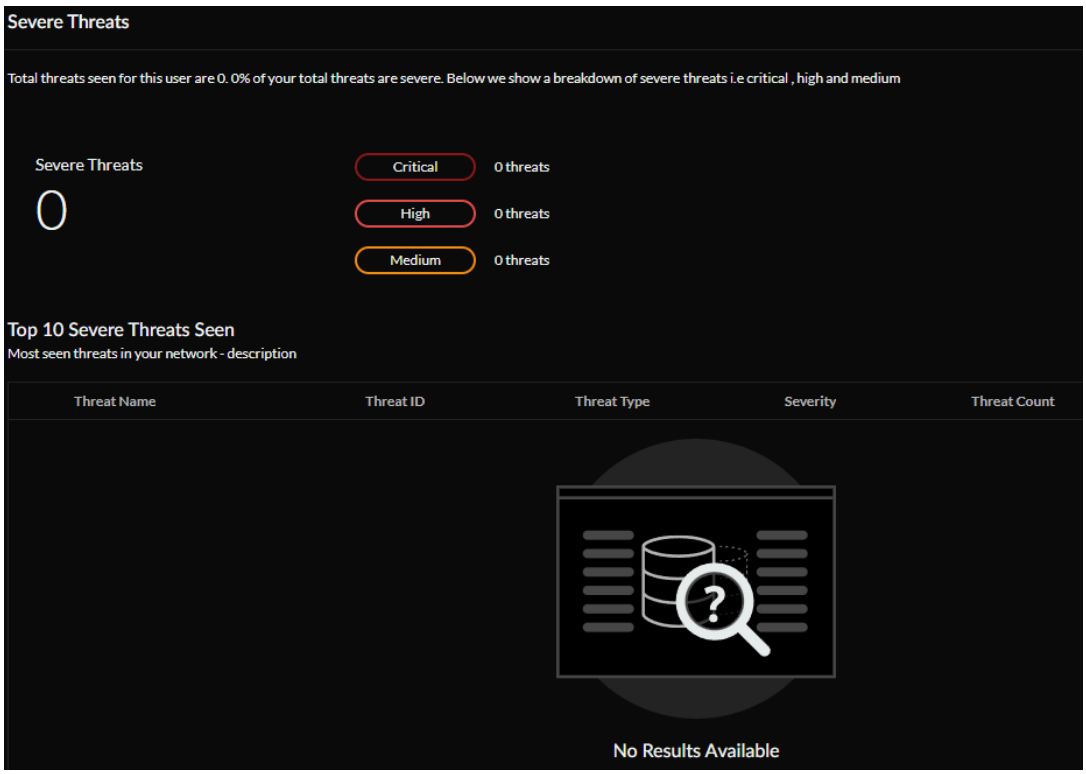
©2025 Palo Alto Networks, Inc.

- 选择日志设置以查看 Strata 日志服务指示板。Strata 日志服务管理日志的交付机制。

按风险屏蔽的 **URL** — 查看您是否访问或尝试访问了任何按风险屏蔽的 URL。高风险 URL 可能会带来额外的安全挑战，例如暴露于潜在的威胁传播、数据丢失或违反合规性。强制进行任何必要的政策更改，以封锁任何不受欢迎的网站。您还可以查看访问次数最多的 **Top 10 Blocked URLs**（前 **10** 个被阻止的网址）列表（按会话数量排序）。



严重威胁 — 查看您的威胁中有多少是严重的。严重威胁进一步细分为严重、高和中等威胁。您还可以查看环境中出现的十大严重威胁列表。



连性

选择任何用户名以查看有关所选时间范围内用户连接的信息。

©2025 Palo Alto Networks, Inc.

活跃项目 — 您可以查看在所选时间范围内哪些项目处于活动状态，以及每个项目生效的日期。

互联用户的设备趋势和联网用户的设备 — 在用户主页面上，您可以看到所有联网用户及其项目。在连接页面上，查看所选时间范围内您的个人连接用户的设备趋势以及有关您的连接用户设备的详细信息，例如设备名称、上次用户来源 IP 地址、上次私有 IP 地址、上次用户位置、上次登录时间、上次注销时间和上次会话持续时间。



项目活动 — 按会话查看用户的项目活动。您可以查看会话的当前状态、用户何时登录每个项目、何时注销以及每个会话持续了多长时间。



按项目划分的用户活动总数 — 查看用户在所选时间范围内在每个项目上花费的时间。

 ©2025 Palo Alto Networks, Inc.

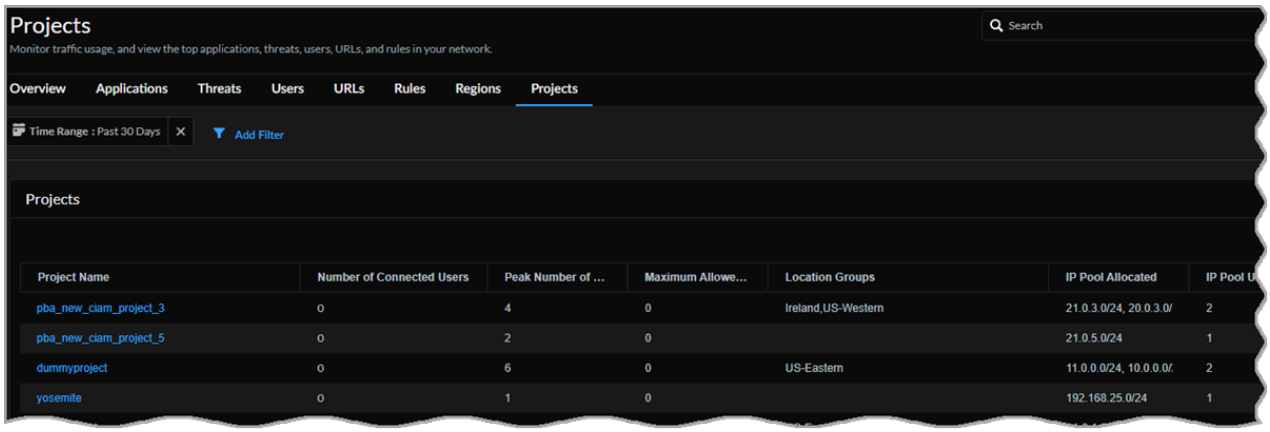
查看和监控动态权限访问项目

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

通过使用 Strata Cloud Manager 监控您的用户项目活动，获得 Prisma Access Agent 部署的可见性。 > 前往 Strata Cloud Manager Command Center 中的活动洞察项目，以查看您环境中的基于项目的访问信息。

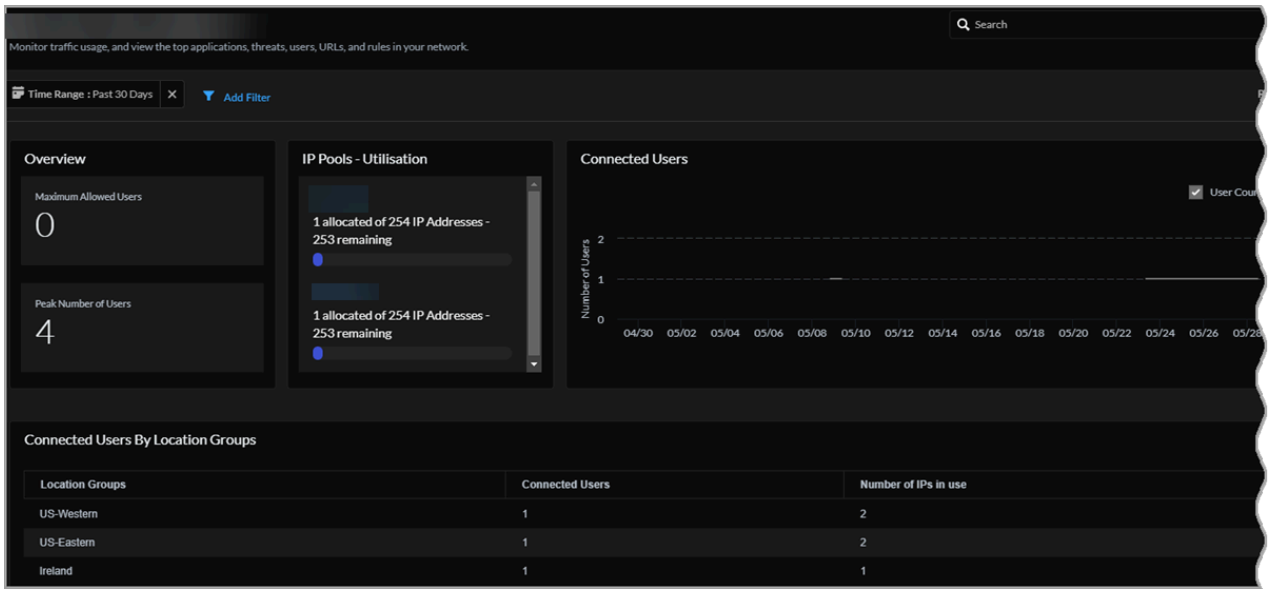
项目

项目表提供了关于用户在选定时间范围内使用 Prisma Access 访问的项目的整体视图。您可以查看每个项目的连接用户数量、用户峰值数量、最大允许用户数量、Prisma Access 位置组、分配的 IP 地址池、已使用的 IP 池、可用 IP 地址数量以及最后连接的 Prisma Access 位置。



选择一个项目名称以进入该项目的详细信息页面。项目名称（在下面的图像中模糊显示）出现在页面的左上角。

©2025 Palo Alto Networks, Inc.

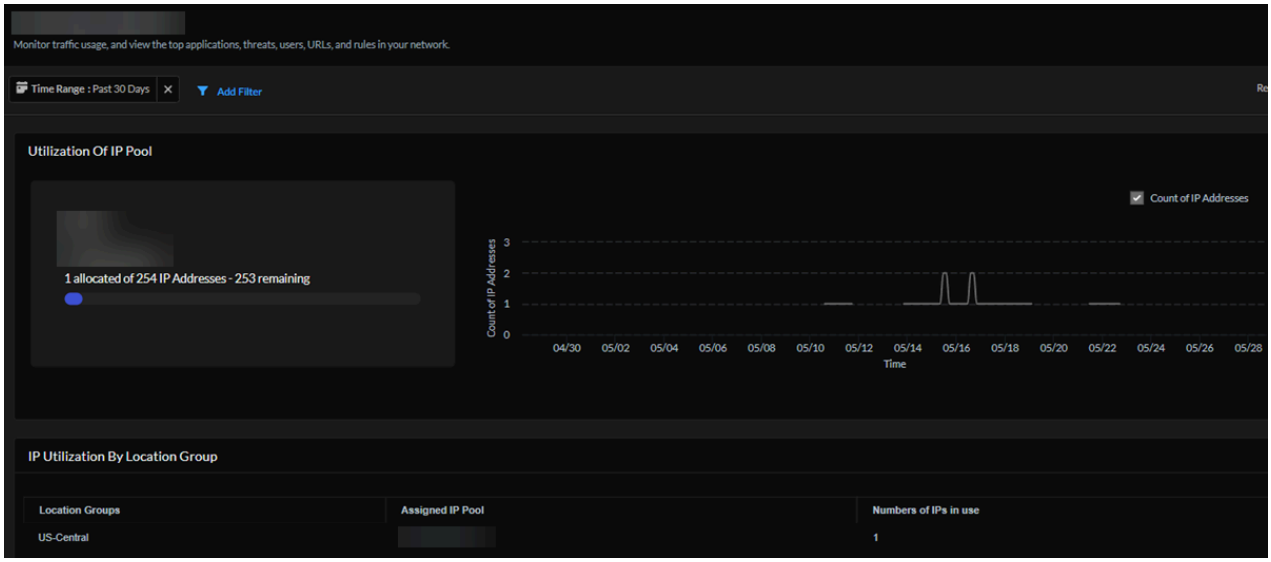


概述

在项目详情页面，**Overview**（概述）显示该项目的最大允许用户数和在选定时间范围内的用户峰值数量。

IP 池 — 利用率

查看此项目中的池正在使用的 IP 数量和仍然可用的 IP 数量。选择一个特定的IP池以进入其详细信息页面（见下图），您可以查看该IP池的利用率、已使用的IP地址数量以及按Prisma Access位置组划分的IP地址利用率。



已连接用户

查看所选时间范围内已连接用户的图形。将鼠标悬停在图表中的任何点上，以查看该点的用户数量。

©2025 Palo Alto Networks, Inc.

按位置组连接的用户

查看用户按他们所在的 Prisma Access **Location Group**（位置组）的数量。您还可以查看每个 **Location Group**（位置组）中使用的 IP 地址数量。

©2025 Palo Alto Networks, Inc.

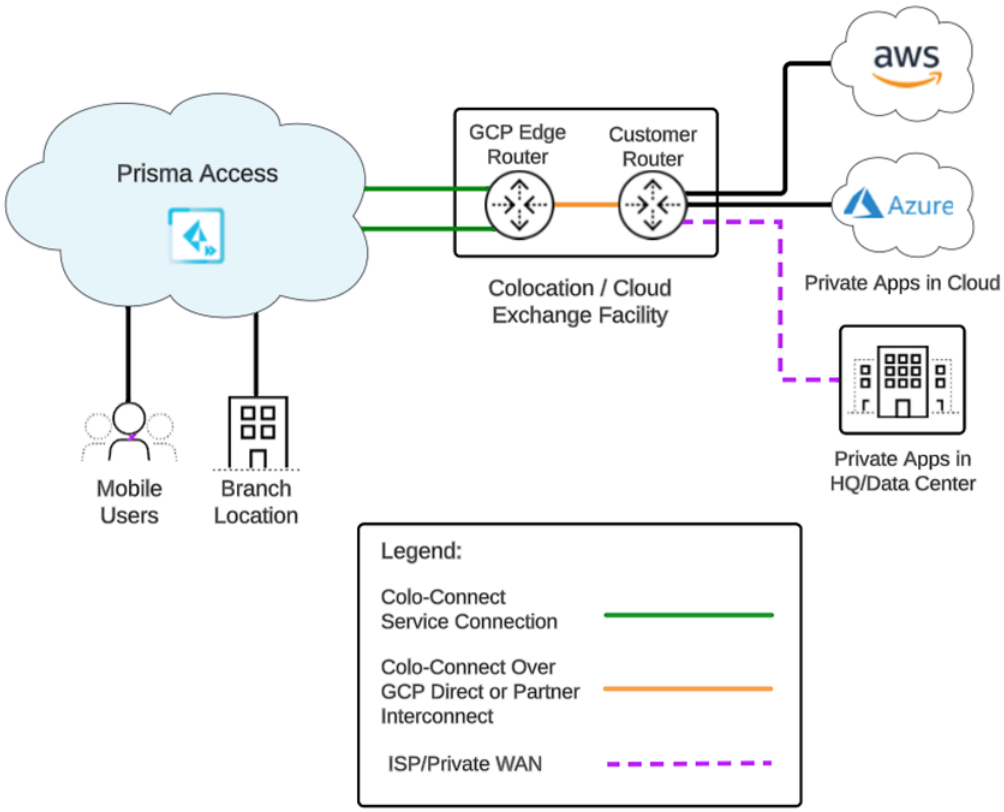
©2025 Palo Alto Networks, Inc.

Prisma Access Colo-Connect

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ 运行云服务插件的最低版本 4.1 以及数据平面的最低版本 10.2.4 的 Prisma Access (Managed by Panorama) 部署 ❑ Colo-Connect 附加许可证

如今，大型企业需要建立基于 Colo 的性能中心，以满足在混合多云架构中访问私有应用程序所需的高带宽和低延迟要求。通常，这些中心包括与一个或多个云提供商的互连以及通过专用或租用 WAN 与内部部署数据中心的连接。性能中心可以在公共云和本地部署基础架构之间以高速路由流量，并且由于底层互连基础架构的原因，性能中心具有弹性。

Colo-Connect 依托于以 Colo 为基础的性能中心概念，具有高带宽（高达 20 Gbps）专用连接，以及从现有性能中心到 Prisma Access 的第 2/3 层无缝连接。下图展示了使用服务连接和直连或合作伙伴互连在 GCP 实例中载入 Prisma Access。此设置限制了与互联网的接触，并允许使用专用连接建立与私有应用程序的连接。



Prisma Access Colo-Connect 利用云原生 GCP 互连技术为您的私有应用程序提供高带宽服务连接，它具有以下功能：

- 每个区域的高带宽（高达 20 Gbps）吞吐量，用于访问私有应用程序

- 支持使用 Google Cloud Platform (GCP) 的专用互连及合作伙伴互连
- 支持每个互连链路的多个 VLAN 连接。
- 区域冗余

 ©2025 Palo Alto Networks, Inc.

Colo-Connect 用例

Prisma Access Colo-Connect 提供高带宽双向连接以保护私有应用程序，如以下用例所示。

对私有应用程序的高带宽访问

如果您的组织在 Colo 中拥有网络，并且您正在利用 Colo 设施建立与本地、公共云托管或这两者同时托管的应用程序的专用连接，则 Prisma Access 可以通过 Colo-Connect 加入 Colo 基础架构。您可以通过 GCP 提供的专用或合作伙伴互连配置 Colo-Connect，以获得访问私有应用程序所需的每个区域高达 20 Gbps 的吞吐量。

例如，您有一个或多个数据中心或总部地点与 Colo 直接连接，并且您想要连接到 Prisma Access 以实现对私有应用程序的安全的高带宽访问。在这种情况下，您可以将合作伙伴互连用于 Prisma Access Colo-Connect，以便用户安全地访问应用程序。由于 Colo 中的设备与公有云以及您的数据中心建立了对等互连，因此您还可以提供对托管在公有云中的任何私有应用程序的访问。

Colo-Connect 与现有的基于 IPSec 隧道的服务连接共存，因此如果您需要为不需要高带宽、多千兆吞吐量的小型数据中心提供对私有应用程序的访问，也可以使用与这些数据中心的服务连接。您可以使用 BGP 路由来配置服务连接，使您的网络与服务连接和 Colo-Connect 连接兼容。

私有应用程序的专用连接

Colo-Connect 可以利用专用网络让用户访问私有应用程序，而不是通过互联网访问，从而为私有应用程序额外增加了一层控制和安全性。

使用第三方 NaaS 提供商

在此用例中，您将利用第三方网络即服务 (NaaS) 提供商（例如 Megaport 和 PacketFabric）在 Colo 和公共云中运行的应用程序之间建立连接，或与 SaaS 提供商（例如 salesforce.com 或 Box）建立连接。您希望在第三方网络和 Prisma Access 之间建立网络连接，以提供对连接的服务、云和应用程序的高带宽访问。您可以：

- 使用 NaaS 提供商的网络设备作为中心，在特定区域的公共云 VPC 或公共 SaaS 提供商中运行的用户和应用程序之间建立连接。
- 在 NaaS 提供商的网络设备和 Prisma Access 之间建立 BGP 会话。

Palo Alto Networks 尚未验证是否可以将第三方 *NaaS* 解决方案与 *Prisma Access Colo-Connect* 结合使用。建议您评估第三方提供商支持的功能，包括设置与 *GCP* 的互连以及为 *Colo-Connect* 服务连接创建 *Prisma Access* 的 *GRE* 隧道。

©2025 Palo Alto Networks, Inc.

Colo-Connect 与服务连接和 ZTNA 连接器有何不同？

Palo Alto Networks 提供三种方式来保护对私有应用程序的访问：服务连接、ZTNA 连接器和 Colo-Connect。服务连接和 ZTNA 连接器均通过互联网保护对私有应用程序的访问，而 Colo-Connect 则建立与数据中心的专用连接。请参阅下表以比较带宽和差异因素。

部署类型			
功能	**Colo-Connect**	**ZTNA 连接器**	服务连接
每个计算区域的最大带宽	20 Gbps	10 Gbps	5 Gbps
吞吐量	与数据中心的 20 Gbps 双向专用连接	每个数据中心高达 10 Gbps	每个连接 1 Gbps
与 Equinix Cross-Connect 和 Megaport 等 SDN/NaaS 提供商兼容	是	否	否
跨数据中心的重叠网络	否	是	否
其他优势	通过 Colo 轻松加入现有的混合和多云部署	简化混合和多云部署中私有应用程序的载入流程	支持本地 Active Directory
是否需要本地部署？	否	是	否

©2025 Palo Alto Networks, Inc.

Colo-Connect 不支持的特性和功能

Colo-Connect 不支持以下特性和功能：

- 使用流量引导时将 Colo-Connect 服务连接配置为目标服务连接
- 适用于私有应用程序访问的 IPv6 支持
- 通过 IPv6 建立 eBGP 对等互连

©2025 Palo Alto Networks, Inc.

Prisma Access Colo-Connect 的要求和先决条件

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access (Managed by Panorama) 部署运行最低版本 4.1 的云服务插件和最低 10.2.4 版本的数据平面 ❑ Colo-Connect 附加许可证

在开始 Colo-Connect 载入和配置之前，请按照此清单了解所需的信息和先决条件。

- ❑ 确保您可以访问 Colo 设施提供商（例如，您可以访问 Equinix 客户门户）。
- ❑ 确保您的 CPE 可以支持 GRE 和 BGP。

  Colo-Connect 服务连接使用 GRE 隧道。
- ❑ 确定将用于 Colo-Connect 的互连类型（合作伙伴或专用互连）。
  - 合作伙伴互连 — 来自 Prisma Access 的配对密钥是合作伙伴互连所必需的。您将在 Prisma Access 载入期间收到此密钥。

    如果您创建合作伙伴互连，请确保服务提供商 (SP) 是经 GCP 批准的 SP，并且 SP 和 GCP 之间的连接已建立。
  - 专用互连 —
    - 在 Prisma Access 中开始载入之前，确定将连接交叉连接电缆的 Colo 的位置。Palo Alto Networks 需要 Colo 位置才能订购专用链路
    - 熟悉基本的网络互连，以便可以配置电路。
    - 配置专用互连后，您必须进行测试。
- ❑ 子网要求 — 确定每个区域的每个 Colo-Connect 连接将使用的 RFC-1918 IPv4 子网。Prisma Access 使用这些子网进行内部通信和联网。

  使子网在给定租户的所有 Colo-Connect 区域中唯一。Colo-Connect 子网不能与 Prisma Access 基础设施子网和移动用户池。使用最小子网大小为 /28。
- ❑ 链路（互连）要求 — 配置链路时请遵循以下准则：
  - 每个 Colo-Connect 附加许可证均包含一条 10 Gbps 容量的链路。您至少需要两个链接，这意味着您需要在 Colo-Connect 部署中购买至少两个许可证。
  - 在每个区域载入两个链接。

    这两个链接都应该位于不同的可用区域（边缘域）。
  - （仅限专用互连部署）如果您想在租户中接入超过六个链接，请联系您的 Palo Alto Networks 客户代表或合作伙伴，他们将联系站点可靠性工程 (SRE) 团队并提交增加给定租户配额的请求。

©2025 Palo Alto Networks, Inc.

- 连接要求 —
  - 在每个区域建立两个连接。

    两个连接应该位于不同的边缘域。
  - 主动/备份或主动/主动模式下的连接必须具有相同的带宽。
  - 决定是否要以主动/主动或主动/备份配置来设置连接。
- **Colo-Connect** 服务连接要求 —
  - 每个服务连接需要两个连接。
  - 给定服务连接的每个连接必须位于不同的链路和不同的边缘域上。
  - 记下将用作 colo-router 的 BGP IP 地址和 GRE 隧道本地 IP 地址的地址。您可以在创建服务连接期间使用这些地址。
  - 服务连接必须属于同一链接类型（合作伙伴互连链接或专用互连链接）。
- 与现有基于 **IPSec** 的服务连接的互操作性 — Palo Alto Networks 强烈建议您在不同区域部署 Colo-Connect 和基于 IPSec 隧道的服务连接。此外，如果您从基于 IPSec 隧道的服务连接迁移到 Colo-Connect 服务连接，则必须安排维护时段。从基于 IPSec 隧道的服务连接迁移到 Colo-Connect 服务连接后，请在 Colo-Connect 服务连接启动并运行后且维护时段到期之前删除基于 IPSec 的服务连接。

©2025 Palo Alto Networks, Inc.

配置 Prisma Access Colo-Connect

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ 运行云服务插件的最低版本 4.1 以及数据平面的最低版本 10.2.4 的 Prisma Access (Managed by Panorama) 部署 ❑ Colo-Connect 附加许可证

Prisma Access Colo-Connect 由以下组件组成：

- **Colo** — 提供机架空间、电源和连接以托管网络、私有云和公共云基础架构（例如 Equinix）的主机托管设施。
- 专用互连 — 路由器与指定 GCP 计算区域中的 GCP 边缘路由器之间的专用第 2 层或第 3 层物理连接。专用互连提供本地网络与 Google 网络之间的直接物理连接。

  在 Prisma Access UI 中，互连称为链路。
- **GCP VLAN** 连接 — 链路上的逻辑第 2 层连接，将流量与共享同一链路的任何其他逻辑连接分隔开来。

  在 Prisma Access UI 中，VLAN 连接称为连接。
- 合作伙伴互连 — 服务提供商拥有的路由器与指定 GCP 计算区域中的 GCP 边缘路由器之间的第 3 层物理连接。合作伙伴互连通过受支持的服务提供商提供本地网络与 VPC 网络之间的连接。

  Colo-Connect 同时支持专用互连和合作伙伴互连。
- **Colo**（客户）路由器 — Colo 设施中的路由设备，通过 Colo 设施中的互连与 GCP 云路由器建立 eBGP，并通过 GRE 隧道与 Colo-Connect 服务建立 eBGP 连接。它是专用互连的客户路由器，或者如果服务提供商通过合作伙伴互连与 GCP 建立了第 2 层连接，则与 GCP 云路由器建立第 3 层连接时，服务提供商拥有 Colo 路由器。
- **GCP** 边缘路由器 — GCP 的网络边缘设备，通过 Colo 在 GCP 与客户/合作伙伴网络之间提供物理连接。
- 云路由器 — 云中的 GCP 软件构造，与 Colo 中的网络设备（例如路由器或第 3 层防火墙）建立 BGP 会话，并在 Prisma Access 与网络之间路由流量。您不需要配置此组件；由 Prisma Access 自动完成配置。

要配置 Colo-Connect，您必须首先收集现有网络环境的相关信息，并确保所有必需的网络组件已安装到位。确保您已满足所有先决条件；然后使用合作伙伴或专用互连在组织的网络中部署 Colo-Connect。

- Strata Cloud Manager
- Panorama

©2025 Palo Alto Networks, Inc.

配置 Prisma Access Colo-Connect (Strata Cloud Manager)

要配置 Colo-Connect，您必须首先收集现有网络环境的相关信息，并确保所有必需的网络组件已安装到位。确保您已满足所有先决条件；然后使用合作伙伴或专用互连在组织的网络中部署 Colo-Connect。

使用合作伙伴互连配置 Prisma Access Colo-Connect—部署

要使用合作伙伴互连配置 Prisma Access Colo-Connect，请完成以下步骤。

STEP 1 | 为 Colo-Connect 连接创建子网。

您可以在后续步骤中创建的连接和服务连接中使用在此处创建的子网。

1. 在 Strata Cloud Manager 中，转到 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Colo-Connect**。
2. 为 Colo-Connect 子网 **Add Prefix**（添加前缀）并为其选择 Prisma Access 地点。

   请在此处查看受支持的 Colo-Connect 地点列表。输入最小子网 /28。
3. （可选）如果您计划为多个地点创建 Colo-Connect 实例，请在每个地点添加更多子网。

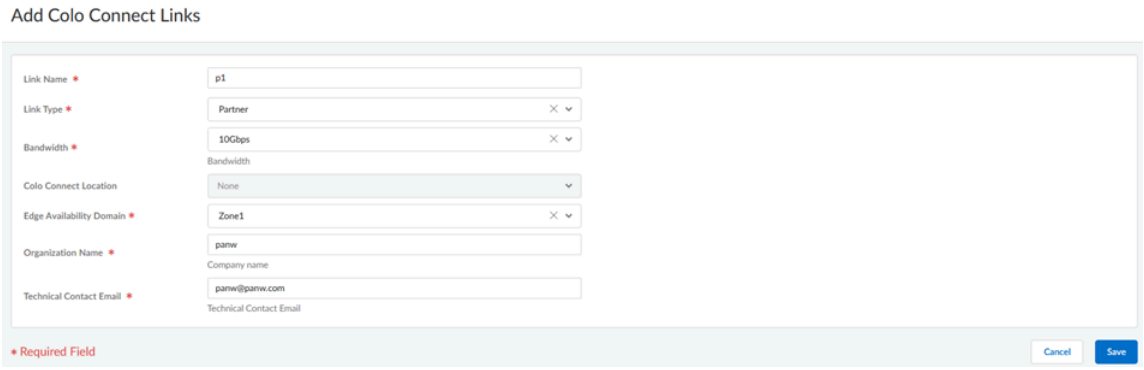
   您可以为每个地点配置一个子网。



 ©2025 Palo Alto Networks, Inc.

STEP 2 | 添加新的 Colo-Connect 链路（也称为互连）。

1. 转到 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Colo-Connect**，然后单击 **Add Link**（添加链路）。
2. 为链路指定唯一的 **Link Name**（链路名称）。
3. 选择 **Partner**（合作伙伴）互连作为 **Link Type**（链路类型）。
4. 指定其余的 Colo-Connect 链路参数。
   - 在 **Bandwidth**（带宽）中选择 **10Gbps** 或 **20Gbps**。
   - 在 **Edge Availability Domain**（边缘可用性域）中选择 **Zone1** 或 **Zone2**。从用于边缘可用性域的 GCP 服务区获取此值。
   - 输入用于此链路的 **Organization Name**（组织名称）。
   - 输入用于此链路的 **Email**（电子邮件）。可接受任何电子邮件地址。



5. 重复步骤 2.a 到 2.d，创建具有不同的 **Edge Availability Domain**（边缘可用性域）的其他链路。

©2025 Palo Alto Networks, Inc.

STEP 3 | 为 Colo-Connect 创建连接（也称为 *VLAN* 连接）。

1. 转到 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Colo-Connect**，然后单击 **Add Connection**（添加连接）。
2. 配置连接设置。
   - 输入唯一的 **Connection Name**（连接名称）。
   - 根据您在上一步中配置的链路选择 **Link Name**（链路名称）。

     您无需输入 **VLAN ID**；对于在合作伙伴互连上创建的 VLAN，它不可配置。
   - 选择连接的 **Bandwidth**（带宽）。

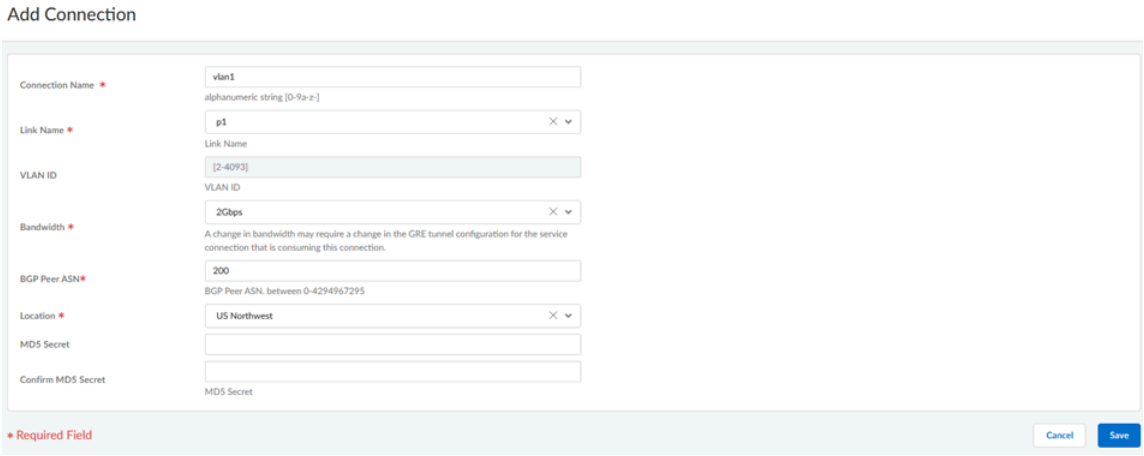
     您可以选择 **1 Gbps**、**2 Gbps**、**5 Gbps**、**10 Gbps**或 **20 Gbps**。

     如果为互连配置多个连接，请确保连接的总带宽不超过互连的带宽。例如，假设合作伙伴互连的带宽为 10 Gbps，则您可以配置 10 个连接，每个连接的带宽为 1 Gbps，但所有连接的总带宽不得超过 10 Gbps。

     如果您的部署需要超过 *16* 个连接，请联系您的 *Palo Alto Networks* 客户团队，他们将提交 *SRE* 案例来满足请求。
   - 输入 **BGP Peer ASN**（**BGP** 对等体 **ASN**）。

     为 Colo 中的客户本地路由器输入自治系统 (AS) 编号。范围介于 1 和 4294967295 之间。
   - 根据您在上一步中创建的连接名称选择 **Location**（地点）。

     您必须已经为指定的任何地点添加了子网。
   - （可选）输入 BGP **MD5 Secret**（**MD5** 密文）。



3. 继续创建连接，直至完成。

   创建两个连接。两个连接必须位于同一区域，并且每个连接必须位于单独的区域。您可以在后面的步骤中所创建的服务连接中使用这些连接。

STEP 4 | **Push Config**（推送配置）。

提交作业完成后，刷新浏览器以查看 **Connections**（连接）下的配对密钥。

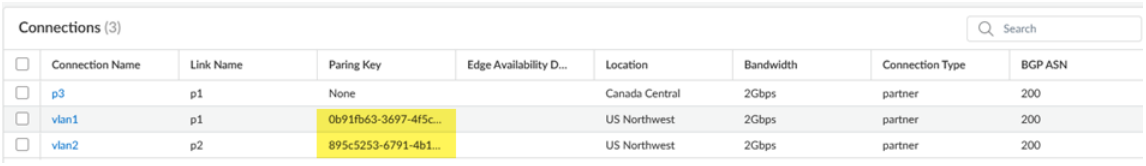
 ©2025 Palo Alto Networks, Inc.

STEP 5 | 检索 **Pairing Key**（配对密钥）并在 GCP 中完成合作伙伴互连配置。

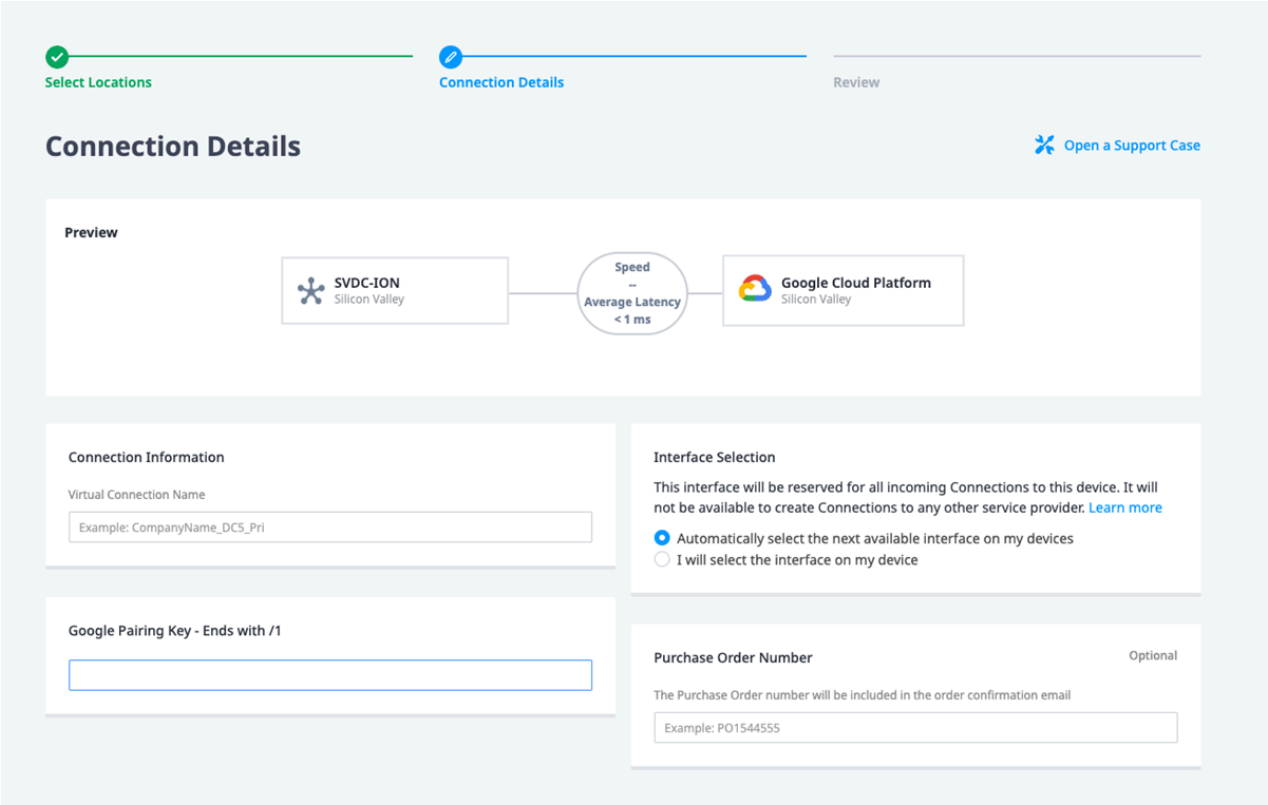
在 Colo 中设置合作伙伴互连时，将需要使用此配对密钥。

首次加入新连接时，**Connections**（连接）区域中的 **Status**（状态）显示 **Status**（状态）为 **PENDING_PARTNER**，**BGP Status**（**BGP** 状态）为 **DOWN**。要将连接状态设为 **ACTIVE**，请检索配对密钥并在 Colo 中输入连接。

1. 转到 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Colo-Connect** > **Connections**（连接），然后复制 **Pairing Key**（配对密钥）。



2. 在 Colo 中创建新的 VLAN 连接。



3. 将配对密钥粘贴到 Colo VLAN 中。

GCP 检测配对密钥的使用时间，将 VLAN 状态设为 **ACTIVE**，并生成 BGP IP 地址以供您在 Colo 中的本地路由器上进行配置。Prisma Access 使用这些 IP 在 Colo 路由器和 GCP 云路由器之间的每个关联的 VLAN 上启动 eBGP 邻接关系。

STEP 6 | 在客户 (Colo) 路由器上为 Colo-Connect 连接创建 eBGP 路由。

您需要设置 BGP 对等体关系，以确保客户路由器和云路由器之间的连接。

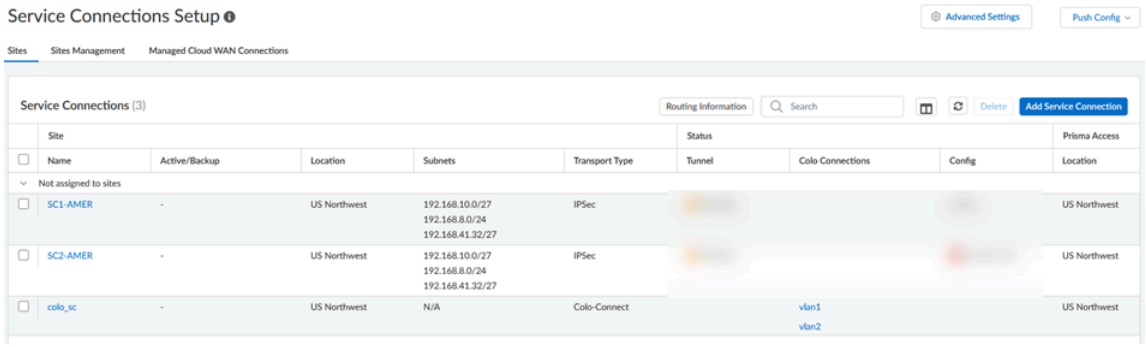
STEP 7 | 设置要用于 Colo-Connect 的服务连接。

©2025 Palo Alto Networks, Inc.

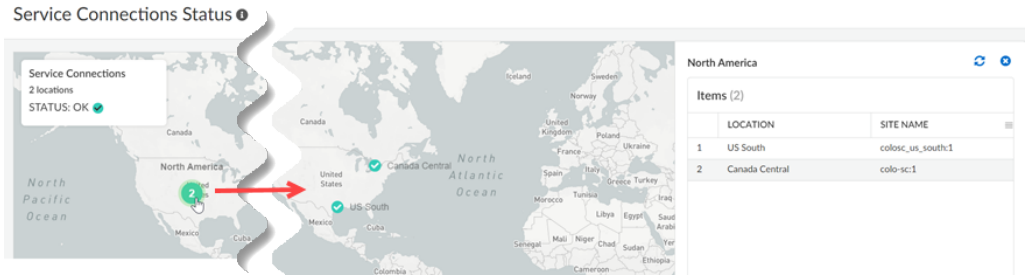
STEP 8 | **Push Config**（推送配置）。

STEP 9 | 检查 Colo-Connect 连接的状态。

1. 要检查 Colo-Connect 连接所使用的服务连接的状态，请转到 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Service Connection**（服务连接）。



2. 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**）。将 **Configuration Scope**（配置范围）设置为 **Prisma Access**。在 Prisma Access 同步状态下，为 **Service Connections**（服务连接）选择 **In Sync**（同步）状态。选择部署了 Colo-Connect 连接的区域。
   - 如果 Colo-Connect 连接和 BGP 路由均已启动，则状态显示 **OK**（正常）。
   - 如果 Colo-Connect 连接已启动但 BGP 路由未启动，则状态显示 **Warning**（警告）。
   - 如果 Colo-Connect 连接和 BGP 路由均已关闭，则状态显示 **Down**（关闭）。
   - 如果 Colo-Connect 连接关闭但 BGP 路由已启动，则状态显示 **Error**（错误）。



3. 有关更多信息，请单击区域框并查看 **Status**（状态）选项卡中的信息。

STEP 10 | 转到 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Colo Connect**，查看连接详细信息，包括 Colo-Connect 连接的配对密钥。

使用专用互连配置 Prisma Access Colo-Connect—部署

要使用专用互连配置 Prisma Access Colo-Connect，请完成以下步骤。

©2025 Palo Alto Networks, Inc.

STEP 1 | 为 Colo-Connect 连接创建子网。

您可以在后续步骤中创建的连接和服务连接中使用在此处创建的子网。

1. 在 Strata Cloud Manager 中，转到 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Colo-Connect**，然后单击齿轮图标以编辑设置。
2. 为 **Colo-Connect Subnet**（**Colo-Connect** 子网）**Add Prefix**（添加前缀），然后为其选择 Prisma Access 地点（**PA Location**（**PA** 地点））。

   输入最小子网 /28。
3. （可选）如果您计划为多个地点创建 Colo-Connect 实例，请在每个地点添加更多子网。

   每个地点只能配置一个子网。

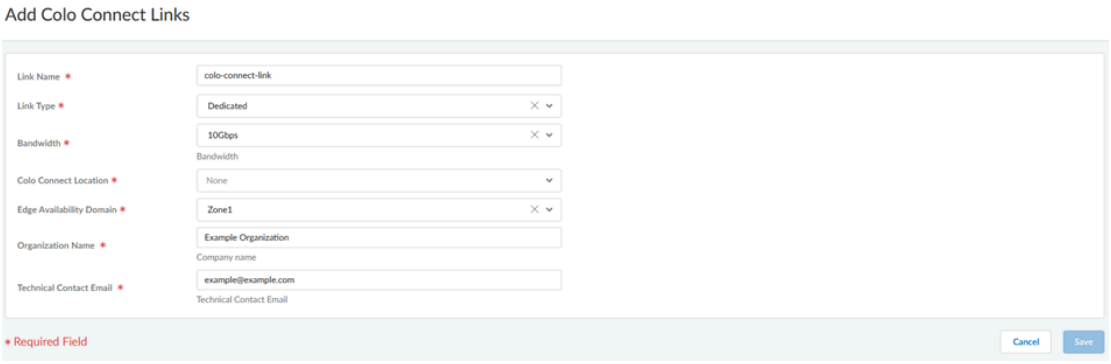
STEP 2 | 添加新的 Colo-Connect 链路（也称为互连）。

1. 转到 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Colo-Connect**，然后单击 **Add Link**（添加链路）。
2. 为链路指定唯一的 **Link Name**（链路名称）。
3. 选择 **Dedicated**（专用）互连作为 **Link Type**（链路类型）。
4. 指定其余的 Colo-Connect 链路参数。
   - 在 **Bandwidth**（带宽）中选择 **10Gbps** 或 **20Gbps**。

     如果选择 *20 Gbps*，则必须使用 LACP 将专用互连链路聚合为两个 *10 Gbps* 链路。

     指定专用互连链路的带宽并提交和推送更改后，您无法更改该带宽。
   - 从下拉列表中选择 **Colo-Connect Location**（**Colo-Connect** 地点）。

     确保选择与专用互连相同的地点。
   - 在 **Edge Availability Domain**（边缘可用性域）中选择 **Zone1** 或 **Zone2**。从用于边缘可用性域的 GCP 服务区获取此值。
   - 输入用于此链路的 **Organization Name**（组织名称）。
   - 输入您想要用于从云提供商处接收 LOA-CFA 详细信息的 **Email**（电子邮件）。
     - GCP 使用此电子邮件发送授权书和连接设施分配 (LOA-CFA)。确保将 LOA-CFA 发送给您的 Colo 提供商，以便他们可以开始安装您的连接。



 ©2025 Palo Alto Networks, Inc.

STEP 3 | 创建专用连接后，Colo 设施会测试您的连接，并通知您连接已测试完毕且可供使用。

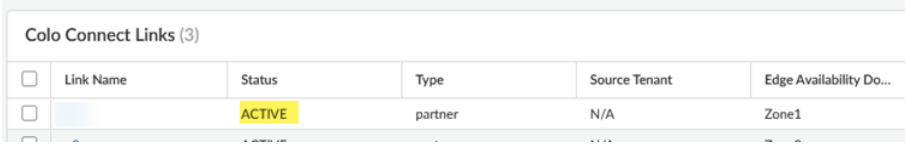
此步骤不需要 Prisma Access 配置。在 Colo 设施通知您连接已测试完毕之前，请勿在 Prisma Access 中创建 Colo-Connect 连接。

©2025 Palo Alto Networks, Inc.

STEP 4 | 为 Colo-Connect 创建连接（也称为 *VLAN* 连接）。

1. 转到 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Colo-Connect** > **Colo Connect Links**（**Colo Connect** 链路），确保专用链路的状态为“活动”。

   在专用链路的状态变为“活动”之前，您无法创建 Colo-Connect 链路。



2. 转到 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Colo-Connect**，然后单击 **Add Connection**（添加连接）。
3. 配置连接设置。
   - 为该连接输入唯一的 **Name**（名称）。
   - 根据您在上一步中配置的链路选择 **Link Name**（链路名称）。
   - （可选）输入该连接的 **VLAN ID**。

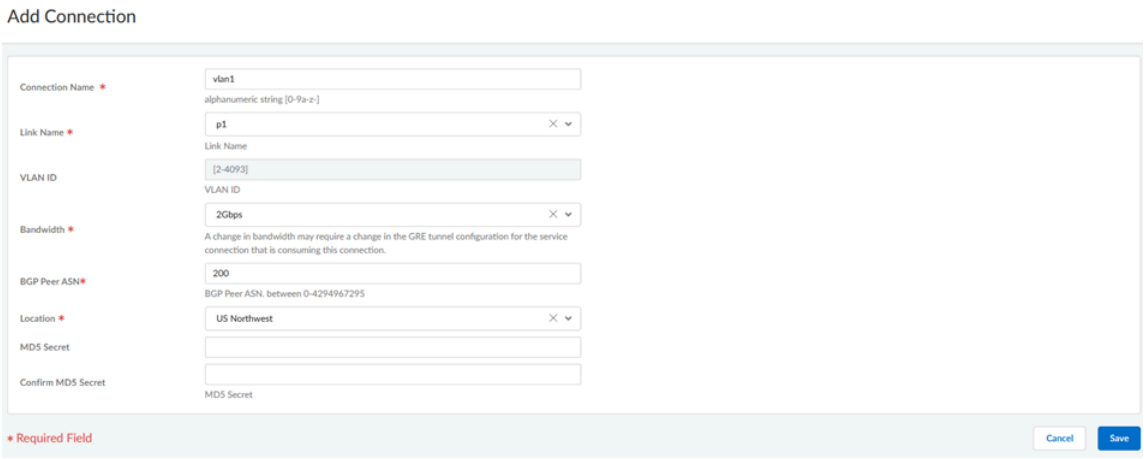
     如果您未手动输入值，则由互连供应商 (GCP) 生成 VLAN ID。
   - 选择连接的 **Bandwidth**（带宽）。

     您可以选择 **1 Gbps**、**2 Gbps**、**5 Gbps**、**10 Gbps**或 **20 Gbps**。

     如果为互连配置多个连接，请确保连接的总带宽不超过互连的带宽。例如，假设专用互连的带宽为 20 Gbps，则您可以配置 10 个连接，每个连接的带宽为 2 Gbps，但所有连接的总带宽不得超过 20 Gbps。
   - 输入 **BGP Peer ASN**（**BGP** 对等体 **ASN**）。

     为 Colo 中的客户本地路由器输入自治系统 (AS) 编号。范围介于 1 和 4294967295 之间。
   - 根据您在上一步中创建的连接名称选择 **Location**（地点）。

     您必须已经为指定的任何地点添加了子网。
   - （可选）输入 BGP **MD5 Secret**（**MD5** 密文）。



4. 继续创建连接，直至完成。

©2025 Palo Alto Networks, Inc.

创建两个连接。两个连接必须位于同一区域，并且每个连接必须位于单独的区域。您可以在后面的步骤中所创建的服务连接中使用这些连接。

STEP 5 | **Push Config**（推送配置）。

STEP 6 | 在客户路由器上配置 eBGP 路由。

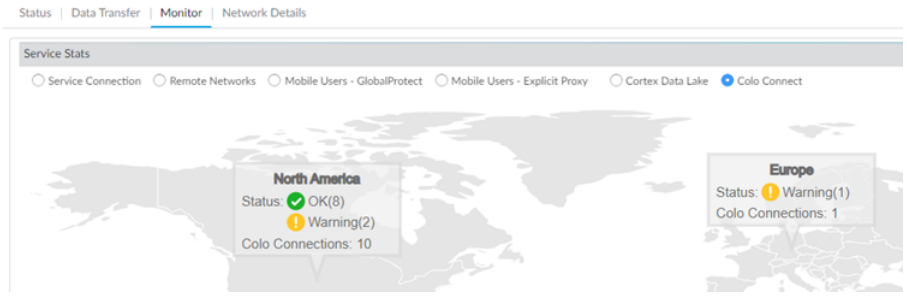
您需要设置 BGP 对等体关系，以确保客户路由器之间的连接。

STEP 7 | 设置要用于 Colo-Connect 的服务连接。

STEP 8 | **Commit and Push**（提交并推送）配置更改，确保在 **Push Scope**（推送范围）中选择 **Colo-Connect**。

STEP 9 | 检查 Colo-Connect 连接的状态。

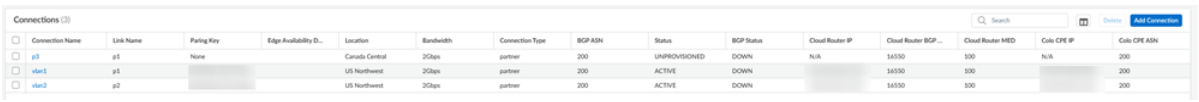
1. 要检查 Colo-Connect 连接所使用的服务连接的状态，请转到 **Manage**（管理）> **Configuration**（配置）> **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**）。将 **Configuration Scope**（配置范围）设置为 **Prisma Access**。
2. 将鼠标悬停在部署了 Colo-Connect 连接的区域上。
   - 如果 Colo-Connect 连接和 BGP 路由均已启动，则状态显示 **OK**（正常）。
   - 如果 Colo-Connect 连接已启动但 BGP 路由未启动，则状态显示 **Warning**（警告）。
   - 如果 Colo-Connect 连接和 BGP 路由均已关闭，则状态显示 **Down**（关闭）。
   - 如果 Colo-Connect 连接关闭但 BGP 路由已启动，则状态显示 **Error**（错误）。



3. 有关更多信息，请单击区域框并查看 **Status**（状态）选项卡中的信息。

STEP 10 | 查看 Colo-Connect 连接的网络详细信息，方法是转到 **Workflows**（工作流）> **Prisma Access Setup**（**Prisma Access** 设置）> **Colo-Connect** > **Connections**（连接），然后查看详细信息。

对于专用链路，**Pairing Key**（配对密钥）显示为 **N/A**（不适用）。



在客户路由器上配置 VLAN eBGP 路由。

GCP 会在部署的以下阶段为客户 (Colo) 路由器和云路由器创建 IP 地址：

- 对于合作伙伴互连，GCP 会在 Colo（例如 Equinix）使用配对密钥后创建 IP 地址。

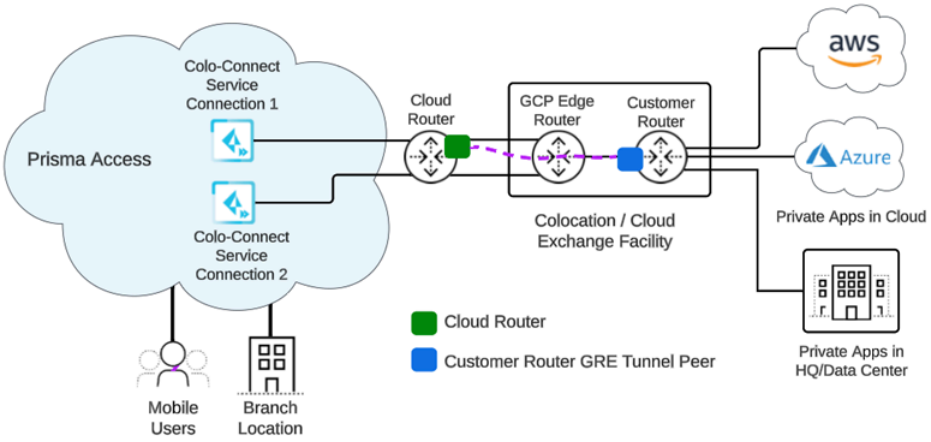
©2025 Palo Alto Networks, Inc.

- 对于专用互连，在您加入 Colo-Connect 连接（VLAN 连接）并提交和推送更改后，GCP 会创建 IP 地址。

为了确保正确路由，您必须执行以下操作：

- 将 Colo 路由器 IP 地址（Prisma Access 中的 **Colo CPE IP**）配置为本地 eBGP IP 地址
- 将云路由器 IP 地址（**Cloud Router IP**（云路由器 **IP**））配置为 Colo 路由器上的 eBGP 对等体地址。

完成后，将为 Colo 路由器和云路由器之间的连接（VLAN 连接）配置 eBGP。



创建此路由是设置 GRE 隧道路由的第一步。在服务连接配置期间设置 GRE 隧道时，即可完成 GRE 隧道路由。

使用以下步骤配置 Colo 和云路由器之间的路由。

STEP 1 | 在 Strata Cloud Manager 中创建子网、链路和连接，然后单击 **Push Config**（推送配置）。

使用特定于互连类型（合作伙伴或专用）的工作流。对于合作伙伴互连，请确保将配对密钥粘贴到 Colo VLAN 中。

STEP 2 | 转到 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Colo-Connect** > **Connections**（连接）。

 ©2025 Palo Alto Networks, Inc.

STEP 3 | 记下以下连接元素：

- **Colo CPE IP**
- 云路由器 **IP**
- 云路由器 **BGP ASN**

在以下示例中：

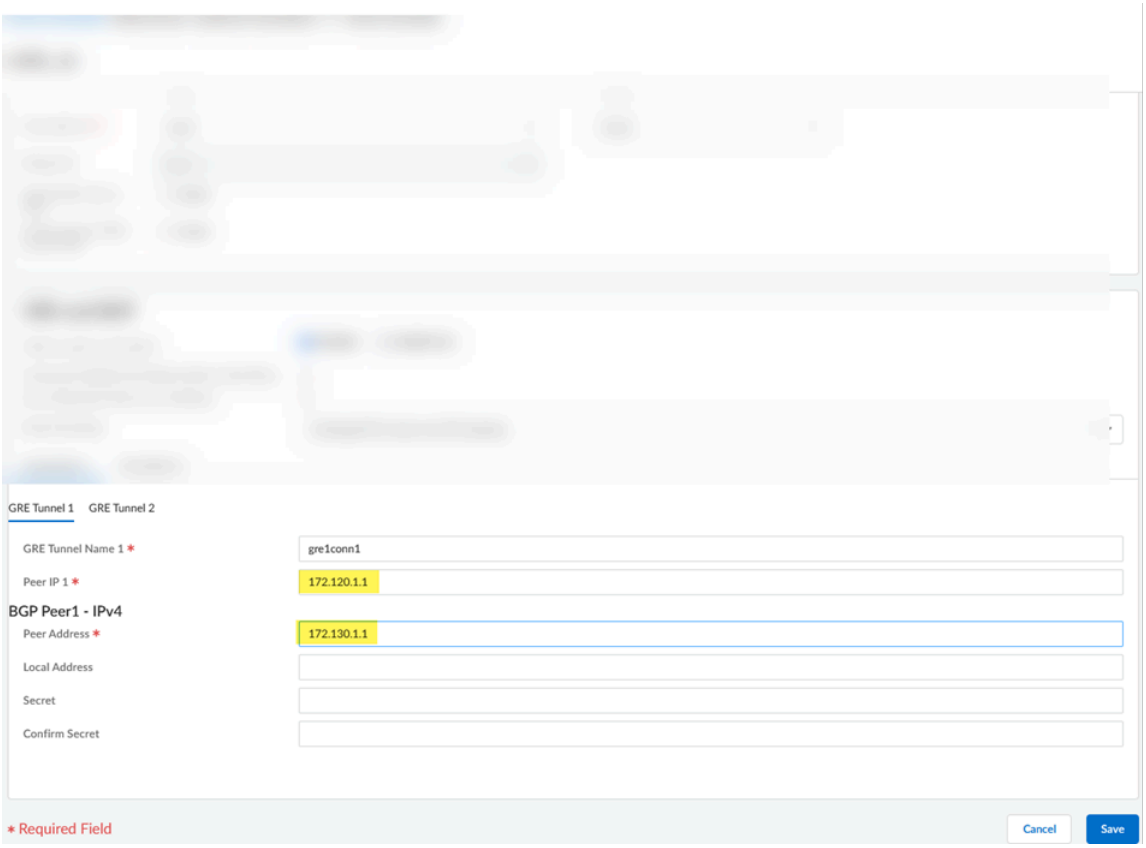
- 对于 vlan-central-1 连接，**Colo CPE IP** 为 169.254.24.170/29，**Cloud Router IP**（云路由器 **IP**）为 169.254.24.169/29，**Cloud Router BGP ASN**（云路由器 **BGP ASN**）为 16550
- 对于 vlan-central-2 连接，**Colo CPE IP** 为 169.254.120.74/29，**Cloud Router IP**（云路由器 **IP**）为 169.254.120.73/29，**Cloud Router BGP ASN**（云路由器 **BGP ASN**）为 16550。
- .



 ©2025 Palo Alto Networks, Inc.

STEP 4 | 确定设置 Colo-Connect 服务连接时将用于本地 GRE IP 地址的 IP 地址。

设置 Colo-Connect 服务连接（**Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Service Connections**（服务连接））时，您可以在 **Peer IP 1**（对等体 **IP 1**）和 **Peer IP 2**（对等体 **IP 2**）（如果需要）区域中配置这些地址。



如果您要配置服务连接以支持高达 10 Gbps 的吞吐量，请在 **Connection 1**（连接 **1**）和 **Connection 2**（连接 **2**）中各建立一个隧道，每个服务连接总共有两个隧道。

如果您要配置服务连接以支持超过 10 Gbps 的吞吐量（不超过 20 Gbps），请在 **Connection 1**（连接 **1**）和 **Connection 2**（连接 **2**）中各建立两个隧道，每个服务连接总共有四个隧道。

以下示例显示为超过 10 Gbps 的吞吐量配置的隧道，因此每个连接使用两个隧道，它们使用以下对等体 IP 地址：

- 连接 1 为 172.120.1.1
- 连接 1 为 172.130.1.1
- 连接 2 为 172.121.1.1
- 连接 2 为 172.131.1.1

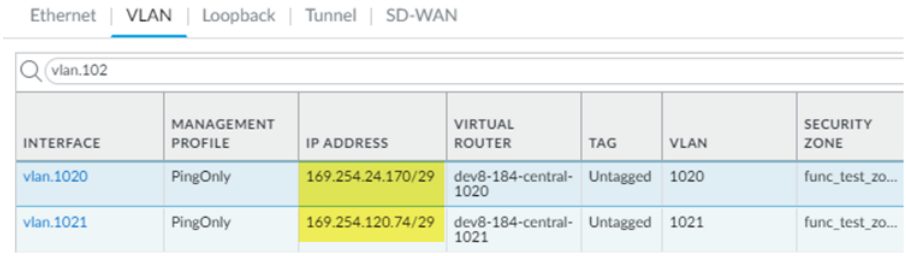
STEP 5 | 登录 Colo 路由器。

以下配置屏幕截图使用 Palo Alto Networks 新一代防火墙作为 Colo 路由器。

 ©2025 Palo Alto Networks, Inc.

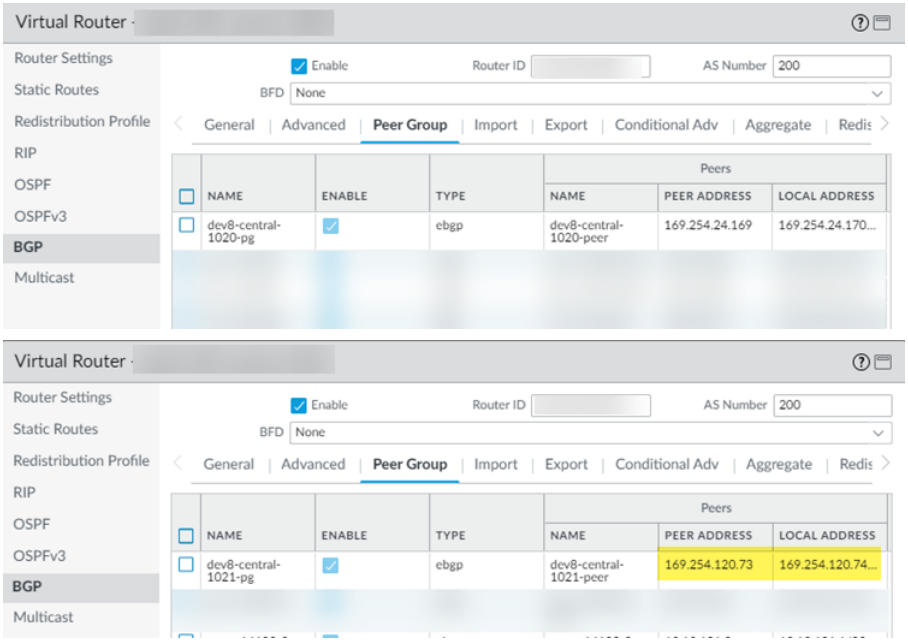
STEP 6 | 添加 VLAN 接口，将 **Colo CPE IP** 地址指定为 IP 地址。

如果要使用新一代防火墙作为 Colo 路由器，请转到 **Network**（网络） > **Interfaces**（接口） > **VLAN**，**Add**（添加）VLAN 接口，指定 **Virtual Router**（虚拟路由器）名称



STEP 7 | 将 Colo 路由器 IP 地址（**Colo CPE IP**）配置为本地 eBGP IP 地址，并将云路由器 IP 地址（**Cloud Router IP**（云路由器 **IP**））配置为 Colo 路由器上的 eBGP 对等体地址。

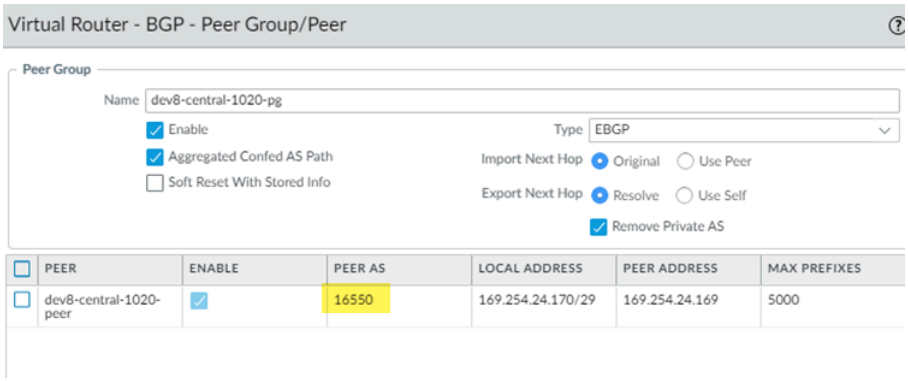
如果要使用新一代防火墙作为 Colo 路由器，请转到 **Network**（网络） > **Virtual Routers**（虚拟路由器），**Add**（添加）虚拟路由器，转到 **BGP** > **Peer Group**（对等体组），然后输入 **Colo CPE IP** 作为 **Peer Address**（对等体地址），输入 **Cloud Router IP**（云路由器 **IP**）作为 **Local Address**（本地地址）。



 ©2025 Palo Alto Networks, Inc.

STEP 8 | 将 **Cloud Router BGP ASN**（云路由器 **BGP ASN**）配置为 eBGP 对等体自治系统编号 (ASN)。

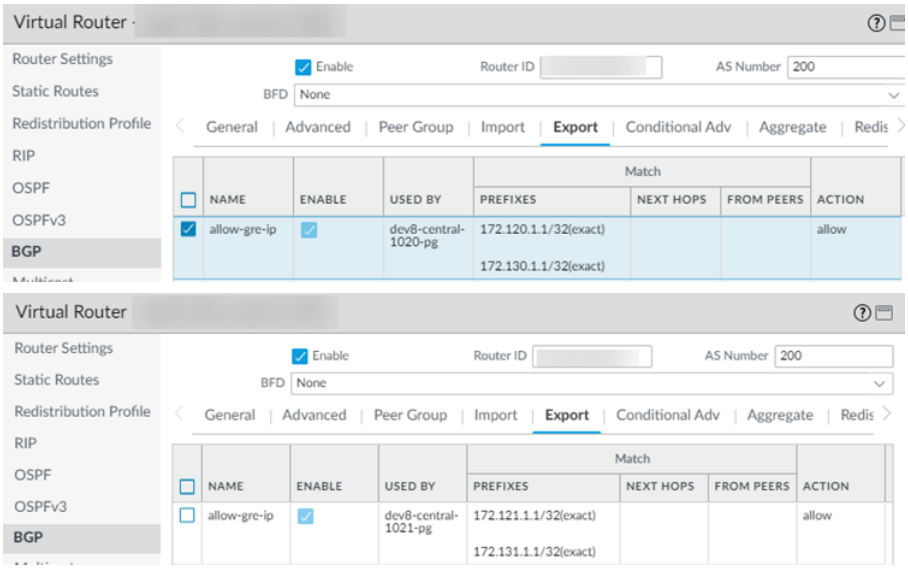
如果要使用新一代防火墙作为 Colo 路由器，请转到 **Network**（网络） > **Virtual Routers**（虚拟路由器），**Add**（添加）虚拟路由器，转到 **BGP** > **Peer Group**（对等体组），**Add**（添加）对等体组，并在 **Peer AS**（对等体 **AS**）中选择 **16500**



STEP 9 | 创建 BGP 导出策略，仅允许向云路由器对等体 IP 地址通告本地 GRE IP 地址。

由于云路由器只能接收有限数量的路由，因此您需要创建策略，以便仅将服务连接 GRE 隧道的 IP 地址之间的路由发送到云路由器。

如果要使用新一代防火墙作为 Colo 路由器，请转到 **Network**（网络） > **Virtual Routers**（虚拟路由器），**Add**（添加）虚拟路由器，转到 **BGP** > **Export**（导出），**Add**（添加）导出规则，**Match**（匹配）用作对等体 IP 地址的 IP 地址，然后创建 **Allow**（允许）**Action**（操作）。



STEP 10 | 创建 Colo-Connect 服务连接。

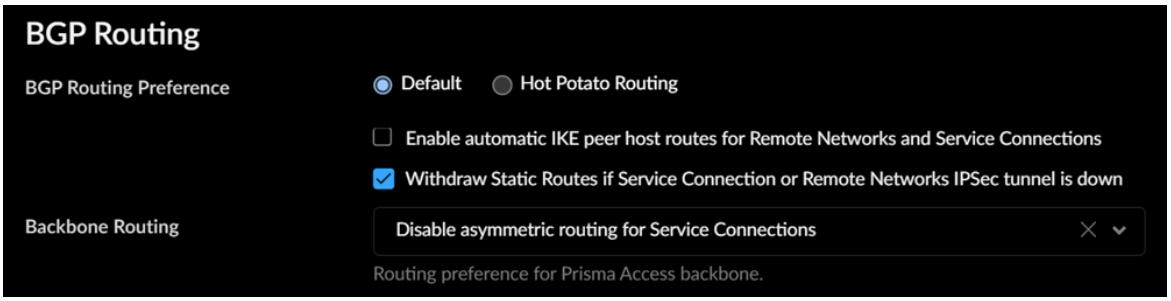
创建 Colo-Connect 服务连接

Colo-Connect 使用服务连接，但它们与 Prisma Access 服务连接的不同之处在于它们使用 GRE 隧道而不是 IPSec 隧道，并且始终使用 BGP 进行路由。要配置 Colo-Connect 服务连接，请完成以下步骤。

©2025 Palo Alto Networks, Inc.

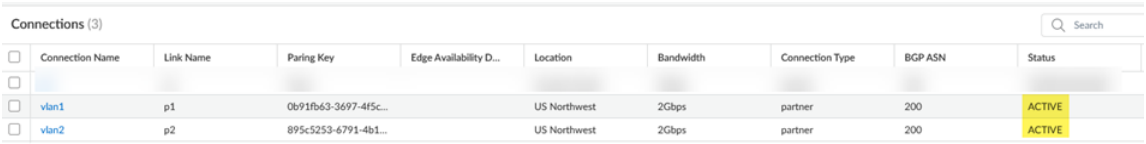
STEP 1 | 确保 Prisma Access 撤回静态路由，方法是转到 **Workflows**（工作流） > **Prisma Access** 设置 > **Service Connections**（服务连接） > **Advanced Settings**（高级设置），并且选择 **Withdraw Static Routes if Service Connection or Remote Network IPSec tunnel is down**（如果服务连接或远程网络 **IPsec** 隧道关闭，则撤回静态路由）。

选择此选项可确保如果 GRE 隧道关闭，则撤回 GRE 隧道使用的静态路由。



STEP 2 | 转到 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Colo-Connect** > **Connections**（连接）选项卡，通过检查连接的 **Status**（状态）确保连接处于 **Active**（活动）状态。

在连接的 **Status**（状态）变为 **Active**（活动）之前，您无法配置服务连接。

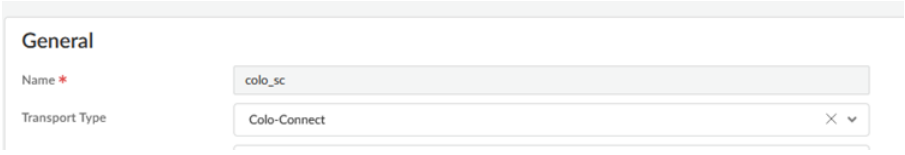


STEP 3 | 转到 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**），将配置范围设置为 **Prisma Access**。

STEP 4 | 刷新 **Prisma Access Sync Status**（**Prisma Access** 同步状态），以便在服务连接区域中配置 Colo-Connect 配置。

STEP 5 | 转到 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Service Connection**（服务连接），单击 **Add Service Connection**（添加服务连接），为其指定唯一的 **Name**（名称），然后在 **Transport Type**（传输类型）中选择 **Colo-Connect**。

确保输入的名称长度不超过 *31* 个字符；若输入 *32* 个字符或更长的名称，会导致该隧道在 *Prisma Access* 基础架构中的映射不正确。



 ©2025 Palo Alto Networks, Inc.

STEP 6 | 选择用于服务连接的两个连接（**Connection 1**（连接 **1**）和 **Connection 2**（连接 **2**））。

这些连接必须位于两个不同的服务区。



STEP 7 | 为 **Connection 1**（连接 **1**）和 **Connection 2**（连接 **2**）选择 **Active**（活动）或 **Backup**（备份）

设置服务连接时请遵循以下准则：

- 可以在以下模式下配置连接：
  - **Active**（活动）**/Active**（活动）
  - **Active**（活动）**/Backup**（备份）
  - **Backup**（备份）**/Active**（活动）

  如果在 **Backup**（备份）**/Backup**（备份）模式下配置两个连接，则配置无效且不受支持。
- 在所有模式下，连接的带宽必须是相同的。
- 连接必须位于不同的服务区。
- 您可以为服务连接指定的最大带宽是 20 Gbps。如果为连接指定 **20 Gbps** 的 **Bandwidth**（带宽），则无法在 **Active**（活动）**/Active**（活动）配置中使用该连接（必须将其设置为 **Active**（活动）**/Backup**（备份））。
- 不要在同一服务连接中混合使用专用互连和合作伙伴互连，并确保服务连接使用不同的服务区。下表列出了针对服务连接允许和不允许的配置，假设服务区、地点、带宽和角色遵循服务连接准则和要求：

连接 **1** 属于	连接 **2** 属于	是否为有效的 **Colo-Connect** 服务连接配置？
合作伙伴连接 1	合作伙伴连接 2	是
专用连接 1	专用连接 2	是
合作伙伴连接 1	合作伙伴连接 1	否
专用连接 1	专用连接 1	No
合作伙伴连接	专用连接	否

©2025 Palo Alto Networks, Inc.

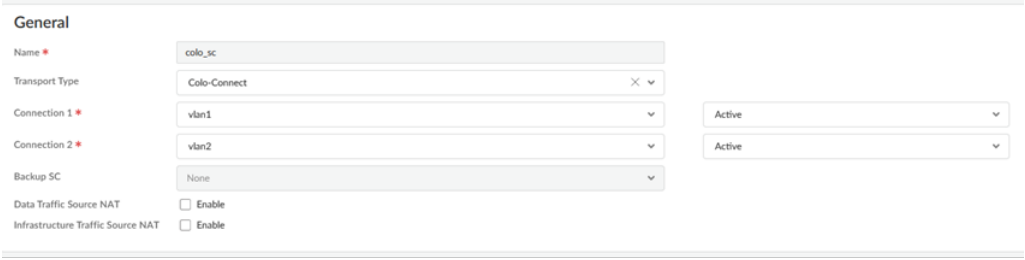
STEP 8 | （可选，仅适用于热土豆路由部署）在热土豆路由配置中，选择用作首选备份的服务连接，即 **Backup SC**（备份 **SC**）。

您只能选择已配置为 Colo-Connect 服务连接的服务连接。如果连接失败，Prisma Access 将使用您选择的备份 SC 作为首选服务连接。选择备份服务连接后，可以防止在创建了两个以上的服务连接的情况下出现非对称路由问题。

STEP 9 | （可选）为移动用户—GlobalProtect IP 池地址、基础架构子网中的 IP 地址（或两者）启用源 NAT。

您可以在一个或多个服务连接中指定一个子网，这些服务连接用于对 Prisma Access GlobalProtect 移动用户与数据中心的私有应用程序和资源之间的流量执行 NAT。

- 启用数据流量源 **NAT** — 对移动用户 IP 地址池地址执行 NAT，以确保不会向数据中心通告这些地址，并且仅会在数据中心内通告和路由您在服务连接中指定的子网。
- 启用基础架构流量源 **NAT** — 对基础架构子网中的地址执行 NAT，以确保不会向数据中心通告这些地址，并且仅会在数据中心内通告和路由您在服务连接中指定的子网。
- **IP** 池 — 指定用于在移动用户 IP 地址池、基础架构子网（或两者）上执行 NAT 的 IP 地址池。使用专用 IP (RFC 1918) 子网或路由域中可路由的合适子网，并且与移动用户—GlobalProtect IP 地址池或基础架构子网不重叠。输入介于 /25 和 /32 之间的子网。



STEP 10 | 在 **GRE and BGP**（**GRE** 和 **BGP**）区域中，配置服务连接的 GRE 隧道和 BGP 设置。

BGP 始终设置为 **Enable**（启用）。

1. （可选）从以下选项中选择：

   - 要将公司接入节点（服务连接）的 **no-export**（无导出）团体添加到客户终端设备 (CPE) 的 eBGP 对等体中的出站前缀，请将 **Add no-export community**（添加无导出团体）设置为 **Enabled Out**（启用出站）。默认情况下 **Disabled**（禁用）此功能。

     请勿在热土豆路由模式下使用此功能。

   - 要减少通过 BGP 向您的客户终端设备 (CPE) 通告的移动用户 IP 子网的数量，请选择 **Summarize Mobile User Routes before advertising**（在通告之前汇总移动用户路由）。

     默认情况下，Prisma Access 以 /24 子网的形式通告移动用户的 IP 地址池；如果将它们汇总起来，Prisma Access 会根据您指定的子网来通告该池。例如，Prisma Access 使用 /20 子网通告公共用户移动 IP 池 10.8.0.0/20，而不是在通告之前将池划分为 10.8.1.0/24、10.8.2.0/24、10.8.3.0/24 等子网。汇总这些通告可以减少 CPE 路由表

 ©2025 Palo Alto Networks, Inc.

中存储的路由数量。例如，您可以将 IP 池汇总与可接受有限数量路由的云 VPN 网关（虚拟专用网关 (VGW) 或传输网关 (TGW)）结合使用。

> 如果启用了热土豆路由并启用了路由汇总，*Prisma Access* 将不再添加 *AS-PATH*，这可能会导致非对称路由问题。在使用热土豆路由启用路由汇总之前，请确保从数据中心或总部位置返回的流量具有保证的对称返回。

- 要防止 Prisma Access BGP 对等体将路由转发到组织的网络中，请选择 **Don't Advertise Prisma Access Routes**（（不通告 **Prisma Access** 路由）。

  默认情况下，Prisma Access 通告所有 BGP 路由信息，包括本地路由以及它从其他服务连接、远程网络和移动用户子网收到的所有前缀。选中此复选框可防止 Prisma Access 发送任何 BGP 通告，但仍使用其收到的 BGP 信息从其他 BGP 邻居学习路由。

  > 如果您选择此选项，*Prisma Access* 不会发送 *BGP* 通告，因此您必须在本地设备上配置静态路由以建立返回 *Prisma Access* 的路由。

- 什么是“路由交换”设置？

2. 为使用 GRE 隧道的服务连接设置路由。
3. 在 Strata Cloud Manager 中，返回到 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Service Connection**（服务连接），为 **Connection 1**（连接 **1**）创建 GRE 隧道，方法是为 **Connection 1**（连接 **1**）输入 **GRE Tunnel Name 1**（**GRE** 隧道名称 **1**）和 **Peer IP 1**（对等体 **IP 1**），如果所需带宽超过 10 Gbps，则为连

©2025 Palo Alto Networks, Inc.

接 1 的第二个隧道输入 **GRE Tunnel Name 2**（**GRE** 隧道名称 **2**）和 **Peer IP 2**（对等体 **IP 2**）；然后，重复上述相同的步骤，为 **Connection 2**（连接 **2**）创建 GRE 隧道。

连接中的每对 GRE 隧道最多支持 10 Gbps 的带宽。如果所需带宽超过 10 Gbps，请为每个连接配置两个隧道。例如：

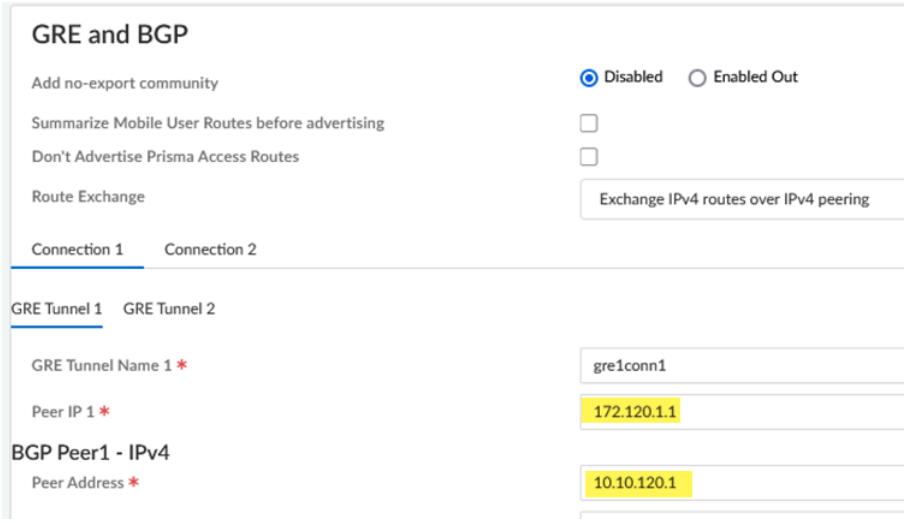
对于对等体 IP，请输入 Colo 中的本地路由器的 GRE IP 地址。

使用 IPv4 地址作为 BGP 值；不支持 IPv6。

4. 输入 BGP 对等体 1 的 **Peer Address**（对等体地址）和 **Local Address**（本地地址），如果连接 1 需要第二个隧道，则创建 BGP 对等体 2。

   对于 **Peer Address**（对等体地址），请输入 Colo 路由器的 BGP 对等体 IP 地址；对于 **Local Address**（本地地址），请输入将用于通过 GRE 隧道建立 BGP 网络的地址。

5. （可选）要配置 BGP 机密，请输入 **Secret**（机密）并 **Confirm Secret**（确认机密）值。

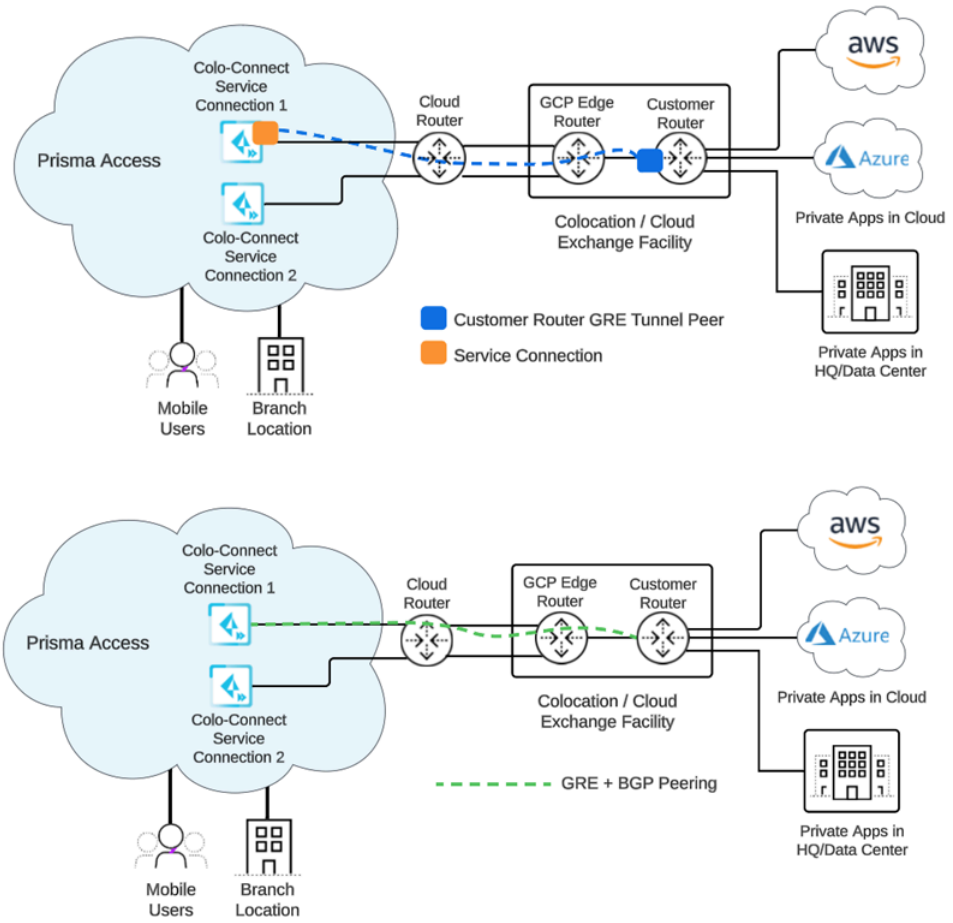


STEP 11 | **Commit and Push**（提交并推送）配置更改，确保在 **Push Scope**（推送范围）中选择 **Colo-Connect**。

为使用 GRE 隧道的服务连接设置路由

Colo 路由器将其 GRE 隧道对等体 IP 地址通告给云路由器，并从云路由器学习 GRE 隧道的子网。当您首次在客户路由器上配置通过 VLAN 的 eBGP 路由时，您已通告 GRE 隧道的本地可达性。在云路由器和 Colo 路由器相互通告并学习 Colo 子网和本地 GRE IP 地址的路由后，服务连接使用的 GRE 隧道将变为活动（开启）状态。

©2025 Palo Alto Networks, Inc.



要设置路由并将 GRE 隧道添加到服务连接，请完成以下步骤。

STEP 1 | 记下将用于 BGP 对等体 1 的 **Peer Address**（对等体地址）和 **Local Address**（本地地址）的 IP 地址，如果连接 1 需要第二个隧道，则创建 BGP 对等体 2。

以下示例使用以下对等体地址和本地地址：

- **Peer Address**（对等体地址）— 连接 1 为 10.10.120.0 和 10.10.130.1，连接 2 为 10.10.120.2 和 10.10.130.2
- **Local Address**（本地地址）— 连接 1 为 10.10.120.2 和 10.10.130.2，连接 2 为 10.10.121.2 和 10.10.131.2

STEP 2 | 记下您将在服务连接中用于 **Peer IP 1**（对等体 **IP 1**）和 **Peer IP 2**（对等体 **IP 2**）地址（如果需要）的 IP 地址。

您可以使用这些 IP 地址创建拒绝策略，以防止将本地 GRE IP 地址通告到 Colo-Connect 服务连接。

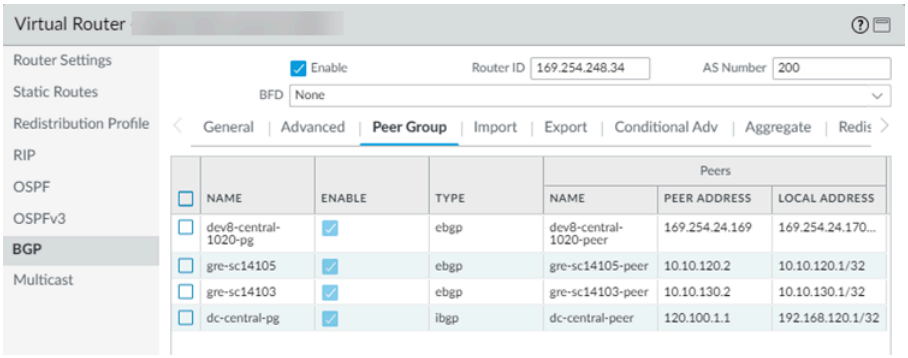
本文档中的所有示例均使用以下 IP 地址：

- 连接 1 为 172.120.1.1
- 连接 2 为 172.121.1.1

©2025 Palo Alto Networks, Inc.

STEP 3 | 为对等体和本地 IP 地址配置对等体组。

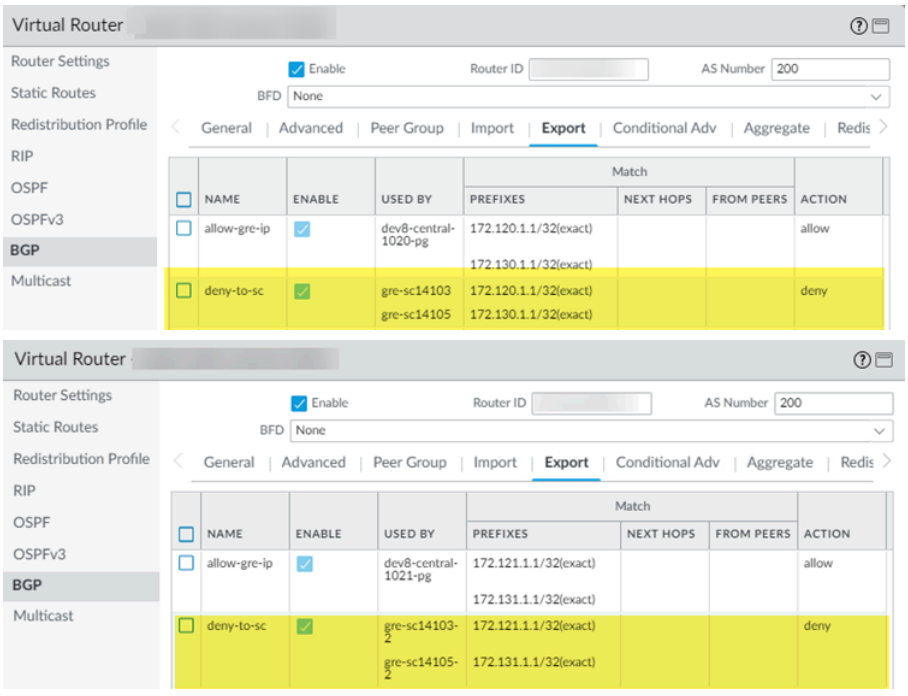
如果要使用新一代防火墙作为 Colo 路由器，请转到 **Network**（网络） > **Virtual Routers**（虚拟路由器），**Add**（添加）虚拟路由器，转到 **BGP** > **Peer Group**（对等体组），然后在 **Peer Address**（对等体地址）中输入对等体地址，在 **Local Address**（本地地址）中输入 **Local Address**（本地地址）。



STEP 4 | 创建 BGP 导出策略以拒绝您配置的对等体 IP 地址（172.120.1.1、172.130.1.1、172.121.1.1 和 172.131.1.1），并将其应用于您创建的对等组。

此导出策略在本地 GRE 隧道对等体 IP 地址上放置 DENY 规则，并允许将所有其他路由通告到该服务连接。

如果要使用新一代防火墙作为 Colo 路由器，请转到 **Network**（网络） > **Virtual Routers**（虚拟路由器），**Add**（添加）虚拟路由器，转到 **BGP** > **Export**（导出），**Add**（添加）导出规则，**Match**（匹配）用作对等体 IP 地址的 IP 地址，然后创建 **Deny**（拒绝）**Action**（操作）。



 ©2025 Palo Alto Networks, Inc.

增加或减少 Colo-Connect 服务连接的带宽

配置服务连接时，可以根据与其关联的连接（VLAN 连接）配置带宽。为每个服务连接分配两个连接，然后为每个连接分配一个或两个 GRE 隧道。

尽管每个 Colo-Connect 服务连接最多支持 20 Gbps 的带宽，但服务连接中的每个 GRE 隧道都支持 10 Gbps 的带宽。因此，您可能必须添加或删除 Colo-Connect 服务连接中的 GRE 隧道，若更改链路中的总带宽，可能会导致服务连接带宽高于或低于 10 Gbps。

增加 Colo-Connect 服务连接的带宽

要将现有服务连接的带宽增加到 10 Gbps 以上，请完成以下步骤：

STEP 1 | 转到 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Colo-Connect**。

STEP 2 | 选择与服务连接相关联的 **Link Name**（链路名称）。

STEP 3 | 增加链路（互连）的 **Bandwidth**（带宽）。

STEP 4 | **Push Config**（推送配置）。

STEP 5 | 转到 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Service Connection**（服务连接）。

STEP 6 | 将额外的 GRE 隧道添加到 Colo-Connect 服务连接。

STEP 7 | **Push Config**（推送配置）。

STEP 8 | 将 GRE 本地（对等体）IP 地址添加到 GRE 隧道的 VLAN eBGP 路由和服务连接路由的导出策略中。

减少 Colo-Connect 服务连接的带宽

要将现有服务连接的带宽减少到 10 Gbps 以上，请完成以下步骤：

STEP 1 | 转到 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Colo-Connect**。

STEP 2 | 选择与服务连接相关联的 **Link Name**（链路名称）。

STEP 3 | 减少链路（互连）的 **Bandwidth**（带宽）。

STEP 4 | **Push Config**（推送配置）。

您无需重新配置服务连接以删除额外的 GRE 隧道；当您在服务连接推送范围内提交并推送更改时，Prisma Access 会检测并降低链路的带宽，然后删除额外的隧道。

删除 Colo-Connect 连接

要删除 Colo-Connect 连接，请按照与配置相反的顺序完成以下步骤：

STEP 1 | 转到 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Service Connections**（服务连接），选择与该连接关联的服务连接，然后单击 **Delete**（删除）即可删除该服务连接。

©2025 Palo Alto Networks, Inc.

STEP 2 | **Push Config**（推送配置）。

STEP 3 | 转到 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Colo-Connect**，在 **Onboarding**（加入）部分中选择 **Connection Name**（连接名称），然后单击 **Delete**（删除）即可删除与该连接关联的 Colo-Connect 连接。

STEP 4 | 选择 **Link Name**（链路名称），单击 **Delete**（删除）即可删除 Colo-Connect 链路。

STEP 5 | 删除 GRE 隧道的 VLAN eBGP 路由和服务连接路由的导出策略中的 GRE 本地（对等体）IP 地址。

配置 Prisma Access Colo-Connect (Panorama)

使用合作伙伴互连配置 Prisma Access Colo-Connect—部署

要使用合作伙伴互连配置 Prisma Access Colo-Connect，请完成以下步骤。

STEP 1 | 为 Colo-Connect 连接创建子网。

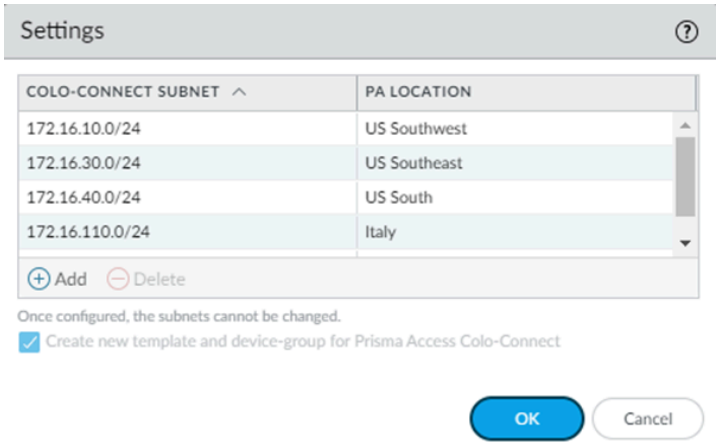
您可以在后续步骤中创建的连接和服务连接中使用在此处创建的子网。

1. 转到 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Colo-Connect**，然后单击齿轮图标以编辑设置。
2. **Add**（添加）（**Colo-Connect** 子网），然后为其选择 Prisma Access 地点（**PA Location**（**PA** 地点））。

   输入最小子网 /28。
3. （可选）如果您计划为多个地点创建 Colo-Connect 实例，请在每个地点添加更多子网。

   您可以为每个地点配置一个子网。
4. 选择 **Create new templates and device-group for Prisma Access Colo-Connect**（为 **Prisma Access Colo-Connect** 创建新模板和设备组）。

   首次配置 Colo-Connect 部署时，选中此复选框，以便为 Colo-Connect 创建模板和设备组（分别为 Colo_Connect_Template 和 Colo_Connect_Device_Group）。创建这些模板和设备组后，此复选框将显示为灰色。



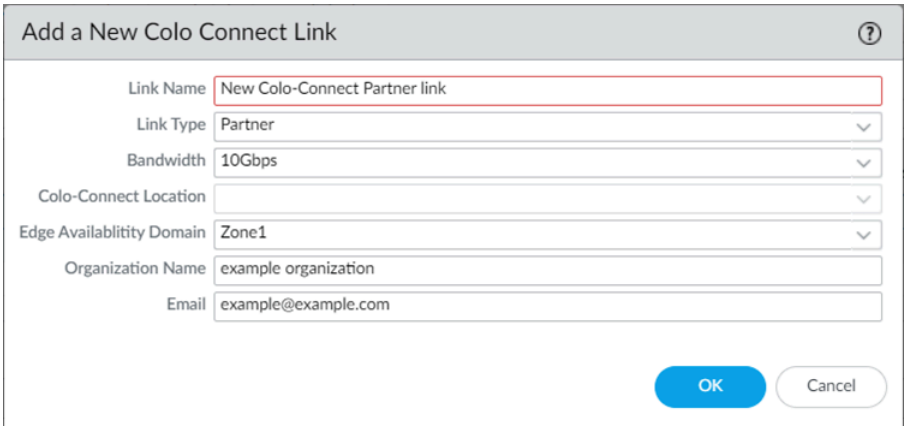
 ©2025 Palo Alto Networks, Inc.

STEP 2 | 添加新的 Colo-Connect 链路（也称为互连）。

1. 转到 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Colo-Connect** > **Colo Connect Link**（**Colo Connect** 链路），然后 **Add**（添加）Colo-Connect 链路。
2. 为链路指定唯一的 **Link Name**（链路名称）。
3. 选择 **Partner**（合作伙伴）互连。

   您不需要输入 **VLAN ID**，当 Colo 使用配对密钥完成 VLAN 连接的配置时，它会提供一个 VLAN ID。
4. 指定其余的 Colo-Connect 链路参数。
   - 在 **Bandwidth**（带宽）中选择 **10Gbps** 或 **20Gbps**。

     指定专用互连链路的带宽并提交和推送更改后，您无法更改该带宽。
   - 在 **Edge Availability Domain**（边缘可用性域）中选择 **Zone1** 或 **Zone2**。从用于边缘可用性域的 GCP 服务区获取此值。
   - 输入用于此链路的 **Organization Name**（组织名称）。
   - 输入用于此链路的 **Email**（电子邮件）。可接受任何电子邮件地址。



 ©2025 Palo Alto Networks, Inc.

STEP 3 | 为 Colo-Connect 创建连接（也称为 *VLAN* 连接）。

1. 转到 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Colo-Connect** > **Onboarding**（加入），然后 **Add**（添加）新连接。
2. 配置连接设置。
   - 为该连接输入唯一的 **Name**（名称）。
   - 根据您在上一步中配置的链路选择 **Link Name**（链路名称）。
   - 选择连接的 **Bandwidth**（带宽）。

     您可以选择 **1 Gbps**、**2 Gbps**、**5 Gbps**、**10 Gbps**或 **20 Gbps**。

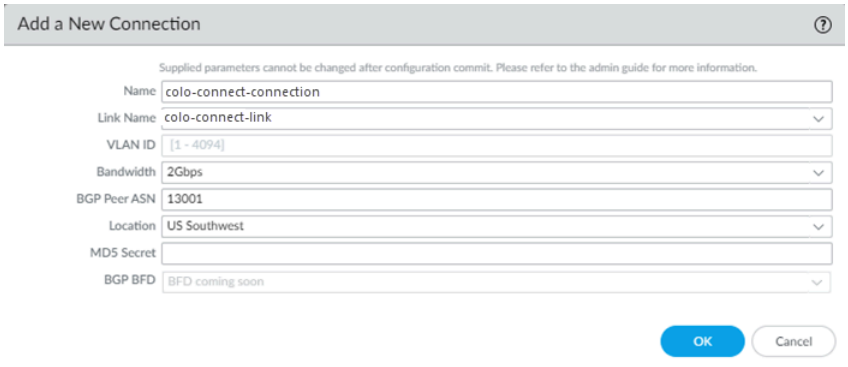
     如果为互连配置多个连接，请确保连接的总带宽不超过互连的带宽。例如，假设合作伙伴互连的带宽为 10 Gbps，则您可以配置 10 个连接，每个连接的带宽为 1 Gbps，但所有连接的总带宽不得超过 10 Gbps。

     如果您的部署需要超过 *16* 个连接，请联系您的 *Palo Alto Networks* 客户团队，他们将提交 *SRE* 案例来满足请求。
   - 输入 **BGP Peer ASN**（**BGP** 对等体 **ASN**）。

     为 Colo 中的客户本地路由器输入自治系统 (AS) 编号。范围介于 1 和 4294967295 之间。
   - 根据您在上一步中创建的连接名称选择 **Location**（地点）。

     您必须已经为指定的任何地点添加了子网。
   - （可选）输入 BGP **MD5 Secret**（**MD5** 密文）。

     忽略 ***BGP BFD*** 字段；它是为未来的 *Colo-Connect* 版本保留的字段。



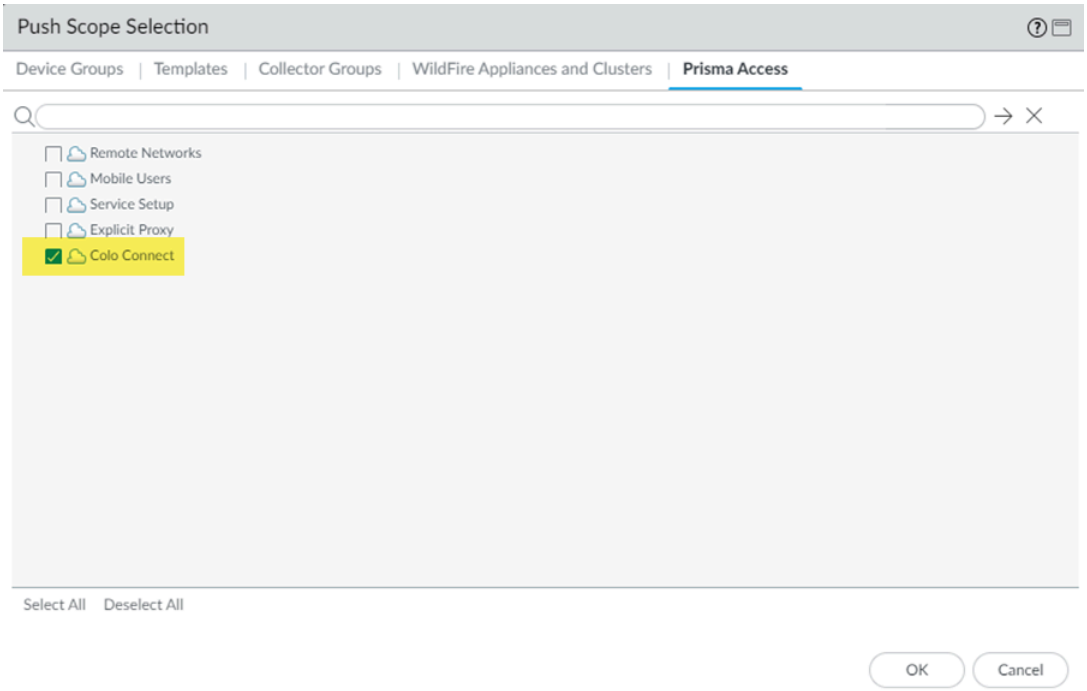
3. 继续创建连接，直至完成。

   您必须创建两个连接。两个连接必须位于同一区域，并且每个连接必须位于单独的区域。您可以在后面的步骤中所创建的服务连接中使用这些连接。

©2025 Palo Alto Networks, Inc.

STEP 4 | 提交并推送更改。

1. 转到 **Commit**（提交） > **Commit and Push**（提交并推送）。
2. **Edit Selections**（编辑选择），确保在推送范围中选择了 Colo-Connect。



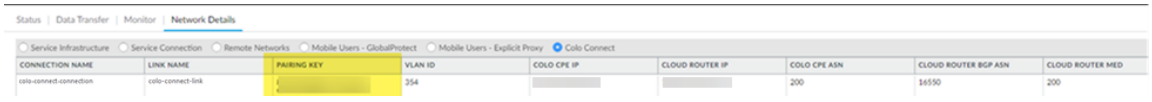
3. 单击 **OK**（确定）保存对推送范围所作的更改。
4. **Commit and Push**（提交并推送）更改。

STEP 5 | 检索 **Pairing Key**（配对密钥）并在 GCP 中完成合作伙伴互连配置。

在 Colo 中设置合作伙伴互连时，将需要使用此配对密钥。

首次加入新连接时，Colo-Connect 加入区域中的 **Status**（状态）显示 **PENDING_PARTNER**，**BGP Status**（**BGP** 状态）显示 **DOWN**。要将连接状态设为 **ACTIVE**，请检索配对密钥并在 Colo 中输入连接。

1. 转到 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息） > **Colo Connect**，然后复制 **Pairing Key**（配对密钥）。



2. 在 Colo 中创建新的 VLAN 连接（例如 Equinix）。
3. 将配对密钥粘贴到 Colo VLAN 中。

   GCP 检测配对密钥的使用时间，将 VLAN 状态设为 **ACTIVE**，并生成 BGP IP 地址以供您在 Colo 中的本地路由器上进行配置。这些操作在 Colo 路由器和 GCP 云路由器之间的 VLAN 上启动 eBGP 路由。

STEP 6 | 在客户 (Colo) 路由器上为 Colo-Connect 连接创建 eBGP 路由。

您需要设置 BGP 对等体关系，以确保客户路由器和云路由器之间的连接。

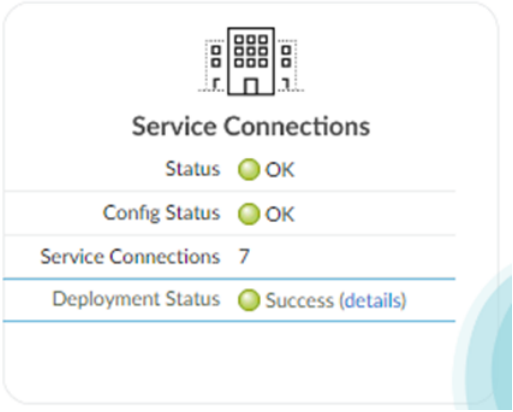
 ©2025 Palo Alto Networks, Inc.

STEP 7 | 设置要用于 Colo-Connect 的服务连接。

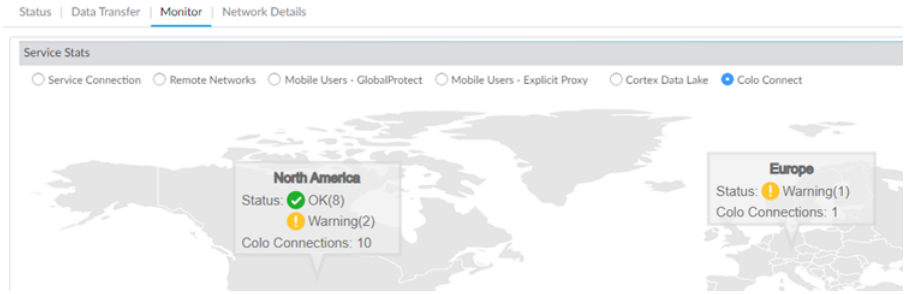
STEP 8 | **Commit and Push**（提交并推送）配置更改，确保在 **Push Scope**（推送范围）中选择 **Colo-Connect**。

STEP 9 | 检查 Colo-Connect 连接的状态。

1. 要检查 Colo-Connect 连接所使用的服务连接的状态，请转到 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > > **Colo Connect** > **Monitor**（监控）



2. 将鼠标悬停在部署了 Colo-Connect 连接的区域上。
   - 如果 Colo-Connect 连接和 BGP 路由均已启动，则状态显示 **OK**（正常）。
   - 如果 Colo-Connect 连接已启动但 BGP 路由未启动，则状态显示 **Warning**（警告）。
   - 如果 Colo-Connect 连接和 BGP 路由均已关闭，则状态显示 **Down**（关闭）。
   - 如果 Colo-Connect 连接关闭但 BGP 路由已启动，则状态显示 **Error**（错误）。



3. 有关更多信息，请单击区域框并查看 **Status**（状态）选项卡中的信息。

STEP 10 | 查看 Colo-Connect 连接的网络详细信息（包括配对密钥），方法是转到 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息） > **Colo Connect**，然后查看以下字段中的详细信息。

使用专用互连配置 Prisma Access Colo-Connect—部署

要使用专用互连配置 Prisma Access Colo-Connect，请完成以下步骤。

©2025 Palo Alto Networks, Inc.

STEP 1 | 为 Colo-Connect 连接创建子网。

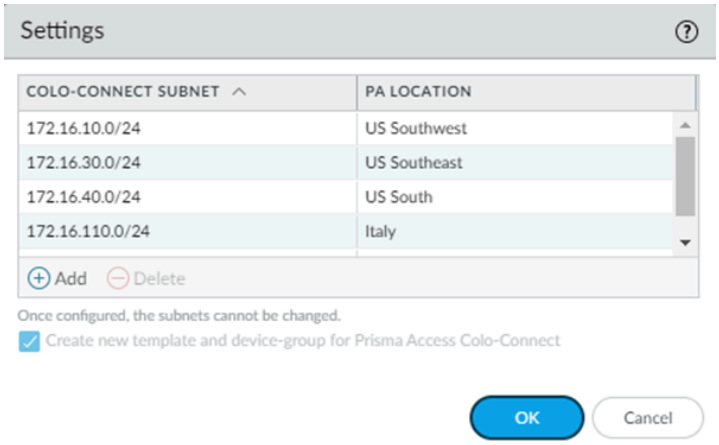
您可以在后续步骤中创建的连接和服务连接中使用在此处创建的子网。

1. 在管理 Prisma Access 的 Panorama 中，转到 **Panorama** > **Cloud Services**云服务） > **Configuration**（配置） > **Colo-Connect**，然后单击齿轮以编辑设置。
2. **Add**（添加）（**Colo-Connect** 子网），然后为其选择 Prisma Access 地点（**PA Location**（**PA** 地点））。

   输入最小子网 /28。
3. （可选）如果您计划为多个地点创建 Colo-Connect 实例，请在每个地点添加更多子网。

   每个地点只能配置一个子网。
4. 选择 **Create new templates and device-group for Prisma Access Colo-Connect**（为 **Prisma Access Colo-Connect** 创建新模板和设备组）。

   首次配置 Colo-Connect 部署时，选中此复选框，以便为 Colo-Connect 创建模板和设备组（分别为 Colo_Connect_Template 和 Colo_Connect_Device_Group）。创建这些模板和设备组后，此复选框将显示为灰色。



 ©2025 Palo Alto Networks, Inc.

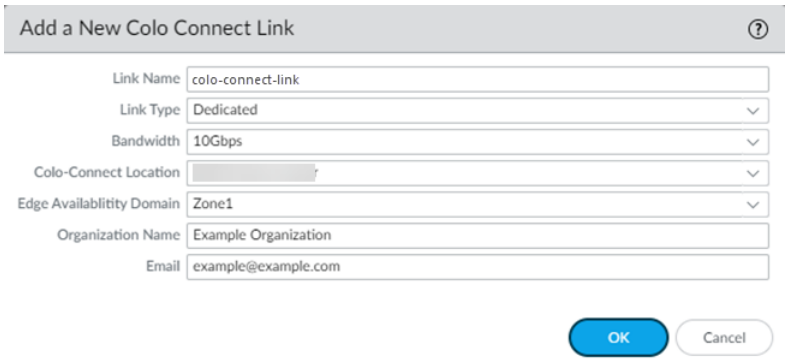
STEP 2 | 添加新的 Colo-Connect 链路（也称为互连）。

1. 转到 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Colo-Connect** > **Colo Connect Link**（**Colo Connect** 链路），然后 **Add**（添加）Colo-Connect 链路。
2. 为链路指定唯一的 **Link Name**（链路名称）。
3. 选择 **Dedicated**（专用）互连。
4. 指定其余的 Colo-Connect 链路参数。
   - 在 **Bandwidth**（带宽）中选择 **10Gbps** 或 **20Gbps**。

     如果选择 *20 Gbps*，则必须使用 LACP 将专用互连链路聚合为两个 *10 Gbps* 链路。

     指定专用互连链路的带宽并提交和推送更改后，您无法更改该带宽。
   - 从下拉列表中选择 **Colo-Connect Location**（**Colo-Connect** 地点）。

     确保选择与专用互连相同的地点。
   - 在 **Edge Availability Domain**（边缘可用性域）中选择 **Zone1** 或 **Zone2**。从用于边缘可用性域的 GCP 服务区获取此值。
   - 输入用于此链路的 **Organization Name**（组织名称）。
   - 输入您想要用于从云提供商处接收 LOA-CFA 详细信息的 **Email**（电子邮件）。
     - GCP 使用此电子邮件发送授权书和连接设施分配 (LOA-CFA)。确保将 LOA-CFA 发送给您的 Colo 提供商，以便他们可以开始安装您的连接。



STEP 3 | 创建专用连接后，Colo 设施会测试您的连接，并通知您连接已测试完毕且可供使用。

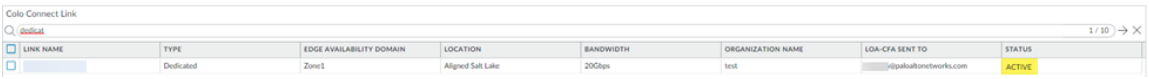
此步骤不需要 Prisma Access 配置。在 Colo 设施通知您连接已测试完毕之前，请勿在 Prisma Access 中创建 Colo-Connect 连接。

©2025 Palo Alto Networks, Inc.

STEP 4 | 为 Colo-Connect 创建连接（也称为 *VLAN* 连接）。

1. 转到 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Colo-Connect** > **Colo Connect Link**（**Colo Connect** 链路），确保专用链路的状态为“活动”。

   在专用链路的状态变为“活动”之前，您无法创建 Colo-Connect 链路。



2. 转到 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Colo-Connect** > **Onboarding**（加入），然后 **Add**（添加）新连接。
3. 配置连接设置。
   - 为该连接输入唯一的 **Name**（名称）。
   - 根据您在上一步中配置的链路选择 **Link Name**（链路名称）。
   - （可选）输入该连接的 **VLAN ID**。

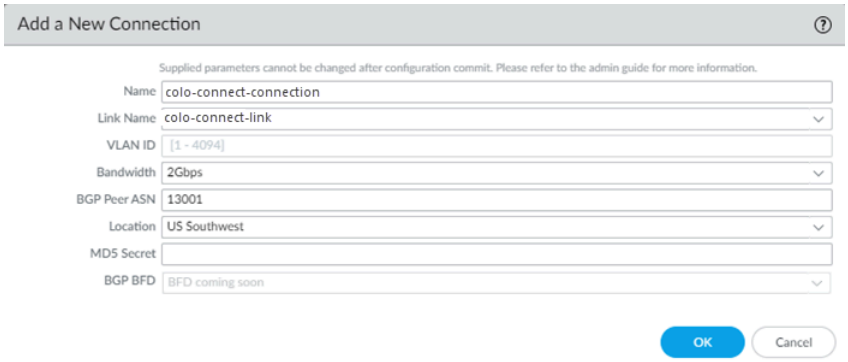
     如果您未手动输入值，则由互连供应商 (GCP) 生成 VLAN ID。
   - 选择连接的 **Bandwidth**（带宽）。

     您可以选择 **1 Gbps**、**2 Gbps**、**5 Gbps**、**10 Gbps**或 **20 Gbps**。

     如果为互连配置多个连接，请确保连接的总带宽不超过互连的带宽。例如，假设专用互连的带宽为 20 Gbps，则您可以配置 10 个连接，每个连接的带宽为 2 Gbps，但所有连接的总带宽不得超过 20 Gbps。
   - 输入 **BGP Peer ASN**（**BGP** 对等体 **ASN**）。

     为 Colo 中的客户本地路由器输入自治系统 (AS) 编号。范围介于 1 和 4294967295 之间。
   - 根据您在上一步中创建的连接名称选择 **Location**（地点）。

     您必须已经为指定的任何地点添加了子网。
   - （可选）输入 BGP **MD5 Secret**（**MD5** 密文）。



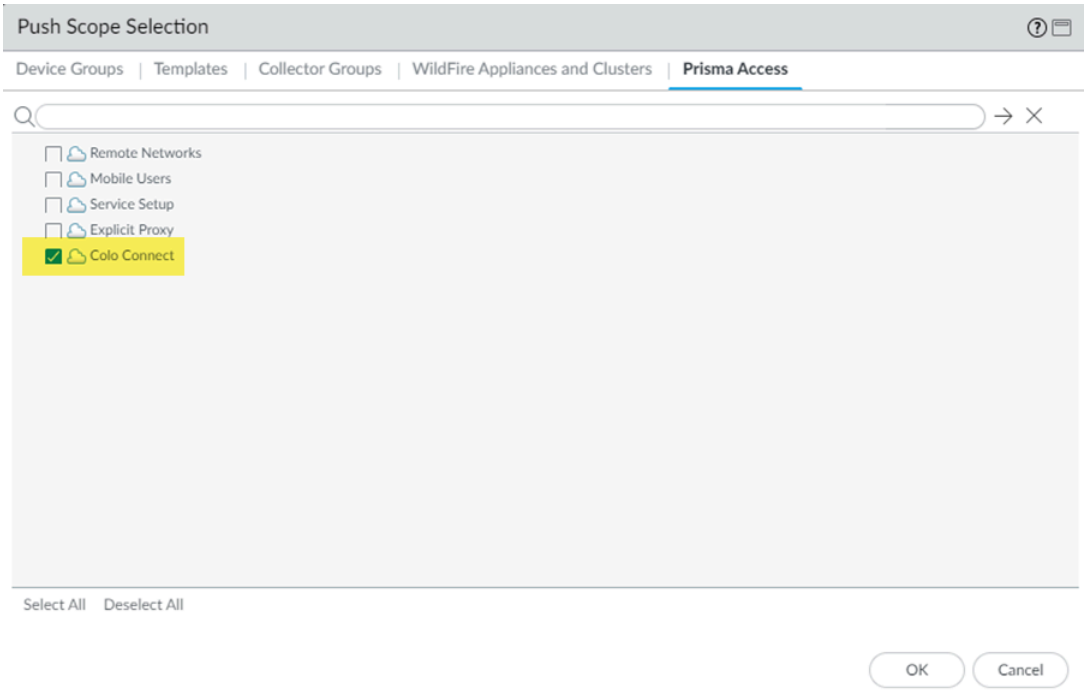
4. 继续创建连接，直至完成。

   您必须创建两个连接。两个连接必须位于同一区域，并且每个连接必须位于单独的区域。您可以在后面的步骤中所创建的服务连接中使用这些连接。

 ©2025 Palo Alto Networks, Inc.

STEP 5 | 提交并推送更改。

1. 转到 **Commit**（提交） > **Commit and Push**（提交并推送）。
2. **Edit Selections**（编辑选择），确保在推送范围中选择了 Colo-Connect。



3. 单击 **OK**（确定）保存对推送范围所作的更改。
4. **Commit and Push**（提交并推送）更改。

STEP 6 | 在客户路由器上配置 eBGP 路由。

您需要设置 BGP 对等体关系，以确保客户路由器之间的连接。

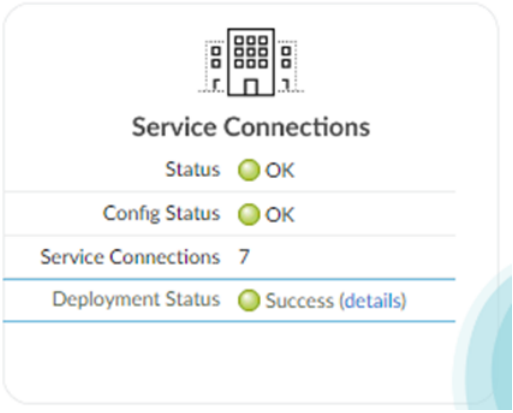
STEP 7 | 设置要用于 Colo-Connect 的服务连接。

STEP 8 | **Commit and Push**（提交并推送）配置更改，确保在 **Push Scope**（推送范围）中选择 **Colo-Connect**。

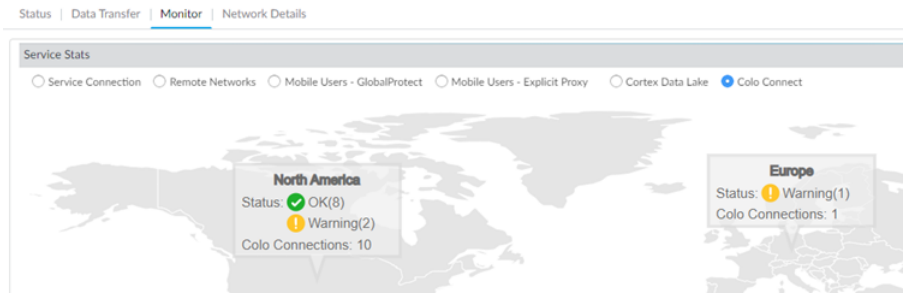
©2025 Palo Alto Networks, Inc.

STEP 9 | 检查 Colo-Connect 连接的状态。

1. 要检查 Colo-Connect 连接所使用的服务连接的状态，请转到 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > > **Colo Connect** > **Monitor**（监控）。



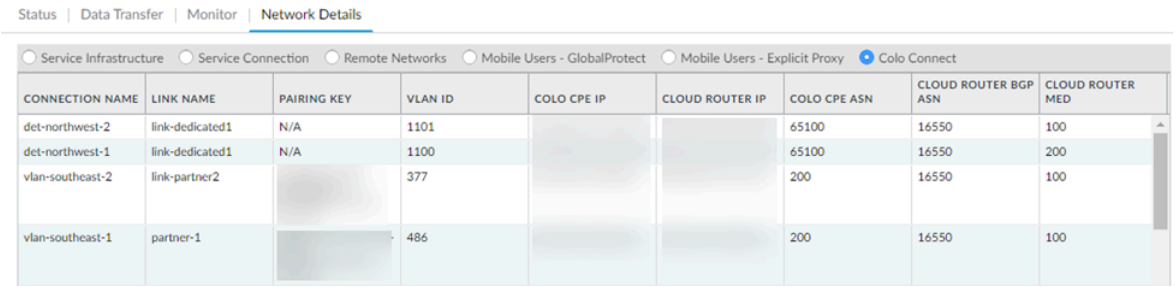
2. 将鼠标悬停在部署了 Colo-Connect 连接的区域上。
   - 如果 Colo-Connect 连接和 BGP 路由均已启动，则状态显示 **OK**（正常）。
   - 如果 Colo-Connect 连接已启动但 BGP 路由未启动，则状态显示 **Warning**（警告）。
   - 如果 Colo-Connect 连接和 BGP 路由均已关闭，则状态显示 **Down**（关闭）。
   - 如果 Colo-Connect 连接关闭但 BGP 路由已启动，则状态显示 **Error**（错误）。



3. 有关更多信息，请单击区域框并查看 **Status**（状态）选项卡中的信息。

STEP 10 | 查看 Colo-Connect 连接的网络详细信息，方法是转到 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息） > **Colo Connect**，然后查看详细信息。

对于专用链路，**Pairing Key**（配对密钥）显示为 **N/A**（不适用）。



 ©2025 Palo Alto Networks, Inc.

在客户路由器上配置 VLAN eBGP 路由。

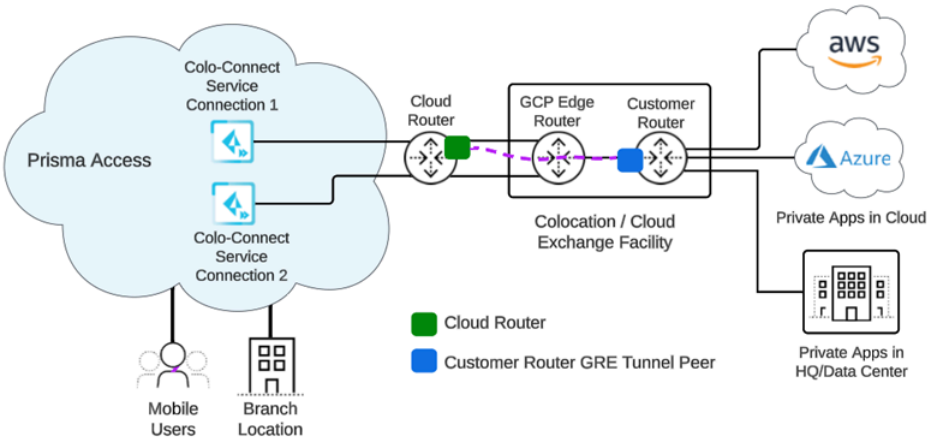
GCP 会在部署的以下阶段为客户 (Colo) 路由器和云路由器创建 IP 地址：

- 对于合作伙伴互连，GCP 会在 Colo（例如 Equinix）使用配对密钥后创建 IP 地址。
- 对于专用互连，在您加入 Colo-Connect 连接（VLAN 连接）并提交和推送更改后，GCP 会创建 IP 地址。

为了确保正确路由，您必须执行以下操作：

- 将 Colo 路由器 IP 地址（Prisma Access 中的 **Colo CPE IP**）配置为本地 VLAN IP 地址和本地 eBGP IP 地址
- 将云路由器 IP 地址（**Cloud Router IP**（云路由器 **IP**））配置为 Colo 路由器上的 eBGP 对等体地址。

完成后，将为 Colo 路由器和云路由器之间的连接（VLAN 连接）配置 eBGP。



创建此路由是设置 GRE 隧道路由的第一步。在服务连接配置期间设置 GRE 隧道时，即可完成 GRE 隧道路由。

使用以下步骤配置 Colo 和云路由器之间的路由。

STEP 1 | 在管理 Prisma Access 的 Panorama 中，创建子网、链路和连接，然后 **Commit and Push**（提交并推送）更改。

使用特定于互连类型（合作伙伴或专用）的工作流。对于合作伙伴互连，请确保将配对密钥粘贴到 Colo VLAN 中。

STEP 2 | 转到 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息） > **Colo Connect**。

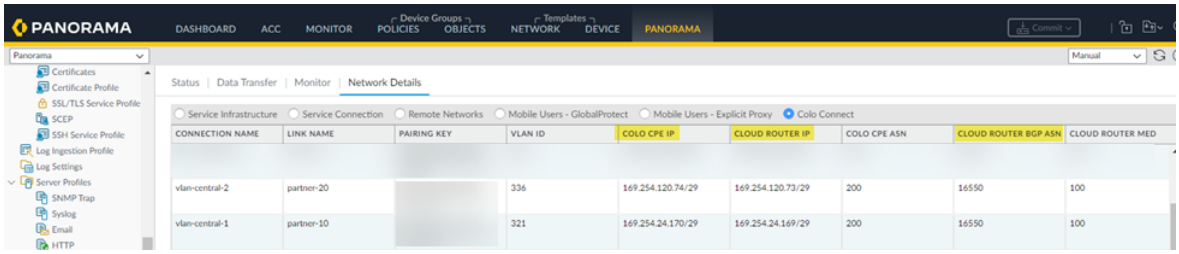
©2025 Palo Alto Networks, Inc.

STEP 3 | 记下以下连接元素：

- **Colo CPE IP**
- 云路由器 **IP**
- 云路由器 **BGP ASN**

在以下示例中：

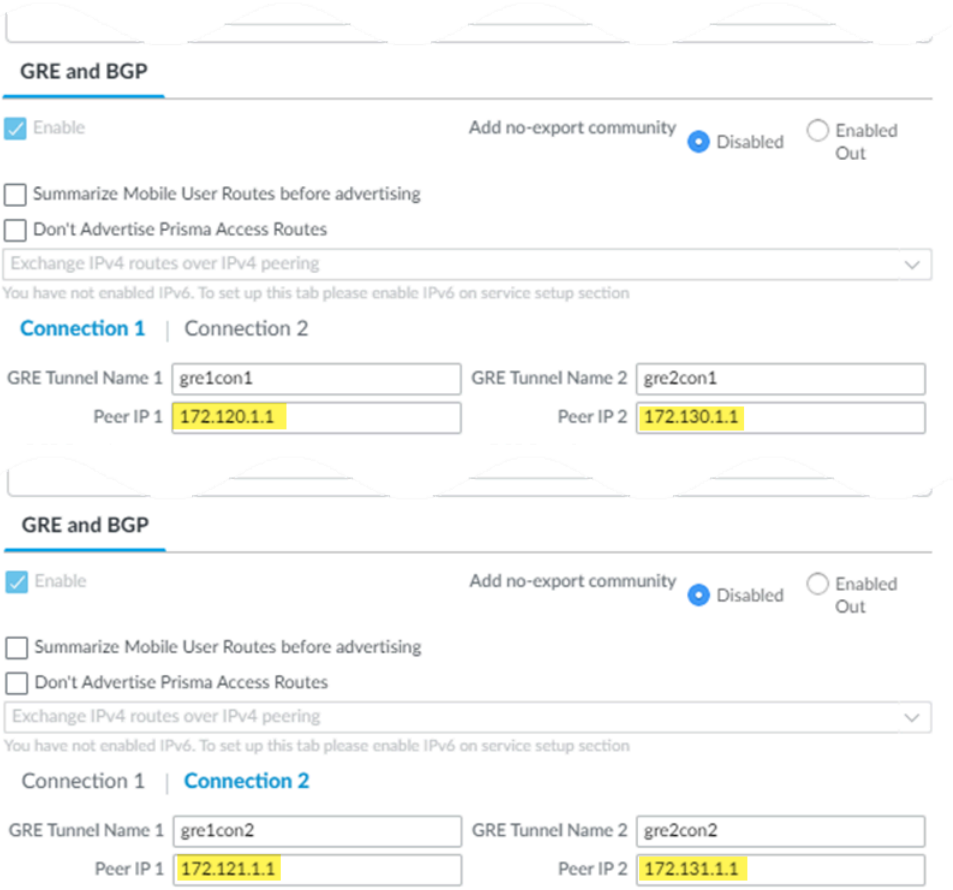
- 对于 vlan-central-1 连接，**Colo CPE IP** 为 169.254.24.170/29，**Cloud Router IP**（云路由器 **IP**）为 169.254.24.169/29，**Cloud Router BGP ASN**（云路由器 **BGP ASN**）为 16550
- 对于 vlan-central-2 连接，**Colo CPE IP** 为 169.254.120.74/29，**Cloud Router IP**（云路由器 **IP**）为 169.254.120.73/29，**Cloud Router BGP ASN**（云路由器 **BGP ASN**）为 16550。
- .



©2025 Palo Alto Networks, Inc.

STEP 4 | 确定设置 Colo-Connect 服务连接时将用于本地 GRE IP 地址的 IP 地址。

设置 Colo-Connect 服务连接（**Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Service Connection**（服务连接））时，在 **Peer IP 1**（对等体 **IP 1**）和 **Peer IP 2**（对等体 **IP 2**）区域中配置这些地址。



如果您要配置服务连接以支持高达 10 Gbps 的吞吐量，请在 **Connection 1**（连接 **1**）和 **Connection 2**（连接 **2**）中各建立一个隧道，每个服务连接总共有两个隧道。

如果您要配置服务连接以支持超过 10 Gbps 的吞吐量（不超过 20 Gbps），请在 **Connection 1**（连接 **1**）和 **Connection 2**（连接 **2**）中各建立两个隧道，每个服务连接总共有四个隧道。

以下示例显示为超过 10 Gbps 的吞吐量配置的隧道，因此每个连接使用两个隧道，它们使用以下对等体 IP 地址：

- 连接 1 为 172.120.1.1
- 连接 1 为 172.130.1.1
- 连接 2 为 172.121.1.1
- 连接 2 为 172.131.1.1

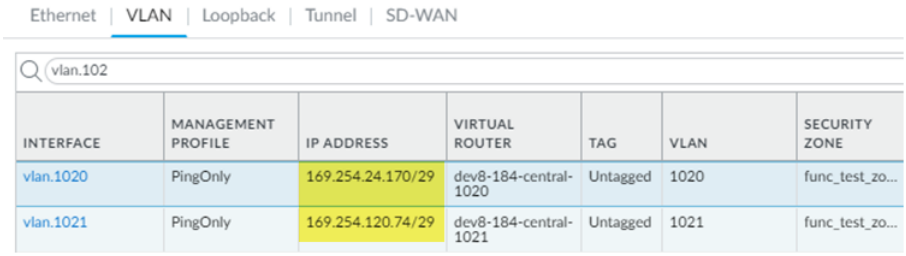
STEP 5 | 登录 Colo 路由器。

以下配置屏幕截图使用 Palo Alto Networks 新一代防火墙作为 Colo 路由器。

 ©2025 Palo Alto Networks, Inc.

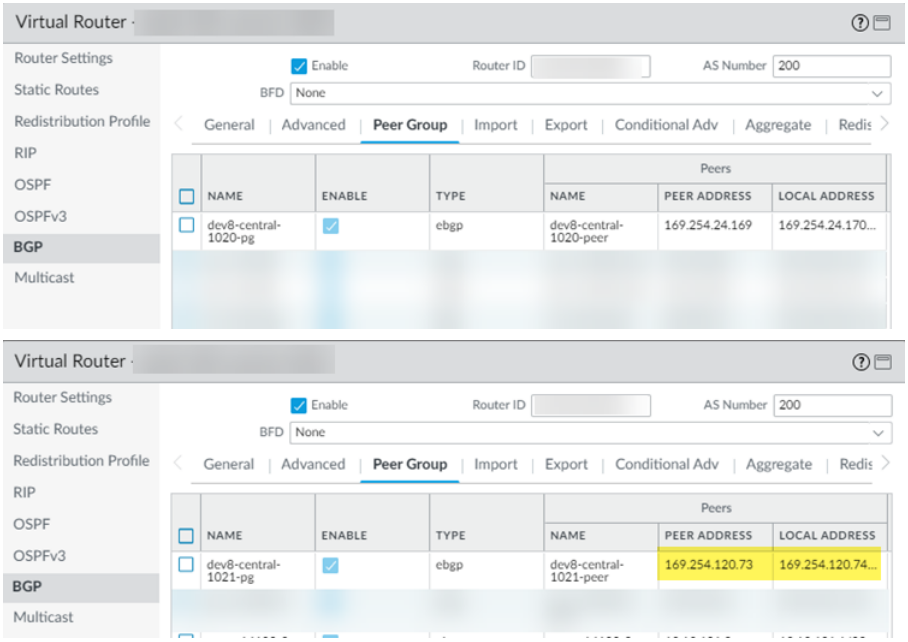
STEP 6 | 添加 VLAN 接口，将 **Colo CPE IP** 地址指定为 IP 地址。

如果要使用新一代防火墙作为 Colo 路由器，请转到 **Network**（网络） > **Interfaces**（接口） > **VLAN**，**Add**（添加）VLAN 接口，指定 **Virtual Router**（虚拟路由器）名称



STEP 7 | 将 Colo 路由器 IP 地址（**Colo CPE IP**）配置为本地 eBGP IP 地址，并将云路由器 IP 地址（**Cloud Router IP**（云路由器 **IP**））配置为 Colo 路由器上的 eBGP 对等体地址。

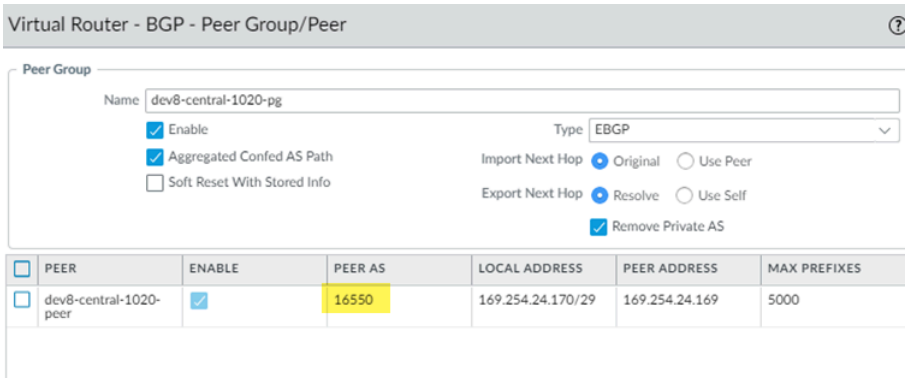
如果要使用新一代防火墙作为 Colo 路由器，请转到 **Network**（网络） > **Virtual Routers**（虚拟路由器），**Add**（添加）虚拟路由器，转到 **BGP** > **Peer Group**（对等体组），然后输入 **Colo CPE IP** 作为 **Peer Address**（对等体地址），输入 **Cloud Router IP**（云路由器 **IP**）作为 **Local Address**（本地地址）。



 ©2025 Palo Alto Networks, Inc.

STEP 8 | 将 **Cloud Router BGP ASN**（云路由器 **BGP ASN**）配置为 eBGP 对等体自治系统编号 (ASN)。

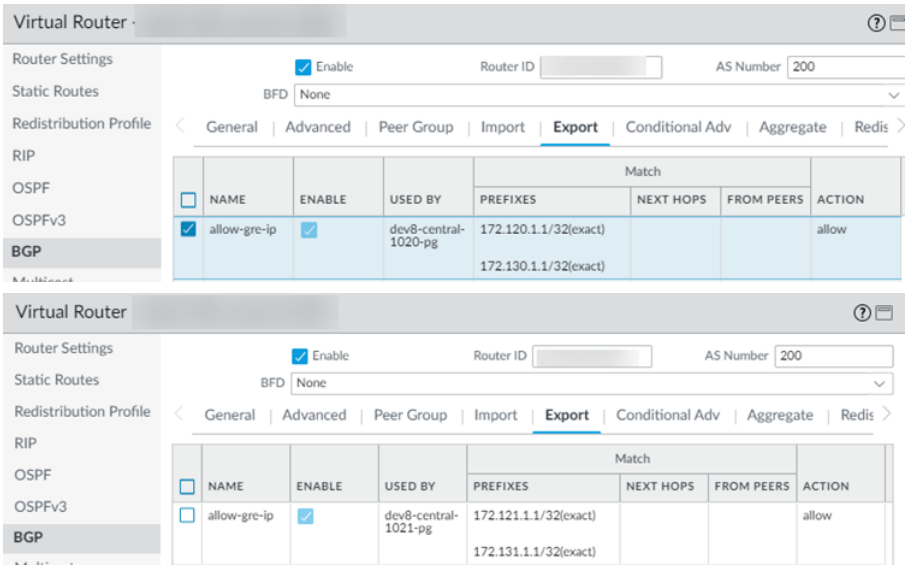
如果要使用新一代防火墙作为 Colo 路由器，请转到 **Network**（网络） > **Virtual Routers**（虚拟路由器），**Add**（添加）虚拟路由器，转到 **BGP** > **Peer Group**（对等体组），**Add**（添加）对等体组，并在 **Peer AS**（对等体 **AS**）中选择 **16500**



STEP 9 | 创建 BGP 导出策略，仅允许向云路由器对等体 IP 地址通告本地 GRE IP 地址。

由于云路由器只能接收有限数量的路由，因此您需要创建策略，以便仅将服务连接 GRE 隧道的 IP 地址之间的路由发送到云路由器。

如果要使用新一代防火墙作为 Colo 路由器，请转到 **Network**（网络） > **Virtual Routers**（虚拟路由器），**Add**（添加）虚拟路由器，转到 **BGP** > **Export**（导出），**Add**（添加）导出规则，**Match**（匹配）用作对等体 IP 地址的 IP 地址，然后创建 **Allow**（允许）**Action**（操作）。



STEP 10 | 创建 Colo-Connect 服务连接。

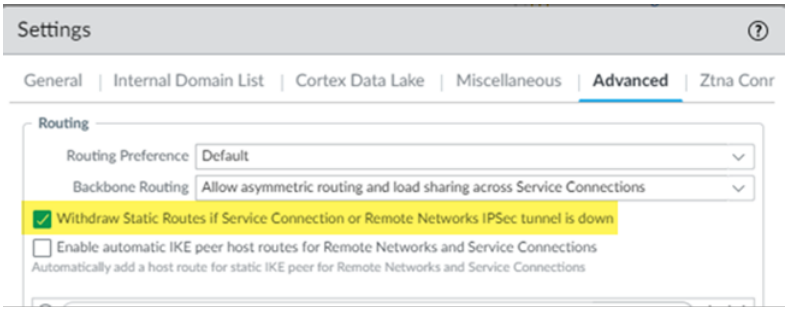
创建 Colo-Connect 服务连接

Colo-Connect 使用服务连接，但它们与 Prisma Access 服务连接的不同之处在于它们使用 GRE 隧道而不是 IPSec 隧道，并且始终使用 BGP 进行路由。要配置 Colo-Connect 服务连接，请完成以下步骤。

 ©2025 Palo Alto Networks, Inc.

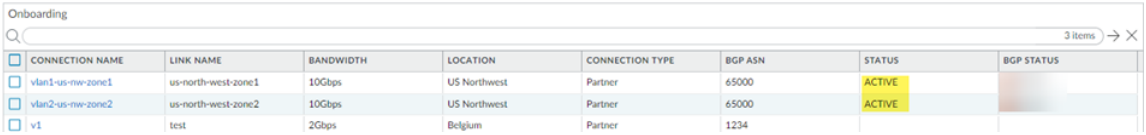
STEP 1 | 在管理 Prisma Access 的 Panorama 中，确保 Prisma Access 撤回静态路由，方法是转到 **Panorama > Cloud Services**（云服务） **> Configuration**（配置） **> Service Setup**（服务设置），单击齿轮图标以编辑 **Settings**（设置），然后选择 **Withdraw Static Routes if Service Connection or Remote Network IPSec tunnel is down**（如果服务连接或远程网络 **IPsec** 隧道关闭，则撤回静态路由）。

选择此选项可确保如果 GRE 隧道关闭，则撤回 GRE 隧道使用的静态路由。



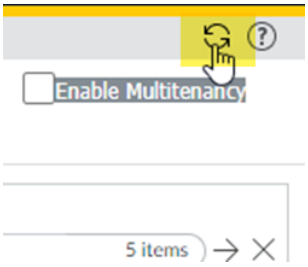
STEP 2 | 转到 **Colo-Connect** 选项卡，并通过查看加入区域中的 **Status**（状态）字段确保连接处于 **Active**（活动）状态。

在连接的 **Status**（状态）变为 **Active**（活动）之前，您无法配置服务连接。



STEP 3 | 转到 **Panorama > Cloud Services**（云服务） **> Configuration**（配置） **> Service Connection**（服务连接）。

STEP 4 | 单击 Panorama UI 右上角的 **Refresh**（刷新），以便在服务连接区域中配置 Colo-Connect 配置。



STEP 5 | **Add**（添加）服务连接，为其指定唯一的 **Name**（名称），并选择 **Colo-Connect**的 **Transport Type**（传输类型）。

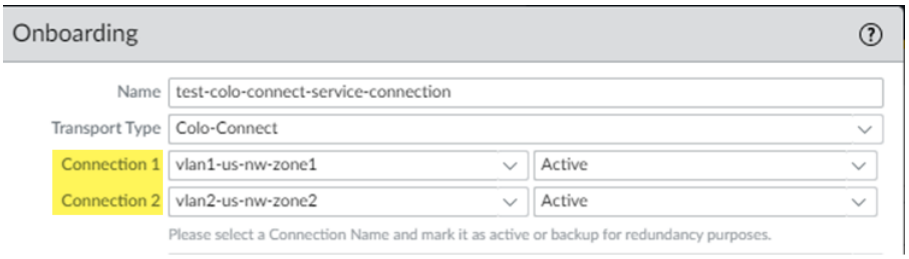
确保输入的名称长度不超过 *31* 个字符；若输入 *32* 个字符或更长的名称，会导致该隧道在 *Prisma Access* 基础架构中的映射不正确。



 ©2025 Palo Alto Networks, Inc.

STEP 6 | 选择用于服务连接的两个连接（**Connection 1**（连接 **1**）和 **Connection 2**（连接 **2**））。

这些连接必须位于两个不同的服务区。



STEP 7 | 为 **Connection 1**（连接 **1**）和 **Connection 2**（连接 **2**）选择 **Active**（活动）或 **Backup**（备份）

设置服务连接时请遵循以下准则：

- 可以在以下模式下配置连接：
  - **Active**（活动）**/Active**（活动）
  - **Active**（活动）**/Backup**（备份）
  - **Backup**（备份）**/Active**（活动）

  如果在 **Backup**（备份）**/Backup**（备份）模式下配置两个连接，则配置无效且不受支持。
- 在所有模式下，连接的带宽必须是相同的。
- 连接必须位于不同的服务区。
- 您可以为服务连接指定的最大带宽是 20 Gbps。如果为连接指定 **20 Gbps** 的 **Bandwidth**（带宽），则无法在 **Active**（活动）**/Active**（活动）配置中使用该连接（必须将其设置为 **Active**（活动）**/Backup**（备份））。
- 不要在同一服务连接中混合使用专用互连和合作伙伴互连，并确保服务连接使用不同的服务区。下表列出了针对服务连接允许和不允许的配置，假设服务区、地点、带宽和角色遵循服务连接准则和要求：

连接 **1** 属于	连接 **2** 属于	是否为有效的 **Colo-Connect** 服务连接配置？
合作伙伴连接 1	合作伙伴连接 2	是
专用连接 1	专用连接 2	是
合作伙伴连接 1	合作伙伴连接 1	否
专用连接 1	专用连接 1	No
合作伙伴连接	专用连接	否

©2025 Palo Alto Networks, Inc.

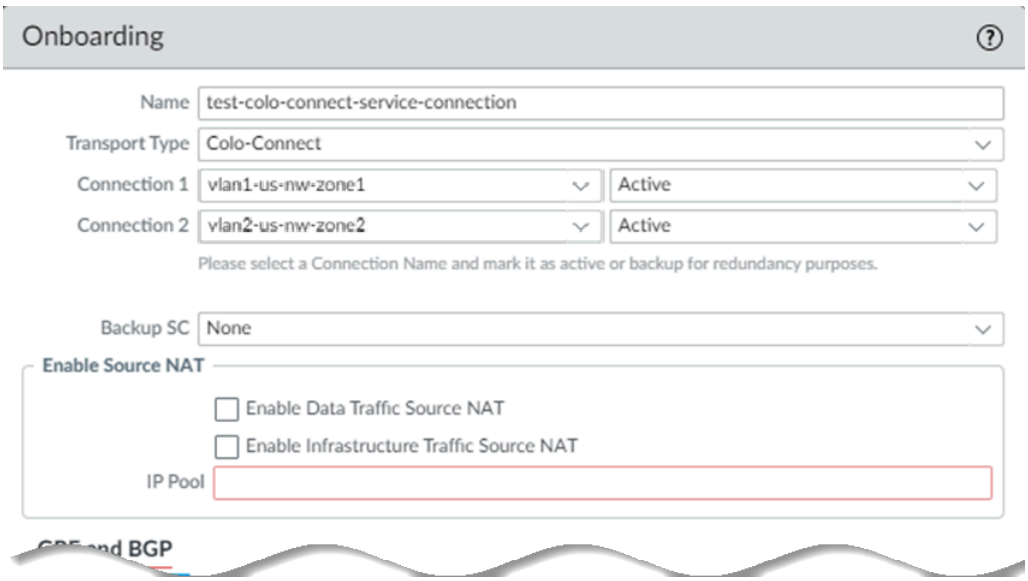
STEP 8 | （可选，仅限 BGP 和热土豆路由部署）— 选择一个服务连接作为首选备份（备份 SC）。

您只能选择已配置为 Colo-Connect 服务连接的服务连接。如果连接失败，Prisma Access 将使用您选择的备份 SC 作为首选服务连接。选择备份服务连接后，可以防止在创建了两个以上的服务连接的情况下出现非对称路由问题。

STEP 9 | （可选）为移动用户—GlobalProtect IP 池地址、基础架构子网中的 IP 地址（或两者）启用源 NAT。

您可以在一个或多个服务连接中指定一个子网，这些服务连接用于对 Prisma Access GlobalProtect 移动用户与数据中心的私有应用程序和资源之间的流量执行 NAT。

- 启用数据流量源 **NAT** — 对移动用户 IP 地址池地址执行 NAT，以确保不会向数据中心通告这些地址，并且仅会在数据中心内通告和路由您在服务连接中指定的子网。
- 启用基础架构流量源 **NAT** — 对基础架构子网中的地址执行 NAT，以确保不会向数据中心通告这些地址，并且仅会在数据中心内通告和路由您在服务连接中指定的子网。
- **IP 池** — 指定用于在移动用户 IP 地址池、基础架构子网（或两者）上执行 NAT 的 IP 地址池。使用专用 IP (RFC 1918) 子网或路由域中可路由的合适子网，并且与移动用户—GlobalProtect IP 地址池或基础架构子网不重叠。输入介于 /25 和 /32 之间的子网。



 ©2025 Palo Alto Networks, Inc.

STEP 10 | 在 **GRE and BGP**（**GRE** 和 **BGP**）区域中，配置服务连接的 GRE 隧道和 BGP 设置。

BGP 始终设置为 **Enable**（启用）。

1. （可选）从以下选项中选择：
   - 要将公司接入节点（服务连接）的 **no-export**（无导出）团体添加到客户终端设备 (CPE) 的 eBGP 对等体中的出站前缀，请将 **Add no-export community**（添加无导出团体）设置为 **Enabled Out**（启用出站）。默认情况下 **Disabled**（禁用）此功能。

     请勿在热土豆路由模式下使用此功能。
   - 要防止 Prisma Access BGP 对等体将路由转发到组织的网络中，请选择 **Don't Advertise Prisma Access Routes**（（不通告 **Prisma Access** 路由）。

     默认情况下，Prisma Access 通告所有 BGP 路由信息，包括本地路由以及它从其他服务连接、远程网络和移动用户子网收到的所有前缀。选中此复选框可防止 Prisma Access 发送任何 BGP 通告，但仍使用其收到的 BGP 信息从其他 BGP 邻居学习路由。

     如果您选择此选项，*Prisma Access* 不会发送 *BGP* 通告，因此您必须在本地设备上配置静态路由以建立返回 *Prisma Access* 的路由。
   - 要减少通过 BGP 向您的客户终端设备 (CPE) 通告的移动用户 IP 子网的数量，请选择 **Summarize Mobile User Routes before advertising**（在通告之前汇总移动用户路由）。

     默认情况下，Prisma Access 以 /24 子网的形式通告移动用户的 IP 地址池；如果将它们汇总起来，Prisma Access 会根据您指定的子网来通告该池。例如，Prisma Access 使用 /20 子网通告公共用户移动 IP 池 10.8.0.0/20，而不是在通告之前将池划分为 10.8.1.0/24、10.8.2.0/24、10.8.3.0/24 等子网。汇总这些通告可以减少 CPE 路由表中存储的路由数量。例如，您可以将 IP 池汇总与可接受有限数量路由的云 VPN 网关（虚拟专用网关 (VGW) 或传输网关 (TGW)）结合使用。

     如果启用了热土豆路由并启用了路由汇总，*Prisma Access* 将不再添加 *AS-PATH*，这可能会导致非对称路由问题。在使用热土豆路由启用路由汇总之前，请确保从数据中心或总部位置返回的流量具有保证的对称返回。
2. 为使用 GRE 隧道的服务连接设置路由。
3. 在管理 Prisma Access 的 Panorama 中，返回到 **Panorama** > **Cloud Service**（云服务）> **Configuration**（配置） > **Service Connection**（服务连接），为 **Connection 1**（连接 **1**）创建 GRE 隧道，方法是为 **Connection 1**（连接 **1**）输入 **GRE Tunnel Name 1**（**GRE** 隧道名称 **1**）和 **Peer IP 1**（对等体 **IP 1**），如果所需带宽超过 10 Gbps，则为连接 1 的

 ©2025 Palo Alto Networks, Inc.

第二个隧道输入 **GRE Tunnel Name 2**（**GRE** 隧道名称 **2**）和 **Peer IP 2**（对等体 **IP 2**）；然后，重复上述相同的步骤，为 **Connection 2**（连接 **2**）创建 GRE 隧道。

连接中的每对 GRE 隧道最多支持 10 Gbps 的带宽。如果所需带宽超过 10 Gbps，请为每个连接配置两个隧道。例如：

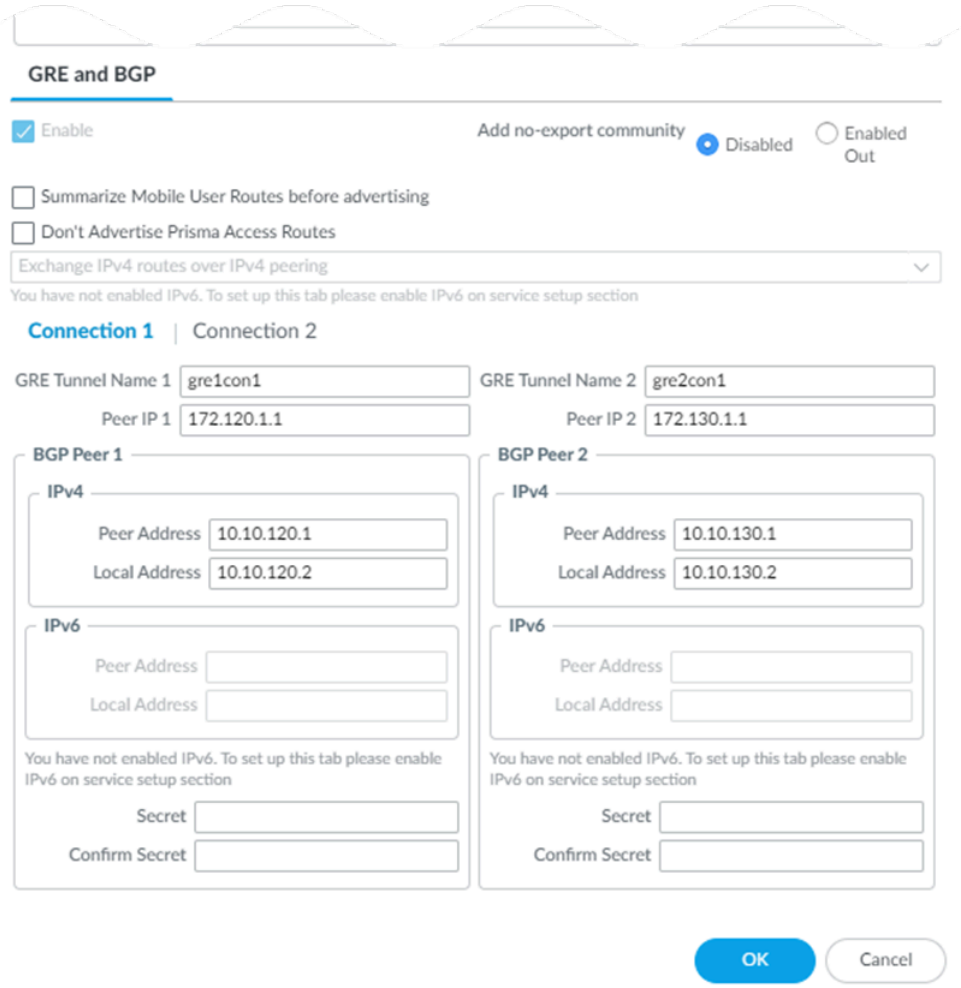
对于对等体 IP，请输入 Colo 中的本地路由器的 GRE IP 地址。

使用 IPv4 地址作为 BGP 值；不支持 IPv6。

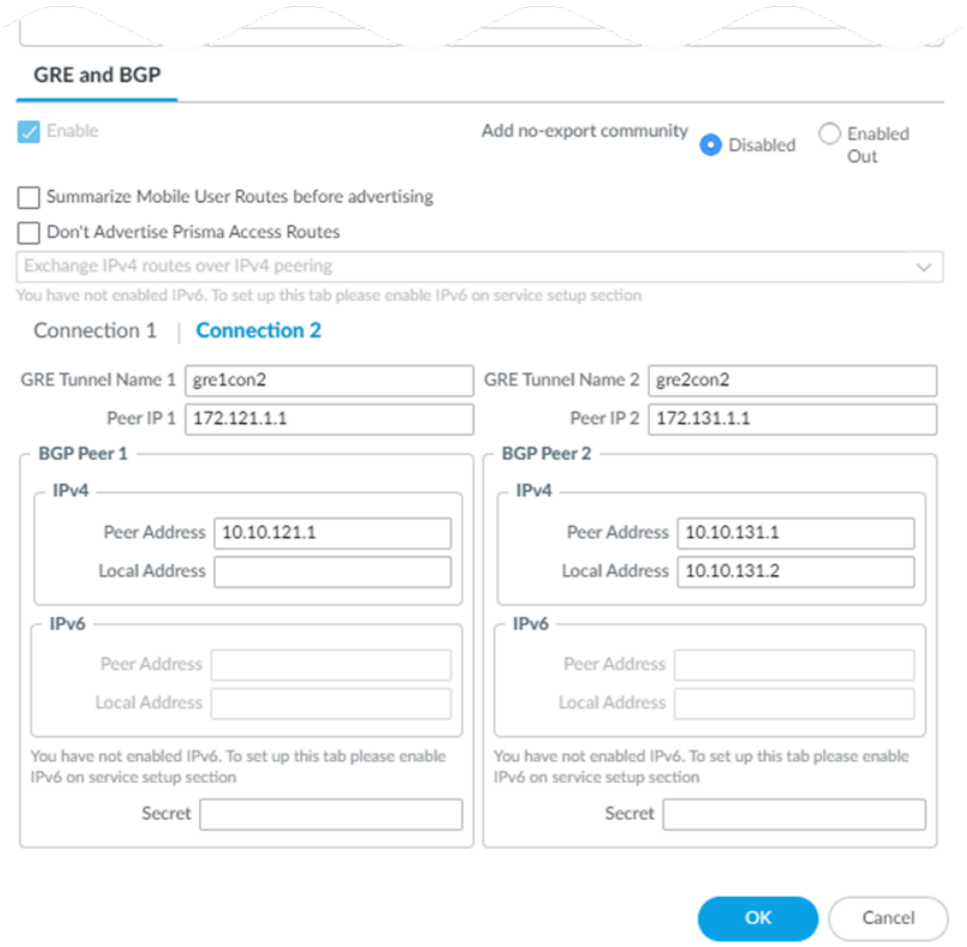
4. 输入 BGP 对等体 1 的 **Peer Address**（对等体地址）和 **Local Address**（本地地址），如果连接 1 需要第二个隧道，则创建 BGP 对等体 2。

   对于 **Peer Address**（对等体地址），请输入 Colo 路由器的 BGP 对等体 IP 地址；对于 **Local Address**（本地地址），请输入将用于通过 GRE 隧道建立 BGP 网络的地址。

5. （可选）要配置 BGP 机密，请输入 **Secret**（机密）并 **Confirm Secret**（确认机密）值。



 ©2025 Palo Alto Networks, Inc.

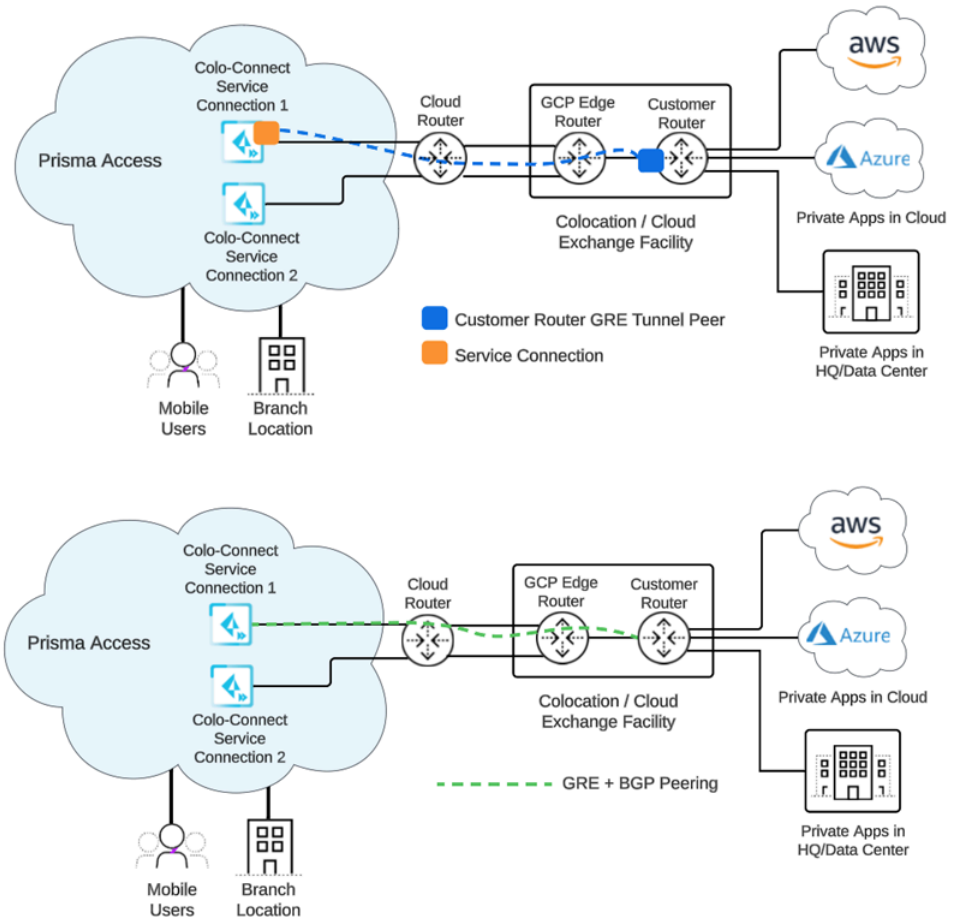


STEP 11 | **Commit and Push**（提交并推送）配置更改，确保在 **Push Scope**（推送范围）中选择 **Colo-Connect**。

为使用 GRE 隧道的服务连接设置路由

Colo 路由器将其 GRE 隧道对等体 IP 地址通告给云路由器，并从云路由器学习 GRE 隧道的子网。当您首次在客户路由器上配置通过 VLAN 的 eBGP 路由时，您已通告 GRE 隧道的本地可达性。在云路由器和 Colo 路由器相互通告并学习 Colo 子网和本地 GRE IP 地址的路由后，服务连接使用的 GRE 隧道将变为活动（开启）状态。

©2025 Palo Alto Networks, Inc.



要设置路由并将 GRE 隧道添加到服务连接，请完成以下步骤。

STEP 1 | 记下将用于 BGP 对等体 1 的 **Peer Address**（对等体地址）和 **Local Address**（本地地址）的 IP 地址，如果连接 1 需要第二个隧道，则创建 BGP 对等体 2。

以下示例使用以下对等体地址和本地地址：

- **Peer Address**（对等体地址）— 连接 1 为 10.10.120.0 和 10.10.130.1，连接 2 为 10.10.120.2 和 10.10.130.2
- **Local Address**（本地地址）— 连接 1 为 10.10.120.2 和 10.10.130.2，连接 2 为 10.10.121.2 和 10.10.131.2

©2025 Palo Alto Networks, Inc.

STEP 2 | 记下您将在服务连接中用于 **Peer IP 1**（对等体 **IP 1**）和 **Peer IP 2**（对等体 **IP 2**）地址（如果需要）的 IP 地址。

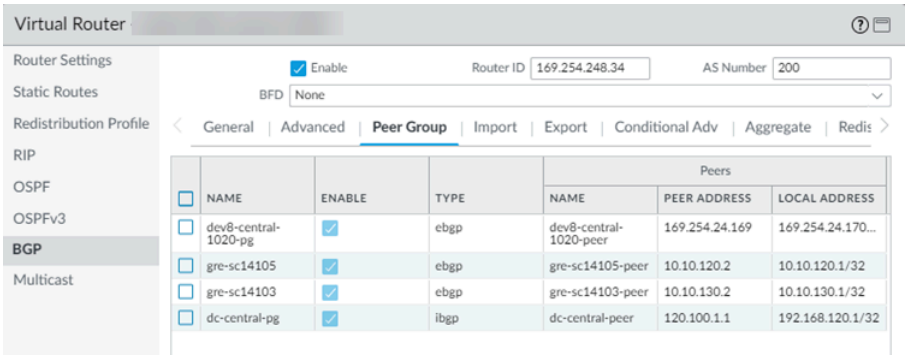
您可以使用这些 IP 地址创建拒绝策略，以防止将本地 GRE IP 地址通告到 Colo-Connect 服务连接。

本文档中的所有示例均使用以下 IP 地址：

- 连接 1 为 172.120.1.1
- 连接 1 为 172.130.1.1
- 连接 2 为 172.121.1.1
- 连接 2 为 172.131.1.1

STEP 3 | 为对等体和本地 IP 地址配置对等体组。

如果要使用新一代防火墙作为 Colo 路由器，请转到 **Network**（网络） > **Virtual Routers**（虚拟路由器），**Add**（添加）虚拟路由器，转到 **BGP** > **Peer Group**（对等体组），然后在 **Peer Address**（对等体地址）中输入对等体地址，在 **Local Address**（本地地址）中输入 **Local Address**（本地地址）。

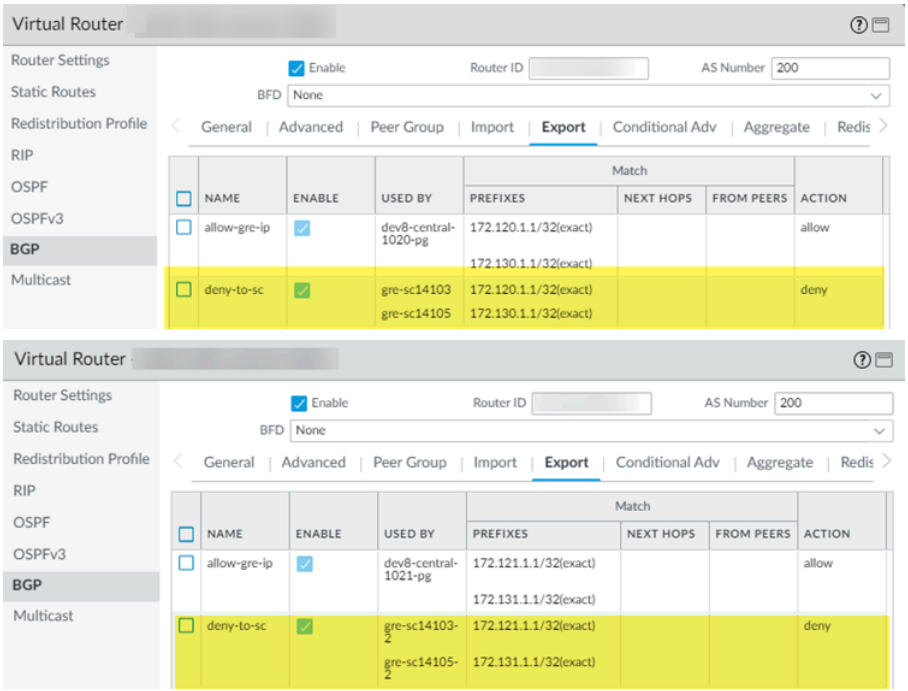


 ©2025 Palo Alto Networks, Inc.

STEP 4 | 创建 BGP 导出策略以拒绝您配置的对等体 IP 地址（172.120.1.1、172.130.1.1、172.121.1.1 和 172.131.1.1），并将其应用于您创建的对等组。

此导出策略在本地 GRE 隧道对等体 IP 地址上放置 DENY 规则，并允许将所有其他路由通告到该服务连接。

如果要使用新一代防火墙作为 Colo 路由器，请转到 **Network**（网络）> **Virtual Routers**（虚拟路由器），**Add**（添加）虚拟路由器，转到 **BGP** > **Export**（导出），**Add**（添加）导出规则，**Match**（匹配）用作对等体 IP 地址的 IP 地址，然后创建 **Deny**（拒绝）**Action**（操作）。



增加或减少 Colo-Connect 服务连接的带宽

配置服务连接时，可以根据与其关联的连接（VLAN 连接）配置带宽。为每个服务连接分配两个连接，然后为每个连接分配一个或两个 GRE 隧道。

尽管每个 Colo-Connect 服务连接最多支持 20 Gbps 的带宽，但服务连接中的每个 GRE 隧道都支持 10 Gbps 的带宽。因此，您可能必须添加或删除 Colo-Connect 服务连接中的 GRE 隧道，若更改链路中的总带宽，可能会导致服务连接带宽高于或低于 10 Gbps。

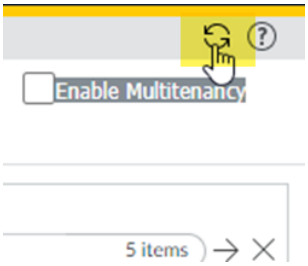
增加 **Colo-Connect** 服务连接的带宽

要将现有服务连接的带宽增加到 10 Gbps 以上，请完成以下步骤：

STEP 1 | 转到 **Panorama** > **Cloud Services**（云服务）> **Configuration**（配置）> **Colo-Connect**。

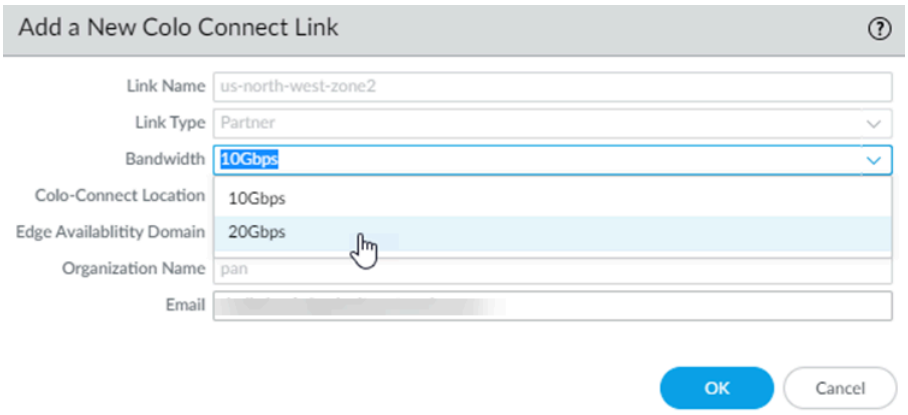
 ©2025 Palo Alto Networks, Inc.

STEP 2 | 转到 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Service Connection**（服务连接），单击 Panorama UI 右上角的 **Refresh**（刷新），以便在服务连接区域中配置 Colo-Connect 配置。



STEP 3 | 选择与服务连接相关联的 **Link Name**（链路名称）。

STEP 4 | 增加链路（互连）的 **Bandwidth**（带宽）。

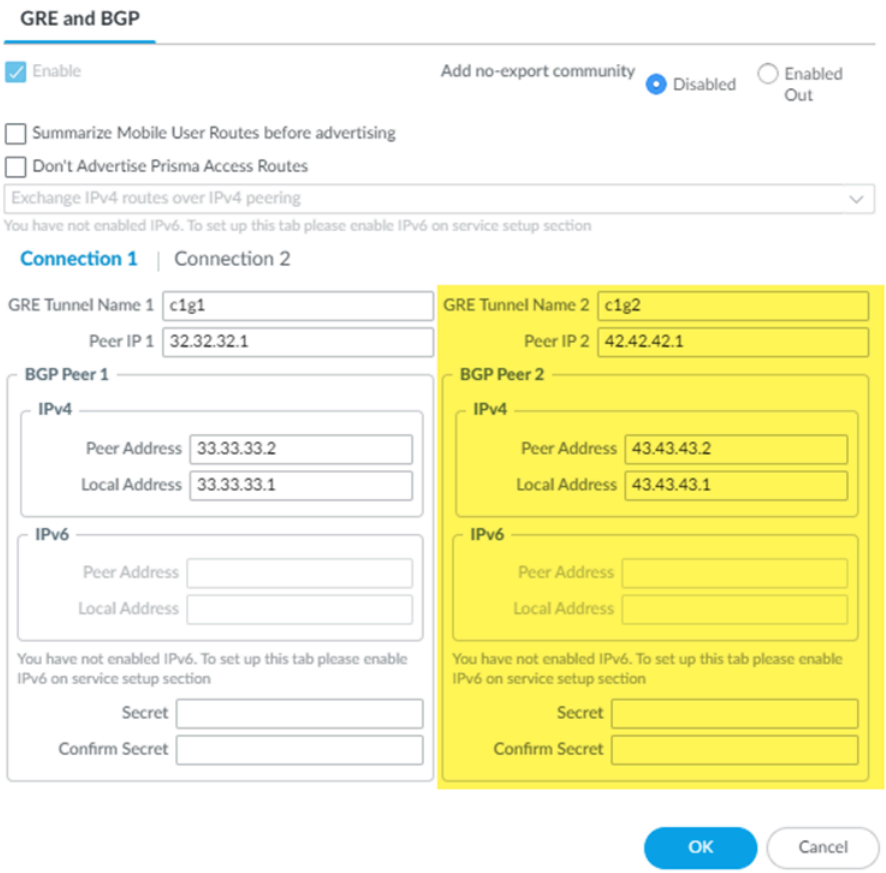


STEP 5 | **Commit and Push**（提交并推送）更改，在 **Push Scope**（推送范围）中仅选择 **Colo-Connect**。

STEP 6 | 转到 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Service Connection**（服务连接） > ***<service-connection-name>*** > **Onboarding**（加入）。

 ©2025 Palo Alto Networks, Inc.

STEP 7 | 将额外的 GRE 隧道添加到 Colo-Connect 服务连接。



STEP 8 | **Commit and Push**（提交并推送）更改，在 **Push Scope**（推送范围）中选择 **Service Connections**（服务连接）。

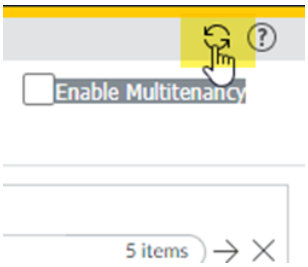
STEP 9 | 将 GRE 本地（对等体）IP 地址添加到 GRE 隧道的 VLAN eBGP 路由和服务连接路由的导出策略中。

减少 **Colo-Connect** 服务连接的带宽

要将现有服务连接的带宽减少到 10 Gbps 以上，请完成以下步骤：

STEP 1 | 转到 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Colo-Connect**。

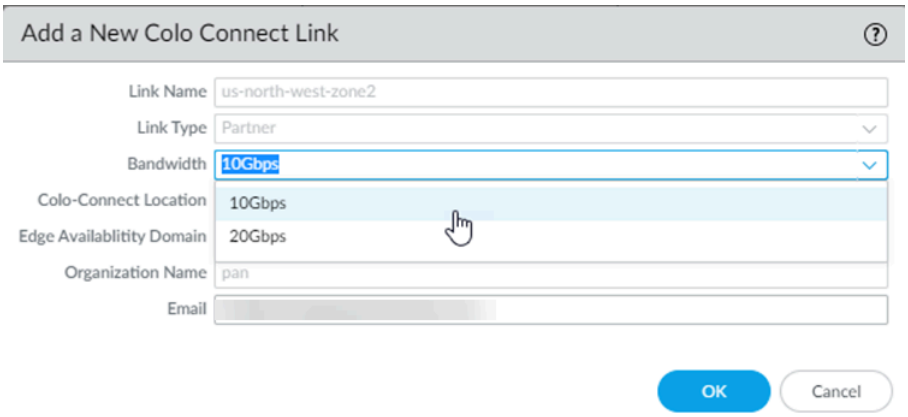
STEP 2 | 转到 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Service Connection**（服务连接），单击 Panorama UI 右上角的 **Refresh**（刷新），以便在服务连接区域中配置 Colo-Connect 配置。



 ©2025 Palo Alto Networks, Inc.

STEP 3 | 选择与服务连接相关联的 **Link Name**（链路名称）。

STEP 4 | 减少链路（互连）的 **Bandwidth**（带宽）。



STEP 5 | **Commit and Push**（提交并推送）更改，在 **Push Scope**（推送范围）中仅选择 **Colo-Connect**。

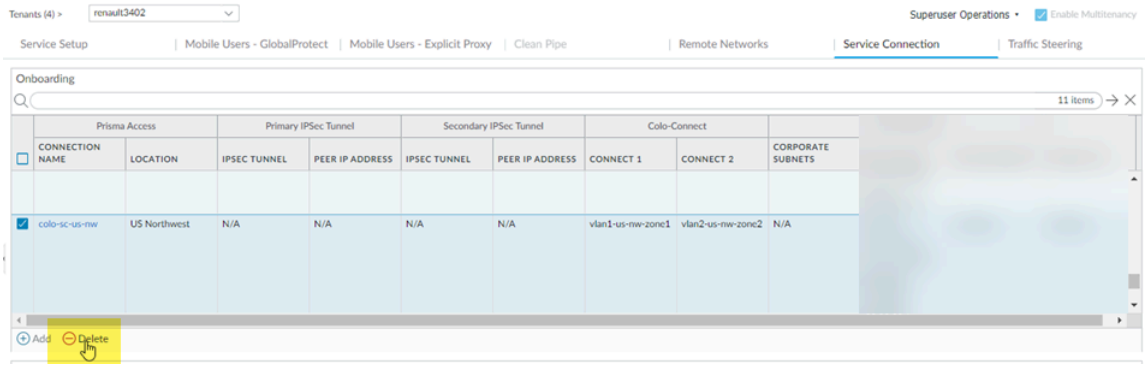
STEP 6 | **Commit and Push**（提交并推送）更改，在 **Push Scope**（推送范围）中选择 **Service Connections**（服务连接）。

您无需重新配置服务连接以删除额外的 GRE 隧道；当您在服务连接推送范围内提交并推送更改时，Prisma Access 会检测并降低链路的带宽，然后删除额外的隧道。

删除 Colo-Connect 连接

要删除 Colo-Connect 连接，请按照与配置相反的顺序完成以下步骤：

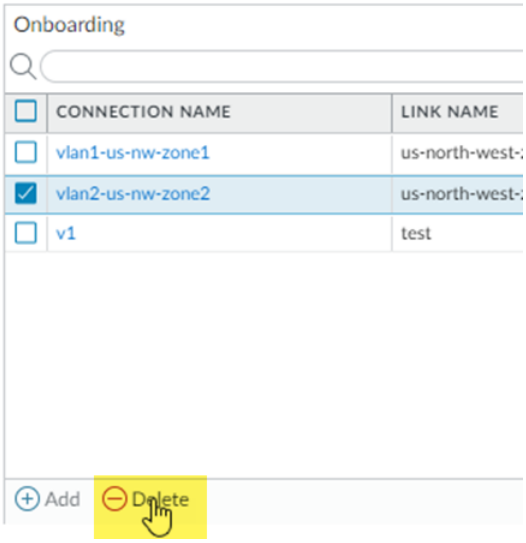
STEP 1 | 转到 **Panorama > Cloud Services**（云服务） **> Configuration**（配置） **> Service Connection**（服务连接），选择与该连接关联的服务连接，然后单击 **Delete**（删除）即可删除该服务连接。



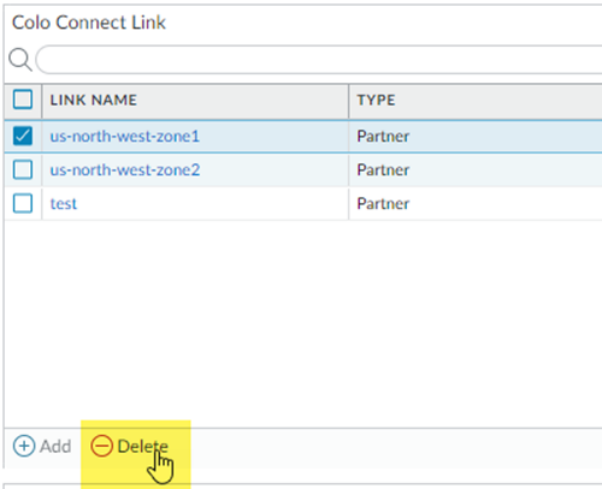
STEP 2 | **Commit and Push**（提交并推送）更改，在 **Push Scope**（推送范围）中选择 **Service Connections**（服务连接）。

©2025 Palo Alto Networks, Inc.

STEP 3 | 转到 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Colo-Connect**, 在 **Onboarding**（加入）部分中选择 **Connection Name**（连接名称）， 然后单击 **Delete**（删除）即可删除与该连接关联的 Colo-Connect 连接。



STEP 4 | 选择 **Link Name**（链路名称）， 单击 **Delete**（删除）即可删除 Colo-Connect 链路。



STEP 5 | 删除 GRE 隧道的 VLAN eBGP 路由和服务连接路由的导出策略中的 GRE 本地（对等体）IP 地址。

 ©2025 Palo Alto Networks, Inc.

Prisma Access 中的 App Acceleration

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ 至少需要 Prisma Access 5.0 Innovation 版本 ❑ Prisma Access 许可证 ❑ App Acceleration 需要 Prisma Access 数据平面版本 10.2.10。 ❑ App Acceleration 附加许可证 App Acceleration 许可证包括自主 DEM (ADEM) 的 30 天评估许可证，因此您可以从 ADEM 检索 App Acceleration 性能指标。

App Acceleration 可直接解决导致应用程序性能不佳的问题，并实时采取行动缓解这些问题，从而显著改善 Prisma Access GlobalProtect 和远程网络用户的用户体验。

访问应用程序时导致用户体验不佳的主要原因是动态内容（必须按需为每个用户单独处理的内容）和网络连接问题。

App Acceleration 为您提供以下功能：

加速主要 **SaaS** 应用程序的性能 — App Acceleration for Prisma SASE 可加速动态内容，以缩短主要 SaaS 应用程序的响应时间。它在用户请求之前安全、智能地准备每个用户所需的动态内容。

因此，App Acceleration 可显著缩短应用程序和 API 的响应时间，从而改善了用户体验并提高了工作效率。

加速应用程序列在支持的应用程序部分中。

网络加速 — 当用户访问应用程序时，他们可能会遇到由于吞吐量下降而导致的应用程序性能不佳的情况，而吞吐量下降的问题可能是由数据包丢失、无线连接降级、网络拥塞及其他因素所造成的。这些网络问题会对员工体验产生不利影响并降低其工作效率。

在互联网诞生之初，网络是同质的，无线连接还处于起步阶段。TCP 等基本协议最初就是为这些网络创建的。如今，网络不再具有同质性，无线连接带来了灵活多变的用户体验。当用户遇到网络状况降级时，TCP 无法区分问题是由于设备限制、网络限制还是物理约束而发生的。

App Acceleration 无需对客户端配置或应用程序进行任何更改，即可安全地了解以下信息：

- 设备功能 — 客户端端点的类型
- 网络能力 — 网络的类型
- 应用程序上下文 — 正在使用的应用程序的类型

利用对设备、网络和应用程序上下文的了解，App Acceleration 可最大限度地提高吞吐量，并根据不断变化的网络状况实时进行调整。

与直接访问互联网相比，通过 Prisma Access 连接时，App Acceleration 可显著提高 TCP 流量的吞吐量。

您可以在 Prisma SASE 事件和警报中查看 App Acceleration 的吞吐量改进情况。AI 驱动的自主 DEM (ADEM) 与 App Acceleration 集成，并为您提供加速的应用程序数量和整体性能提升等指标。

©2025 Palo Alto Networks, Inc.

App Acceleration 要求和准则

配置 App Acceleration 时，请注意以下准则和要求：

- 支持的应用程序 — App Acceleration 支持以下应用程序：
  - Amazon S3
  - Azure Storage
  - Box
  - Google Drive
  - Microsoft 365：
    - My Content
  - Microsoft OneDrive
  - Salesforce
  - SAP Ariba
  - ServiceNow
  - Slack（文件下载）
  - Zoom：
    - 从聊天中下载文件
    - 云录制内容下载
    - Zoom Team Chat
- 支持的地点 — App Acceleration 适用于除以下地点之外的所有 Prisma Access 地点：
  - 所有本地服务区
  - 巴林
  - 中国
  - 爱尔兰
  - 南非西部
  - 瑞典
  - 阿拉伯联合酋长国
- 可信的根 **CA** 上传 — 您需要设置可信的根 CA 并执行提交和推送操作，然后在 App Acceleration 设置期间选择它，如以下步骤所示。如果使用 Strata Cloud Manager 配置 App Acceleration，请在 Prisma Access 范围内设置根 CA。如果您更改所使用的证书，还必须提交并推送更改后的证书，然后才能选择该证书。
- 转发信任证书和可信的根 **CA** — 将您上传的 CA/证书启用为转发信任证书和可信的根 CA，如以下步骤所示。如果将 SSL 解密应用于任何加速应用程序，则必须将证书标记为转发信任证书和可信的根 CA，否则用户在尝试访问这些应用程序时会遇到 SSL 错误。

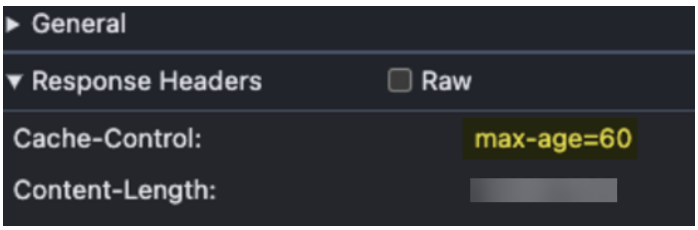
©2025 Palo Alto Networks, Inc.

- 不支持的 **Prisma Access** 功能 — 以下功能不支持 App Acceleration，启用这些功能的 Prisma Access 部署将不会加速：
  - IPv6 协议

    配置 IPv6 时，App Acceleration 与 IPv6 网络共存；但是，只有 IPv4 TCP 流量会加速。IPv6 流量不会加速，但可正常运行。
  - 使用重叠子网的远程网络（默认情况下在 Prisma Access (Managed by Strata Cloud Manager) 部署中支持，可在 Prisma Access (Managed by Panorama) 部署中配置。
- **App Acceleration** 准则：
  - **QUIC** 协议支持 — 某些浏览器（例如 Google Chrome）可能默认使用快速 UDP 互联网连接 (QUIC) 协议。第 7 层 App Acceleration 不能用于使用 QUIC 的流量。解决方法是，在配置 App Acceleration 时禁用 QUIC 协议。
  - **SaaS** 应用程序和 **Zy-*** 响应标头 — 连接到为主要 SaaS 应用程序启用了 App Acceleration 的 Prisma Access 部署的用户将会看到名称为 Zy-* 的响应标头，例如 Zy-Server 和 Zy-Accelerated，以及 zy_sid 会话 Cookie。

    如果响应标头是 Zy-Accelerated，则值为 **1** 表示响应已加速，值为 **0** 表示响应未加速。
  - 内容本地化 — 如果加速的 SaaS 应用程序仅根据用户的 IP 地址或用户 ID 对内容进行本地化，则为该应用程序启用加速时，其内容将不会本地化。
  - 将“操作”设置为“拒绝”的安全策略规则的默认行为的更改 — 如果您拥有将操作设置为 **Deny**（拒绝）的安全策略规则，并且使用基于源地址或目标地址、应用程序或服务的规则将其应用于通过 App Acceleration 传输的流量，则流量将完成三次握手，但 Prisma Access 将阻止该规则，而 **Deny**（拒绝）策略将按配置运行。
  - **Amazon S3** 和 **Azure Blob** 存储 **`cache-control`** — Amazon S3 和 Azure Blob 存储桶和文件具有一系列与之关联的 HTTP 响应标头。其中一个值是 `cache-control`。如果 `cache-control` 为以下值，则文件不会加速：
    - 未设置
    - 设置为 `max-age=0` 的值
    - 设置为 `max-age=no-cache` 的值

    为了使 Amazon S3 和 Azure Blob 存储获得 App Acceleration 的好处，请将 `cache-control max-age` 值设置为大于零的值。

- **Activity Insights** 中具有共享域的应用程序 — 使用 App Acceleration 时，第 7 层加速基于域。在某些情况下，如果两个应用程序共享同一个域，Activity Insights 中的应用程序报告可能会将一个应用程序的第 7 层流量归因于另一个应用程序。例如，如果来自 MS Teams 和 OneDrive 应用程序的某些流量共享同一个域，则 MS Teams 应用程序报告将显示在 OneDrive 下。

 ©2025 Palo Alto Networks, Inc.

- 长连接和系统日志 — 当单个 TCP 连接结束时，App Acceleration 会写入第 4 层日志。对于短连接而言，此行为是透明的，因为短连接通常由应用程序创建。

  App Acceleration 收集连接处于活动状态的整个期间的指标。对于长连接（例如由已挂载的 SMB 网络驱动器使用的连接）而言，此行为可能会使其看起来好像仅在连接结束时收集指标。

©2025 Palo Alto Networks, Inc.

配置 App Acceleration

要在 Prisma Access 中配置 App Acceleration，请根据您的部署选择以下选项卡之一（Prisma Access (Managed by Strata Cloud Manager) 或 Prisma Access (Managed by Panorama)）。

- Strata Cloud Manager
- Panorama

©2025 Palo Alto Networks, Inc.

在 Prisma Access (Strata Cloud Manager) 中配置 App Acceleration

要在 Prisma Access (Managed by Strata Cloud Manager) 部署中配置 App Acceleration，请完成此任务。

©2025 Palo Alto Networks, Inc.

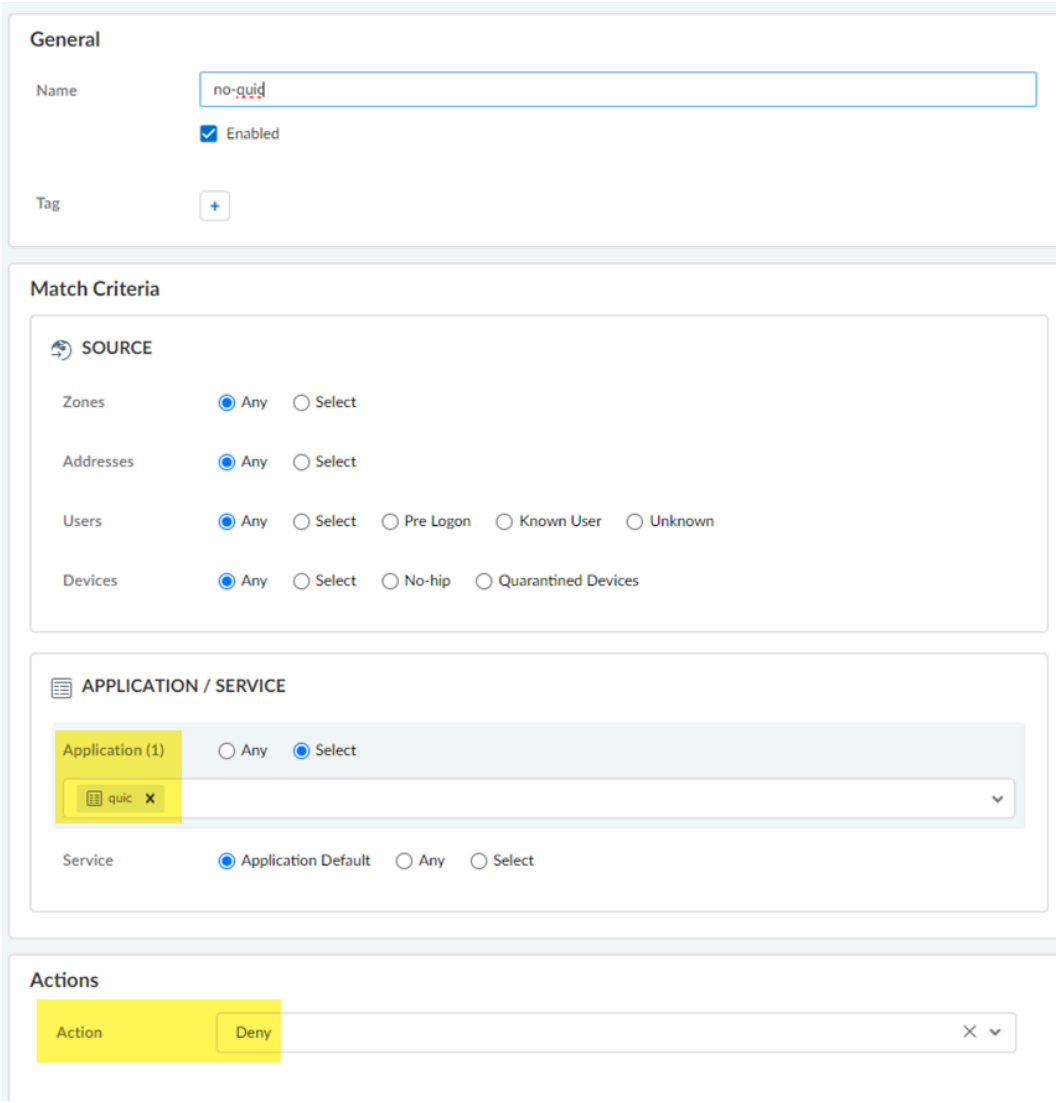
STEP 1 | （可选）禁用快速 UDP 互联网连接 (QUIC) 协议。

如果不禁用 QUIC，App Acceleration 无法在第 7 层加速应用程序。

1. 转到 **Manage**（管理） > **Configuration**（配置） > **NGFW & Prisma Access**（**NGFW** 和 **Prisma Access**） > **Security Services**（安全服务） > **Security Policy**（安全策略），然后转到 **Add Rule**（添加规则） > **Pre Rules**（预规则）。

   在 **Global**（全局）配置范围内创建此安全策略规则。

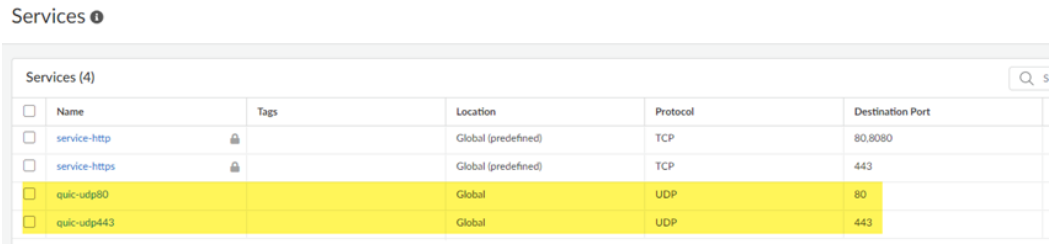
2. 在 **Application / Service**（应用程序/服务）中选择 **quic**，在 **Actions**（操作）中选择 **Deny**（拒绝）。



3. **Save**（保存）更改。
4. 转到 **Manage**（管理） > **Configuration**（配置） > **NGFW & Prisma Access**（**NGFW** 和 **Prisma Access**） > **Objects**（对象） > **Services**（服务） > **Service**（服务），然后为 UDP 端口 80 和 UDP 端口 443 **Add**（添加）服务。

   Palo Alto Networks 建议为 UDP 端口 80 和 UDP 端口 443 添加服务，并创建额外的安全策略来阻止这些端口上的 UDP 流量，因为较新版本的 QUIC 可能会被错误识别为 **unknown-udp**。

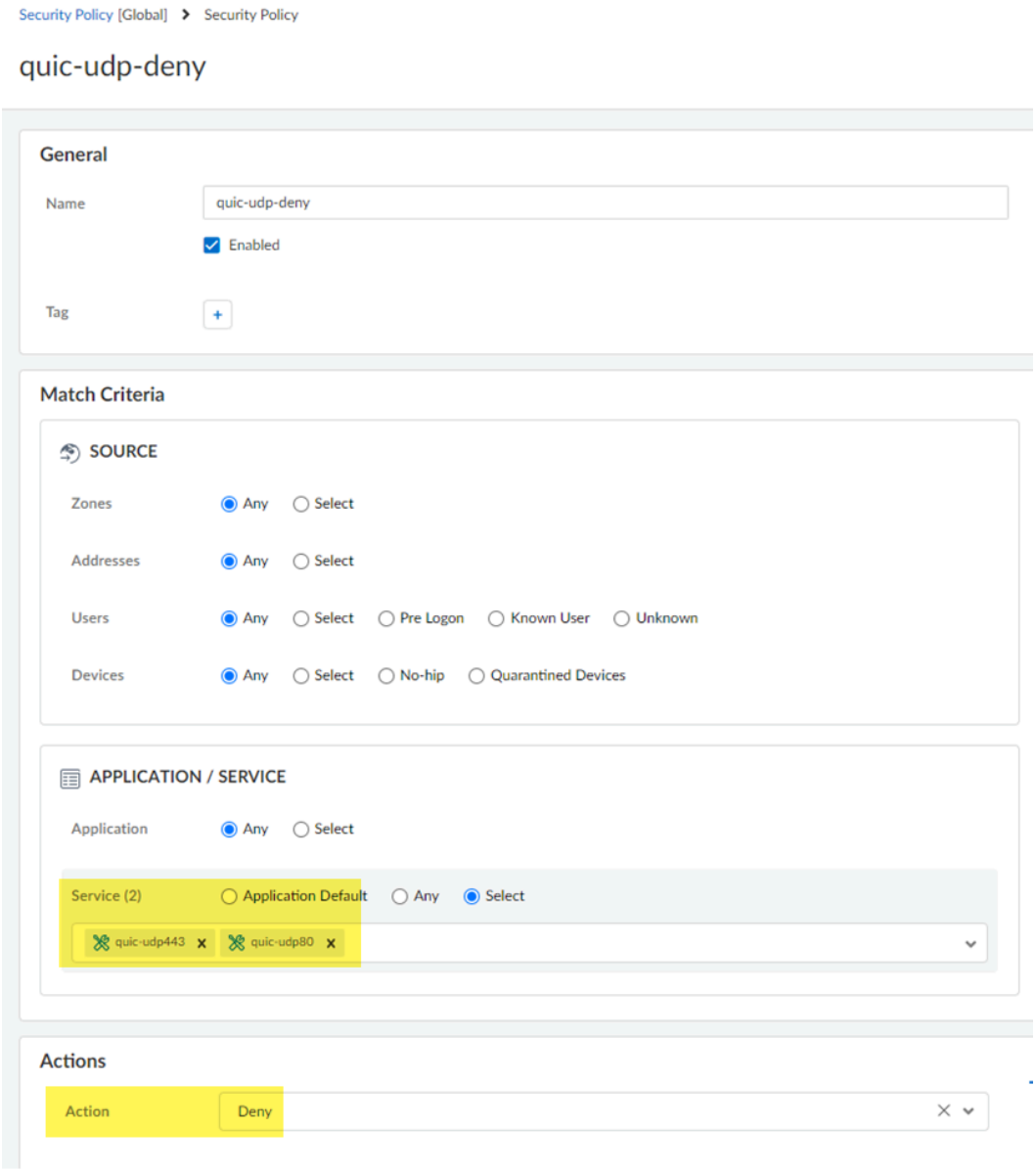
 ©2025 Palo Alto Networks, Inc.



5. 返回 **Manage**（管理） > **Configuration**（配置） > **NGFW & Prisma Access**（**NGFW** 和 **Prisma Access**） > **Security Services**（安全服务） > **Security Policy**（安全策略），针对

 ©2025 Palo Alto Networks, Inc.

第二个安全策略选择 **Add Rule**（添加规则），在 **Application / Services**（应用程序/服务）下指定服务，然后在 **Action**（操作）中指定 **Deny**（拒绝）。



完成后，您将拥有两个安全策略：一个安全策略用于阻止 QUIC 协议，另一个安全策略用于阻止 UDP 端口 80 和 443 上的流量。



 ©2025 Palo Alto Networks, Inc.

STEP 2 | 在 Prisma Access 范围内的 Strata Cloud Manager 中导入根证书颁发机构 (CA) 证书和私钥，以便与 App Acceleration 一起使用并推送您的更改。

自签名根 CA/证书是证书链中的最顶层证书。App Acceleration 使用根 CA/证书为加速应用程序创建证书。在 Prisma Access 中推送根 CA/证书，以便 App Acceleration 可以开始创建特定于应用程序的证书。

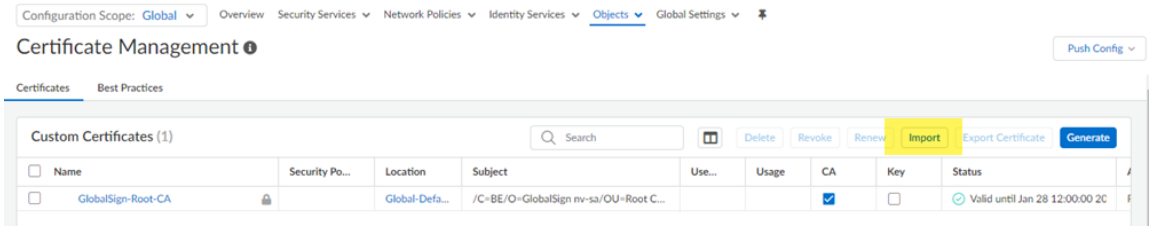
根 CA/证书必须具有以下特征：

- CA 必须是受信任的 CA。
- （推荐）CA 应该是唯一的，并且仅用于 App Acceleration。
- CA 不能过期。请记下 CA 的到期日期，并在证书到期之前进行续订。如果 App Acceleration 使用的 CA/证书已过期，用户在尝试访问加速应用程序时将收到 SSL 错误。当您的组织使用 App Acceleration 时，确保 CA 有效至关重要。
- 它必须包含密钥。
- 它必须使用密码。
- 它必须在 **Prisma Access** 范围内。
- （仅限移动用户 — GlobalProtect 部署）它必须安装在本地根证书存储区中。

  您可以通过将其添加到可信证书列表中来执行此安装，如本步骤所述，或者，如果您使用的是 ActiveDirectory，则可以使用 Active Directory 组策略对象 (GPO) 从 AD 分发根 CA。

如果您需要更改根 CA/证书，则必须先上传并提交更改，然后才能使用更改后的证书。

1. 转到 **Manage**（管理） > **Configuration**（配置） > **Identity and Access Services**（身份和访问服务） > **Objects**（对象） > **Certificate Management**（证书管理）。
2. **Import**（导入）证书。



3. 选择以下参数：
   - 为证书输入唯一的 **Certificate Name**（证书名称），例如 `AppAcceleration_CA`。

     名称区分大小写，最长可达 31 个字符。名称中只能使用字母、数字、连字符和下划线。
   - **Choose File**（选择文件）并浏览从 CA 收到的 **Certificate File**（证书文件），然后 **Open**（打开）该文件。
   - 选择 **Format**（格式）：
     - **Encrypted Private Key and Certificate (PKCS12)**（加密私钥和证书 **(PKCS12)**）— 这是默认和最常见的格式，其中密钥和证书在同一个容器（证书文件）中。
     - **Base64 Encoded Certificate (PEM)**（**Base64** 编码证书 **(PEM)**）— 必须从证书单独导入密钥。如果您选择此格式，则需要选择一个 **Key File**（密钥文件）。

 ©2025 Palo Alto Networks, Inc.

- 输入 **Passphrase**（密码）并 **Confirm Passphrase**（确认密码）。

4. **Save**（保存）更改。

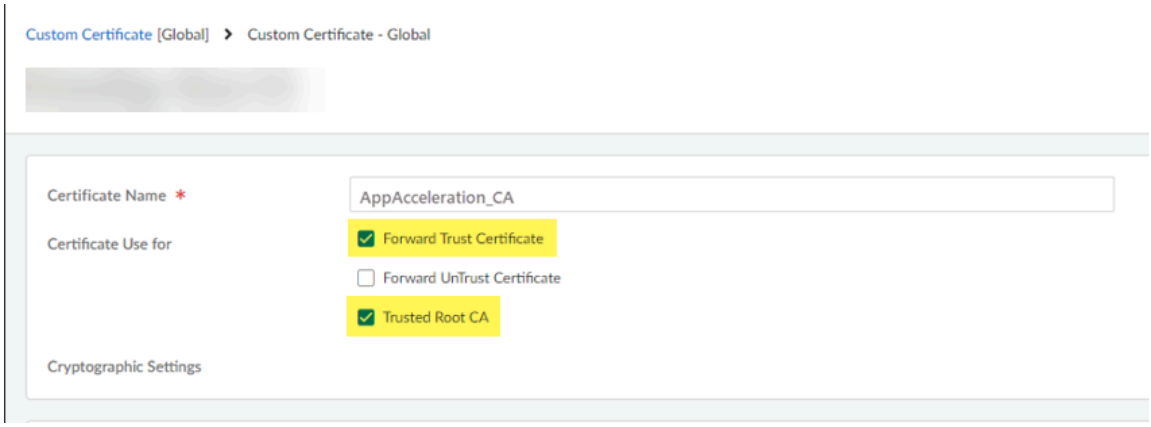


©2025 Palo Alto Networks, Inc.

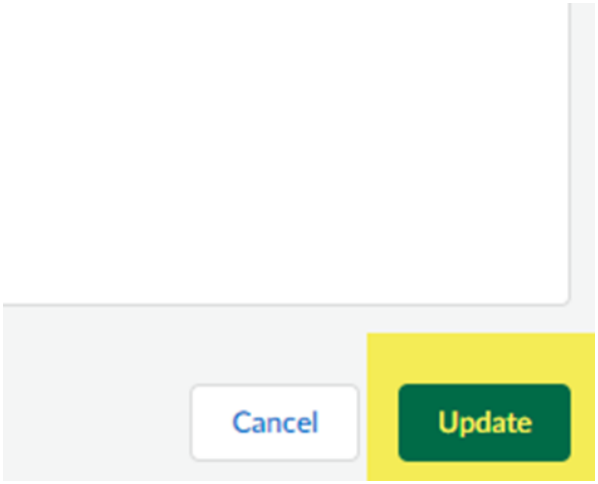
STEP 3 | 将您添加的根 CA/证书标记为转发信任证书和可信的根 CA。

如果未将证书指定为转发信任证书和可信的根 CA，则用户在使用 SSL 解密尝试访问加速应用程序时将遇到 SSL 错误。

1. 选择您添加的根 CA/证书。
2. 选择该证书作为 **Forward Trust Certificate**（转发信任证书）和 **Trusted Root CA**（可信的根 **CA**）。

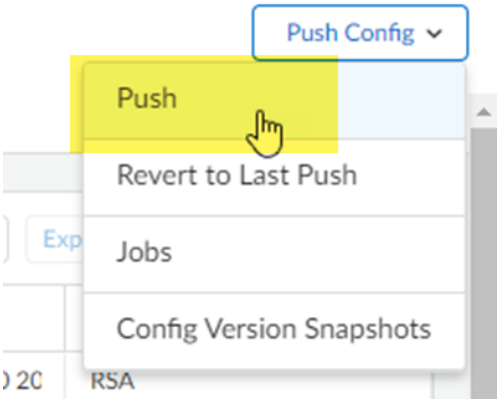


3. **Update**（更新）证书。



 ©2025 Palo Alto Networks, Inc.

STEP 4 | **Push**（推送）您的更改。

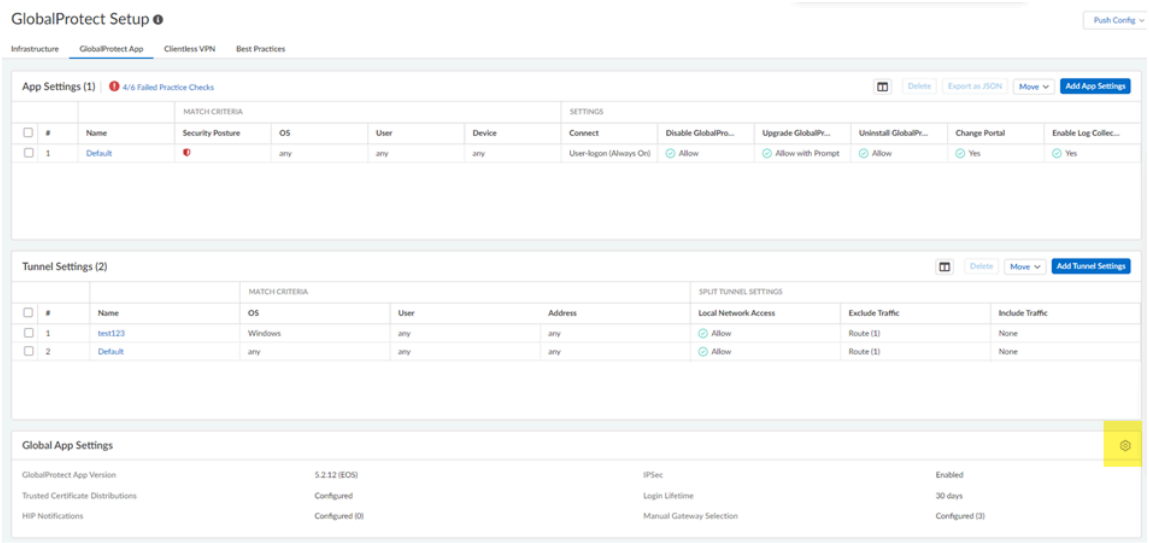


©2025 Palo Alto Networks, Inc.

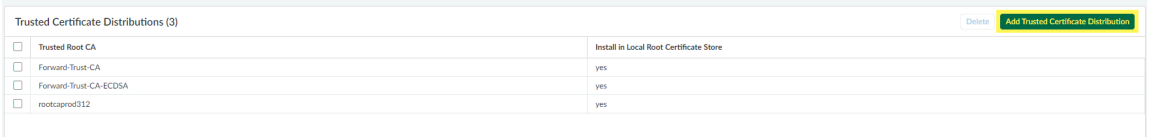
STEP 5 | （仅限移动用户 — GlobalProtect 部署）将您添加的根 CA/证书添加到 GlobalProtect 可信证书列表中，并将其安装在本地根证书存储区中。

或者，如果您使用的是 *Active Directory*，则可以使用 *Active Directory GPO* 从 *AD* 分发根 *CA*。

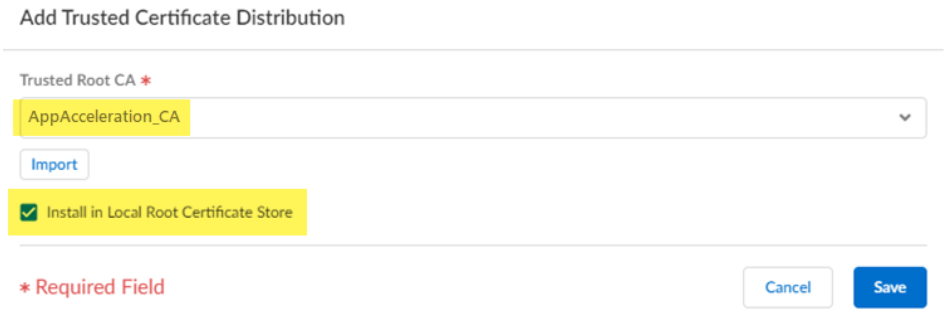
1. 转到 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **GlobalProtect** > **GlobalProtect App**（**GlobalProtect** 应用程序） > **Global App Settings**（全局应用程序设置）。
2. 单击齿轮以编辑 **Settings**（设置）。



3. **Add Trusted Certificate Distribution**（添加可信证书分发）。



4. 选择您在上一个步骤中创建的 **Trusted Root CA**（可信的根 **CA**），然后选择 **Install in Local Root Certificate Store**（在本地根证书存储区中安装）。

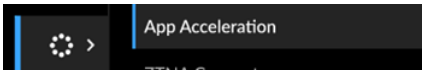


5. **Save**（保存）更改。
6. **Push**（推送）您的更改。

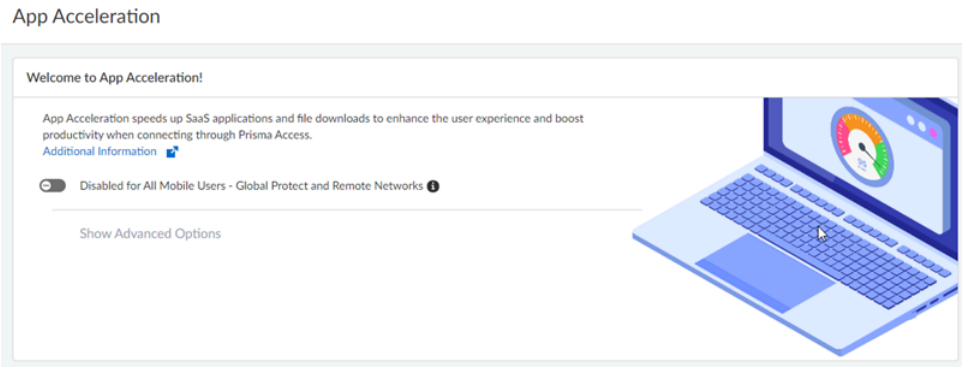
©2025 Palo Alto Networks, Inc.

STEP 6 | 启用 App Acceleration 并选择您创建的证书文件。

1. 从左侧导航栏转到 **Workflows**（工作流） > **App Acceleration**。

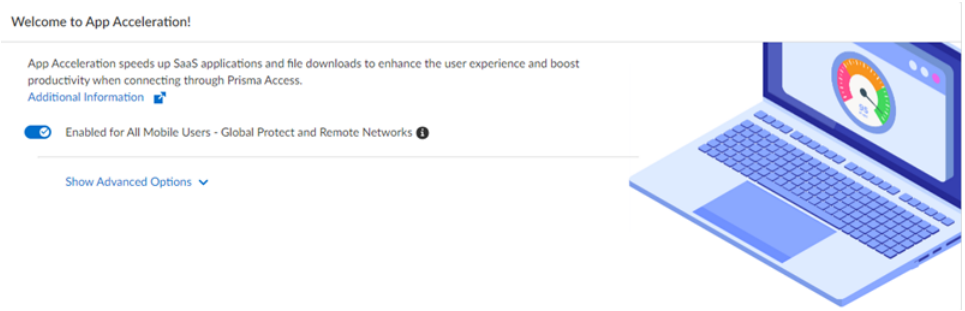


此时会显示 App Acceleration 窗口。



2. 将滑块向右移动，以便 **Enabled for all Mobile Users—GlobalProtect and Remote Networks**（为所有移动用户 — **GlobalProtect** 和远程网络启用）App Acceleration。

如果提交正在进行中，*App Acceleration* 设置将在所有提交完成后生效。

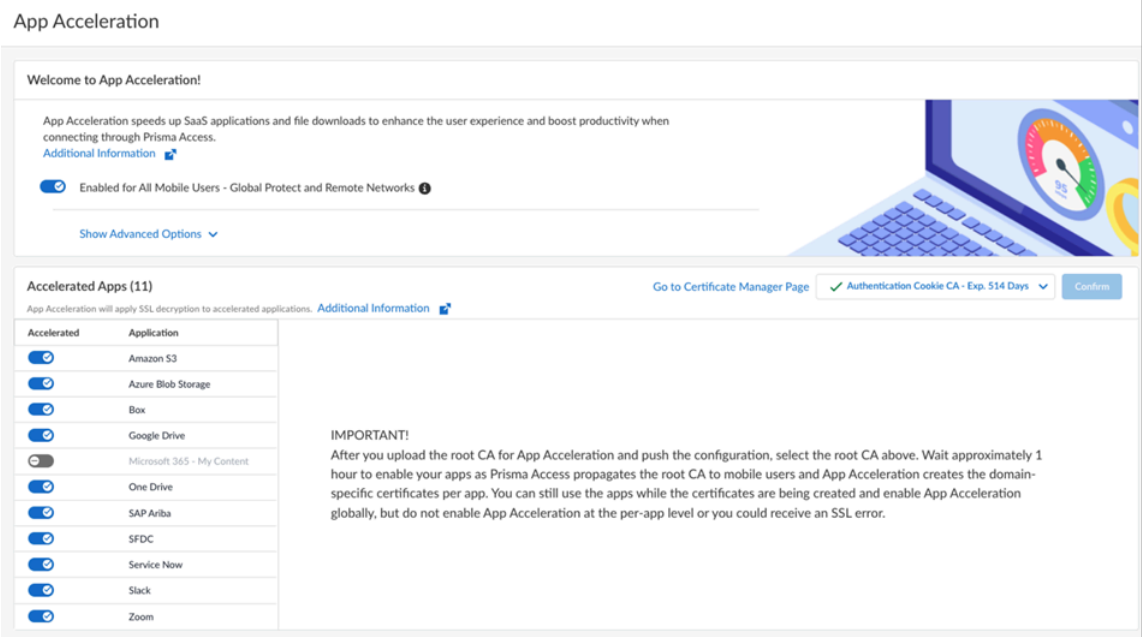


将为所有 TCP 流量将启用 App Acceleration。如果您希望加速 SaaS 应用程序，则需要选择根 CA/证书，如下一个步骤所示。

©2025 Palo Alto Networks, Inc.

STEP 7 | 选择您在上一个步骤中创建的证书。

如果您需要更改现有证书，请确保您已提交证书并将其推送到防火墙和用户，然后在此处选择该证书。您必须先提交新证书，然后才能选择该证书。



导入证书后，您必须等到 *App Acceleration* 为每个应用程序生成特定于域的证书。此过程可能需要最长一小时的时间才能完成。在此期间，您可以将 ***Accelerated Apps***（加速应用程序）的滑块向左移动，以暂时禁用 *App Acceleration* 并访问应用程序，直到生成证书为止；否则，您可能会收到 *SSL* 错误，直到生成证书为止。

在您为特定应用程序开启加速后，最多需要 *10* 分钟的时间以使加速功能生效。

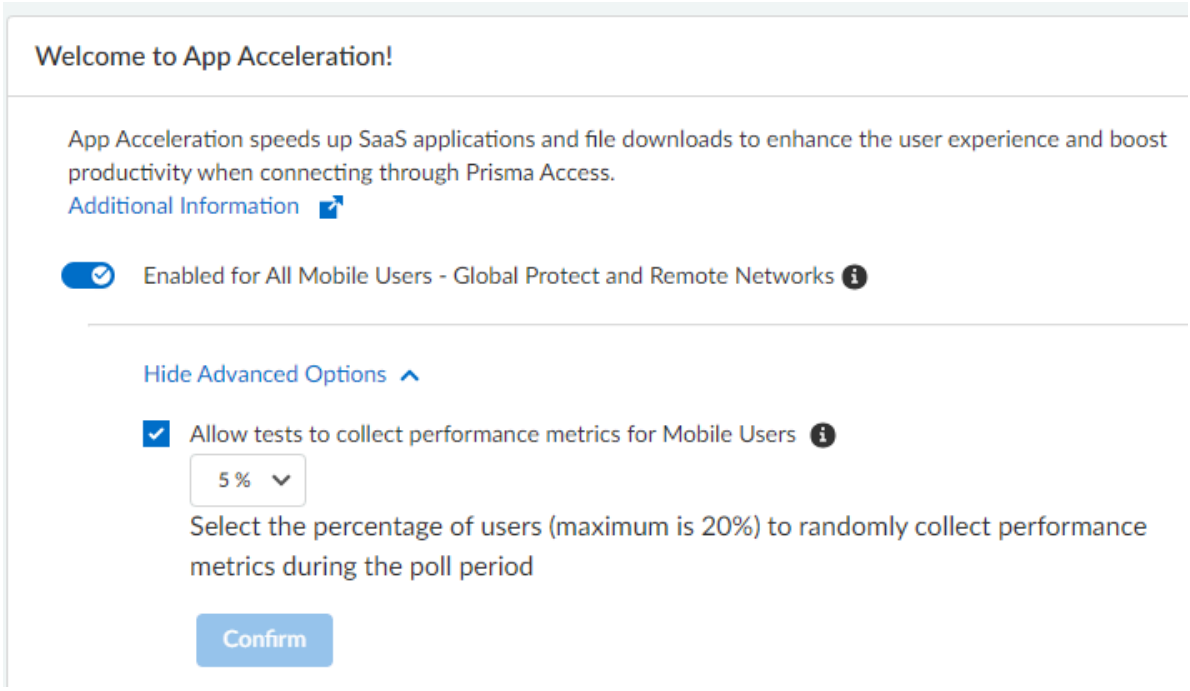
 ©2025 Palo Alto Networks, Inc.

STEP 8 | （可选）**Show Advanced Options**（显示高级选项）并更改指标测试参数。

- （可选）要禁用指标收集功能以获取性能信息，请取消选择 **Allow tests to collect performance metrics for Mobile Users**（允许测试以收集移动用户的性能指标）。

  Palo Alto Networks 建议您启用指标收集功能，以查看使用 App Acceleration 时应用程序性能的改善。

- （可选）要将处理预测测试的用户百分比从默认值 5% 更改为其他百分比，请在下拉列表中选择另一个百分比并 **Confirm**（确认）更改。



 ©2025 Palo Alto Networks, Inc.

在 Prisma Access (Panorama) 中配置 App Acceleration

要在 Prisma Access (Managed by Panorama) 部署中配置 App Acceleration，请完成此任务。

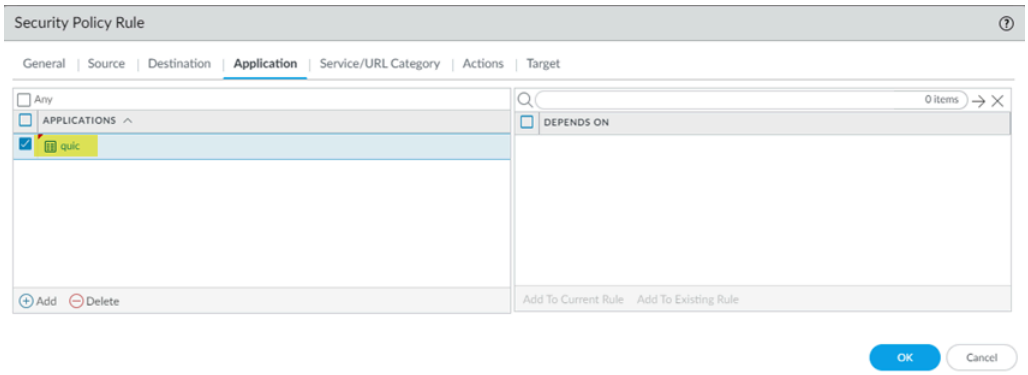
STEP 1 | （可选）禁用快速 UDP 互联网连接 (QUIC) 协议。

如果不禁用 QUIC，App Acceleration 无法在第 7 层加速应用程序。

1. 转到 **Policies**（策略） > **Security**（安全） > **Pre Rules**（预规则），然后 **Add**（添加）安全策略。

   在 **Shared**（共享）设备组中创建此安全策略规则。

2. 在 **Application**（应用程序）中选择 **quic**，在 **Actions**（操作）中选择 **Deny**（拒绝）。



3. **Add**（添加）第二个安全策略。

   QUIC 的较新版本可能被错误识别为 **unknown-udp**。因此，Palo Alto Networks 建议为 UDP 端口 80 和 UDP 端口 443 添加服务，并创建额外的安全策略来阻止这些端口上的 UDP 流量。

4. 在 **Service/URL Category**（服务/URL 类别）下，为 UDP 端口 80 和 UDP 端口 443 **Add**（添加）新服务，并在 **Action**（操作）中选择 **Deny**（拒绝）。

   完成后，您将拥有两个安全策略：一个安全策略用于阻止 QUIC 协议，另一个安全策略用于阻止 UDP 端口 80 和 443 上的流量。

	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 quic-udp443	none

©2025 Palo Alto Networks, Inc.

STEP 2 | 在 Panorama 中导入根证书颁发机构 (CA) 证书和私钥以与 App Acceleration 一起使用，然后提交并推送您的更改。

自签名根 CA/证书是证书链中的最顶层证书。App Acceleration 使用根 CA/证书为加速应用程序创建证书。在 Prisma Access 中推送根 CA/证书，以便 App Acceleration 可以开始创建特定于应用程序的证书。

根 CA/证书必须具有以下特征：

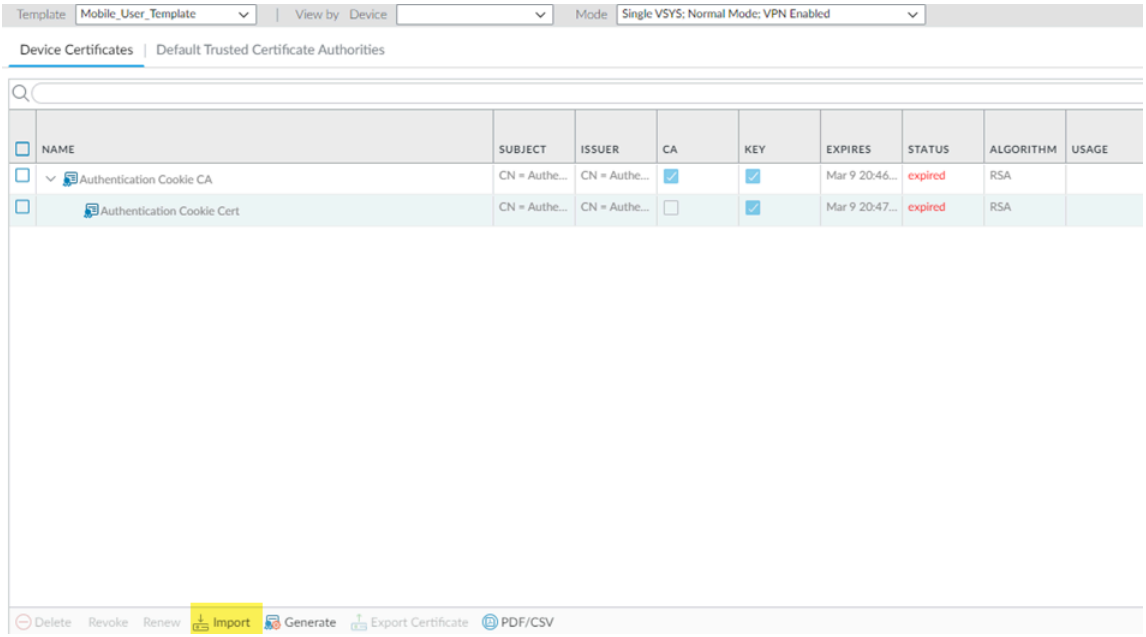
- CA 必须是受信任的 CA。
- （推荐）CA 应该是唯一的，并且仅用于 App Acceleration。
- CA 不能过期。请记下 CA 的到期日期，并在证书到期之前进行续订。如果 App Acceleration 使用的 CA/证书已过期，用户在尝试访问加速应用程序时将收到 SSL 错误。当您的组织使用 App Acceleration 时，确保 CA 有效至关重要。
- 它必须包含密钥。
- 它必须使用密码。
- （仅限移动用户 — GlobalProtect 部署）它必须安装在本地根证书存储区中。

  您可以通过将其添加到可信证书列表中来执行此安装，如本步骤所述，或者，如果您使用的是 ActiveDirectory，则可以使用 Active Directory 组策略对象 (GPO) 从 AD 分发根 CA。

如果您需要更改根 CA/证书，则必须先上传并提交和推送更改，然后才能使用更改后的证书。

1. 转到 **Device**（设备） > **Certificates**（证书） > **Certificate Management**（证书管理）。

   确保您位于 Mobile_User_Template 中。
2. **Import**（导入）证书。



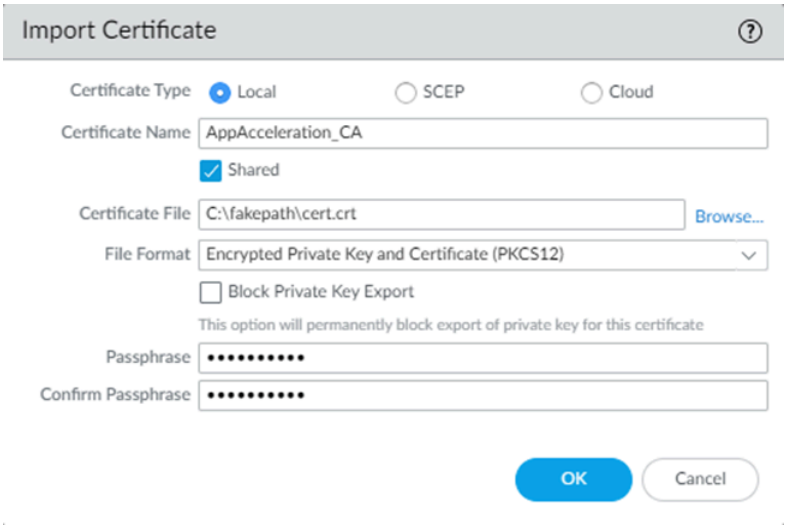
3. 选择以下参数：
   - 为证书输入唯一的 **Certificate Name**（证书名称），例如 `AppAcceleration_CA`。

 ©2025 Palo Alto Networks, Inc.

名称区分大小写，最长可达 31 个字符。名称中只能使用字母、数字、连字符和下划线。

- 浏览从 CA 收到的 **Certificate File**（证书文件），然后 **Open**（打开）该文件。
- 选择 **Format**（格式）：
  - **Encrypted Private Key and Certificate (PKCS12)**（加密私钥和证书 **(PKCS12)**）— 这是默认和最常见的格式，其中密钥和证书在同一个容器（证书文件）中。
  - **Base64 Encoded Certificate (PEM)**（**Base64** 编码证书 **(PEM)**）— 必须从证书单独导入密钥。如果您选择此格式，则需要 **Import Private Key**（导入私钥）并选择一个 **Key File**（密钥文件）。
  - 输入 **Passphrase**（密码）并 **Confirm Passphrase**（确认密码）。

4. 单击 **OK**（确定）。



5. 重复上述步骤，将 Remote_Network_Template 替换为 Mobile_User_Template。

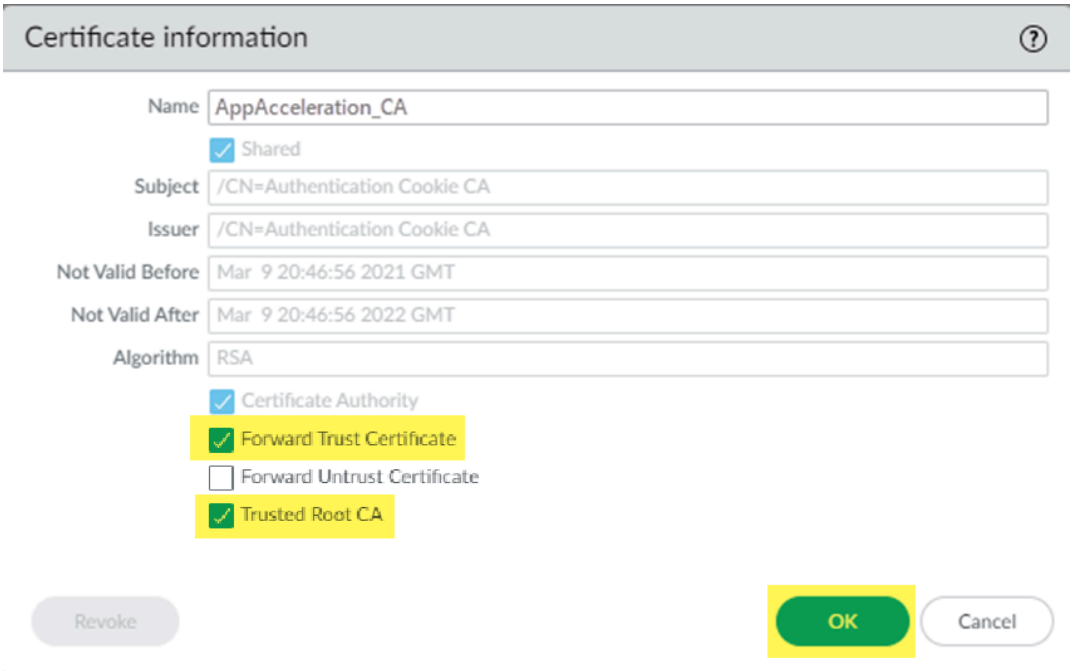
   您必须在 Mobile_User_Template 和 Remote_Network_Template 中导入这些证书，以便为移动用户和远程网络站点的用户加速应用程序。

©2025 Palo Alto Networks, Inc.

STEP 3 | 将您添加的根 CA/证书标记为转发信任证书和可信的根 CA。

如果未将证书指定为转发信任证书和可信的根 CA，则用户在使用 SSL 解密尝试访问加速应用程序时将遇到 SSL 错误。如果您在 Mobile_User_Template 和 Remote_Network_Template 中拥有证书，请在这两个模板中执行此步骤。

1. 选择您添加的根 CA/证书。
2. 选择该证书作为 **Forward Trust Certificate**（转发信任证书）和 **Trusted Root CA**（可信的根 **CA**），然后单击 **OK**（确定）。



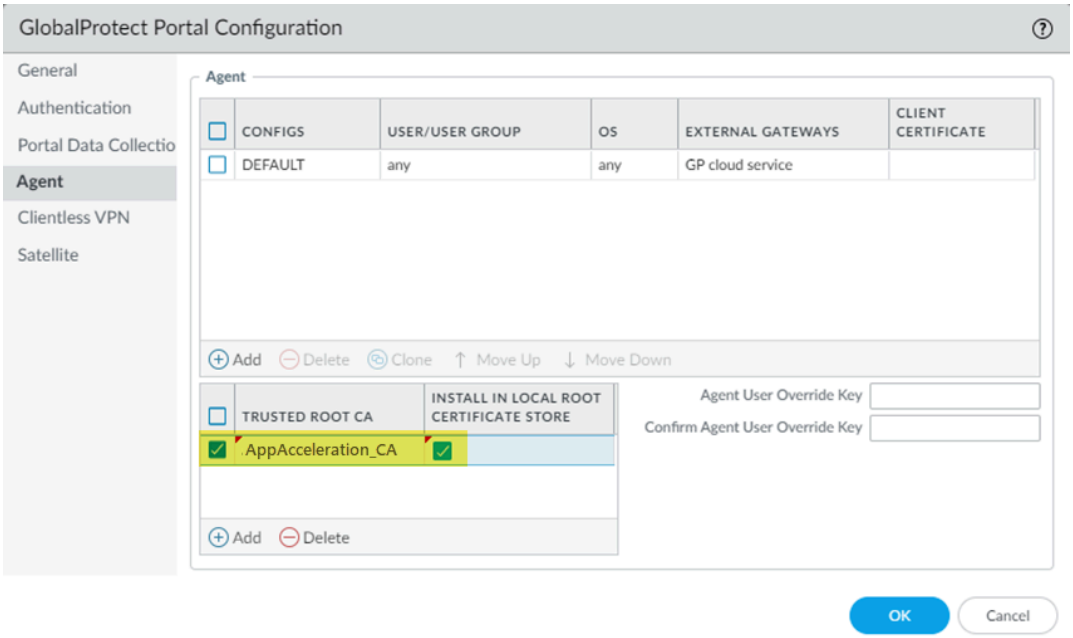
STEP 4 | **Commit and Push**（提交并推送）更改。

©2025 Palo Alto Networks, Inc.

STEP 5 | （仅限移动用户 — GlobalProtect 部署）将您添加的根 CA/证书添加到 GlobalProtect 门户配置中的 GlobalProtect 可信证书列表。

或者，如果您使用的是 *Active Directory*，则可以使用 *Active Directory GPO* 从 *AD* 分发根 *CA*。

1. 转到 **Network**（网络） > **GlobalProtect** > **Portals**（门户） > **GlobalProtect_Portal** > **Agent**（代理）。
   确保您位于 Mobile_User_Template 中。
2. **Add**（添加）您在上一个步骤中创建的可信的根 CA。
3. 选择 **Install in Local Root Certificate Store**（在本地根证书存储区中安装）。
4. 单击 **OK**（确定）。

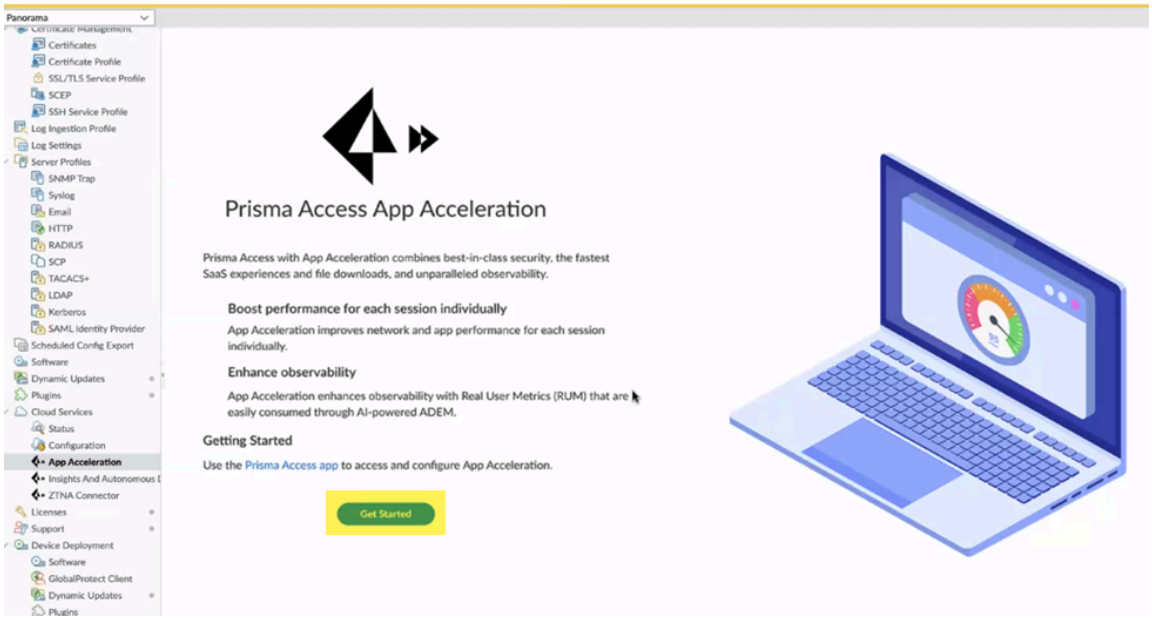


5. **Commit and Push**（提交并推送）更改。

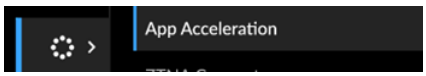
 ©2025 Palo Alto Networks, Inc.

STEP 6 | 启用 App Acceleration 并选择您创建的证书文件。

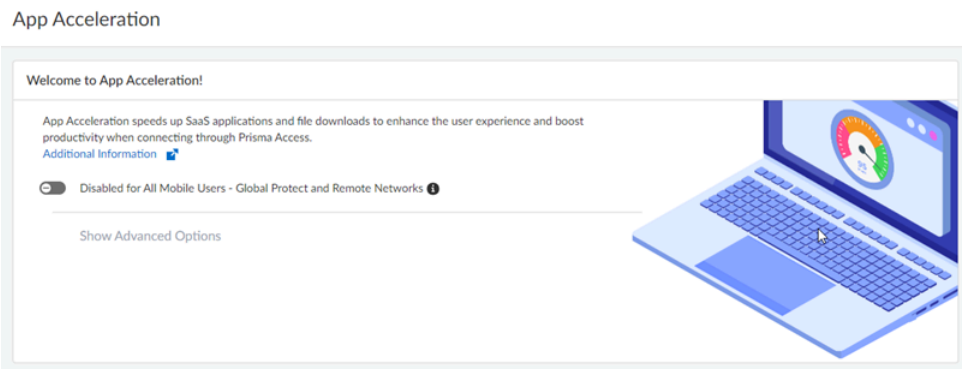
1. 转到 **Panorama** > **Cloud Services**（云服务） > **App Acceleration**，然后 **Get Started**（开始使用） App Acceleration。



2. 从左侧导航栏转到 **Workflows**（工作流） > **App Acceleration**。



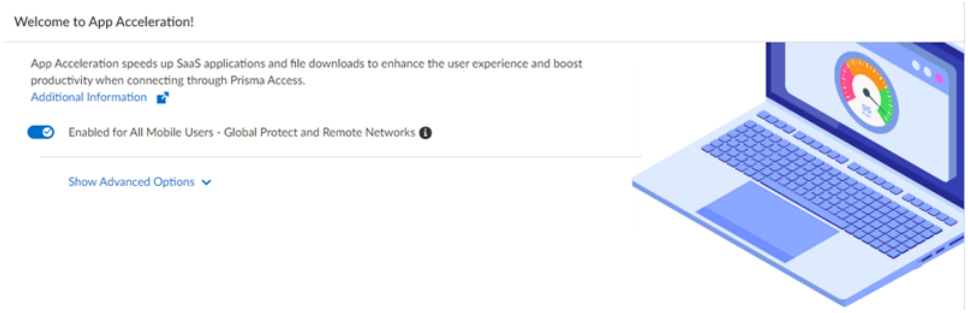
此时会显示 App Acceleration 窗口。



3. 将滑块向右移动，以便 **Enabled for all Mobile Users—GlobalProtect and Remote Networks**（为所有移动用户 — **GlobalProtect** 和远程网络启用）App Acceleration。

如果提交正在进行中，*App Acceleration* 设置将在所有提交完成后生效。

 ©2025 Palo Alto Networks, Inc.



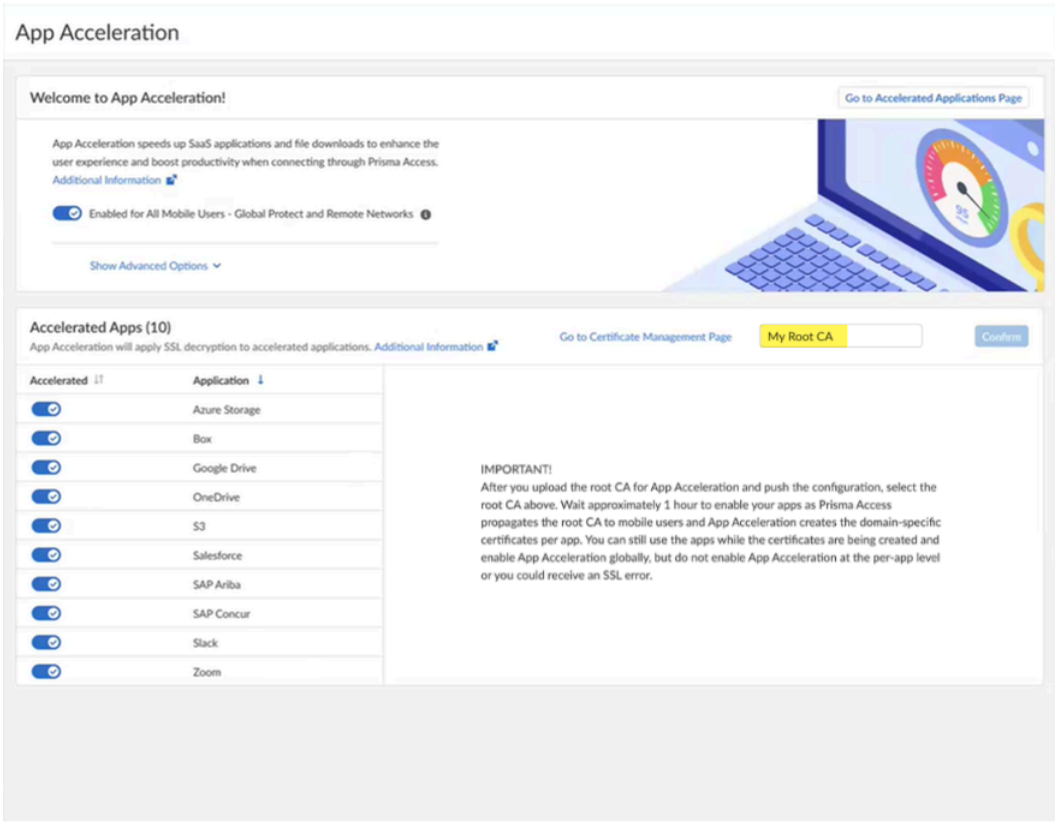
将为所有 TCP 流量将启用 App Acceleration。如果您希望加速 SaaS 应用程序，则需要选择根 CA/证书，如下一个步骤所示。

©2025 Palo Alto Networks, Inc.

STEP 7 | 在 App Acceleration 配置中，键入您在之前的步骤中创建的证书的名称，该名称与 Panorama 中列出的名称完全相同。

在键入名称之前，请确保您已提交并推送证书。

如果需要从现有证书更改证书，请键入新名称。您必须键入名称（不能从列表中选择），并且必须在输入名称之前提交并推送新证书。



导入证书后，您必须等到 *App Acceleration* 为每个应用程序生成特定于域的证书。此过程可能需要最长一小时的时间才能完成。在此期间，您可以将 ***Accelerated Apps***（加速应用程序）的滑块向左移动，以暂时禁用 *App Acceleration* 并访问应用程序，直到生成证书为止；否则，您可能会收到 *SSL* 错误，直到生成证书为止。

在您为特定应用程序开启加速后，最多需要 *10* 分钟的时间以使加速功能生效。

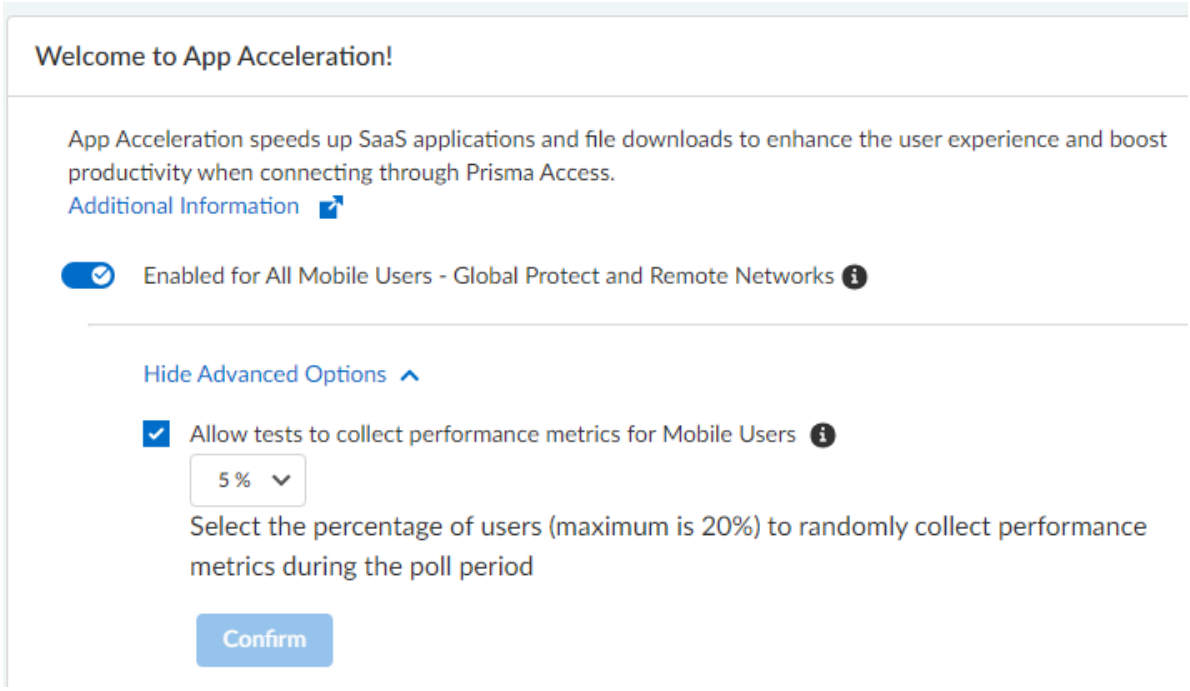
©2025 Palo Alto Networks, Inc.

STEP 8 | （可选）**Show Advanced Options**（显示高级选项）并更改指标测试参数。

- （可选）要禁用指标收集功能以获取性能信息，请取消选择 **Allow tests to collect performance metrics for Mobile Users**（允许测试以收集移动用户的性能指标）。

  Palo Alto Networks 建议您启用指标收集功能，以查看使用 App Acceleration 时应用程序性能的改善。

- （可选）要将处理预测测试的用户百分比从默认值 5% 更改为其他百分比，请在下拉列表中选择另一个百分比并 **Confirm**（确认）更改。



 ©2025 Palo Alto Networks, Inc.

©2025 Palo Alto Networks, Inc.

Prisma Access 移动用户

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证

Prisma Access 提供两种连接方法来保护移动用户：用户可以使用 GlobalProtect 应用程序或使用代理自动配置 (PAC) 文件连接到 Prisma Access。

- 使用 **GlobalProtect** 应用程序保护移动用户

  可以在以下模式下使用 GlobalProtect：

  - 隧道模式—Prisma Access 中 GlobalProtect 的默认代理模式。建立与 Prisma Access 的隧道（IPsec 或 SSL），以保障移动用户对所有应用程序、端口和协议的安全访问，并且无论用户是在您的网络内部还是外部，都能获得一致的安全防护。

    安装在用户端点上的 GlobalProtect 应用程序可保护用户到互联网、SaaS 应用程序以及内部和公共云资源的流量。将 GlobalProtect 应用程序部署到您的用户（该应用程序适用于运行 Microsoft Windows、Apple macOS 和 iOS、Android、Google Chrome OS 以及 Linux 系统的智能手机、平板电脑或笔记本电脑），这样用户就可以将流量通过隧道传输至 Prisma Access，以实现策略执行和威胁防范。GlobalProtect 应用程序还提供主机信息配置文件 (HIP) 报告，以便您可以根据设备状态创建精细规则，以确保端点只有遵守您的安全标准（例如，它们配备了最新的补丁程序、加密和病毒定义）才能访问您最敏感的应用程序。或者，要对非托管设备上的用户启用安全访问，可以启用 无客户端 VPN。Prisma Access 根据用户当前所处的位置，按区域动态扩展。
  - 代理模式—此模式可让您使用第三方 VPN 代理，同时仍使用 Prisma Access 作为安全 Web 网关，从而实现一致且卓越的 SaaS 安全性。如果您尚未准备好更换现有的专用应用程序 VPN，但希望更换安全 Web 网关，则这种连接方法非常理想。例如，您正在使用第三方 VPN 代理进行专用访问，但您希望仅使用 Prisma Access 以实现互联网安全。这种连接方法的优点包括：
    - 满足需要代理的合规性或网络要求
    - 减轻 PAC 文件管理的负担，并支持浏览器之外的代理感知应用程序
    - 由于不需要回传到本地 Web 代理，从而改善用户体验
  - 隧道和代理模式—此模式使您能够通过代理模式保障对互联网和 SaaS 应用程序的安全访问，并通过隧道模式保障对私有应用程序的安全访问。如果您需要以最快速度、最低延迟访问私有应用程序，且 Prisma Access 节点不在您所在地区，这种模式尤其有用。

    在这种模式下，GlobalProtect 应用程序首先会评估您定义的显式代理转发规则，然后将所有发往互联网的流量发送到 Prisma Access 显式代理。对于所有其他流量，应用程序根据您定义的任何分割隧道规则，确定哪些流量要通过隧道发送到 GlobalProtect 网关，以及哪些流量要从隧道中排除。您还可以使用隧道来保护任何不支持代理的应用程序。

- 使用 **PAC** 文件保护移动用户

  除了使用 GlobalProtect 保护移动用户外，您还可以使用 Prisma Access 配置显式代理。使用显式代理，端点使用 PAC 文件指示 Web 浏览器和代理感知应用程序将流量转发到 Web 代理服务器而不是目标服务器，从而保护基于 Web 的互联网（HTTP 和 HTTPS）流量。

  如果您组织的现有网络已经使用显式代理并在您的客户端端点和服务器上部署 PAC 文件，您可以顺利地从基于代理的旧 SWG 解决方案迁移到 Prisma Access，保护移动用户的出站互联网流量。如果您是出于审核或合规性目的而需要使用代理，也可以使用显式代理。

- 使用 **Prisma Access Browser Mobile** 保护移动用户

  Prisma Access Browser Mobile 通过将强大的访问控制与清晰直观的界面相结合，简化了对移动用户的安全防护。它允许用户在不依赖 VPN、证书或移动设备管理 (MDM) 系统的情况下安全地访问私有应用程序，从而降低了复杂性并简化了连接过程。

  它专为自带设备 (BYOD) 环境而设计，可确保在非托管设备上安全访问私有应用程序，使组织能够将关键资源扩展到整个员工队伍。借助 Prisma Access Browser Mobile，平板电脑成为功能多样的桌面设备，能提供与传统端点相同级别的安全性和访问能力。

  借助 Prisma Access Browser Mobile，您的组织可以简化对专用应用程序的访问，提高基于平板电脑的工作效率，并在各种移动平台上保持可靠的安全性。

©2025 Palo Alto Networks, Inc.

移动用户：GlobalProtect

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证

GlobalProtect 将在移动用户的端点上安装 GlobalProtect 应用程序，并在 Prisma Access 中配置 GlobalProtect 设置，从而为移动用户提供保护。GlobalProtect 允许您保护移动用户对所有应用程序、端口和协议的访问，并获得一致的安全性，无论用户是在您的网络内部还是外部。

使用 GlobalProtect 保护移动用户时，您需要定义设置以在云端配置门户和网关。例如，您将定义门户主机名，为移动用户设置 IP 地址池，并为内部域配置 DNS 设置。您可以利用现有配置来实现某些必需的设置，例如使用什么身份验证配置文件对移动用户进行身份验证。如果您已经有了包含身份验证配置文件、证书、证书配置文件和服务器配置文件的模板，则可以在接入期间将该模板添加到预定义的模板堆栈中，以简化设置过程。

此外，如果希望您的移动用户能够连接到您的远程网络位置，或者有位于不同地理区域的移动用户需要直接相互访问彼此的端点设备，即使您不打算使用该连接来提供对您的数据中心或总部位置的访问权限，也必须配置至少一个带有占位符值的服务连接。之所以需要这样做，是因为虽然所有远程网络位置为全网状互联，但 Prisma Access 网关（也称为位置）会以星型拓扑结构连接到服务连接，从而为您的 Prisma Access 基础设施中的内部网络提供访问途径。

- Prisma Access 上的 GlobalProtect 规划清单
- 设置“GlobalProtect—移动用户”
- GlobalProtect—自定义隧道设置
- 禁用 GlobalProtect 的工单请求 (Strata Cloud Manager)
- 监控 GlobalProtect 移动用户
- GlobalProtect 移动用户部署的 IP 地址池
- GlobalProtect 应用程序如何为移动用户选择 Prisma Access 接入位置
- 允许列出 GlobalProtect 移动用户
- GlobalProtect 应用程序升级
- 将 Prisma 访问与本地 GlobalProtect 网关集成

Prisma Access 上的 GlobalProtect 规划清单

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证

©2025 Palo Alto Networks, Inc.

如果您使用 GlobalProtect 来保护移动用户，请使用以下清单来确保您能够成功启用服务并为您的移动用户实施一致的策略（使用安装在其端点上的 GlobalProtect 应用程序保护用户，并允许用户使用无客户端 VPN 安全地访问应用程序）。

- 安装前检查清单：
  - **IP** 地址池—要为用户配置 Prisma Access，您需要提供一个 IP 地址池，并且这个地址池不能与内部使用的其他 IP 地址重叠，也不能与您为基础设施子网指定的 IP 地址池重叠。

    我们建议使用符合 *RFC 1918* 的 *IP* 地址池。虽然支持使用不符合 *RFC 1918* 的（公共）*IP* 地址，但我们不建议这样做，因为它可能与互联网公共 *IP* 地址空间发生冲突。

    请勿指定与以下 IP 地址和子网重叠的任何子网，因为 Prisma Access 保留这些 IP 地址和子网供其内部使用：

    169.254.0.0/16 和 100.64.0.0/10

    当端点使用 GlobalProtect 应用程序连接到 Prisma Access 时，Prisma Access 使用此 IP 地址池将 IP 地址分配给端点的虚拟网络适配器。连接到 Prisma Access 移动用户网关的每个设备都需要自己的 IP 地址。您可以在移动用户接入过程中指定这些池。

    Palo Alto Networks 建议池中的 IP 地址数量是将连接到 Prisma Access 的移动用户设备数量的 2 倍如果您的组织制定了自带设备 (BYOD) 策略，或者如果单个用户有多个用户帐户，请确保在分配 IP 池时考虑这些额外的设备和帐户。如果 IP 地址池达到其限制，其他移动用户设备将无法连接。

    当移动用户设备连接到网关时，Prisma Access 会从您指定的池中获取 IP 地址，并以 /24 块为单位将其分配给网关。随着更多用户设备登录，当 /24 块达到其限制时，Prisma Access 会将更多/24 块从池中分配给网关。Prisma Access 会将这些 /24 子网通告到其主干中，因为它们是根据其网关分配进行分配的。
  - 模板—Prisma Access GlobalProtect 部署会自动创建一个模板堆栈和一个顶级模板。如果您已经在内部运行 GlobalProtect，并且希望利用现有配置，则可以将其他模板添加到堆栈中，以将现有的 GlobalProtect 门户、GlobalProtect 网关、User-ID、服务器配置文件（例如，用于连接到您的身份验证服务）、证书和 SSL/TLS 服务配置文件配置推送到适用于用户的 Prisma Access。如果您没有具有现有配置设置的模板，您可以在 Prisma Access (Managed

 ©2025 Palo Alto Networks, Inc.

by Panorama) 中设置 GlobalProtect 时手动输入所需的配置设置。此外，您添加到堆栈的任何模板都必须包含用于为移动用户实施安全策略的区域的区域配置。

- 父设备组—配置适用于用户的 Prisma Access 时，必须指定要使用的父设备组，用于推送地址组和安全策略、安全配置文件、其他策略对象（如应用程序组和对象）、HIP 对象和配置文件以及服务所需的身份验证策略，以便对远程用户强制实施一致的策略。
- 接入位置—Prisma Access 为您提供全球位置，您可以在全球位置中在 Prisma Access (Managed by Panorama) 上设置 GlobalProtect。在接入您的位置之前，请查看此列表以确定应接入哪些位置以进行移动用户部署。

  选择距离您的用户最近或与您的用户位于同一国家/地区的位置。如果某个位置在您的移动用户所在的国家/地区不可用，您可以选择使用与您的移动用户相同语言的位置。

  您还可以按地理区域划分位置。通过将所有位置保留在单个区域中，您可以仅为该区域指定 IP 地址池，在可分配给池的 IP 地址数量有限的情况下这一功能非常有用。单一区域 IP 地址池还可以对部署区域提供更精细的控制，并允许您根据政策或行业法规的要求排除区域。

  如果您有适用于用户的 Prisma Access 的本地许可证，并且您拥有 GlobalProtect 部署和显式代理部署，您最多可以为两个部署组合部署五个位置。您需要在两个部署之间分配五个位置（例如，两个位置用于“移动用户—GlobalProtect”，三个位置用于“移动用户—显式代理”）。如果您拥有 Worldwide（全球）许可证，则对最大位置数量没有限制。
- 门户主机名—借助适用于用户的 Prisma Access，您可以使用默认域名 (`.gpcloudservice.com`) 快速轻松地设置门户主机名。在这种情况下，云服务会自动将主机名发布到公共 DNS 服务器并处理所有证书生成。但您可以选择在门户主机名中使用您自己的公司域名。如果您计划使用公司域名，则必须为门户获取自己的证书，并在配置服务之前将 SSL/TLS 服务配置文件配置为指向该证书。此外，如果您在门户主机名中使用自己的域名，则还需要配置 DNS 服务器以指向门户 DNS CNAME（该域名在配置过程中提供）。
- 服务连接—如果您想让移动用户能够访问内部网络上的资源（例如，数据中心或总部位置的身份验证服务器）或让移动用户访问远程网络位置，则必须创建和配置服务连接。

  即使您不打算使用该连接来提供对内部资源的访问，如果您希望移动用户能够连接到远程网络位置，或者如果您的移动用户位于不同的地理区域并且需要直接访问彼此的端点，则必须配置至少一个具有占位符值的服务连接。
- 网络中的 **IPv6** 使用情况—确定是否要对网络中的 IPv6 流量执行任何缓解措施以减少攻击面。在可以同时处理 IPv4 和 IPv6 流量的双栈端点中，移动用户 IPv6 流量默认不会发送到 Prisma Access，而是发送到端点上的本地网络适配器。因此，Palo Alto Networks 建议您将 Prisma Access 配置为 sinkhole IPv6 流量。
- **GlobalProtect** 端点日志记录—您有两种方式来收集使用 GlobalProtect 应用程序的移动用户的日志：
  - 从 **GlobalProtect** 端点手动收集日志—让移动用户从适用于 Windows、macOS和 Linux 设备的 GlobalProtect 应用程序收集日志。此选项不需要额外的配置。
  - **GlobalProtect** 应用程序日志收集用于故障排除—允许 GlobalProtect 应用程序执行端到端诊断测试，以解决连接、性能和访问问题，并生成故障排除和诊断日志，以便发送到 Strata Logging Service 进行进一步分析。您需要生成证书，以便 GlobalProtect 应用程序能够向 Strata Logging Service 进行身份验证，从而收集故障排除日志。利用 **Prisma Access (Managed by Strata Cloud Manager)**，您可以使 GlobalProtect 应用程序能够从 Strata Logging Service 收集日志以进行故障排除。对于 **Prisma Access (Managed by Panorama)**，此功能的路径为：**Panorama** > **Cloud Services**（云服务）

 ©2025 Palo Alto Networks, Inc.

> **Configuration**（配置） > **Service Setup**（服务设置） > **Generate Certificate for GlobalProtect App Log Collection and Autonomous DEM**（为 **GlobalProtect** 应用程序日志收集和自治 **DEM** 生成证书）。有关配置详细信息，请参阅 GlobalProtect 应用程序日志收集以进行故障排除。

- 安装后检查清单：
  - 将公共 **IP** 地址添加到您的网络中的允许列表—接入您的位置后，您需要检索每个位置使用的公共和 IP 地址，并将这些位置的 IP 地址添加到您的网络中的允许列表中，以允许移动用户访问 SaaS 或公共应用程序。如果添加更多位置，您还需要检索 Prisma Access 为新添加的位置分配的新 IP 地址。
  - 网关命名一致性—如果已实施了“移动用户—GlobalProtect 部署”，并且您的组织进行了并购 (M&A) 活动，您可能需要现有网关不引用早期的品牌名称或引用新的品牌名称。在这种情况下，请联系您的 Palo Alto Networks 客户团队，他们将提交 SRE 案例来满足请求。Palo Alto Networks 建议您将这项更改安排在维护时段或非高峰时段。Palo Alto Networks 将在维护期内升级部署中需要更改名称的所有网关。

设置“GlobalProtect—移动用户”

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证

在配置移动用户版之前，请确保您拥有所需的许可证（用于移动用户的 Prisma Access 许可证，以及具有适当防火墙存储空间的 Strata Logging Service 许可证）。如果移动用户要连接到其他已连接的网络，您将需要提供连接所需的企业接入节点 (CAN) 的零信任网络访问 (ZTNA) 或企业版 Prisma Access 许可证。

要配置用于移动用户的 Prisma Access，您需要以下几项：

- 用于移动用户的 Prisma Access 许可证验证用于移动用户的 Prisma Access 许可证是否已激活。
- 适用于移动用户的 IP 地址池：验证您有一个或多个不重叠的 IP 地址池可供移动用户使用。
- 门户主机名：确保您知道门户的完全限定域名 (FQDN)。
- 适用于移动用户的 GlobalProtect 代理：适用于移动用户的 Prisma Access 需要在每个支持的端点上安装 GlobalProtect 应用程序。您需要一条部署策略才能在移动用户设备上安装 Prisma Access 代理。
- 安全策略规则信息：您将部署安全策略规则以通过 Prisma Access 允许或拒绝流量。在配置适用于移动用户的 Prisma Access 时，您需要知道要部署哪些规则。
- 您的移动用户的地理位置：配置移动用户时，应选择距离移动用户最近的可用地理位置。

了解如何让 GlobalProtect 移动用户版载入 Prisma Access。

- Strata Cloud Manager
- Panorama

 ©2025 Palo Alto Networks, Inc.

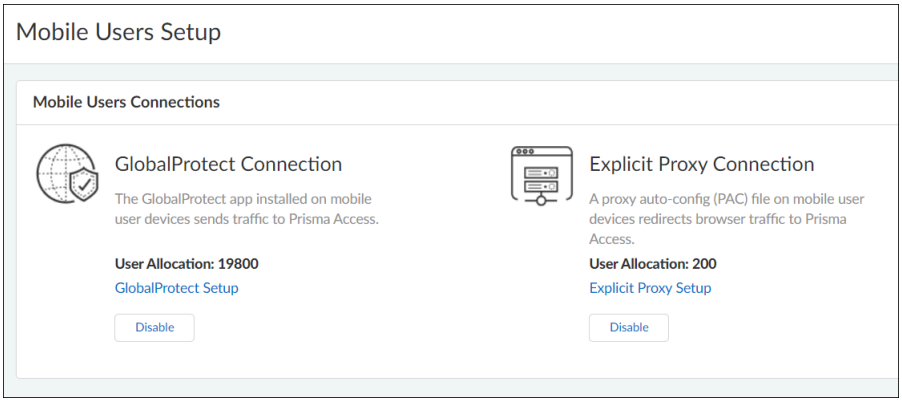
设置 GlobalProtect 移动用户(Strata Cloud Manager)

只需几个步骤，这里介绍如何开始将 GlobalProtect 移动用户带到Prisma Access。

1. 启用 **GlobalProtect** 以作为移动用户连接类型

   转到工作流 > **Prisma Access**设置 > 移动用户。

   您可以在 GlobalProtect 和显式代理连接之间划分移动用户许可证；一些用户可以通过 GlobalProtect 连接，其他用户可以通过显式代理连接。通过 **GlobalProtect Connection**,安装在移动用户设备上的 GlobalProtect 应用程序将向 Prisma Access 发送流量。

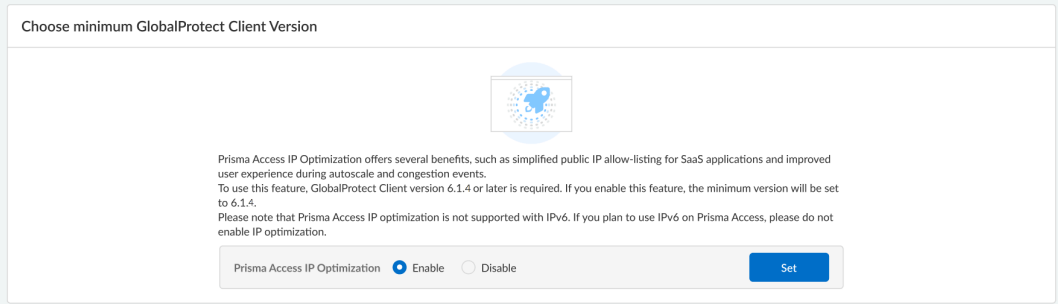


©2025 Palo Alto Networks, Inc.

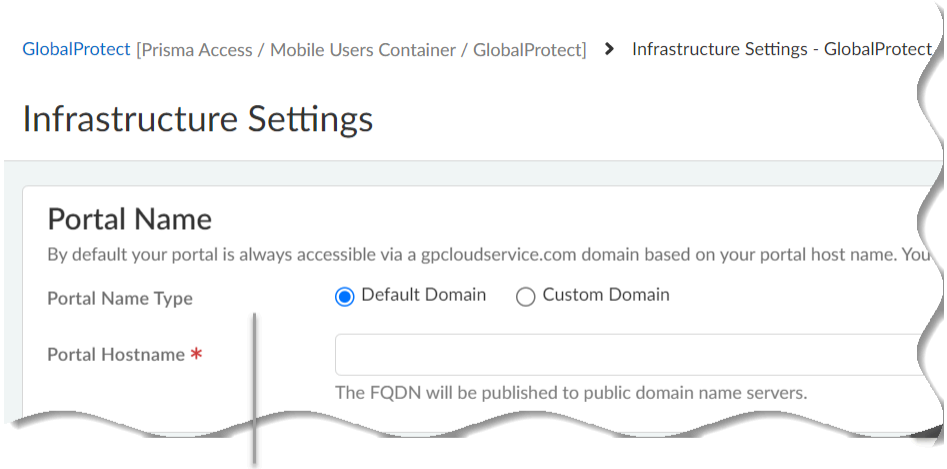
2. 设置基础架构设置

   配置特定于 GlobalProtect 的基础架构设置。有一些必需设置需要您先填写，以便Prisma Access可以配置您的移动用户环境。

   - 首次设置 *GlobalProtect* 时，您将决定是否启用*Prisma Access IP* 优化。选择启用 *IP* 优化需要 GlobalProtect 客户端版本 *6.1.4* 及更高版本、*6.2.3* 及更高版本或 *6.3.0* 及更高版本，并且不支持 *IPv6*。请谨慎选择，因为您以后无法更改此设置。
   - *IP* 优化功能仅适用于新的 *Prisma Access GlobalProtect* 部署。现有 *GlobalProtect* 部署(包括您从现有多租户部署创建的新租户)不符合条件。
   - 如果您要将 *GlobalProtect* 部署迁移到 *Prisma Access*(远离使用内部网关和门户),请确保所有用户都运行 *GlobalProtect* 应用程序版本 *6.1.4* 及更高版本、*6.2.3* 及更高版本或 *6.3* 及更高版本，然后才能启用此功能。



转到工作流 > **Prisma Access**设置 > 全局保护基础 > 结构基础 > 结构设置。



GlobalProtect Infrastructure Settings

©2025 Palo Alto Networks, Inc.

- 指定门户名称。
  - 默认域 — 如果选择此选项，您的门户主机名将使用默认域名：`.gpcloudservice.com`。这种情况下，只需输入一个**Portal Hostname**来附加到默认域名上。Prisma Access for Users将自动创建必要的证书，并将主机名发布到公共DNS服务器。
  - 自定义域 — 如果希望门户主机名中的域与您的公司域名(例如 myportal.mydomain.com)匹配，您也可以自定义门户地址。
- 输入 GlobalProtect 部署的客户端 **DNS** 解析设置。
  - 为 **DNS** 服务器
  - 选择一个区域(添加区域).

    选择全球或大区。如果指定多个代理设置，同时使用全球设置和大区设置，则 Prisma Access 将使用位置组的设置，然后使用大区设置，最后使用全球设置。Prisma Access 将在列表中从上到下评估规则。
  - 选择是否要让 Prisma Access **Resolve internal domains**（解析内部域名）；如果需要，请 **Add**（添加）一个或多个 **Internal Domain Resolve Rules**（内部域名解析规则）。
  - 为规则输入一个 **Name**（名称）。
  - 选择**Prisma Access**默认使用默认Prisma Access DNS服务器解析内部域。您希望内部 DNS 服务器仅解析您指定的域，请在域列表中输入要解析的域。在域前面指定一个星号；例如 *.acme.com。最多可以指定 1024 个域条目。
  - 如果您有可以访问内部域的 **Custom**（自定义）DNS 服务器，请指定 **Primary DNS**（主要 **DNS**）和 **Secondary DNS**（备用 **DNS**）服务器 IP 地址。
  - 如果您希望内部 DNS 服务器仅解析指定的域名，则在 **Domain Lists**（域名列表）中输入要解析的域名。在域前面指定一个星号；例如 *.acme.com。最多可以指定 1024 个域条目。
  - 完成后 **Save**（保存）更改。
- (可选)指定客户端 **IP** 池。

  默认情况下，Prisma Access 为您提供默认的移动用户 IP 地址池 100.127.0.0/16 ,该池可用于全球任何位置。Prisma Access 会从此池为每个 GlobalProtect 连接的设备分配 IP 地址。您可以选择在此处按区域添加 IP 地址池。
  - 可以为每个位置输入所需的最小子网 /23 (512 个 IP 地址）。其他位置需要最小 /23 子网。如果您指定了 Worldwide 子网，则所需的最小子网为 /23,但我们建议GlobalProtect

 ©2025 Palo Alto Networks, Inc.

移动用户部署的 IP 地址池分配等于或大于许可移动用户数量的 IP 地址，以便他们能够同时登录。

不要指定与内部使用的其他网络或配置 Prisma Access 服务基础设施 (Panorama)时分配的池重叠的地址。此外，不要使用以下 IP 地址和子网，因为 Prisma Access 保留这些 IP 地址和子网以供内部使用：

- 169.254.0.0/16
- 100.64.0.0/10

我们建议使用符合 *RFC 1918* 的 *IP* 地址池。对于移动用户，虽然我们支持使用不符合 *RFC 1918* 的（公共）*IP* 地址，但建议不要使用这些地址，因为它们可能与互联网公共 *IP* 地址空间发生冲突。

- 指定 **Primary DNS for public domains**（公共域的主 **DNS**）和 **Secondary DNS for public domains**（公共域的辅助 **DNS**）的 DNS 设置。
  - **Prisma Access**默认值—使用默认的Prisma Access DNS 服务器。
  - **Internal DNS**（内部 **DNS**） — 使用您用于解析内部域的同一服务器。
  - **Custom**（自定义）— 如果您有可以访问公共（外部）域的 DNS 服务器，请在该字段中输入主要 DNS 服务器地址。
  - 您可以添加 **Client DNS Suffix List**（客户端 **DNS** 后缀列表），以便在输入无法解析的非限定主机名时，指定客户端应在本地使用的后缀，例如，acme.local。请勿在域名后缀前输入通配符 (*) 字符（例如，acme.com）。可以添加多个后缀。

3. 设置 **Advanced Settings**（高级设置）。
   - (可选)使用静态条目将 FQDN 解析为特定 IP 地址。

     如果您的组织有来宾 Internet 服务，并且希望来宾安全使用搜索引擎，防止他们搜索可能违反公司策略的潜在不当或攻击性材料，此功能将非常有用。要执行此操作，请输入静态条目规则的唯一名称、**FQDN** 以及应定向 FQDN 请求的 IP 地址。

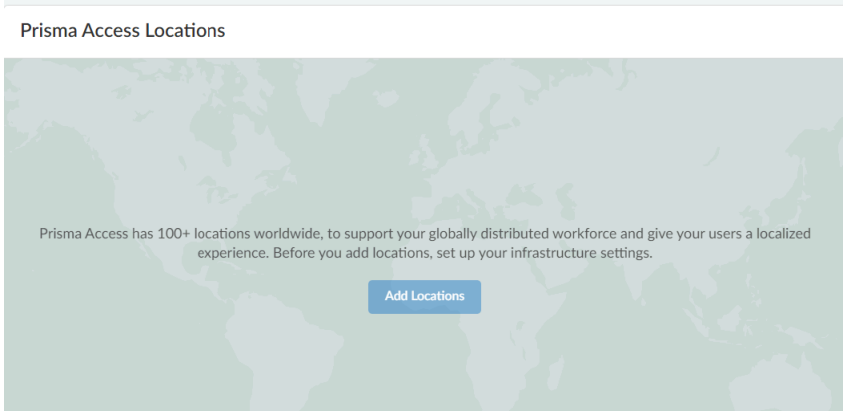
   - 如果要 Prisma Access 代理 DNS 请求，请为 **UDP** 查询重试配 置值（以秒为单位重试查询的时间间 隔（秒 ）和执行重试 尝试 的次数

     。

 ©2025 Palo Alto Networks, Inc.

4. 选择 **GlobalProtect** 用户将连接到的**Prisma Access**位置

   添加要支持 GlobalProtect 用户的Prisma Access位置。转到工作流 > **Prisma Access**设置 > 全局保护基础 > 结构 > **Prisma Access**位置。



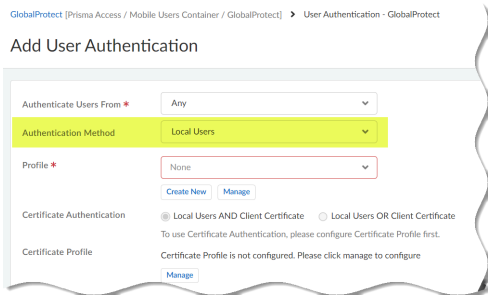
   该地图显示您可以为用户部署 Prisma Access 的全球区域。此外，Prisma Access 在每个区域内提供多个位置，以确保您的用户可以连接到提供根据用户所在区域定制的用户体验的位置。要获得最佳性能，请全选。或者，选择每个选定区域内用户需要访问的特定位置。通过将部署限制在单个区域，您可以更精细地控制已部署区域，并排除策略或行业法规要求的区域。

   如果要限制位置数量，请选择离用户最近或与用户位于同一国家/地区的位置，以提供最佳用户体验。如果某个位置在您的移动用户居住的国家/地区不可用，请选择离用户最近的位置以提供最佳性能。

5. 验证 **GlobalProtect** 用户

   设置用户身份验证，以便只有合法用户才能访问您的服务和应用程序。转到工作流 > **Prisma Access**设置 > 全局保护基础 > 架构 > 用户身份验证。

   要测试您的设置，您可以添加 Prisma Access 在本地进行身份验证的用户，也可以直接设置企业级身份验证。了解有关如何允许移动用户向 Prisma Access 进行身份验证的详细信息



6. Prisma Access 默认执行最佳实践的安全策略规则。这些规则允许您的用户安全地浏览一般互联网网站。用户是：

   - 根据 URL 阻止访问已知恶意网站
   - 禁止上传或下载已知恶意的文件
   - 防范未知、前所未见的威胁
   - 免受恶意软件、间谍软件(命令和控制攻击)和漏洞的攻击

   完成初始设置后，您可以查看并更新这些默认规则以满足您的企业需求。

©2025 Palo Alto Networks, Inc.

7. 验证移动用户的位置是否处于活动状态

   将初始配置推送到 Prisma Access，Prisma Access 会开始配置 GlobalProtect 移动用户环境。这可能需要最多 15 分钟。

   您还可以通过选择“工作流” > ***“Prisma Access*设置”** > ***Prisma Access*** > “基础结构设置”来验证您的设置，并编辑基础结构设置以确认在每个设置的位置都设置了网关。

GlobalProtect — 自定义门户地址

Prisma Access只需要最少的设置即可调配移动用户的环境，以便您可以进行测试。如果您希望在门户地址中使用公司域，可以在初始环境设置后更改地址。

默认情况下，Prisma Access使用 *gpcloudservice.com* 域设置您的移动用户需要连接到的Prisma Access入口地址，以便安全地访问互联网以及总部和数据中心。初始设置和测试环境时必须使用此默认域。如果您想在初始设置后自定义域名以使用您的公司域，您可以返回并编辑环境设置，以便您的用户连接到的门户地址包含您自己的公司域(例如 prisma-access.acme.com)。

*. gpcloudservice.com 域与 *Palo Alto Networks* 应用程序关联。

要将Prisma Access配置为使用自己的域，您必须：

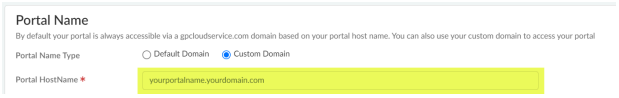
- 获取服务的证书。
- 在 DNS 服务器上创建 DNS CNAME 条目，将使用默认域的默认入口地址映射到使用公司域的自定义入口地址。您需要这样做，因为 Prisma Access 会将您在初始设置期间设置的入口地址发布到公共域服务器。

STEP 1 | 选择 **Workflows**（工作流） > **Prisma Access** 设置 > **GlobalProtect** > **Infrastructure**（基础架构），然后编辑 **Infrastructure Settings**（基础架构设置）。

在 *Strata Cloud Manager* 中，默认在门户或网关与服务连接之间启用网络冗余，确保移动用户能够冗余连接到可访问的服务和应用。

STEP 2 | 将门户名称类型设置为自定义域。

STEP 3 | 输入要使用的门户主机名。



STEP 4 | 添加要将 DNS 服务器条目映射到的门户 **DNS CNAME**。

©2025 Palo Alto Networks, Inc.

STEP 5 | **Import**（导入）您为自定义域门户地址配置的 **Certificate**（证书）。

1. 选择要导入的证书的证书 **Format**（格式）：
   - 加密私钥和证书 **(PKCS12)**— 密钥和证书位于单个容器（证书文件）中。单击 **Choose File**（选择文件）并浏览到要导入的 PKCS12 文件。
   - **Base64 Encoded Certificate (PEM)**（**Base64** 编码证书 **(PEM)**）— 如果选择此选项，则必须从证书中单独导入 **Key File**（密钥文件）。要导入 PEM 证书和密钥文件，请单击 **Choose File**（选择文件）。
2. 输入要加密密钥的 **Passphrase**（密码）和 **Confirm Passphrase**（确认密码），然后单击 **Save**（保存）。

STEP 6 | 如果您尚未这样做，请配置 DNS 服务器以指向您定义的 Prisma Access DNS CNAME。

STEP 7 | 保存环境设置并将配置推送到Prisma Access。

确保同时选择显式代理和全局保护配置范围。

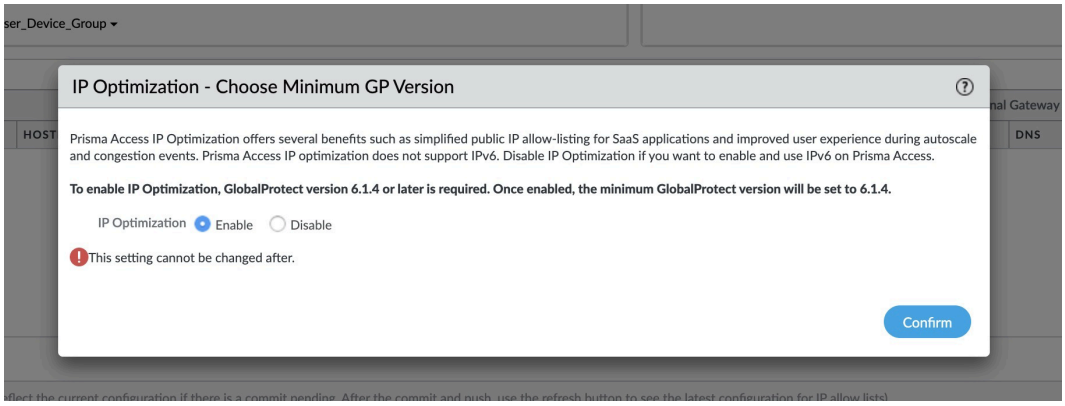
设置 GlobalProtect 移动用户(Panorama)

要配置移动用户—GlobalProtect 部署，请完成以下步骤。Prisma AccessPrisma Access 上的 GlobalProtect 规划清单在开始之前，请确保您了解如何运作，并使用清单来规划您的 GlobalProtect 部署。

©2025 Palo Alto Networks, Inc.

STEP 1 | > > > 选择Panorama云服务配置移动用户—全球保护。

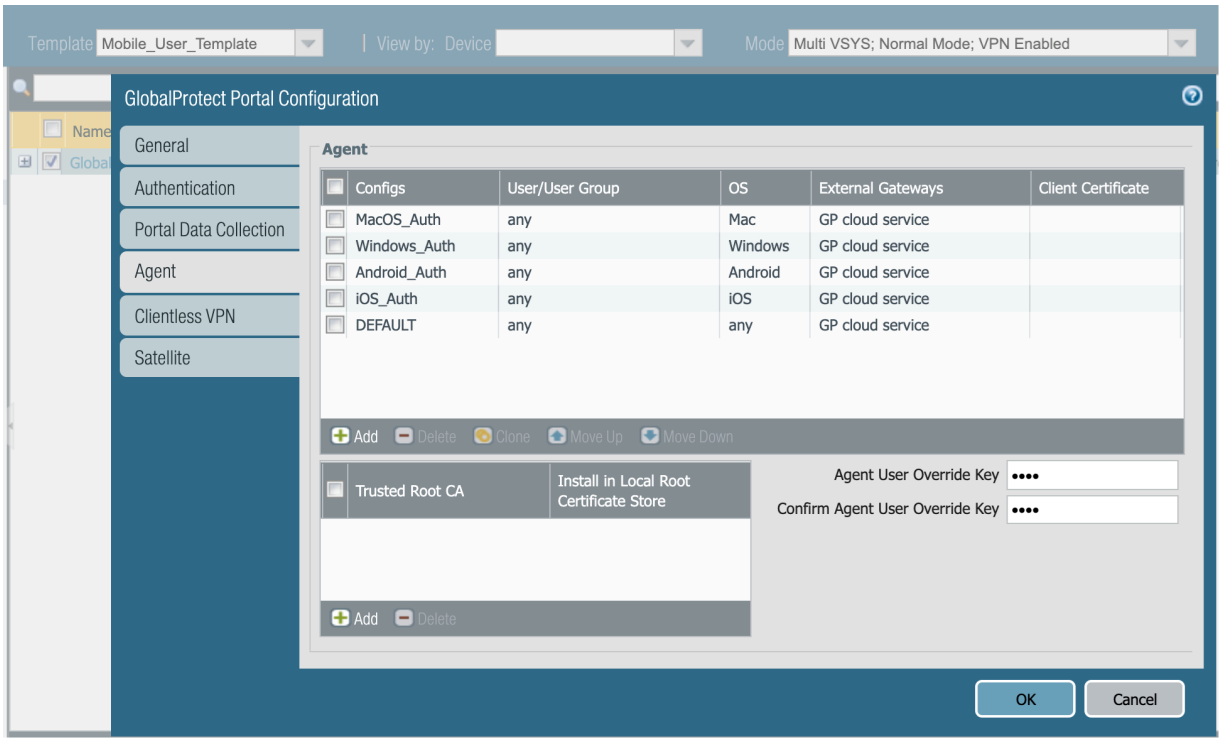
- *Prisma Access* 当您第一次设置 *GlobalProtect* 时，系统会询问您是否希望启用 *IP* 优化。选择启用 *IP* 优化需要 GlobalProtect 客户端版本 *6.1.4* 及更高版本、*6.2.3* 及更高版本或 *6.3.0* 及更高版本，并且不支持 *IPv6*。请谨慎选择，因为您以后无法更改此设置。
- *IP* 优化功能仅适用于新的 *Prisma Access GlobalProtect* 部署。现有的全球保护部署，包括您从现有的多租户部署中创建的新租户，不符合资格。
- *Prisma Access* 如果您正在将 *GlobalProtect* 部署迁移到（远离使用本地网关和门户），请确保所有用户都在启用此功能之前运行 *GlobalProtect* 应用程序版本 *6.1.4* 及更高版本、*6.2.3* 及更高版本或 *6.3* 及更高版本。



STEP 2 | Prisma Access（可选）如果您想自定义推送到客户端的代理配置，请在 Mobile_User_Template 中编辑 GlobalProtect 门户配置以添加新的代理配置。在配置代理配

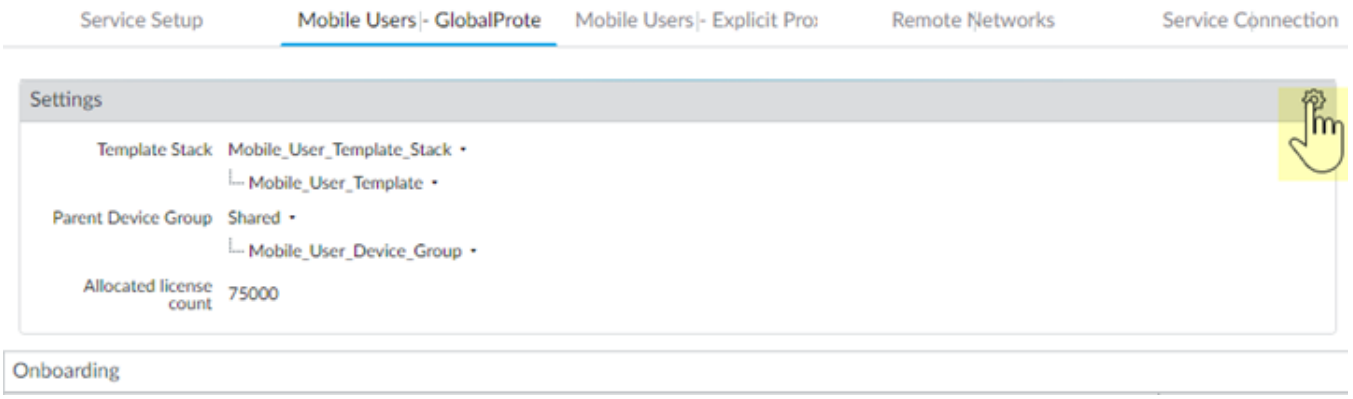
 ©2025 Palo Alto Networks, Inc.

置后，将其移动到模板中预定义的默认代理配置之上，以确保您的设置优先于默认设置。在编辑此模板时，请勿删除或更改外部网关条目。



STEP 3 | 配置云服务将推送到门户和网关的设备组层次结构。

1. 编辑 **Settings**（设置）。



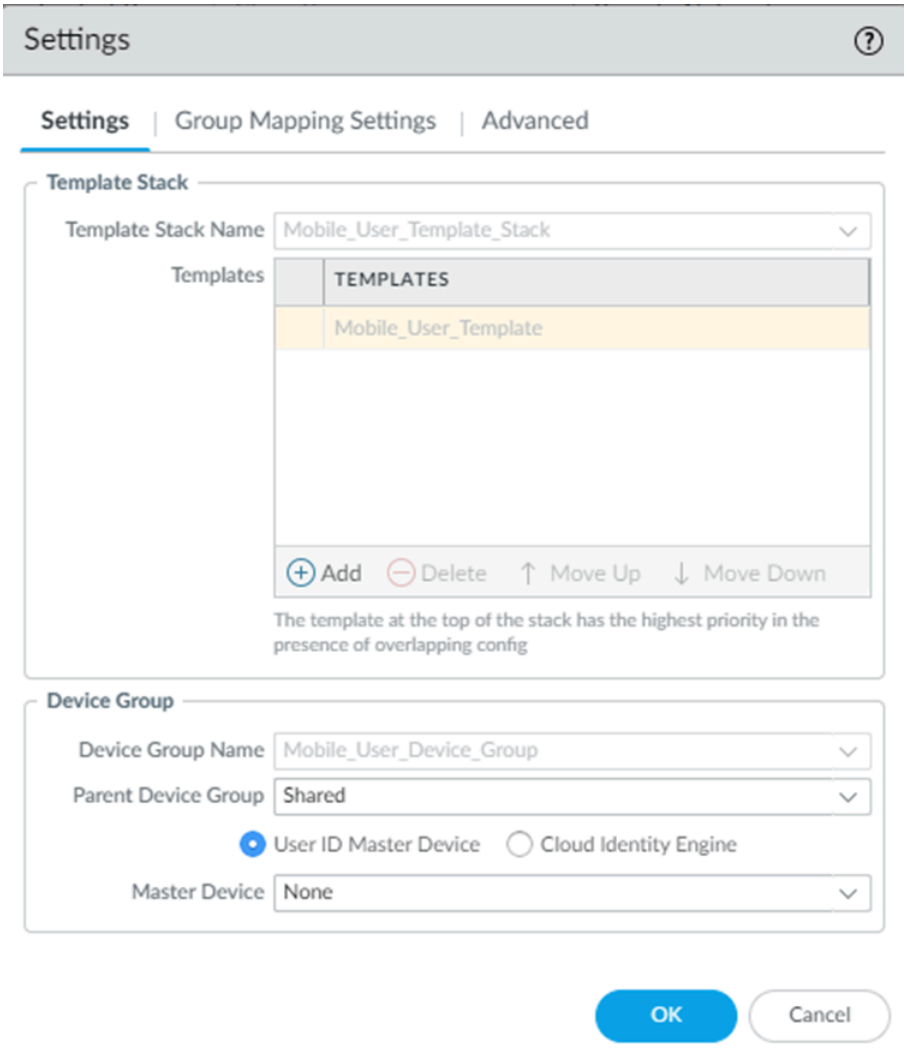
2. Prisma AccessPrisma Access在设备组部分，选择包含您要推送给用户的配置设置的父设备组，或者将父设备组保留为共享，以使用设备组共享层次结构。

   https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/policy/security-policy.htmlhttps://docs.paloaltonetworks.com/pan-os/10-1/pan-

©2025 Palo Alto Networks, Inc.

os-admin/policy/security-profiles.htmlhttps://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/host-information/configure-hip-based-policy-enforcement.htmlhttps://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/authentication.htmlPrisma Accesshttps://docs.paloaltonetworks.com/panorama/10-1/panorama-admin/panorama-overview/centralized-firewall-configuration-and-update-management/device-groups/device-group-hierarchy.html您将推动所有配置 — 包括地址组、安全策略、安全配置文件和其他策略对象（例如应用程序组和对象）、HIP对象和配置文件以及身份验证策略 — 以便用户需要使用您在此处指定的设备组层次结构来强制执行一致的策略。https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/monitoring/configure-log-forwarding.htmlPrisma AccessStrata Logging Service此外，您必须确保已配置一个日志转发配置文件，该配置文件将所需的日志类型转发到 Panorama/Strata 日志服务，且该配置文件在一个设备组中被推送给用户；这是云服务知道要转发哪些日志的唯一方式。

3. Prisma Access 基于用户的策略 (Panorama)https://docs.paloaltonetworks.com/cloud-identity/cloud-identity-engine-getting-started/get-started-with-the-cloud-identity-enginePrisma Access 基于用户的策略 (Panorama)（可选）如果您已将新一代防火墙配置为主设备或添加了云身份引擎配置文件以使用户和组信息在安全策略中可选，请选择用户-ID主设备或云身份引擎；然后，选择您创建的主设备或云身份引擎配置文件。



 ©2025 Palo Alto Networks, Inc.

STEP 4 | Prisma Access（可选）配置以使用云身份引擎的目录同步组件来检索用户和组信息。

将 Cloud Identity Engine 与 Prisma Access (Panorama) 集成https://docs.paloaltonetworks.com/cloud-identity/cloud-identity-engine-getting-started/get-started-with-the-cloud-identity-enginePrisma Access您必须配置云身份引擎的目录同步组件，以在启用和配置组映射设置中的目录同步集成之前，从云目录或活动目录（AD）检索用户和组信息。

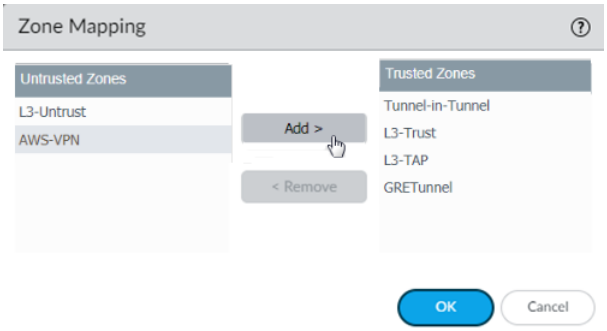
STEP 5 | 点击确定以保存移动用户设置。

STEP 6 | 在模板堆栈中将配置的区域映射为受信任或不受信任。

在Palo Alto Networks新一代防火墙上，安全策略在区域之间强制执行，这些区域映射到防火墙上的物理或虚拟接口。Prisma Access然而，对于用户来说，网络基础设施会为您自动设置，这意味着您不再需要配置接口并将其与区域关联。Prisma Access然而，为了实现一致的安全策略执行，您必须将组织内使用的区域映射为可信或不可信，以便用户可以将您推送到云服务的策略规则转换为网络基础设施内的内部区域。

1. Prisma Access 区域编辑区域映射设置。

   默认情况下，Mobile_User_Template_Stack 中的所有区域都被分类为不受信任区域。
2. 对于您想要指定为受信任的每个区域，选择它并单击添加，将其移动到受信任区域列表中。



3. 单击 **OK**（确定）保存更改。

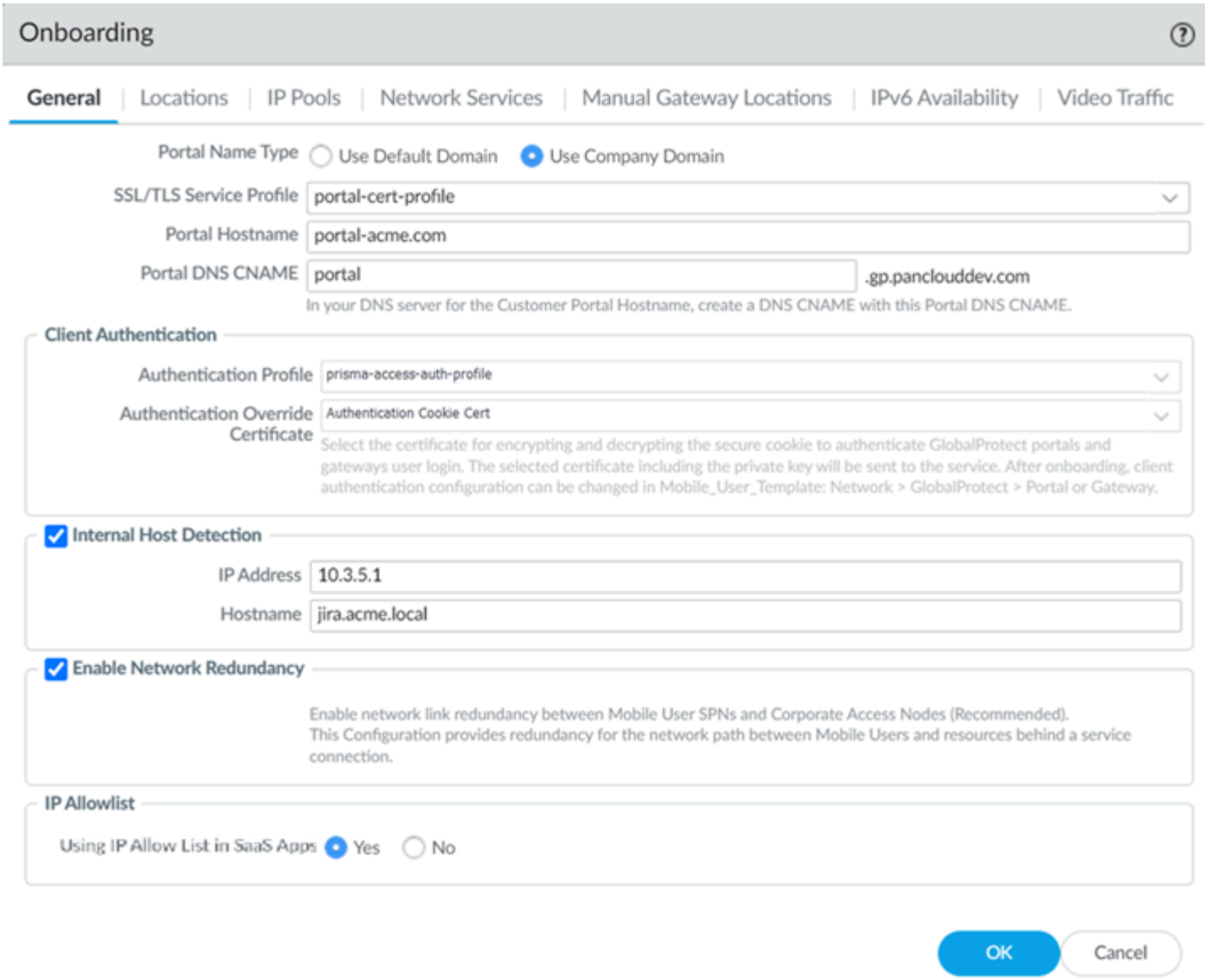
STEP 7 | 配置 GlobalProtect 门户和外部网关设置。

Prisma Access您只能将网关配置为外部网关，而不能作为内部网关。

1. 在接入部分，点击配置。
2. 在常规选项卡中，指定门户名称类型：
   - 使用默认域名—如果您选择此选项，您的门户主机名将使用默认域名：.gpcloudservice.com。Prisma Access在这种情况下，只需输入一个门户主机名以

 ©2025 Palo Alto Networks, Inc.

附加到默认域名。对于用户，将自动创建必要的证书并将主机名发布到公共 DNS 服务器。



Prisma Access如果您已经有一个 GlobalProtect 部署，并且有一个现有的门户名称，并且您想继续使用该门户名称，请添加一个 CNAME 条目，将门户名称映射到您现有的门户名称。Prisma Access例如，如果您有一个名为 portal.acme.com 的现有门户，并且您想将新门户映射到相同的名称，您需要将 gpcs2.gpcloudservice.com 的 CNAME 添加到现有门户的 DNS 条目中。

*. gpcloudservice.com 域与 *Palo Alto Networks* 应用程序关联。

- 使用公司域名—如果您希望门户主机名中的域名与您的公司域名匹配（例如，myportal.mydomain.com），请选择此选项。https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/get-started/enable-ssl-between-globalprotect-components/deploy-server-certificates-to-the-globalprotect-

©2025 Palo Alto Networks, Inc.

componentshttps://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/certificate-management/configure-an-ssltls-service-profile.html如果您想使用此选项，您必须首先获得自己的证书并配置指向它的 SSL/TLS 服务配置文件。然后，您可以通过选择 SSL/TLS 服务配置文件并输入门户主机名来配置门户名称。如果您使用此选项，则必须将您的内部 DNS 服务器指向门户 DNS CNAME，即带有 .gpcloudservice.com 域的门户的主机名。例如，如果您指定了 DNS 主机名 acme-portal.acme.com，您需要在内部 DNS 服务器上创建一个 DNS CNAME 条目，将该主机名映射到 acme-portal.gpcloudservice.com。



https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/certificate-management/obtain-certificates/import-a-certificate-and-private-key*Prisma Access* > > > > 如果您需要上传新的证书，请导入证书和私钥；然后，在网络 *GlobalProtect* 门户 *GlobalProtect_Portal* 身份验证下查看正在使用的 *SSL/TLS* 服务，并检查 *SSL/TLS* 服务配置文件名称。此字段仅在您使用公司域而不是默认域时显示。 > > 然后，您可以选择设备证书管理 *SSL/TLS* 证书配置文件，并用您导入的证书替换门户使用的 *SSL/TLS* 配置文件中的证书。

3. Prisma Access选择一个身份验证配置文件，该配置文件指定如何验证移动用户，或创建一个新的配置文件。

   如果您添加了一个包含身份验证配置文件配置的父设备组，您应该在可用配置文件列表中看到它。https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/globalprotect-user-authentication/set-up-external-authentication如果您没有在设备组中推送配置文件，您现在可以创建一个身份验证配置文件。

   在您提交并推送更改后，您无法对此区域中的身份验证配置文件和身份验证覆盖证书进行任何更改，选择变为只读。https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/globalprotect-portals/define-the-globalprotect-client-authentication-configurations要在初始接入后进行更改，请在 *Mobile_User_Template* 下修改或添加一个或多个 *GlobalProtect* 客户端身份验证配置。

4. 选择一个身份验证覆盖证书，以加密移动用户对门户和网关进行身份验证的安全 cookie。

   如果您添加了一个包含您想要用于加密身份验证 Cookie 的证书的父设备组，您应该在可用证书列表中看到它。https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/certificate-management/obtain-certificates/import-a-certificate-and-private-keyhttps://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/certificate-management/obtain-certificates/generate-a-certificate如果您没有在设备组中推送证书，您现在可以导入或生成一个。

5. （可选）为了确保您的移动用户始终可以访问通过服务连接访问的服务和应用程序，请在门户或网关与服务连接之间启用网络冗余。

   此功能在移动用户数据平面和不同计算位置的服务连接之间提供冗余网络路径。启用冗余为用户提供了更强大的访问能力，以便在数据中心或总部位置通过服务连接访问资源。由于移动用户需要服务连接才能从远程网络访问资源，因此用户在访问远程网络位置的资源时也具有更强的弹性。

 ©2025 Palo Alto Networks, Inc.

6. （可选）如果您不要求 GlobalProtect 端点在内部网络上具有隧道连接，请启用内部主机检测。

   1. 选择内部主机检测复选框。
   2. 输入用户只能从内部网络访问的主机的 **IP Address**（IP 地址）。
   3. 输入与该 IP 地址对应的 DNS **Hostname**（主机名）。尝试连接的客户端会对指定地址执行反向DNS查找。Prisma Access如果查找失败，客户端确定它需要一个隧道连接到用户。

   *Prisma Access*https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/globalprotect-portals/define-the-globalprotect-client-authentication-configurations/define-the-globalprotect-app-configurations > > > > > > 将您在此处指定的内部主机检测设置复制到您的 *GlobalProtect* 门户配置中的默认代理设置（*NetworkGlobalProtect Portals<portal-config> AgentDEFAULTInternal*）。如果您在 *GlobalProtect* 门户中为默认代理输入了内部主机检测设置，则无法在此处更改选项，必须在门户中进行更改。*Prisma Access* > > > > 如果您需要多个代理配置，请在 *GlobalProtect* 门户中输入默认代理配置的设置，并将这些设置用于，然后选择 *NetworkGlobalProtect* 门户*<portal-config>* 代理并添加非默认配置，并在部署的其他部分指定该配置。

7. （可选）如果您的组织使用允许列表来控制对公共或SaaS应用程序的访问，请说明您是否在SaaS应用程序中使用IP允许列表。

   检索 Prisma Access 的 IP 地址Prisma Access允许列出 GlobalProtect 移动用户 (Panorama)为了使您能够将 GlobalProtect - 移动用户部署的公共（出口）IP 地址添加到您在组织内使用的任何 SaaS 应用程序允许列表中，提供给您 IP 地址，并让您在使用它们之前验证您已将其添加到允许列表中。Prisma Access您可以为现有部署和新部署实施出站 IP 地址的允许列表。

8. > > > > https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/globalprotect-portals/define-the-globalprotect-client-authentication-configurations/customize-the-globalprotect-app（可选）通过选择网络 GlobalProtectPortals GlobalProtect_PortalAgent，自定义 GlobalProtect 应用程序设置（例如，指定 GlobalProtect 使用的连接方法），选择您想要自定义的配置或选择默认值，选择应用程序，然后自定义 GlobalProtect 应用程序。

STEP 8 | 选择您希望部署移动用户的位置及与这些位置相关的区域。

“位置”选项卡显示地图。地图突出显示了全球区域（美洲、欧洲和亚太地区）以及每个区域内的可用位置。选择一个区域，然后选择每个区域想要部署的位置。通过将部署限制在单个区

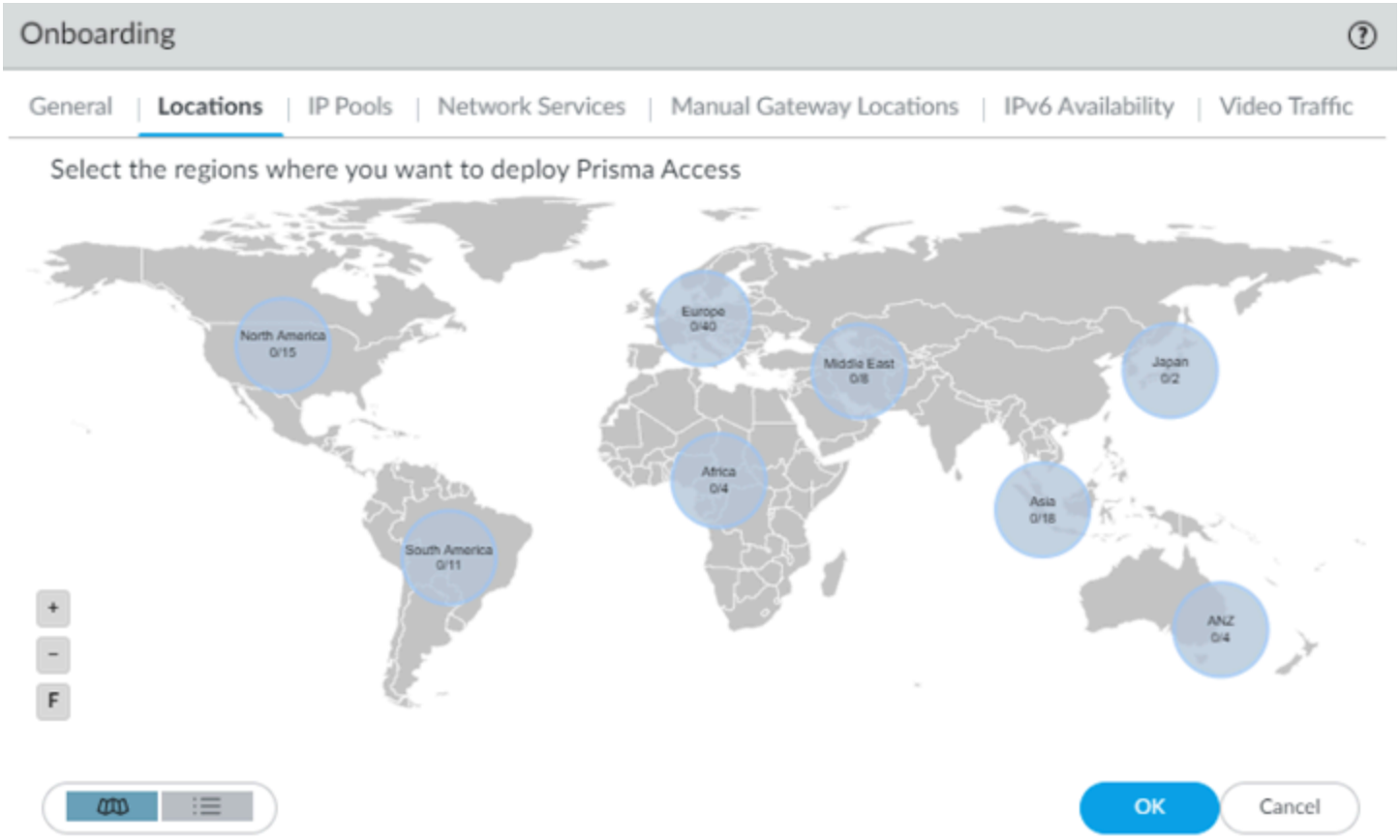
 ©2025 Palo Alto Networks, Inc.

域，您可以更精细地控制已部署区域，并根据策略或行业法规的要求排除区域。您可以选择一个离您的移动用户最近的区域位置，或者根据您的政策或行业规定选择一个位置。

*Prisma Access*如果其他位置不可用，则使用香港、荷兰中央和美国西北地区作为备用移动用户位置。因此，*Palo Alto Networks* 强烈建议您在移动用户接入期间启用至少一个这些位置。

用两个星号表示的位置是本地区域。这些位置将计算、存储、数据库和基础架构服务置于人口密集和工业中心附近；然而，它们也存在一些局限性。要添加本地区域，请联系您的 Palo Alto Networks 代表。

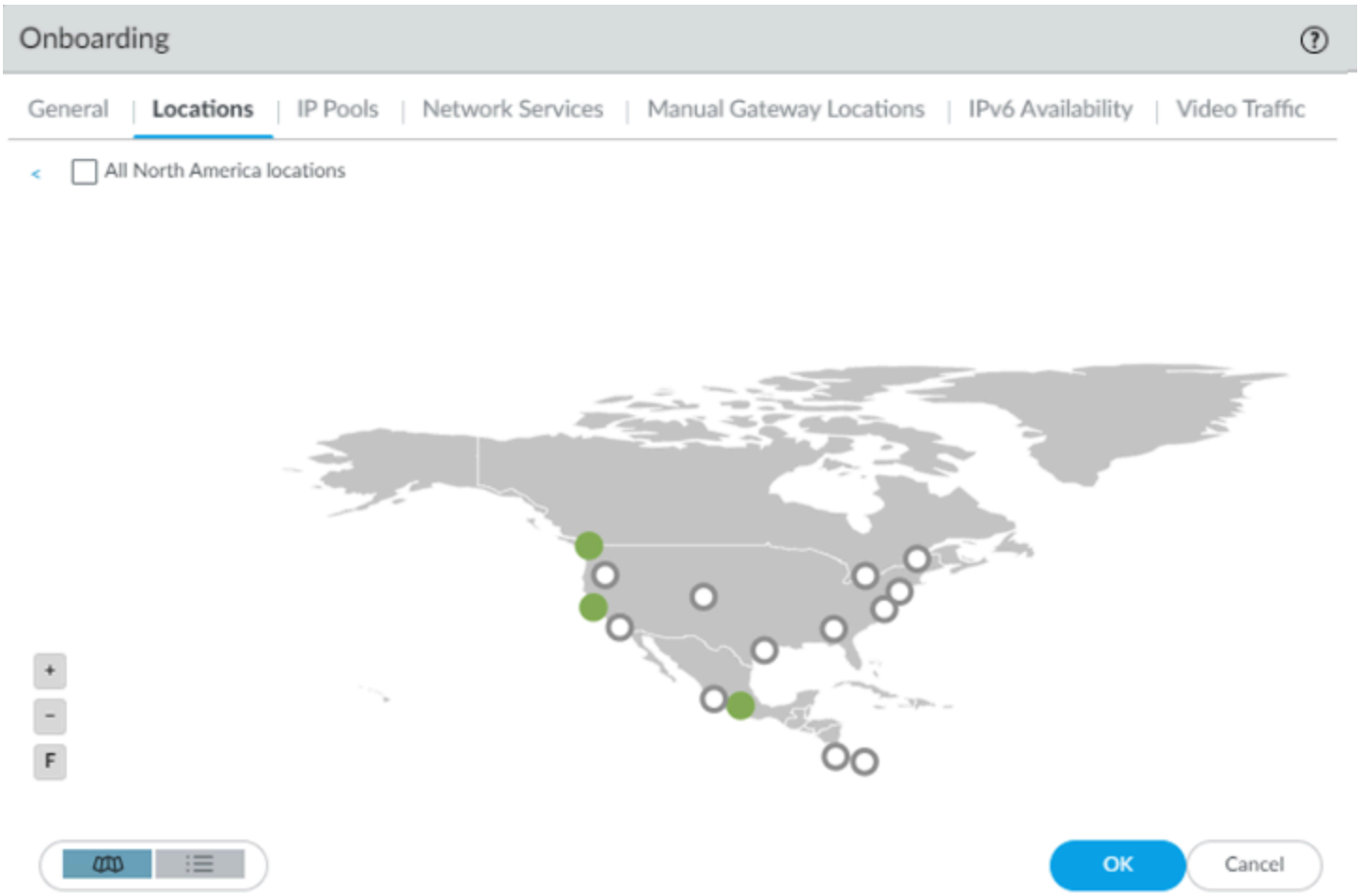
1. Prisma Access 位置点击位置选项卡并选择一个区域。



2. Prisma Access在地图上选择您所选区域内的一个或多个网关。

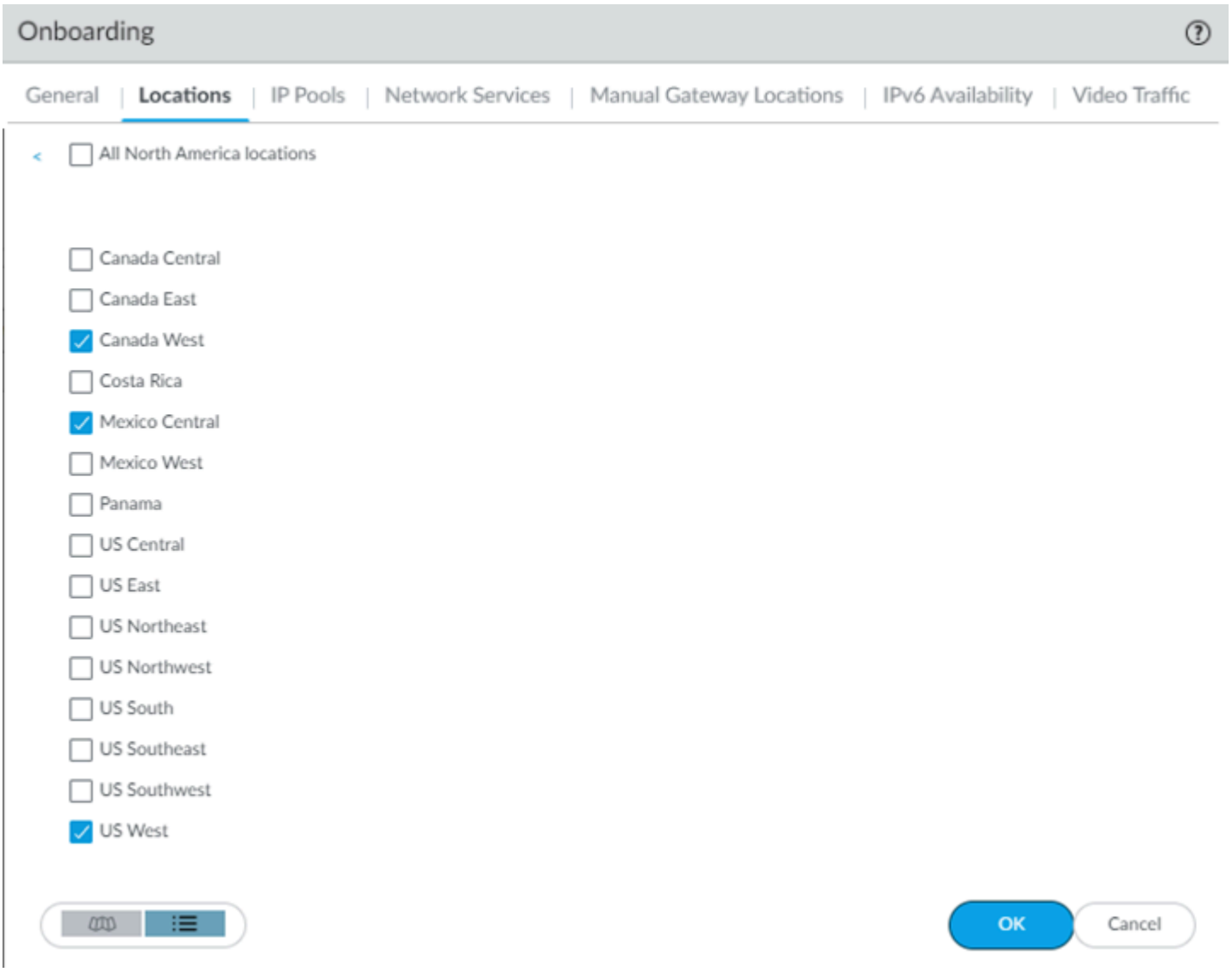
   将光标悬停在某个位置上即可突出显示该位置。白色圆圈表示可用位置；绿色圆圈表示您已选择该位置。

 ©2025 Palo Alto Networks, Inc.



除了地图视图，您还可以查看地区和位置的列表。从左下角选择地图视图和列表视图。在列表视图中，列表显示按列排序的区域，所有位置均按区域排序。您可以选择某个区域内的 所有 站点（对话框顶部）。

©2025 Palo Alto Networks, Inc.



STEP 9 | 通过选择 IP 池选项卡并添加 IP 地址池，设置用于分配 IP 地址给 GlobalProtect 终端的 IP 地址池。

1. 指定IP地址池的区域。

   您可以将单个 IP 地址池用于全球（**Worldwide**（全球））所有 GlobalProtect 端点，您可以将单独的地址池用于拥有移动用户的每个大区，也可以为每个位置组指定地址池（位置组是指比大区小的一组位置）。您还可以指定全球、每个大区或每个位置组 IP 池的组合。例如，您可以为特定位置组添加一个池，然后添加一个 **Worldwide**（全球）池以用于所有其他位置。

   如果您有依赖于用户源IP地址来识别用户详细信息（例如基于位置的服务或基于用户组或功能的服务）的服务，请使用位置组特定的IP地址池，以便您可以应用访问控制策略，或

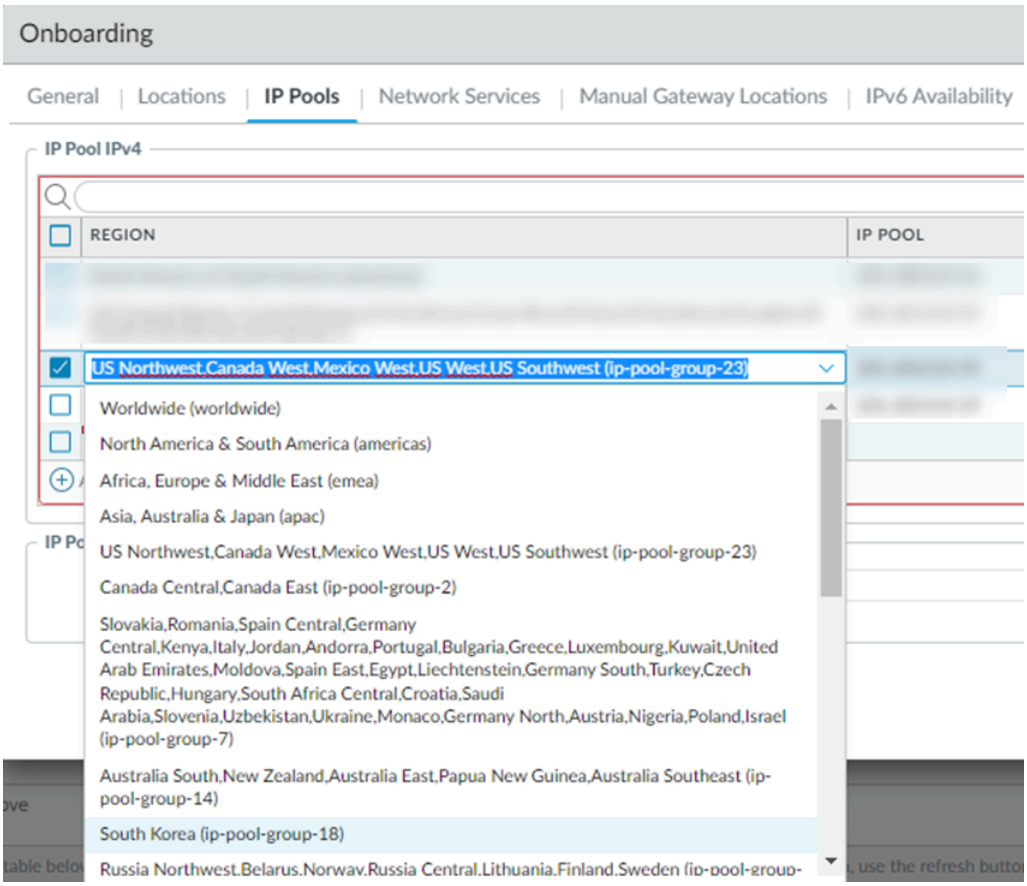
 ©2025 Palo Alto Networks, Inc.

在不同计算区域的不同国家之间执行路由或策略操作。例如，您可以为位于不同计算位置的加拿大和巴西使用单独的 IP 地址池，以提供不同的访问和安全控制。

要使用特定于位置组的 IP 地址池，还必须指定全球或大区特定的地址池。

GlobalProtect 移动用户首先消耗位置组中的 IP 地址，然后消耗特定于大区的 IP 地址，最后消耗全球 IP 地址。例如，如果您为位置组和全球指定了一个池，然后用尽了位置组池中的可用 IP 地址，则 Prisma Access 将从 **Worldwide**（全球）池中获取 IP 地址以在该位置组中使用。

- 要指定可由所有 GlobalProtect 移动用户使用的 IP 池，请选择 **Worldwide**（全球）。
- 要指定 GlobalProtect 用户可以在特定大区使用的 IP 池，请选择该大区。
- 要指定特定于位置组的 IP 池，请从列表中选择这些 IP 池。



2. 输入一个 IP 池以分配给您选择的区域中的端点。
   - 可以为每个位置输入所需的最小子网 /23 (512 个 IP 地址）。其他位置需要最小 /23 子网。如果您指定一个全球子网，最低要求的子网是 /23，但我们建议分配的 IP 地

 ©2025 Palo Alto Networks, Inc.

址GlobalProtect 移动用户部署的 IP 地址池数量应等于或大于已授权的移动用户数量，以便他们可以同时登录。

配置 Prisma Access 服务基础设施 (Panorama)不要指定与您内部使用的其他网络或您分配的池重叠的地址。此外，不要使用以下 IP 地址和子网，因为 Prisma Access 会保留这些 IP 地址和子网以供内部使用：

- 169.254.0.0/16
- 100.64.0.0/10



我们建议使用符合 *RFC 1918* 的 *IP* 地址池。对于移动用户，虽然我们支持使用不符合 *RFC 1918* 的（公共）*IP* 地址，但建议不要使用这些地址，因为它们可能与互联网公共 *IP* 地址空间发生冲突。

STEP 10 | https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-panorama-admin/prisma-access-advanced-deployments/advanced-deployments-that-apply-to-all-prisma-access-types/dns-resolution-for-mobile-users-and-remote-networks/dns-resolution-for-

 ©2025 Palo Alto Networks, Inc.

mobile-users-globalprotect-deployments要为您的内部和外部（公共）域指定 DNS 解析设置，请选择网络服务选项卡并添加设置。

使用活动隧道连接的GlobalProtect终端使用其虚拟网络适配器而不是物理网络适配器，因此需要单独的DNS解析设置。

在网络服务窗口中配置网络设置。

- 从下拉菜单中选择一个区域。

  选择全球，选择一个大区，或选择一个位置组以全局应用 DNS 设置。Prisma AccessPrisma Access如果您指定了多个代理设置，混合了全球、大区和特定位置组的设置，系统将使用位置组的设置，然后是大区设置，最后是全球设置。系统从列表的顶部到底部评估规则。
- 为内部域添加一个或多个规则以配置DNS设置。
  - 在 **Rule Name**（规则名称）中输入规则的唯一名称。
  - Prisma Access请勿输入127.0.0.1地址，因为这可能会导致内部路由问题。
  - 如果您希望内部 DNS 服务器仅解析您指定的域，请在 **Domain Lists**（域列表）中输入要解析的域。在域前面指定一个星号；例如 *.acme.com。最多可以指定 1024 个域条目。

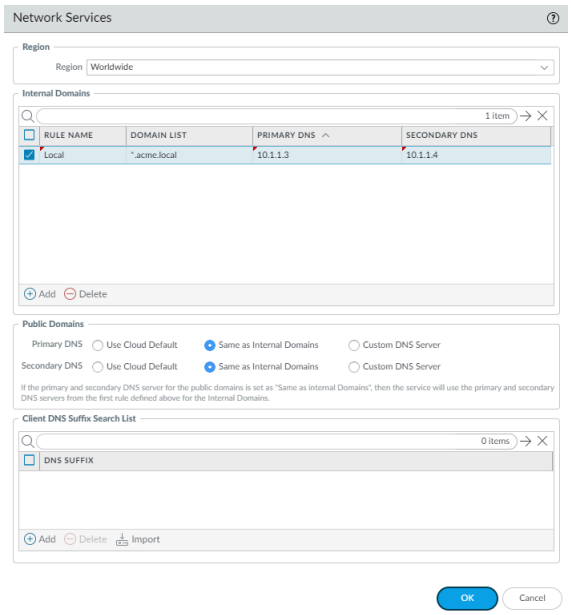
    *Prisma Access*具有预定义规则，通过 *Cloud Default* 服务器解析 **.amazonaws.com*、**.aws.amazon.com*、**.googleapis.com* 和 **.google.internal* 域名。*Prisma Access*如果您希望内部 *DNS* 服务器解析更具体的域名（例如，**.s3.amazonaws.com* 而不是 **.amazonaws.com*），请在域名列表中输入 *URL*。它会从最长到最短评估域名，然后从列表的顶部到底部。
  - Prisma Access如果您有一个可以访问您内部域的自定义 DNS 服务器，请指定主 DNS 和备用 DNS 服务器的 IP 地址，或选择使用云默认值以使用默认 DNS 服务器。
- 指定公共域的DNS设置。
  - Prisma Access使用云默认—使用默认的 DNS 服务器。
  - **Same as Internal Domains**（与内部域相同）—使用您用于解析内部域的同一服务器。当您选择此选项时，用于解析公共域的 DNS 服务器与内部域部分中第一个规则配置的服务器相同。
  - **Custom DNS server**（自定义 **DNS** 服务器）—如果您有可以访问公共（外部）域的 DNS 服务器，请在该字段中输入主 DNS 服务器地址。

  （可选）您可以选择 **Add**（添加）一个 **DNS Suffix**（**DNS** 后缀），以便在用户输入客户端无法解析的非限定主机名时，指定应在本地使用的后缀，例如 acme.local。请勿在域名后缀前输入通配符 (*) 字符（例如，acme.com）。可以添加多个后缀。
- Prisma Access如果您想代理 DNS 请求，请配置 UDP 查询的值（重试查询的间隔时间（以秒为单位）和要执行的重试次数）。

  Prisma Accesshttps://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-panorama-admin/prisma-access-advanced-deployments/advanced-deployments-that-apply-to-all-prisma-access-types/dns-resolution-for-mobile-users-and-remote-networks/

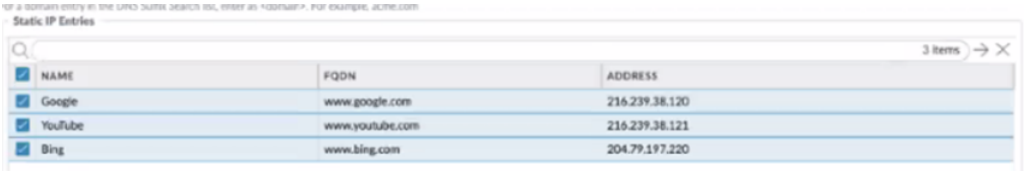
 ©2025 Palo Alto Networks, Inc.

dns-resolution-for-mobile-users-globalprotect-deployments有关代理 DNS 请求的更多信息，请参阅移动用户的 DNS 解析 — GlobalProtect 部署。



STEP 11 | （可选）使用 **Static Entries**（静态条目）以将 FQDN 解析为特定的 IP 地址。

此功能在您的组织中提供访客互联网服务时非常有用，您希望您的客人安全地使用搜索引擎，防止他们搜索可能不当或冒犯的材料，这可能违反公司政策。要执行此操作，请输入静态条目规则的唯一名称、**FQDN** 以及应定向 FQDN 请求的 IP 地址。



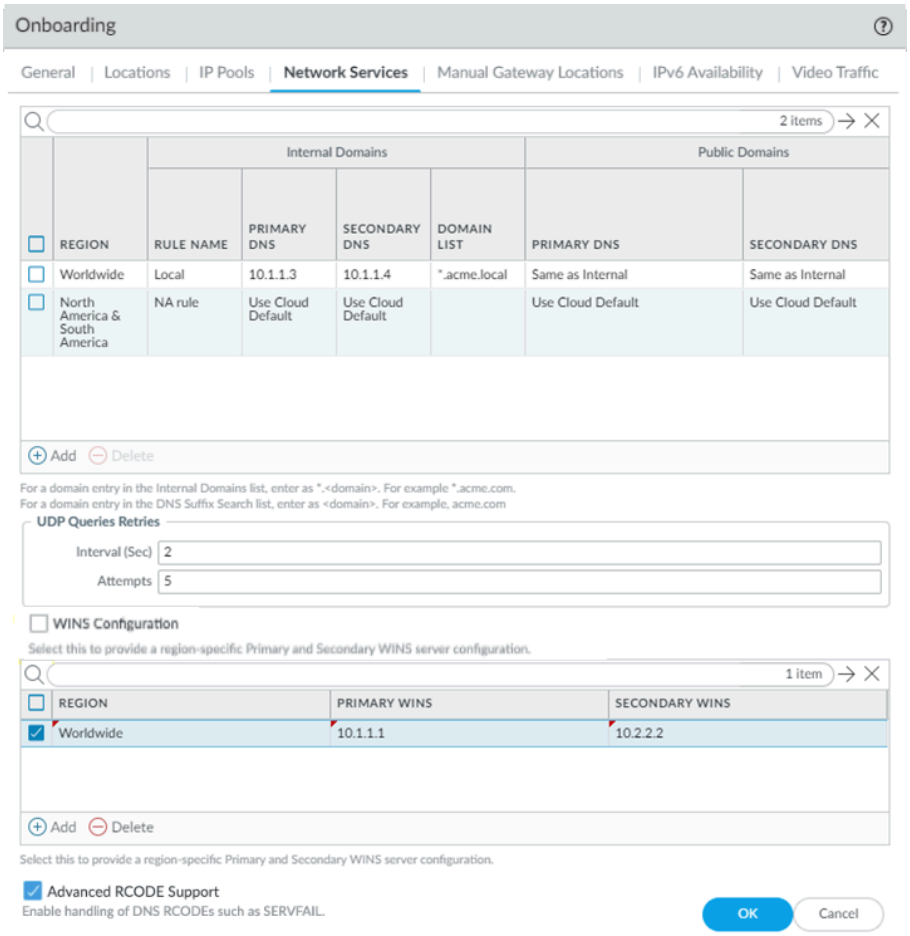
STEP 12 | （可选）如果您的部署使用基于 Windows Internet Name Service (WINS)，您可以通过选择 WINS 配置来指定 WINS 服务器以解析 NetBIOS 名称到 IP 地址的映射；选择 WINS 服务器的区域或选择全球以在全球范围内应用 WINS 配置，然后指定一个主 WINS 和（可选）一个次 WINS 服务器地址。

Prisma Access在您启用 WINS 后，可以通过 GlobalProtect 将 WINS 配置推送到移动用户的终端。

©2025 Palo Alto Networks, Inc.

STEP 13 | （可选）选择 Advanced RCODE Support（高级 RCODE 支持）可在收到 RCODE 2 (SERVFAIL) 和 RCODE 5 (REFUSED) DNS 返回码的情况下让主 DNS 服务器故障转移到辅助 DNS 服务器。

DNS 响应代码 SERVFAIL 表示与主 DNS 服务器的通信错误，DNS 响应代码 REFUSED 表示主 DNS 服务器拒绝提供请求的信息。在这两种情况下，服务都会故障切换到辅助 DNS 服务器。



 ©2025 Palo Alto Networks, Inc.

STEP 14 | （可选）如果您允许移动用户从 GlobalProtect 应用程序手动选择网关，请选择用户可以从其 GlobalProtect 应用程序查看的手动网关位置。

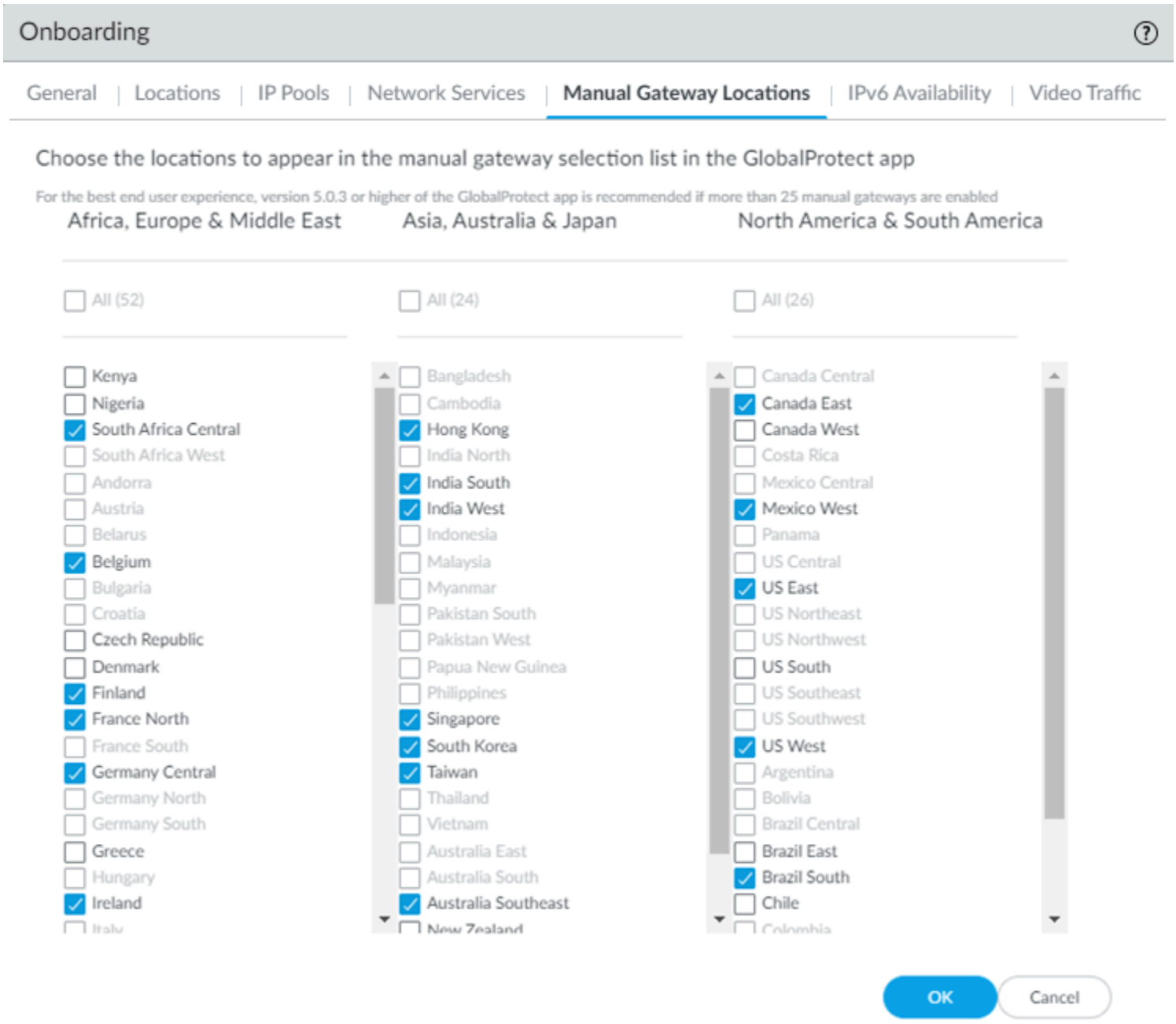
选择一部分已入驻的位置会减少移动用户在其 GlobalProtect 应用中可以查看的可用网关数量，以便手动选择网关。

Prisma Access如果您在此选项卡中不选择手动网关，则默认选择以下网关列表。

- 澳大利亚东南部
- 比利时
- 巴西南部
- 加拿大东部
- 芬兰
- 法国北部
- 德国中部
- 中国香港
- 印度西部
- 爱尔兰
- 以色列
- 日本中部
- 荷兰中部
- 沙特阿拉伯
- 新加坡
- 南非中部
- 韩国
- 中国台湾
- 英国
- 美国东部
- 美国西部

Prisma Access让您仅选择已接入的网关。例如，如果您在选择位置时不选择英国，则无法将英国选择为手动网关（该位置已变灰）。

 ©2025 Palo Alto Networks, Inc.



根据与*Yogesh*的‘恢复绿色’和工单*02116470*的讨论，添加了此项。如果您需要在上载后删除一个位置，并且它被选为手动网关位置之一，请确保在此处以及在位置选项卡中取消选择它。

STEP 15 | 点击确定以保存接入设置。

STEP 16 | 配置 IPv6 可用性选项。

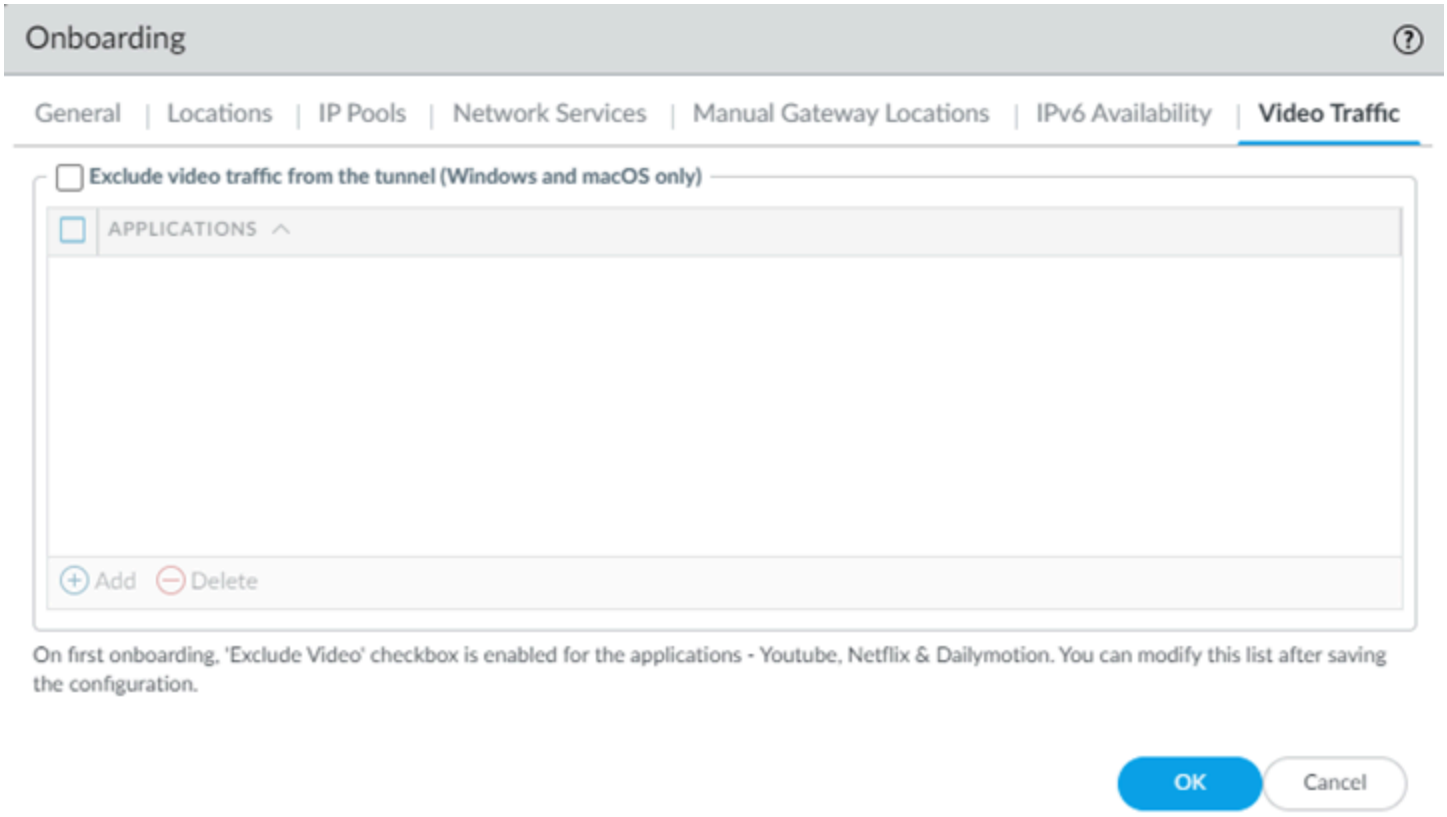
https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-panorama-admin/prisma-access-advanced-deployments/advanced-deployments-that-apply-to-all-prisma-access-types/ipv6-support-for-private-app-accesshttps://docs.paloaltonetworks.com/prisma/

©2025 Palo Alto Networks, Inc.

prisma-access/prisma-access-panorama-admin/prisma-access-advanced-deployments/advanced-deployments-that-apply-to-all-prisma-access-types/ipv6-support-for-private-app-access/enable-ipv6-networking-for-a-mobile-users-globalprotect-deploymentPrisma Access如果您在移动用户 - GlobalProtect 部署中使用 IPv6 网络，您可以配置以在移动用户网络中使用 IPv6 地址。https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-panorama-admin/prisma-access-advanced-deployments/advanced-deployments-that-apply-to-all-prisma-access-types/ipv6-support-for-private-app-access/enable-and-configure-ipv6-networking-and-ip-pools-in-your-prisma-access-infrastructurePrisma Access在您可以使用 IPv6 地址之前，您还需要在基础设施中全局启用 IPv6 网络。

STEP 17 | （可选，仅适用于 Windows 和 macOS）从 GlobalProtect 隧道中排除视频流量。

从隧道中排除视频流量；然后，添加或删除您想要从 GlobalProtect 隧道中排除的视频流应用程序。



STEP 18 | 为您的移动用户创建安全策略规则，以保护流量。

1. 选择要添加策略规则的设备组。您可以选择移动用户设备组或您在为移动用户设置 Prisma Access 时选择的父设备组。
2. 创建安全策略规则。确保您不要定义安全策略规则，以允许来自任何区域的流量到任何区域。在安全策略规则中，使用您在模板堆栈中定义的区域。

 ©2025 Palo Alto Networks, Inc.

STEP 19 | 配置日志以转发到 Strata Logging Service。

> Prisma AccessPrisma Access云服务插件在新安装后或从模板堆栈中移除非模板时，会自动添加以下日志设置（设备日志设置）：

- 系统日志（system-gpcs-default）、用户ID日志（userid-gpcs-default）、HIP匹配日志（hipmatch-gpcs-default）和GlobalProtect日志（gp-prismaaccess-default）的日志设置已添加到Mobile_User_Template中。
- 系统日志（system-gpcs-default）、用户ID日志（userid-gpcs-default）和GlobalProtect日志（gp-prismaaccess-default）的日志设置已添加到Remote_Network_Template。
- 系统日志（system-gpcs-default）和 GlobalProtect 日志（gp-prismaaccess-default）的日志设置已添加到 Service_Conn_Template。

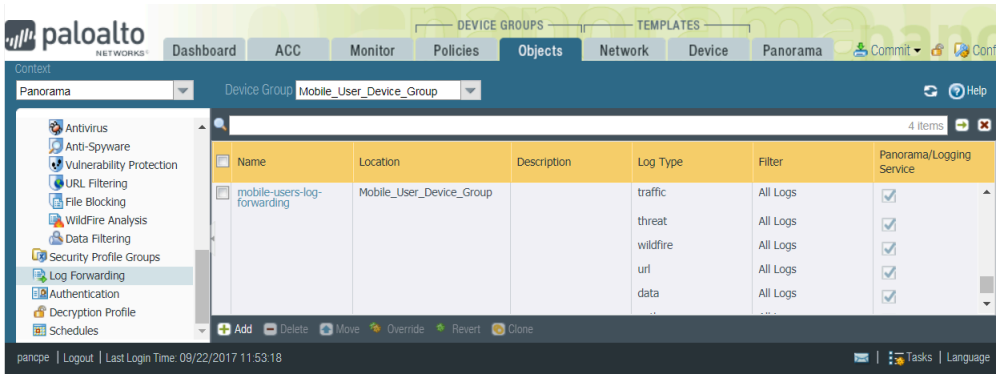
这些日志设置配置会自动将系统、用户ID和HIP匹配日志转发到 Strata Logging Service。

STEP 20 | （可选）将其他日志类型的日志转发到 Strata Logging Service。

为此，您必须创建日志转发配置文件，并将其附加到想要转发日志所用的每个策略规则。

1. 选择您添加策略规则的设备组。
2. 选择 **Objects**（对象） > **Log Forwarding**（日志转发）并 **Add**（添加）配置文件。在日志转发配置文件匹配列表，**Add**（添加）您想要转发的每种日志类型。

   以下示例启用流量、威胁防护、WildFire 提交、URL 过滤、数据过滤和身份验证日志的转发。
3. 选择Panorama/层状日志服务作为转发方法。Strata Logging Service当您选择Panorama时，日志将被转发到。Strata Logging ServiceStrata Logging Service您将能够从 Panorama 监控日志并生成报告。提供无缝集成以存储日志，而无需将其回传到您在公司总部的 Panorama，Panorama 可以根据需要进行查询。

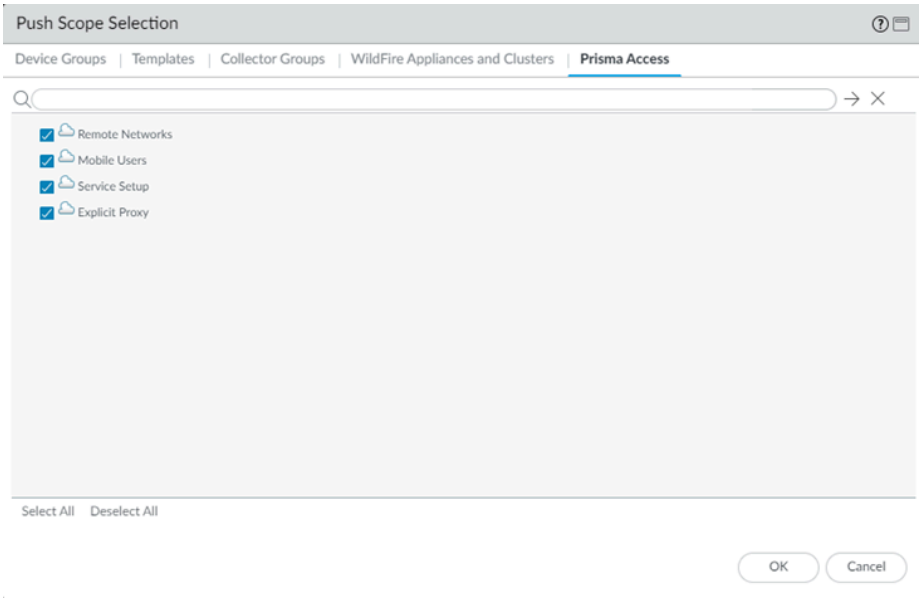


4. 选择 **Policies**（策略） > **Security**（安全）并编辑规则。在 **Actions**（操作）中，选择您创建的日志转发配置文件。

 ©2025 Palo Alto Networks, Inc.

STEP 21 | 将您所有的更改提交到 Panorama，并将配置更改推送到 Prisma Access。

1. 单击 **Commit**（提交） > **Commit and Push**（提交并推送）。
2. 编辑选择，并在选项卡中确保在推送范围内选择了移动用户和显式代理，然后单击确定。**Prisma Access**



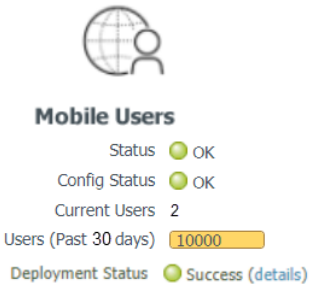
3. 在设备组选项卡中，请确保您已选择显式代理和 GlobalProtect 设备组。
4. 单击 **Commit and Push**（提交并推送）。

©2025 Palo Alto Networks, Inc.

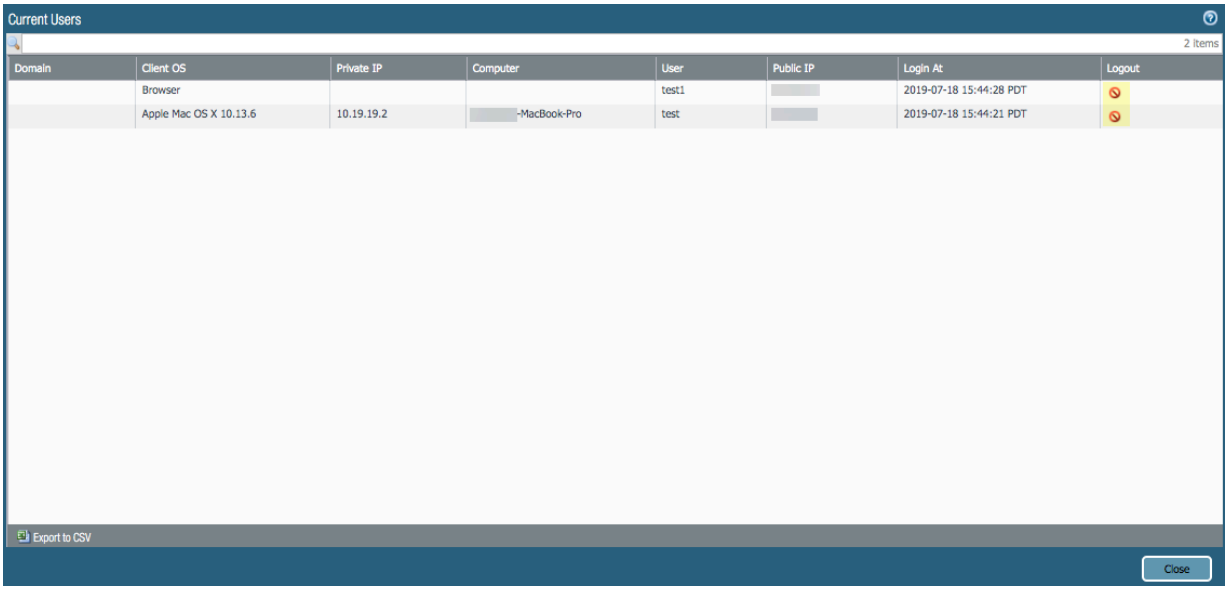
STEP 22 | Prisma Access > > > 要验证用户的功能是否已部署并处于活动状态，请选择Panorama云服务状态。

在配置完成后，移动用户的状态和配置状态应显示为正常。

部署状态区域允许您在接入和部署作业完成之前查看进度，以及查看有关已完成作业状态的更多信息。



要查看当前登录的唯一用户数量，或注销已登录的用户，请单击当前用户旁边的超链接数字。

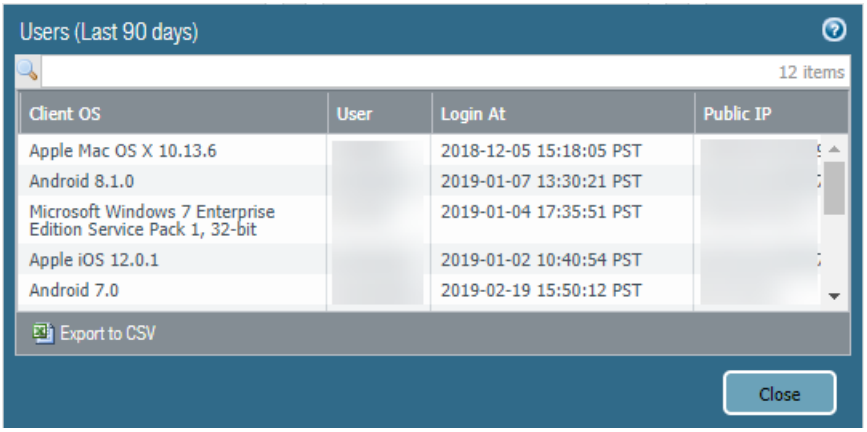


 ©2025 Palo Alto Networks, Inc.

要查看过去90天内已登录用户的历史信息，请单击用户（过去90天）旁边的数字。

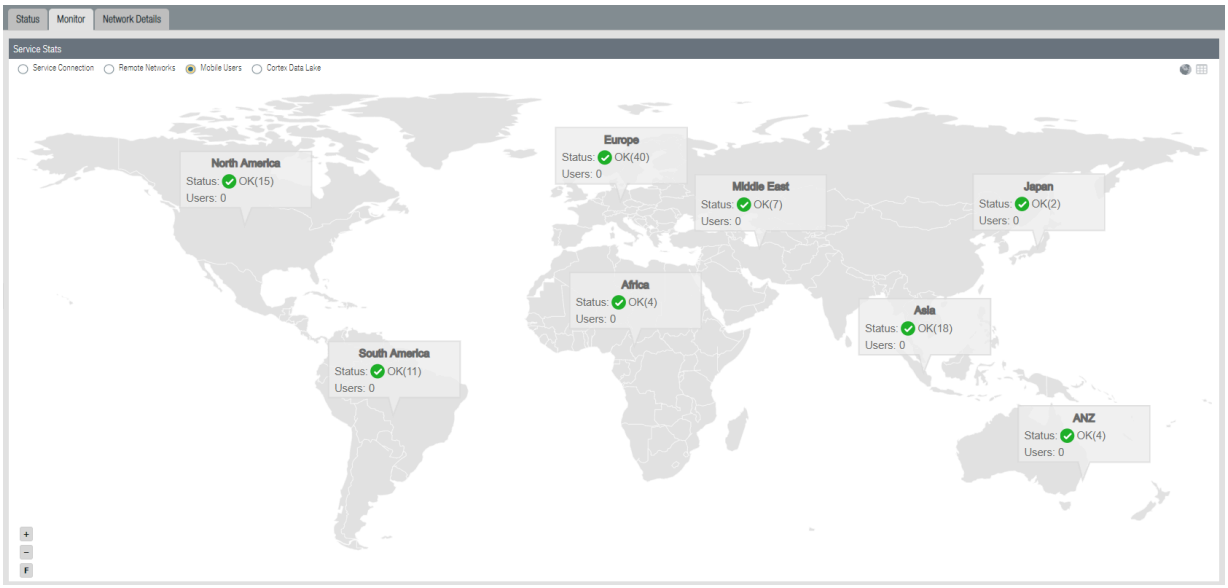
当用户（过去90天）字段中的用户数量达到总许可数量的80%时，数字将以红色显示。

要将用户列表导出到 CSV 文件，请选择导出到 CSV。请注意，最多可以将 45,000 个用户导出到 CSV 文件中。



Prisma Access要显示一张地图，显示您所选择区域中运行的门户和网关的位置，请选择监控；然后，选择移动用户。

 ©2025 Palo Alto Networks, Inc.



选择一个区域以获取该区域的更多详细信息。

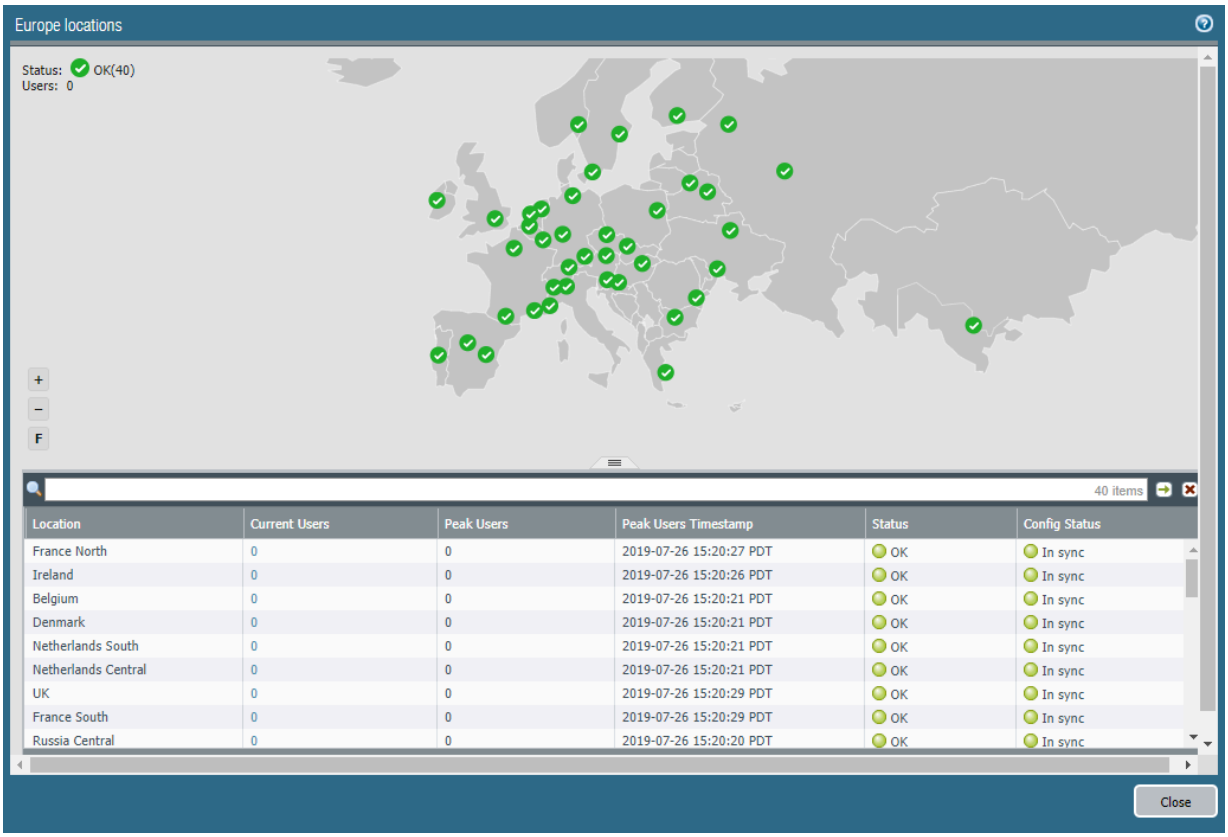
- 位置—您的云服务基础设施部署的位置，以保护网络上的移动用户。

©2025 Palo Alto Networks, Inc.

- 当前用户 — 连接并受到服务保护的用户数量。

  当当前移动用户数量达到其总许可数量的80%时，该数字将以红色显示。
- 峰值用户 — 同时在线用户的最大数量。
- 峰值用户时间戳 - 最后一次检索峰值用户数据的时间戳。
- Prisma Access状态—您与移动用户之间连接的操作状态。
- 配置状态 - 您上次向服务推送的配置状态。如果您在本地进行了更改，但尚未将配置推送到云端，则可能会显示状态为不同步。将鼠标悬停在状态指示器上以获取更详细的信息。Prisma Access在将配置提交并推送到后，配置状态更改为同步。

 ©2025 Palo Alto Networks, Inc.



STEP 23 | > > > > 如果您选择使用公司域名作为您的门户主机名，则必须在内部 DNS 服务器上添加 DNS 条目，以将您定义的门户主机名映射到在云服务配置移动用户接入常规选项卡上显示的门户 DNS CNAME（例如，<portal_hostname>.gpcloudservice.com）。

 ©2025 Palo Alto Networks, Inc.

STEP 24 | https://docs.paloaltonetworks.com/globalprotect.html将 GlobalProtect 应用程序软件部署到您的最终用户。

对于Mac OS或Windows用户，您可以将用户引导到 Prisma Access 门户地址，在那里他们可以从门户下载GlobalProtect应用程序。

*Prisma Access*GlobalProtect 应用程序升级管理门户上 *GlobalProtect* 应用程序的版本，您可以从 *Prisma Access* 托管的版本中选择活动版本，并控制用户下载它的能力。

https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/globalprotect-apps/deploy-the-globalprotect-app-software/host-app-updates-on-a-web-serverPrisma Accesshttps://www.paloaltonetworks.com/services/support/end-of-life-announcements/end-of-life-summary或者，您可以在网络服务器上托管适用于 Mac OS 和 Windows 用户的 GlobalProtect 应用软件。与未列为生命周期结束的任何 GlobalProtect 应用版本兼容。

https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/globalprotect-apps/deploy-the-globalprotect-app-software/download-and-install-the-globalprotect-mobile-app移动应用程序用户可以从适合其操作系统的应用商店下载和安装 GlobalProtect 移动应用程序。

GlobalProtect—自定义隧道设置

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证

自定义 GlobalProtect 应用程序为连接到 Prisma Access 而建立的 VPN 隧道的设置。隧道设置包含拆分隧道选项，可以使用这些选项来定义应用程序将哪些流量发送至 Prisma Access，以及哪些流量可改为在本地路由（例如非业务使用所需的高带宽应用程序产生的流量）。

您为隧道设置定义的 **Match Criteria**（匹配标准）会告诉 Prisma Access 应接收设置的用户、设备或系统。例如，可以指定某个隧道设置规则适用于特定区域内 GlobalProtect 应用程序的所有实例。在 Prisma Access (Managed by Panorama) 中，您可以根据访问路由、域和应用程序配置拆分通道设置。

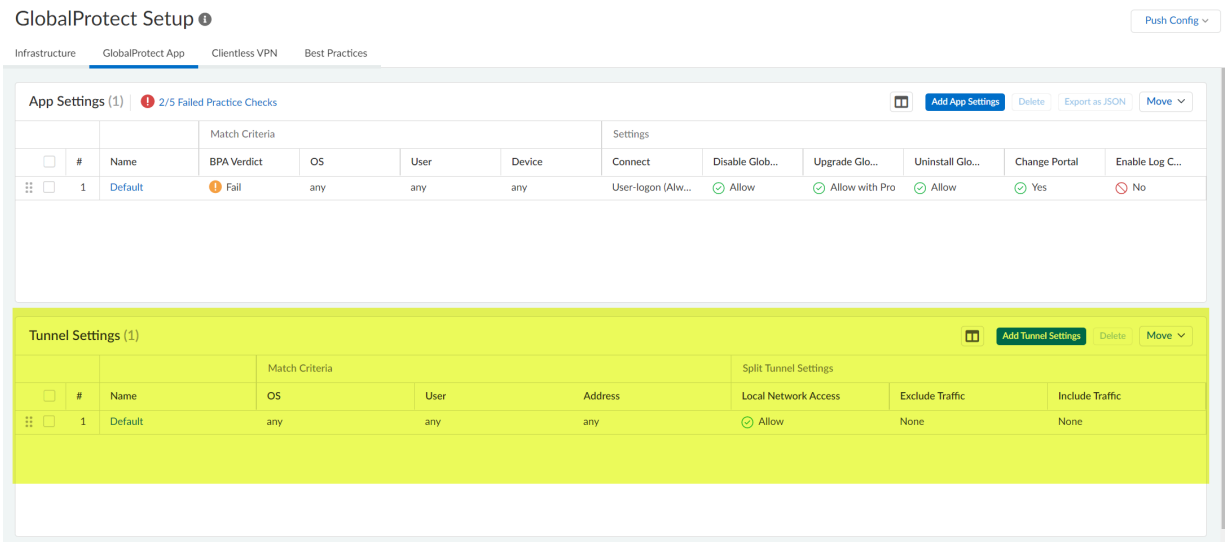
- Strata Cloud Manager
- Panorama

GlobalProtect—自定义隧道设置 (Strata Cloud Manager)

 ©2025 Palo Alto Networks, Inc.

STEP 1 | 点击 **Manage**（管理）**> Service Setup**（服务设置）**> Mobile Users**（移动用户）**> GlobalProtect Setup**（**GlobalProtect** 设置）**> GlobalProtect App**（**GlobalProtect** 应用程序）**> Add Tunnel Settings**（添加隧道设置）。

如果正在使用 *Strata Cloud Manager*，请单击 ***Workflow***（工作流）***> Prisma Access Setup***（***Prisma*** 接入设置）***> Mobile User***（移动用户）***> GlobalProtect Setup***（***GlobalProtect*** 设置）***> GlobalProtect App***（***GlobalProtect*** 应用程序）***> Add Tunnel Settings***（添加隧道设置）。



STEP 2 | 输入名称并在 **Match Criteria**（匹配条件）中输入条件，以指定应接收设置的用户、设备或系统。例如，可以指定某个隧道设置规则适用于特定区域内 GlobalProtect 应用程序的所有实例。

STEP 3 | 为 Prisma Access 启用 **Authentication Override**（身份验证覆盖）选项，以生成并接受用于用户身份验证的安全加密 Cookie。此设置允许用户在指定时间段内只需提供一次登录凭据。

- **Generate cookie for authentication override**（生成用于身份验证覆盖的 **Cookie**）—允许 Prisma Access 生成加密的特定端点 Cookie 并将身份验证 Cookie 颁发至端点。
- **Accept cookie for authentication override**（接受用于身份验证覆盖的 **Cookie**）—允许 Prisma Access 使用有效的加密 Cookie 对用户进行身份验证。当应用程序提供有效的 Cookie 时，Prisma Access 首先确认该 Cookie 最初由 Prisma Access 加密，随后解密 Cookie，然后对用户进行身份验证。

GlobalProtect 应用程序必须知道连接用户的用户名，才能从用户的端点匹配和检索相关的身份验证 *Cookie*。在应用程序检索 *Cookie* 后，会将 *Cookie* 发送至 *Prisma Access* 进行用户身份验证。

 ©2025 Palo Alto Networks, Inc.

STEP 4 | 启用 **Split Tunneling**（拆分隧道），以定义 GlobalProtect 应用程序允许或限制通过 VPN 隧道传输至 Prisma Access 的流量类型。拆分隧道通过排除非关键业务或不能提高工作效率的 Prisma Access 流量来节省带宽。

- **Local Network Access**（本地网络访问）—选择此选项可允许 Windows 和 Mac 用户访问本地资源，无需首先连接到 Prisma Access。

  Exclude Traffic（排除流量）—选择此选项可根据应用程序、域和路由（如 IP 地址）指定要从 Prisma Access 策略检查和强制实施中排除的流量。

  Customize Include Traffic（自定义包含流量）—默认情况下，GlobalProtect 应用程序会将排除列表中的流量以外的所有流量路由到 Prisma Access。指定 GlobalProtect 应用程序应始终路由到 Prisma Access 的流量，即使它满足排除列表标准。

STEP 5 | 选择 **Exclude Video Stream Traffic**（排除视频串流流量），便不会将列出的应用程序中的视频串流流量发送到 Prisma Access。从 VPN 隧道排除低风险的视频流流量（YouTube 和 Netflix 等）时，您可以减少带宽消耗。视频串流排除项适用于 GlobalProtect 应用程序发送到 Prisma Access 的所有流量，不仅限于符合您为此规则定义的匹配条件的流量。

STEP 6 | 保存设置。重复以上步骤以添加更多隧道设置。

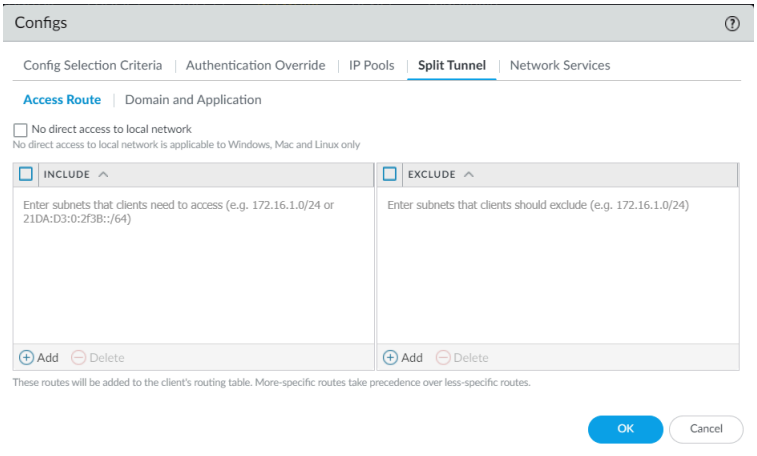
STEP 7 | （可选）上下移动以设置连接到 Prisma Access 时使用 VPN 隧道设置的优先顺序。

GlobalProtect—自定义隧道设置 (Panorama)

您可以根据访问路由或域和应用程序配置拆分通道设置。

 ©2025 Palo Alto Networks, Inc.

- 根据访问路由配置拆分隧道设置。
  1. 单击 **Panorama > Network**（网络）**> GlobalProtect > Gateways**（网关），然后选择要自定义的网关。
  2. 单击 **Agent**（代理）**> Client Settings**（客户端设置），然后选择配置。
  3. 单击 **Split Tunnel**（拆分隧道）**> Access Route**（访问路由）。当 GlobalProtect 应用程序与 Prisma Access 建立隧道时，此拆分隧道配置将分配至端点上的虚拟网络适配器。您可以包括或排除通过 VPN 隧道发送的特定目标 IP 子网流量。



  4. 启用 **No direct access to local network**（禁止直接访问本地网络）选项，可阻止用户在连接到 GlobalProtect 时将流量直接发送到代理服务器或本地资源。

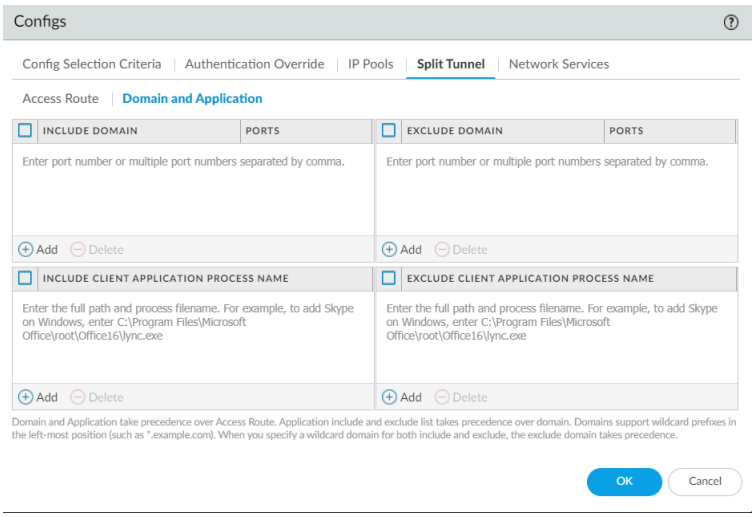
     启用 ***No direct access to local network***（禁止直接访问本地网络）设置，以降低不可信网络（例如恶意 *Wi-Fi* 访问点）中的风险。
  5. 选择 **Include**（包含），然后单击 **Add**（添加）以添加目标子网或地址对象（IP Netmask（IP 网络掩码）类型），以便仅将指定给 LAN 的特定流量路由到 GlobalProtect。您可以包含 IPv6 或 IPv4 子网。要包括所有的目标子网或地址对象，则 **Include**（包含）作为访问路由的 0.0.0.0/0 和 ::/0。
  6. 选择 **Exclude**（排除）中，单击 **Add**（添加）以添加您希望应用程序排除的目标子网或地址对象（IP Netmask（IP 网络掩码）类型）。排除的路由应比包括的路由更具体，以免排除不想排除的流量。可以排除 IPv6 或 IPv4 子网。

     不能排除在 *Chromebook* 上运行 *Android* 的端点的访问路由。*Chromebook* 只支持 *IPv4* 路由。
  7. 保存隧道设置。

©2025 Palo Alto Networks, Inc.

- 根据域和应用程序来配置拆分通道设置。
  1. 单击 **Panorama > Network**（网络）**> GlobalProtect > Gateways**（网关），然后选择要自定义的网关。
  2. 单击 **Agent**（代理）**> Client Settings**（客户端设置），然后选择配置。
  3. 单击 **Split Tunnel**（分流隧道）**> Domain and Application**（域和应用程序）选项卡，以根据目标域名配置拆分隧道设置。

     在 *macOS* 端点上使用第三方端点安全产品（例如 *Sophos*）时，可能会遇到一些不兼容问题。



     - （可选）选择 **Include Domain**（包含域名），然后单击 **Add**（添加）以使用目标域和端口来添加您希望通过 VPN 连接路由到 GlobalProtect 的 SaaS 或公共云应用程序。您最多可在列表上添加 200 个条目。例如，添加 *.gmail.com 允许所有 Gmail 流量通过 VPN 隧道。
     - （可选）选择 **Exclude Domain**（排除域名），然后单击 **Add**（添加）以使用目标域和端口添加您希望从 VPN 隧道中排除的 SaaS 或公共云应用程序。您最多可在列表上添加 200 个条目。例如，添加 *.target.com 可排除来自 VPN 隧道的所有 Target 流量。
  4. 根据应用程序配置拆分隧道设置。

     在 *macOS* 端点上，无法将 *Safari* 流量添加到基于应用程序的拆分隧道规则中。

     可以使用环境变量在 *Windows* 和 *macOS* 端点上基于应用程序配置拆分隧道。

     - （可选）选择 **Include Client Application Process Name**（包含客户端应用程序进程名称），然后单击 **Add**（添加）以使用应用程序进程名称添加您希望通过 VPN 连接路由到 GlobalProtect 的 SaaS 或公共云应用程序。您最多可在列表上添加 200 个条目。
     - （可选）选择 **Exclude Client Application Process Name**（排除客户端应用程序进程名称），然后单击 **Add**（添加）以使用应用程序进程名称添加要从 VPN 隧道中排除的 SaaS 或公共云应用程序。您最多可在列表上添加 200 个条目。
  5. 保存隧道设置。

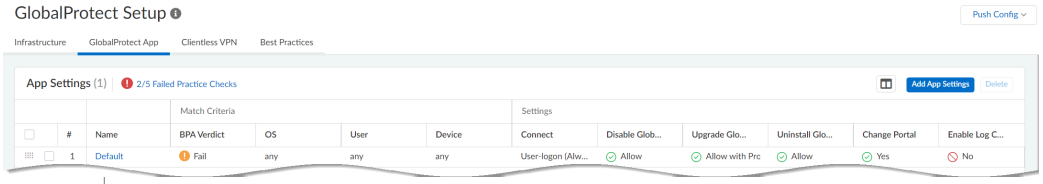
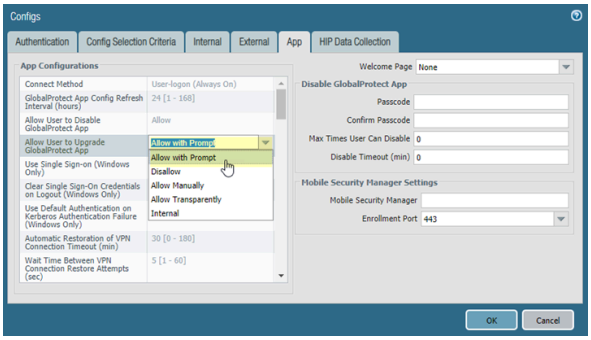
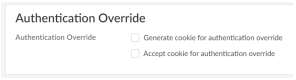
©2025 Palo Alto Networks, Inc.

GlobalProtect—自定义应用程序设置

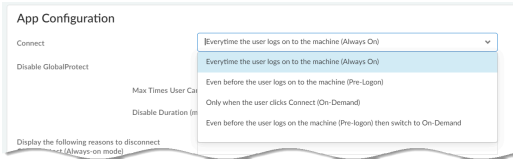
在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

自定义最终用户与 GlobalProtect 应用程序交互的方式。

有一些设置您可以全局自定义。这些全局应用程序设置适用于所有设备上的 GlobalProtect 应用程序。其他 GlobalProtect 应用程序设置均为默认设置。然后可以自定义这些选项，并根据匹配条件，将它们定向应用程序于特定的用户和设备。您为应用程序设置定义的匹配条件会告知 Prisma Access 应接收设置的用户、设备或系统。例如，你可以指定一条规则仅适用于序列号与 Active Directory 条目匹配的设备。

GlobalProtect 应用程序设置	
在此处探索和自定义应用程序设置（下面显示云管理示例）—>	Prisma Access (Managed by Strata Cloud Manager)  Panorama Managed Prisma Access 
身份验证覆盖	启用 Prisma Access 以生成并接受用于用户身份验证的安全加密 Cookie。开启后，用户在指定时间段内只需提供一次登录凭据。  • **Generate cookie for authentication override**（生成用于身份验证覆盖的 **Cookie**）—允许 Prisma Access 生成加密的特定端点 Cookie 并将身份验证 Cookie 颁发至端点。

 ©2025 Palo Alto Networks, Inc.

GlobalProtect 应用程序设置	
	• **Accept cookie for authentication override**（接受用于身份验证覆盖的 **Cookie**）—允许 Prisma Access 使用有效的加密 Cookie 对用户进行身份验证。应用程序出示有效 Cookie 后，Prisma Access 将验证此 Cookie 是否最初已经过 Prisma Access 加密，再对其进行解密，然后对用户进行身份验证。 *GlobalProtect* 应用程序必须知道正在连接的用户的用户名，才能从用户端点匹配和检索相关身份验证 *Cookie*。在应用程序检索 *Cookie* 后，会将 *Cookie* 发送至 *Prisma Access* 进行用户身份验证。 • **Cookie Lifetime**（**Cookie** 生命周期）—指定 Cookie 有效的小时数、天数或周数（默认为 24 小时）。小时数范围为 1 至 72；周数范围为 1 至 52；天数范围为 1 至 365。Cookie 过期后，用户必须再次输入登录凭据，Prisma Access 随后会加密新 Cookie 以发送到应用程序。该值可与配置的 Cookie 生命周期相同或不同。 • **Certificate to Encrypt/Decrypt Cookie**（加密/解密 **Cookie** 的证书）—选择对 Cookie 进行加密和解密时所使用的 RSA 证书。
连接设置	指定 GlobalProtect 应用程序用于连接到 Prisma Access 的方法。  • **User-logon (Always On)**（用户登录（始终启用））—用户一旦登录，GlobalProtect 应用程序便会自动连接至 Prisma Access。与 SSO（仅限 Windows 端点）一同使用时，登录对最终用户透明。 在 *iOS* 端点上，此设置可防止一次性密码 *(OTP)* 应用程序运行，因为 *GlobalProtect* 应用程序会强制所有流量通过隧道。 • **Pre-logon (Always On)**（预登录（始终启用））—GlobalProtect 应用程序在用户登录之前对用户进行身份验证，并建立至 Prisma Access 的 VPN 隧道。该选项要求使用外部 PKI 解决方案为接收这些设置的所有设备预部署计算机证书。 • **On-demand (Manual user initiated connection)**（按需（用户手动发起连接））—用户须手动启动应用程序以便连接至 GlobalProtect。

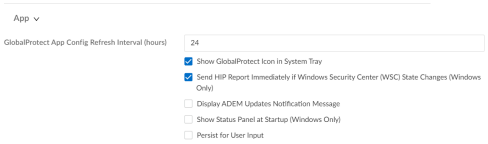
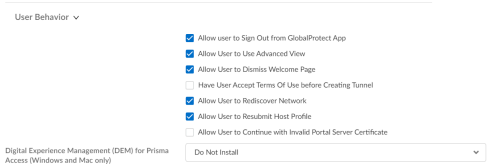
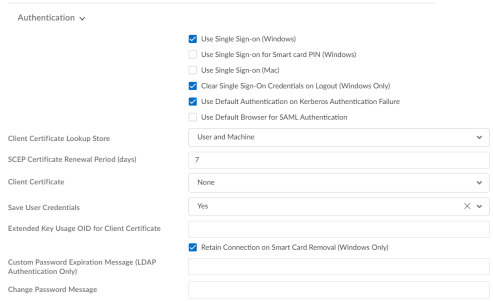
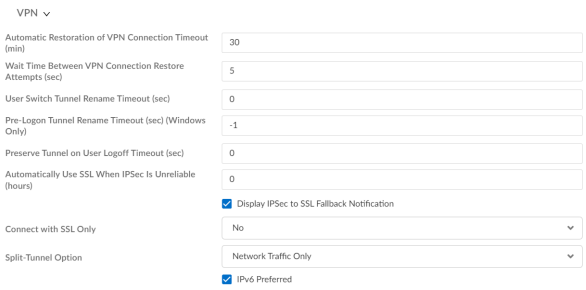
 ©2025 Palo Alto Networks, Inc.

GlobalProtect 应用程序设置	
	• **Pre-logon then On-demand**（预登录后按需）—与 Pre-logon (Always On)（预登录（始终启用））连接方法类似，该连接方法（要求“内容发布”版本为 590-3397 或更高）使 GlobalProtect 应用程序能够在用户登录端点之前对用户进行身份验证并建立至 Prisma Access 的 VPN 隧道。与预登录连接方法不同的是，在用户登录之后，如果连接因故终止，用户必须手动启动应用程序以便连接至 GlobalProtect。此选项的好处在于，您可允许用户在密码过期或用户忘记其密码时指定新密码，但仍要求用户在登录后手动发起连接。

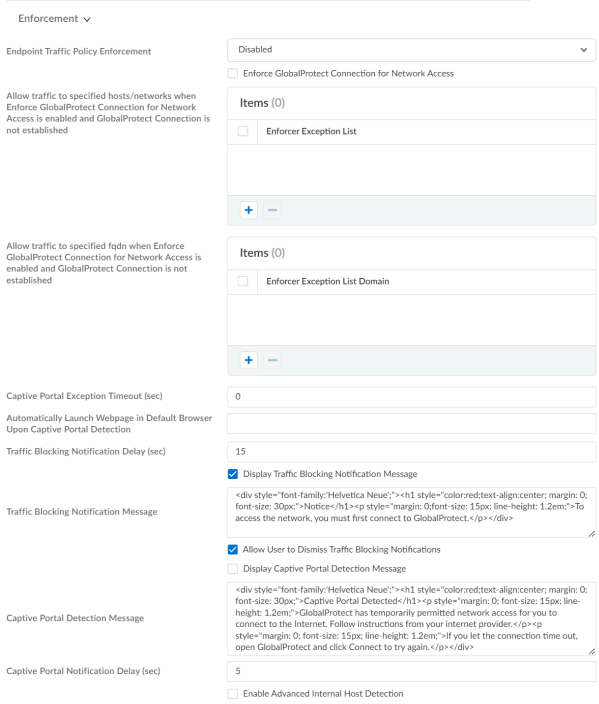
GlobalProtect	确定用户可以调整哪些 GlobalProtect 应用程序设置：
	• **Disable GlobalProtect**（禁用 **GlobalProtect**）—决定用户是否可以禁用 GlobalProtect 应用程序。禁用 GlobalProtect 应用程序的用户无法连接到 Prisma Access（以及您受保护的公司资源），直到他们重新打开该应用程序。
	• **Upgrade GlobalProtect**（升级 **GlobalProtect**）—指定应用程序升级方式，包括用户是否可以启动更新。
	如果要控制用户何时可以升级，则可以根据每个配置自定义应用升级。例如，如果您想对一小组用户测试发行版，然后将其部署到整个用户群中，则可以创建一个适用于您的 IT 小组中的用户的配置，从而允许他们升级和测试，并禁止所有其他用户/组配置升级。当新版本彻底测试完毕后，则可为其余用户修改代理配置以便进行升级。
	  • **Allow with Prompt**（允许并提示）—当应用程序有新版本可用时提示用户升级。
	  • **Allow Transparently**（以透明方式允许）—自动升级，无需与用户交互。
	  • **Internal**（内部）—当用户连接到 Prisma Access 时自动升级，无需用户交互。
	  • **Disallow**（不允许）—阻止应用程序升级。
	  • **Allow Manually**（允许手动）—允许用户从 GlobalProtect 应用程序内部启动应用程序升级。
	• **Uninstall GlobalProtect**（卸载 **GlobalProtect**）—允许用户卸载 GlobalProtect 应用程序，阻止他们卸载 GlobalProtect 应用程序，或允许他们在指定您创建的密码时卸载。
	• **User Can Change Portal**（用户可以更改门户）—允许用户更改 GlobalProtect 应用程序用于连接 Prisma Access 的门户。

应用程序配置 - 高级选项	

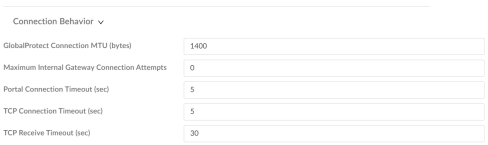
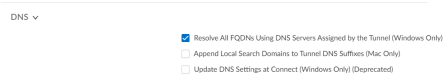
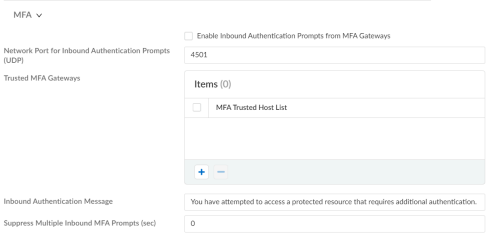
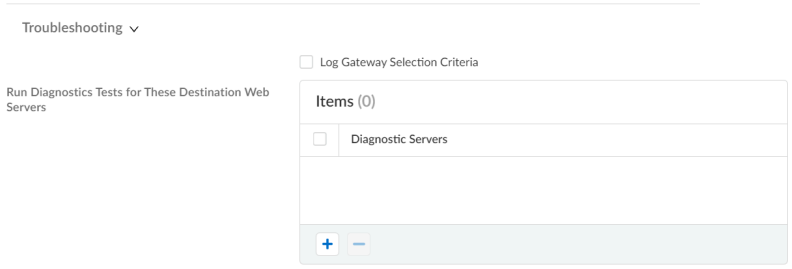
©2025 Palo Alto Networks, Inc.

GlobalProtect 应用程序设置	
应用程序设置	• Send HIP Report Immediately if Windows Security Center (WSC) State Changes (Windows Only)（Windows 安全中心 (WSC) 状态变更后立即发送 HIP 报告（仅限 Windows））—选择 No（否）可防止 GlobalProtect 应用程序在 Windows 安全中心 (WSC) 状态变更后发送 HIP 数据。选择“Yes（是）”（默认）可在 Windows 安全中心 (WSC) 状态变更后立即发送 HIP 数据。 
用户行为设置	用户行为设置包括： 
身份验证设置	身份验证设置包括： 
VPN 设置	配置 VPN 超时和隧道设置： • 显示 **IPSec** 到 **SSL** 回退通知—选择 **No**（否）可在 GlobalProtect 应用程序无法建立与 IPSec 隧道的连接并回退到 SSL 隧道的情况下阻止显示弹出通知。选择 **Yes**（是）（默认）可允许在连接改变时显示弹出通知。 

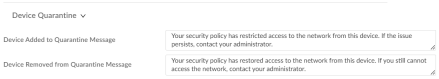
 ©2025 Palo Alto Networks, Inc.

GlobalProtect 应用程序设置	
强制执行设置	指定流量的强制执行设置： • 当已启用“强制执行 **GlobalProtect** 连接来访问网络”且未建立 **GlobalProtect** 连接时，允许传输到指定 **FQDN** 的流量—了解详情。 • 强制网络门户检测时自动在默认浏览器中启动网页—要自动启动默认 Web 浏览器，以便用户可以无缝登录到身份验证门户，请输入希望用于在默认网页浏览器启动时发起 Web 流量的初始连接尝试的网站的 FQDN 或 IP 地址（最长为 256 个字符）。随后，身份验证门户会拦截该网站连接尝试，并将默认 Web 浏览器重定向到身份验证门户登录页面。如果此字段为空（默认），则 Prisma Access 不会在身份验证门户检测时自动启动默认 Web 浏览器。 • **Enable Advance Internal Host Detection**（启用高级内部主机检测）—启用高级内部主机检测以在 GlobalProtect 应用程序进行内部主机检测期间增加额外的安全层。通过高级内部主机检测，应用程序除了对内部主机执行反向 DNS 查找以确定应用程序是否在企业网络内部之外，还验证内部网关的服务器证书。启用高级内部主机检测可阻止恶意行为者在内部主机检测期间欺骗反向 DNS 服务器响应，从而防止未经授权访问企业网络中的端点。如果不启用高级内部主机检测，现有的内部主机检测将按预期工作。 
连接行为设置	连接行为设置包括：

 ©2025 Palo Alto Networks, Inc.

GlobalProtect 应用程序设置	
	 了解详情。
DNS 设置	DNS 设置包括： 
代理设置	指定要推送到端点以配置代理设置的 **Proxy Auto-Configuration (PAC) File URL**（代理自动配置 **(PAC)** 文件 **URL**）。URL 的最大长度为 256 个字符。支持以下代理自动配置 (PAC) 文件 URL 方法： • 代理自动配置 (PAC) 标准（例如，http://pac.<hostname or IP>/proxy.pac）。 • Web 代理自动发现协议 (WPAD) 标准（例如，http://wpad.<hostname or IP>/wpad.dat）。 
MFA 设置	MFA 设置包括： 
故障排除设置	故障排除设置包括： 

 ©2025 Palo Alto Networks, Inc.

GlobalProtect 应用程序设置	
设备隔离设置	设备隔离设置包括： 
内部主机检测	如果您不要求移动用户在处于内部网络时连接到 Prisma Access，则启用内部主机检测功能，以便让 GlobalProtect 应用程序能够判断自身是处于内部网络还是外部网络。 • 输入只能从内部网络解析的主机的 IP 地址（IPv4 或 IPv6）。 • 输入解析为您输入的 IP 地址的 DNS 主机名。 当移动用户连接到 Prisma Access，GlobalProtect 应用程序尝试对指定地址进行反向 DNS 查找。如果查找失败，GlobalProtect 应用程序将确定该地址位于外部网络上，然后启动与 Prisma Access 的连接。
启用内部主机检测	如果您希望在配置了内部网关和内部主机检测且外部网关和内部主机检测失败的情况下，GlobalProtect 应用程序重试网络发现，则将 **Enable Intelligent Internal Host Detection**（启用智能内部主机检测）参数设置为“yes（是）”。
网关	默认情况下，用户可以使用您的 Prisma Access 位置中的所有网关。如果您希望用户能够连接到其他 GlobalProtect 网关（内部或外部），则可以在此处添加这些网关。
HIP 数据收集	定义需要应用程序收集或在收集时排除的自定义主机信息配置文件 (HIP) 数据。启用此选项后，应用程序将从运行 Windows、Mac 或 Linux 操作系统的设备收集数据。 例如，通过自定义检查，您可以了解某个应用程序是否已在端点上安装或运行。您定义要在自定义检查中收集的数据包含在原始主机信息数据中，GlobalProtect 应用程序会收集这些数据，然后在应用程序连接时提交到 Prisma Access。 要监控使用自定义检查收集的数据，请创建 HIP 对象。然后，可以将 HIP 对象添加到 HIP 配置文件，以便使用所收集的数据来匹配端点流量和执行安全规则。 转到 **Manage**（管理） > **Configuration**（配置） > **NGFW** 和 **Prisma Access** > **Objects**（对象） > **HIP** 和 **HIP Objects**（HIP 对象）或 **HIP Profiles**（HIP 配置文件）。选择 **Prisma Access** > **Mobile Users Container**（移动用户容器） > **GlobalProtect** 配置范围。

 ©2025 Palo Alto Networks, Inc.

GlobalProtect 应用程序设置	
超时设置	• 在“GlobalProtect Setup（GlobalProtect 设置）”页面上，选择“Global App Settings（全局应用程序设置）”区域中的齿轮图标。 • 修改单个网关登录会话的最长 **Login Lifetime**（登录生命周期）（默认为 30 天）。在此期间，只要网关在 **Inactivity Logout**（非活动注销）期间从端点收到 HIP 检查，则用户保持登录状态。在此期限后，登录会话自动结束。 • 设置提前通知的时长，以告知用户其应用程序会话将在指定时间后因登录有效期到期而到期。默认值为 30 分钟。可接受的范围是 0 到 60 分钟。 • 自定义超时通知消息。 • 修改 **Inactivity Logout**（非活动注销）期间，指定空闲用户从 GlobalProtect 注销后的时间量。您可以实施安全策略，以在连接到 GlobalProtect 时监控来自端点的流量，并快速注销不活动的 GlobalProtect 会话（通过设置更短的非活动注销期限）。如果 GlobalProtect 应用程序在配置的时间内未通过 VPN 隧道路由流量或者未从端点收到 HIP 检查，则用户将从 GlobalProtect 注销。 默认值为 180 分钟。可接受的范围是 5 到 43200 分钟。 • 设置提前通知的时长，以告知用户其应用程序会话将在指定时间后因不活动而到期。默认值为 30 分钟。可接受的范围是 0 到 60 分钟。 • 自定义非活动通知消息。 • 指定在管理员注销最终用户时是否通知最终用户并设置显示消息。 • 单击 **Save**（保存）。
身份验证 **Cookie** 的源 **IP** 地址强制执行	配置 VPN 连接设置和身份验证 Cookie 使用限制，以增强安全态势。 • 在“GlobalProtect Setup（GlobalProtect 设置）”页面上，选择“Global App Settings（全局应用程序设置）”区域中的齿轮图标。 • 配置 SSL VPN 隧道的自动恢复。 如果在 GlobalProtect 门户上启用了 VPN 连接自动恢复，则可以通过选择 **Disable Automatic Restoration of SSL VPN**（禁用自动恢复 **SSL VPN**）来为此网关禁用该功能。 • 为身份验证 Cookie 配置源 IP 地址实施。 您可以配置 GlobalProtect 门户或网关，以仅在端点 IP 地址与发布 Cookie 的源 IP 地址匹配时，或当端点 IP 地址与指定的网络 IP 地址范围匹配时，接受来自端点的 Cookie。

©2025 Palo Alto Networks, Inc.

GlobalProtect 应用程序设置	
	您可以通过 CIDR 子网掩码，如 /24 或 /32 定义网络 IP 地址范围。例如，如果身份验证 Cookie 最初颁发给公共源 IP 地址为 201.109.11.10 的端点，并且网络 IP 地址范围的子网掩码设置为 /24，那么随后该身份验证 Cookie 在公共源 IP 地址处于 201.109.11.0/24 网络 IP 地址范围内的端点上有效。 在“Authentication Cookie Usage Restrictions（身份验证 Cookie 使用限制）”部分中，选择 **Restrict Authentication Cookie Usage (for Automatic Restoration of VPN tunnel or Authentication Override)**（限制身份验证 **Cookie** 使用量（用于自动恢复 **VPN** 隧道或身份验证替代）），然后配置以下条件之一： • 如果您选择 **The original Source IP for which the authentication cookie was issued**（颁布验证 **Cookie** 的原源 **IP**），则仅在尝试使用 Cookie 的端点公共源 IP 地址为接受所发布 Cookie 的端点的相同公共源 IP 地址时，验证 Cookie 才有效。 • 如果您选择 **The original Source IP network range**（原源 **IP** 网络范围），仅当尝试使用 Cookie 的端点公共源 IP 地址位于指定网络 IP 地址范围内时，身份验证 Cookie 才有效。输入“Source IPv4 Netmask（源 IPv4 网络掩码）”或“Source IPv6 Netmask（源 IPv6 网络掩码）”以定义对身份验证 Cookie 有效的网络 IP 地址范围的子网掩码（例如，32 或 128）。

禁用 GlobalProtect 的工单请求

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

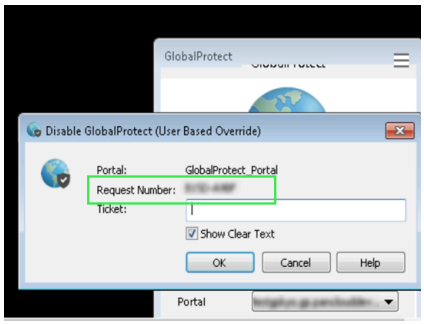
您可以允许用户创建工单以禁用 GlobalProtect，而不是让用户直接禁用 GlobalProtect。然后，GlobalProtect 管理员可以决定是否允许每个特定用户禁用 GlobalProtect。

工作原理

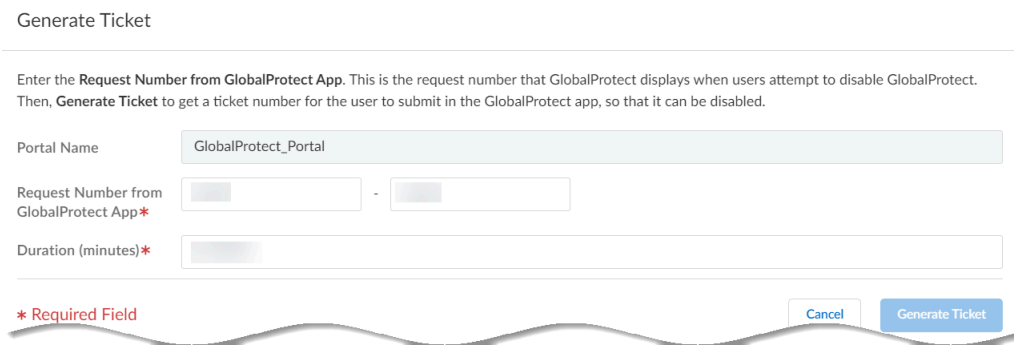
设置此功能后，以下是通过工单请求禁用 GlobalProtect 的工作流程：

©2025 Palo Alto Networks, Inc.

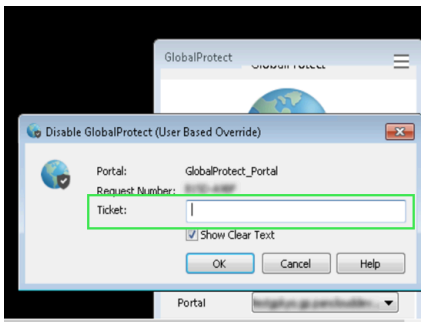
- 用户尝试在 GlobalProtect 应用程序中禁用 GlobalProtect。GlobalProtect 向用户显示请求编号。



- 用户与 GlobalProtect 管理员共享请求编号。
- GlobalProtect 管理员登录 Prisma Access (Managed by Strata Cloud Manager) 并使用请求编号生成工单。



- GlobalProtect 管理员与用户共享工单编号。用户在应用程序中输入工单编号以禁用 GlobalProtect。



完成设置

- Strata Cloud Manager
- Panorama

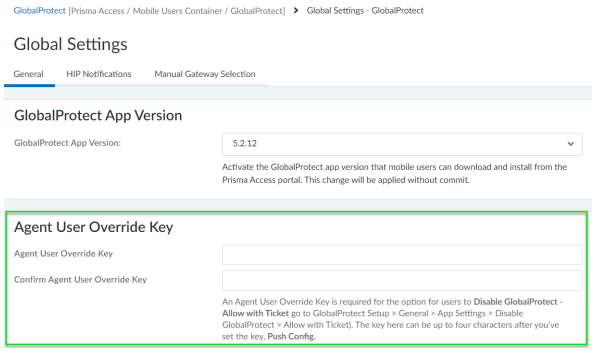
禁用 GlobalProtect 的工单请求 (Strata Cloud Manager)

©2025 Palo Alto Networks, Inc.

STEP 1 | 设置客户端覆盖密钥

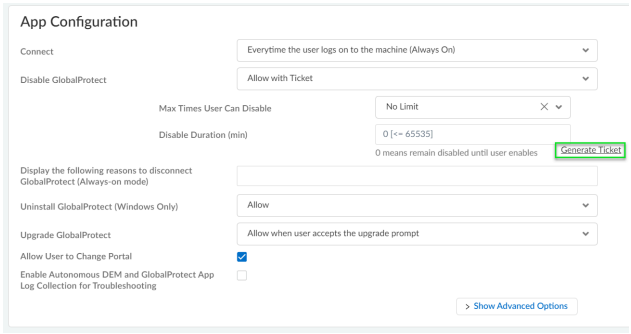
您需要先设置客户端用户覆盖密钥，然后才能启用允许用户提交工单请求来禁用 GlobalProtect 的选项。

转到 **Workflows**（工作流） > **Prisma Access** 设置 > **GlobalProtect** > **GlobalProtect App**（**GlobalProtect** 应用程序） > **Global App Settings**（**Global** 应用程序设置），并输入一个包含四个字符的密钥来设置 **Agent Override Key**（客户端覆盖密钥）。



STEP 2 | 允许使用工单禁用 GlobalProtect

转到 **Workflows**（工作流） > **Prisma Access** 设置 > **GlobalProtect** > **GlobalProtect App**（**GlobalProtect** 应用程序） > **App Settings**（应用程序设置） > **App Configuration**（应用程序配置） > **Disable GlobalProtect**（禁用 **GlobalProtect**），并将选项设置为 **Allow with Ticket**（允许使用工单）。

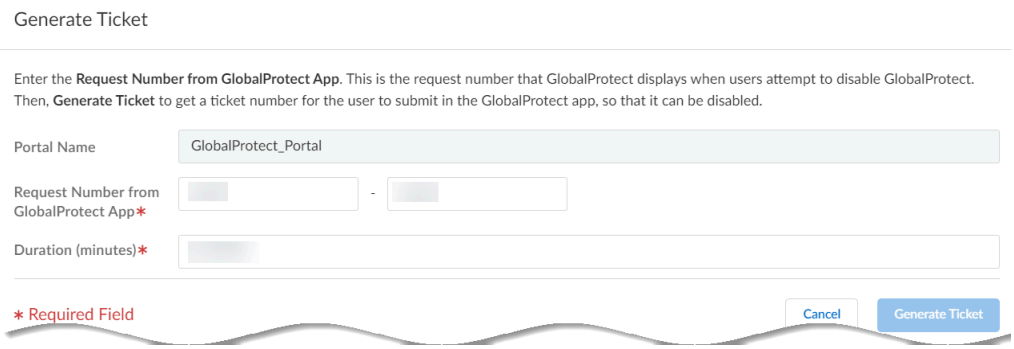


 ©2025 Palo Alto Networks, Inc.

STEP 3 | 生成工单

设置 **Agent Override Key**（客户端覆盖密钥）和 **Allow with Ticket**（允许使用工单）的选项后，您可以 **Generate Ticket**（生成工单）。

当用户尝试在应用程序中禁用 GlobalProtect 时，GlobalProtect 会向他们显示请求编号。在此处提交该请求编号，以生成要为该用户禁用 GlobalProtect 的工单。

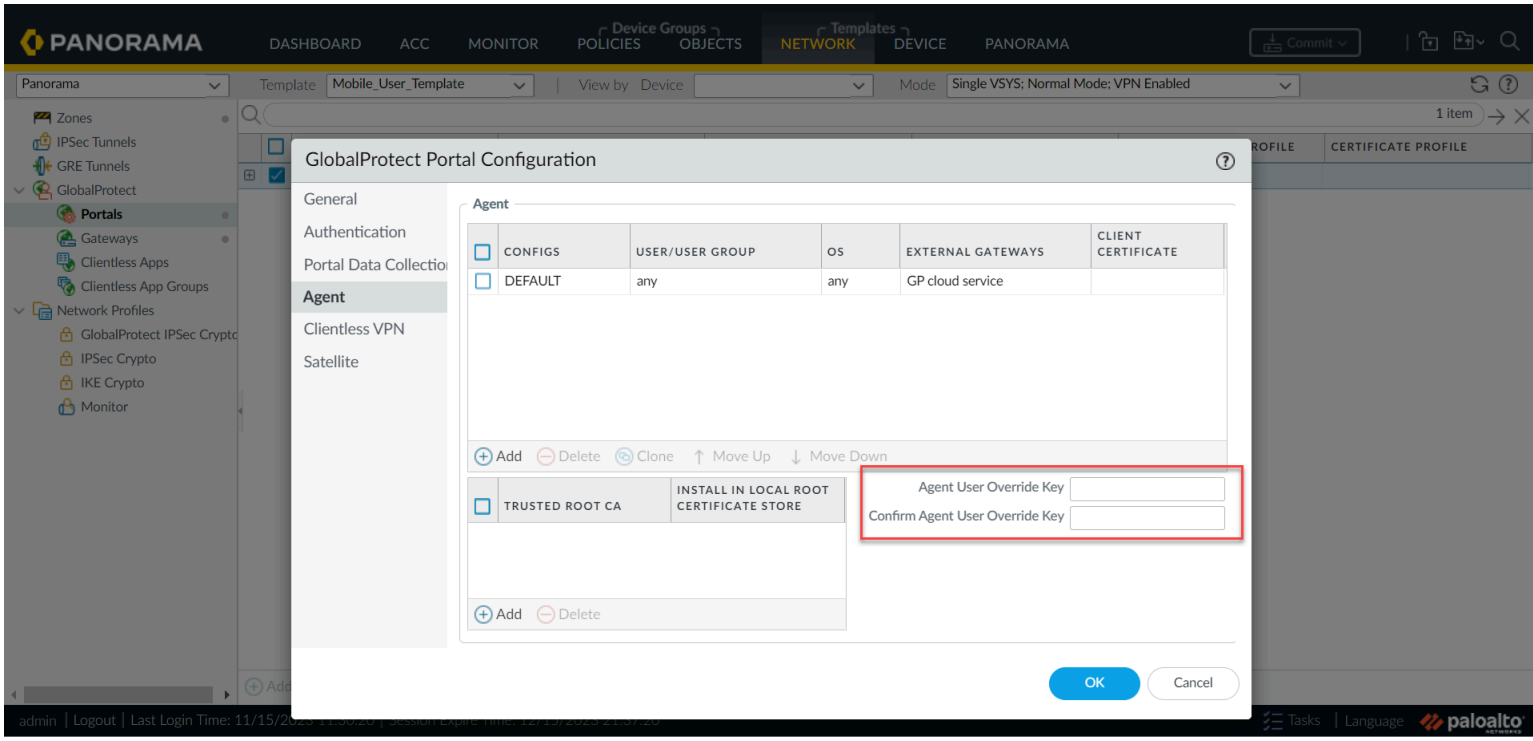


禁用 GlobalProtect 的工单请求 (Panorama)

STEP 1 | 设置客户端覆盖密钥

您需要先设置客户端用户覆盖密钥，然后才能启用允许用户提交工单请求来禁用 GlobalProtect 的选项。

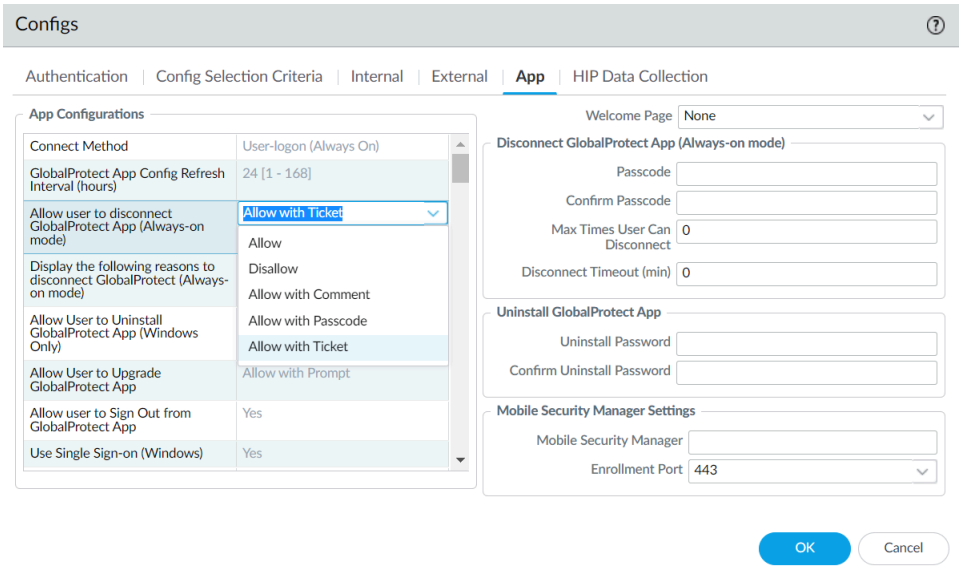
转到 **Network**（网络） > **GlobalProtect** > **Portals**（门户），选择要为其设置覆盖密钥的连接名称。选择 **Agent**（代理），然后输入密钥以设置 **Agent Override Key**（代理覆盖密钥）。



 ©2025 Palo Alto Networks, Inc.

STEP 2 | 允许使用工单禁用 GlobalProtect

转到 **Network**（网络） > **GlobalProtect** > **Portals**（门户），选择您想要允许用户断开连接的连接名称。选择 **Agent**（代理），选择 **Config**（配置），选择 **App**（应用程序） > **App Configurations**（应用程序配置） > **Allow user to disconnect GlobalProtect App (Always-on mode)**（允许用户断开 **GlobalProtect** 应用程序（始终开启模式）），并将该选项设置为 **Allow with Ticket**（允许使用工单）。

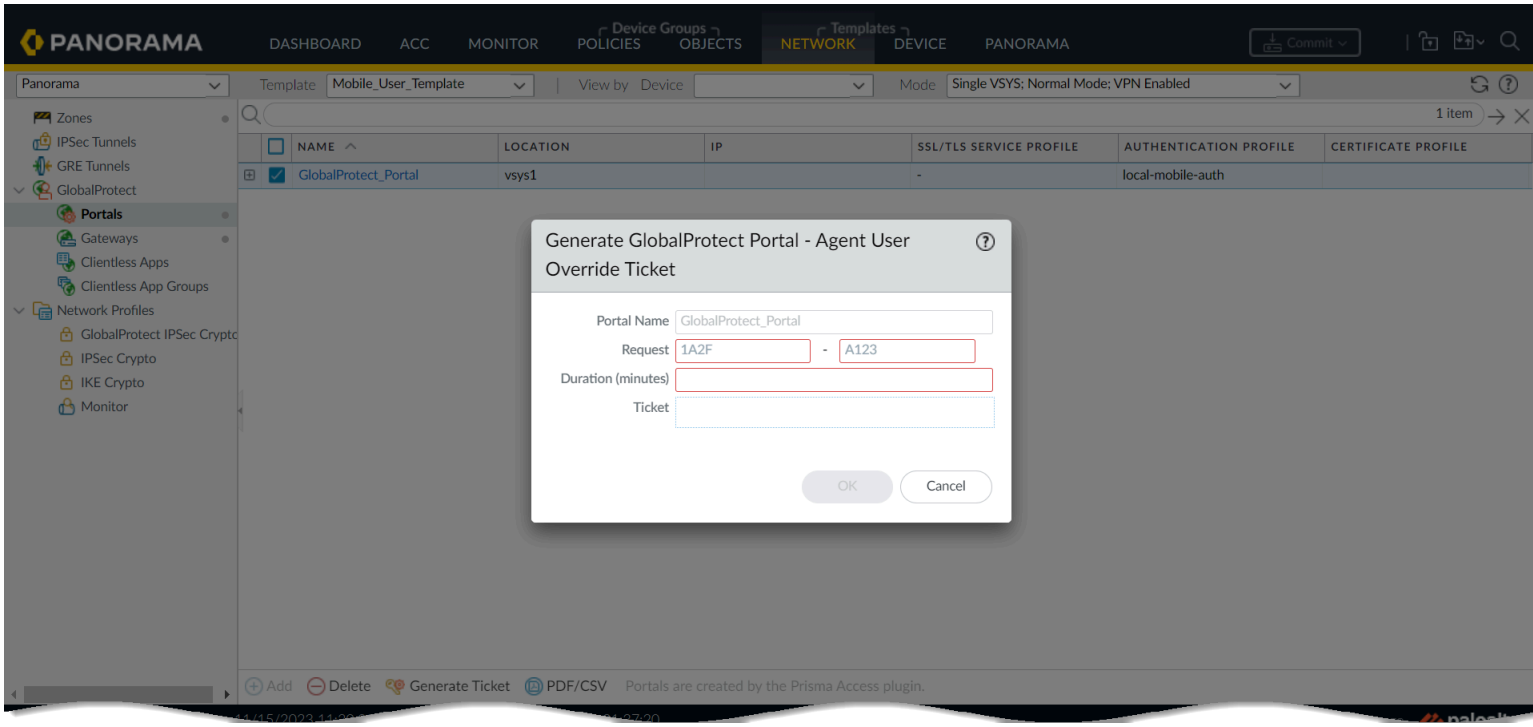


 ©2025 Palo Alto Networks, Inc.

STEP 3 | 生成工单

设置 **Agent Override Key**（客户端覆盖密钥）和 **Allow with Ticket**（允许使用工单）的选项后，您可以 **Generate Ticket**（生成工单）。

当用户尝试在应用程序中禁用 GlobalProtect 时，GlobalProtect 会向他们显示请求编号。在此处提交该请求编号，以生成要为该用户禁用 GlobalProtect 的工单。



GlobalProtect 预登录

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 许可证 ❑ 对要安装计算机证书的端点的管理员访问权 ❑ 端点上部署了可信 PKI 证书

预登录是在用户登录之前建立 VPN 隧道的一种连接方法。预登录的目的是对端点（而非用户）进行身份验证，进而使域脚本和所选择的其他任务能够在端点启动时立即运行。机器证书使端点能够建立至 GlobalProtect 网关的 VPN 隧道。IT 管理员的一般做法是在划分用户端点时安装机器证书。预登录 VPN 隧道使用通用预登录用户名，因为用户尚未登录。要让端点可访问资源，必须创建与预登录用户匹配的安全策略。此类策略规则应仅允许访问启动系统所需的基础服务，例如 DHCP、DNS、特定 Active Directory 服务、防病毒或其他更新服务。用户向网关进行身份验证后，GlobalProtect 应用程序会将 VPN 隧道重新分配给该用户。Prisma Access 上的 IP 地址映射从预登录端点更改为经过身份验证的用户。

©2025 Palo Alto Networks, Inc.

用于预登录身份验证的证书位于端点的个人证书存储中。使用受信任的第三方 CA、自签名 CA 或内部 PKI CA 颁发计算机证书。您需要配置计算机证书作为身份验证方法，以便在登录 Prisma Access 之前建立与端点的隧道，然后创建包含预登录 CA 证书的证书配置文件。

- Strata Cloud Manager
- Panorama

GlobalProtect 预登录 (Strata Cloud Manager)

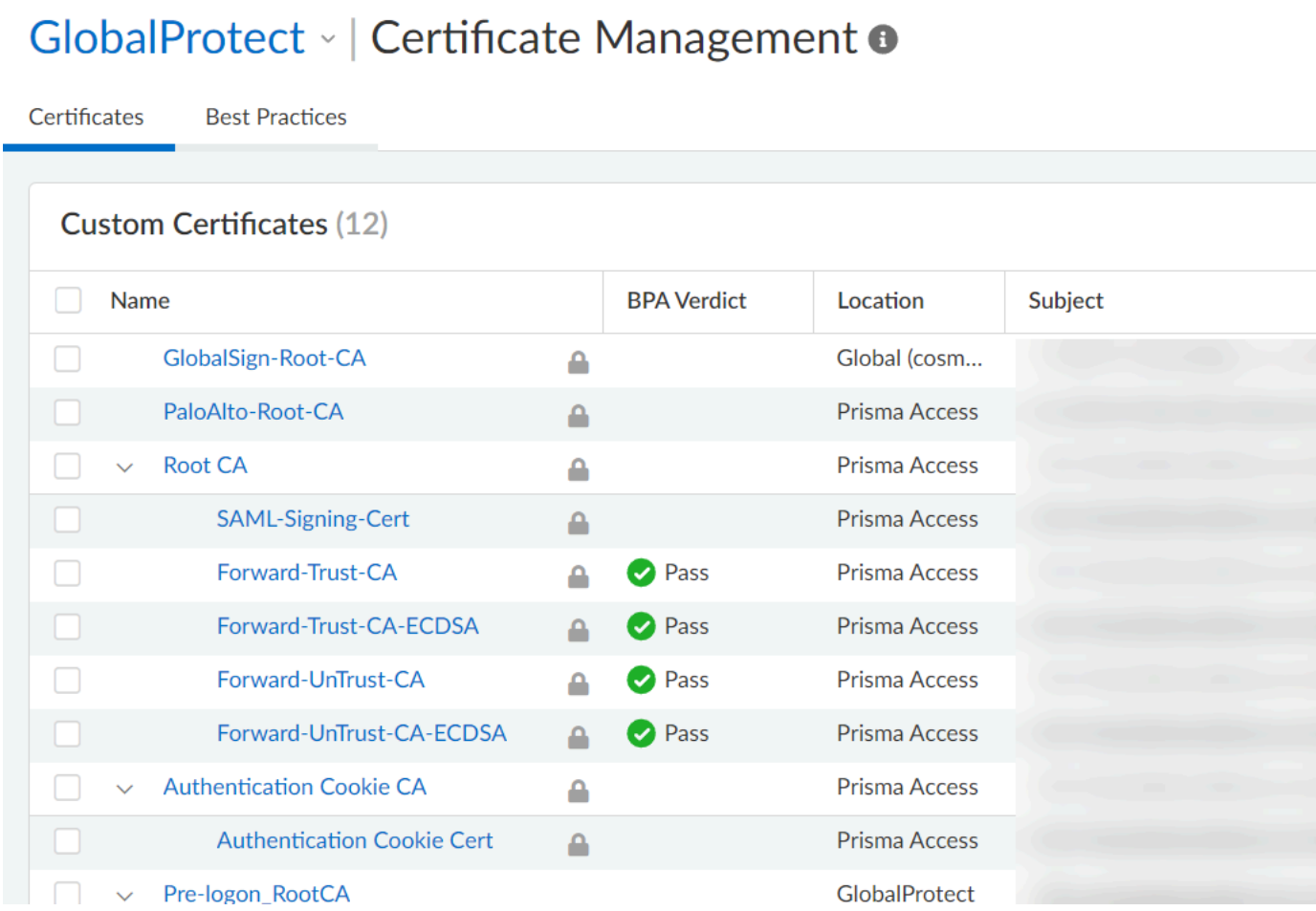
导入第三方根 CA 证书

使用计算机证书作为身份验证方法，以在登录 Prisma Access 之前建立与端点之间的隧道。

STEP 1 | 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access** > **Objects**（**NGFW** 和对象） > **Certificate Management**（证书管理）。选择 **Prisma Access** 配置范围

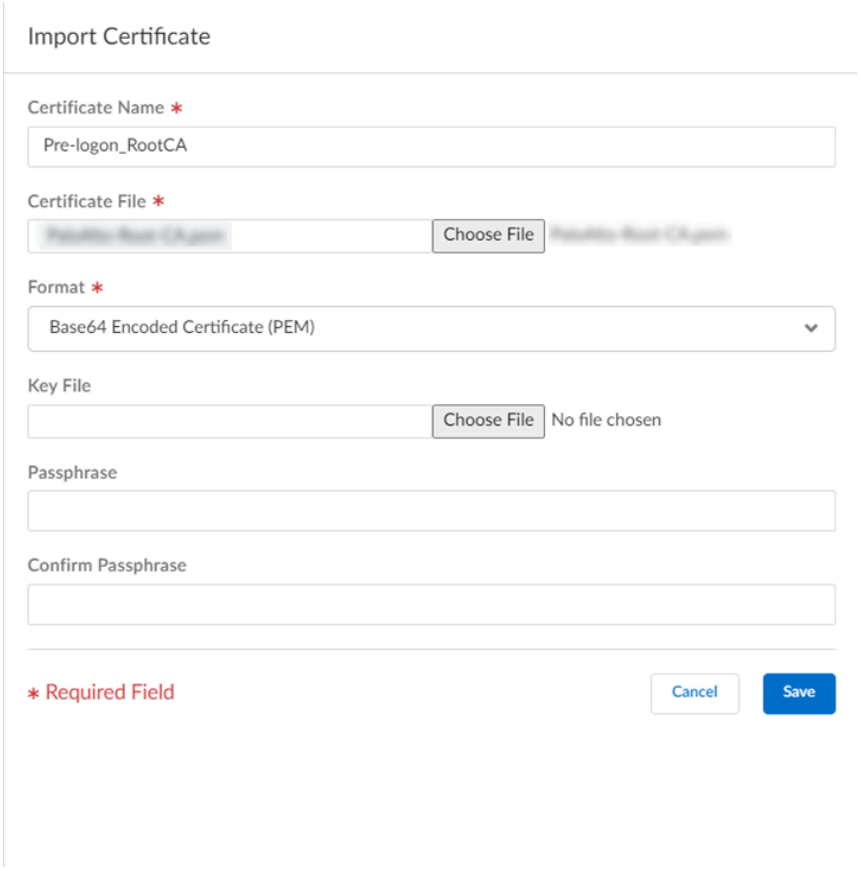
确保您正在为 GlobalProtect 移动用户导入证书。

STEP 2 | 单击 **Import**（导入）以导入自定义证书。



 ©2025 Palo Alto Networks, Inc.

STEP 3 | 输入值，单击 **Save**（保存）以保存证书设置。



创建登录前证书配置文件

创建证书配置文件并包含自签名根 CA。此 CA 会在预登录期间对 GlobalProtect 移动用户所使用的计算机证书进行验证。

STEP 1 | 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access** > **Objects**（**NGFW** 和对象） > **Certificate Management**（证书管理）。选择 **Prisma Access** 配置范围

STEP 2 | 选择 **Add Profile**（添加配置文件）。

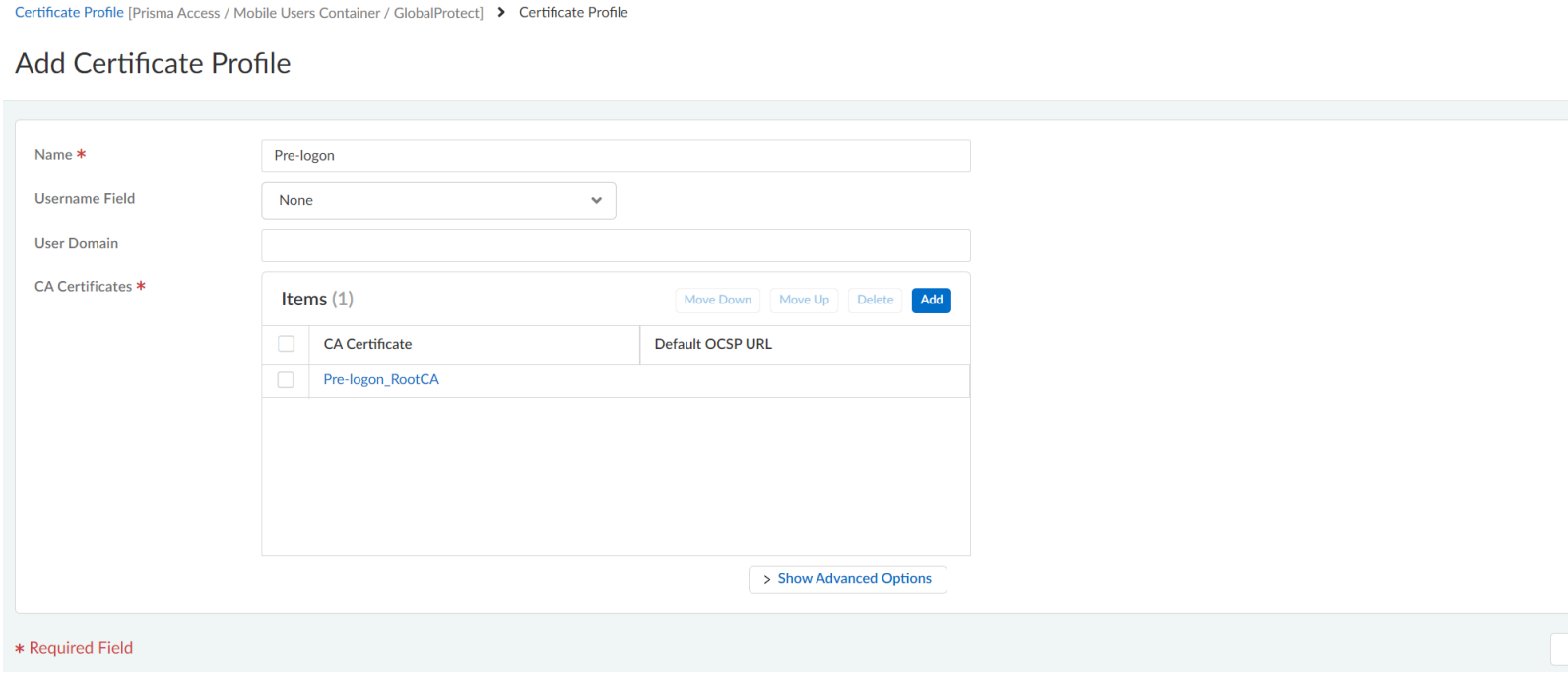
 ©2025 Palo Alto Networks, Inc.

STEP 3 | 输入值。

1. 确保 **Username Field**（用户名字段）为 **None**（无），以防止证书映射到用户。

   如果您按照步骤2中所述，使用任何一种身份验证方法或客户端证书来对证书进行身份验证，则 ***Username Field***（用户名字段）字段不能为 ***None***（无）。

2. 选择 **Add**（添加）以添加在步骤 1 中导入的预登录 CA 根证书。
3. 选择 **Save**（保存）以保存证书配置文件设置。



为预登录配置 GlobalProtect 门户

配置 GlobalProtect 门户以使用计算机证书对连接进行身份验证。

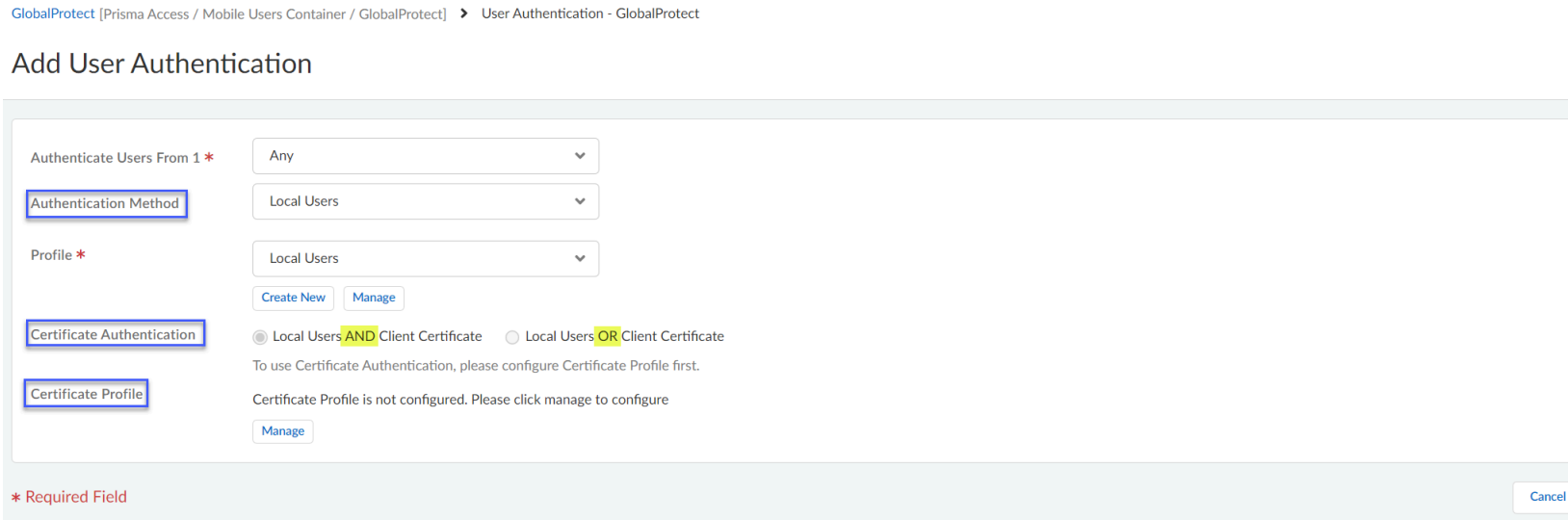
STEP 1 | 选择 **Workflows**（工作流） > **Prisma Access** 设置 > **GlobalProtect** > **Infrastructure**（基础设施）。

 ©2025 Palo Alto Networks, Inc.

STEP 2 | 编辑用户身份验证配置设置。

选择 GlobalProtect 支持的身份验证方法、您创建的预登录证书配置文件以及证书身份验证。

选择 *GlobalProtect* 支持的任何证书身份验证。

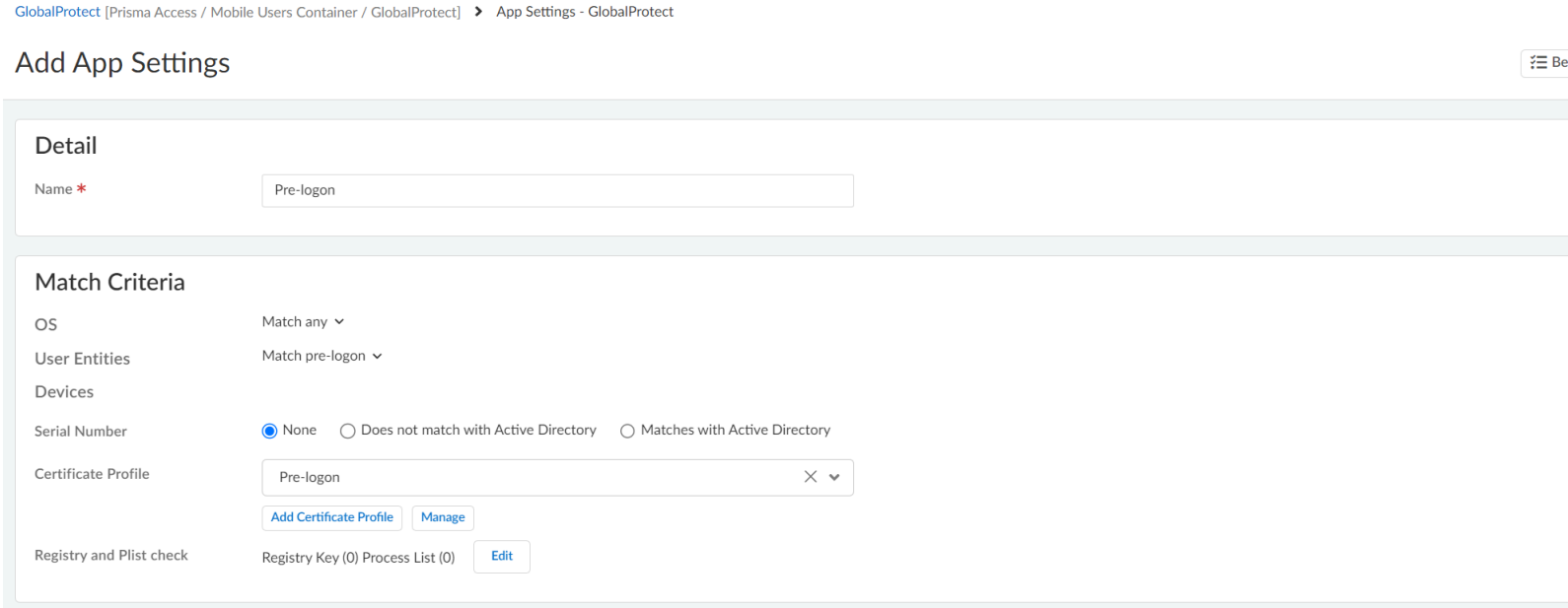


©2025 Palo Alto Networks, Inc.

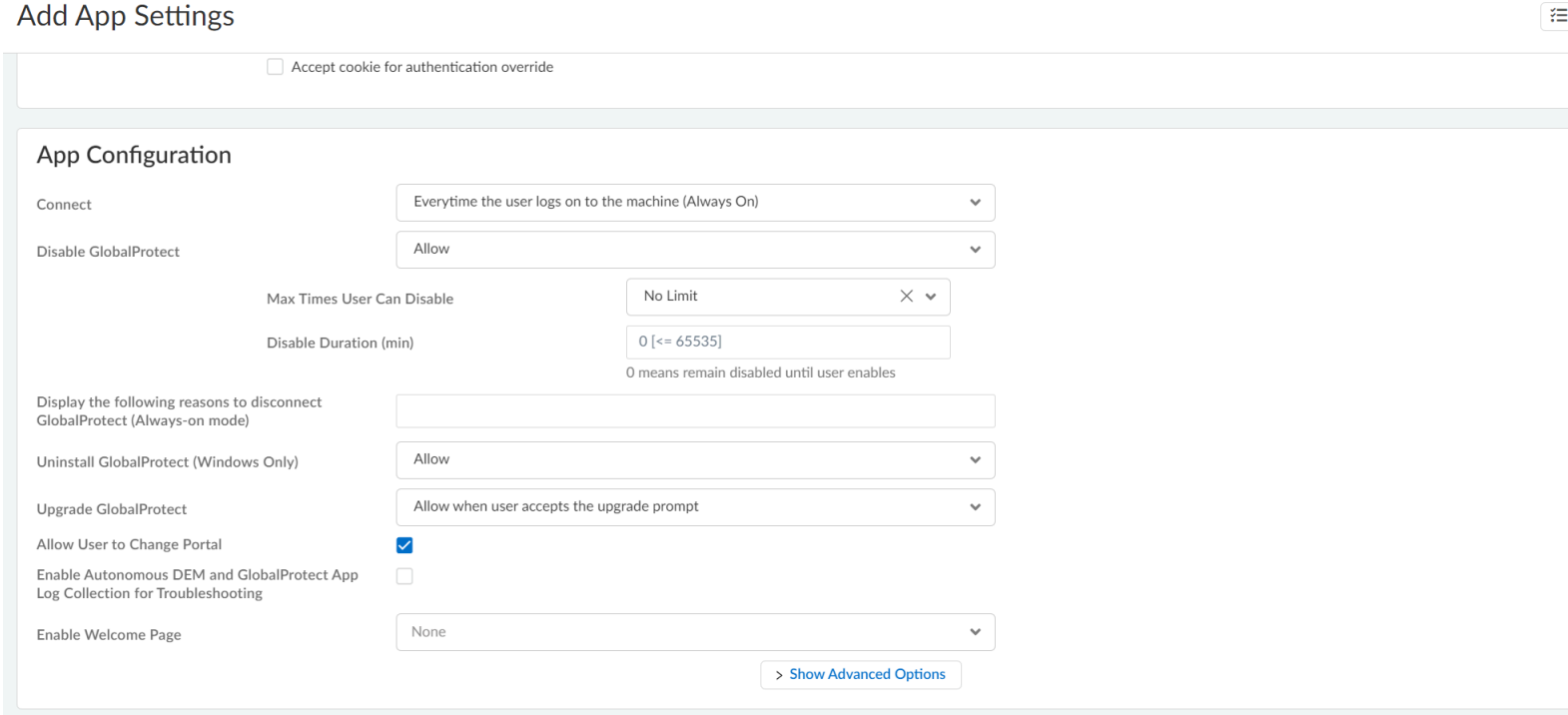
STEP 3 | 配置 GlobalProtect 应用程序设置以匹配预登录条件。

1. 导航到 **GlobalProtect App**（**GlobalProtect** 应用程序）选项卡。
2. 添加应用程序设置。

输入值时，请确保“*User Entities*（用户实体）”设置为 ***Match pre-logon***（匹配预登录），且“*Certificate Profile*（证书配置文件）”设置为 Pre-logon（预登录）。

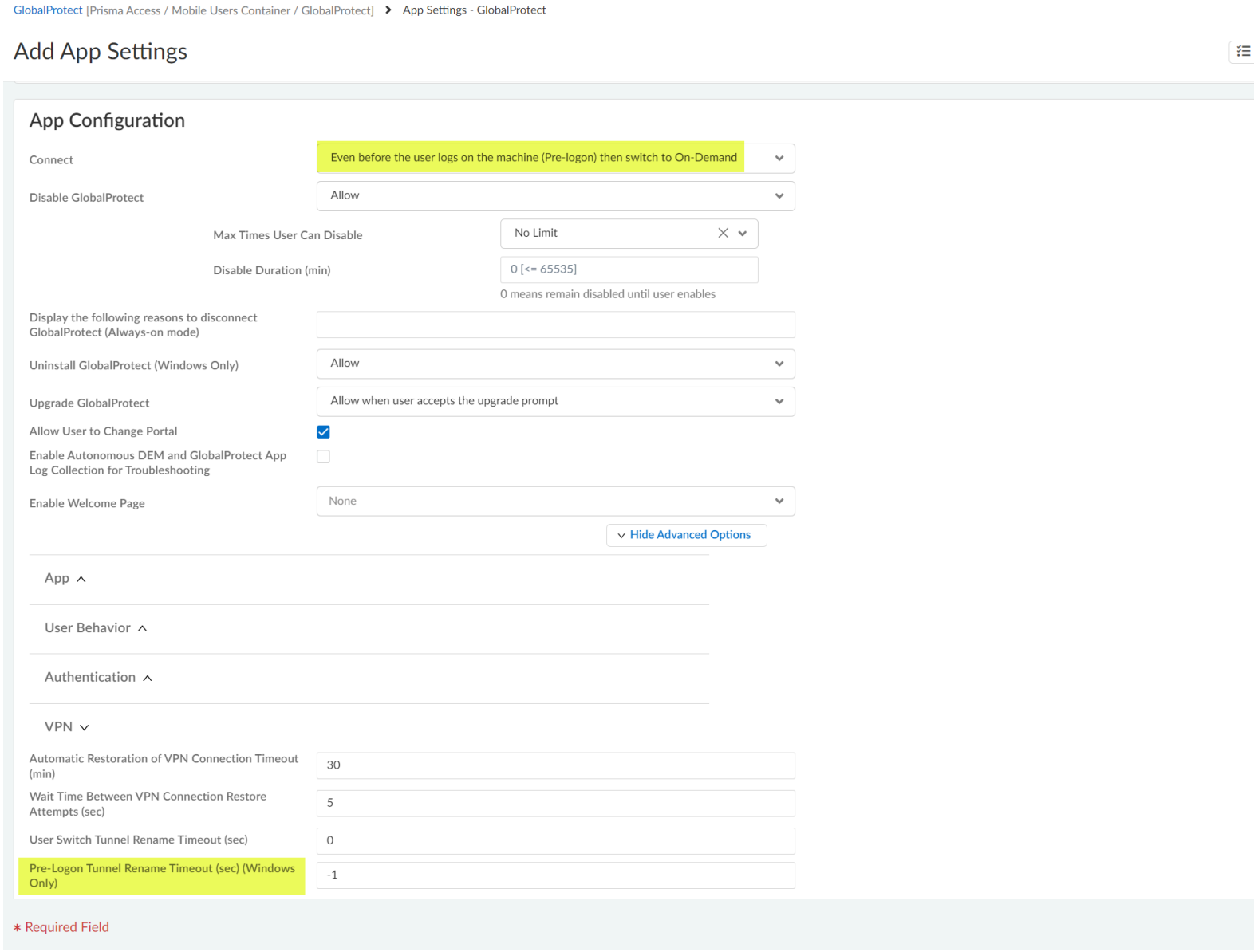


- 选择预登录连接方法。



 ©2025 Palo Alto Networks, Inc.

- 如果选择 **Even before the user logs on the machine (Pre-logon) then switch to On-Demand**（甚至在用户登录计算机之前（预登录），然后切换到按需），则将 **Pre-logon Tunnel Rename Timeout**（登录前隧道重命名超时）设置为 **–1**。查看 VPN 高级选项来编辑该字段。



3. 将预登录应用程序设置移至其他应用程序设置上方。
4. 编辑经过身份验证的用户的所有其他应用程序设置。

   更新连接方法和证书配置文件。

STEP 4 | 将更改推送至 Prisma Access。

安装计算机证书—**Windows**

在端点安装用于身份验证的计算机证书。

STEP 1 | 以 二进制编码证书 **(DER)** 格式从 PKI 导出自签名根 CA 证书。

 ©2025 Palo Alto Networks, Inc.

STEP 2 | 将证书文件传输到 Windows 计算机。

STEP 3 | 在本地计算机的 **Trusted Root Certification Authorities**（受信任的根证书颁发机构）存储中安装登录前 CA 根证书。

STEP 4 | 在本地计算机存储位置安装预登录计算机证书。

STEP 5 | 继续安装，在提示时输入密码短语，然后完成安装。

STEP 6 | 连接到 GlobalProtect 门户，并从主机中删除所有 Cookie。

STEP 7 | （可选）从您的计算机注销，然后查看 GlobalProtect 日志以验证登录前连接。

GlobalProtect 预登录 (Panorama)

配置域登录证书和配置文件

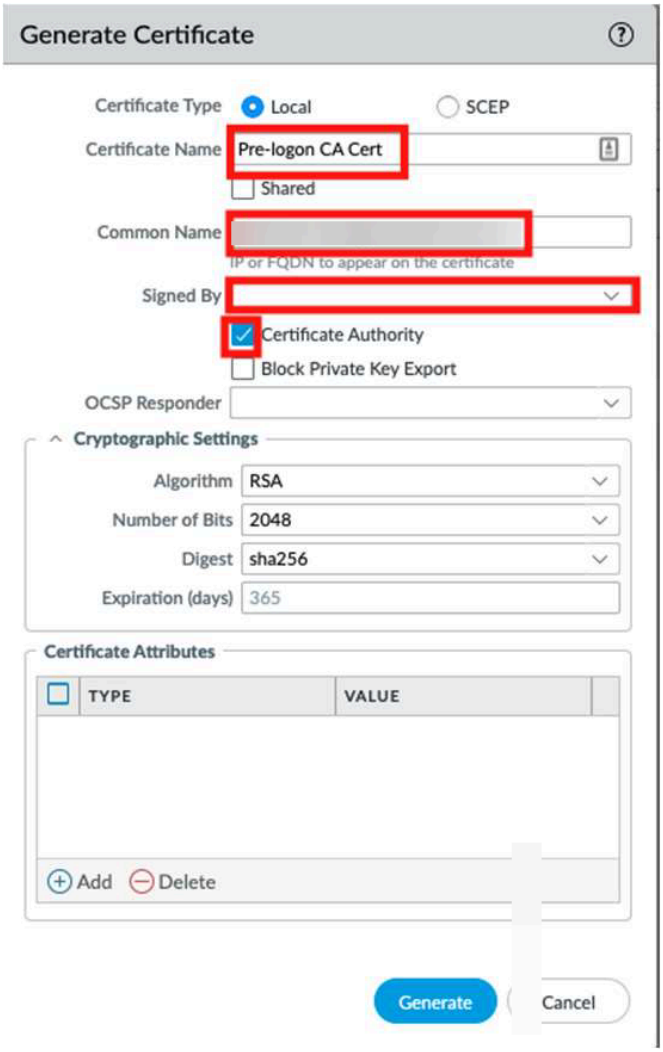
配置计算机证书作为身份验证方法，以便在登录 Prisma Access 之前建立与端点的隧道，然后创建包含预登录 CA 证书的证书配置文件。

©2025 Palo Alto Networks, Inc.

STEP 1 | 配置自签名 CA，并使用它在“Mobile User（移动用户）”模板中生成计算机证书。转到 **Device**（设备） > **Certificate Management**（证书管理） > **Certificates**（证书）。

确保您在 **Mobile_User_Template** 中，并且 **Location**（位置）设置为 **Shared**（共享）。

1. 为证书命名；例如 **Pre-logon CA Cert**。
2. 在 **Common Name**（通用名称）中输入名称。
   通用名称 (CN) 是您希望使用证书保护的域名，例如 www.yourdomainname.com。
3. 将 **Signed By**（签名者）字段留空，然后选中 **Certificate Authority**（证书颁发机构）复选框。
4. 选择 **Generate**（生成）以生成用于预登录连接的证书。

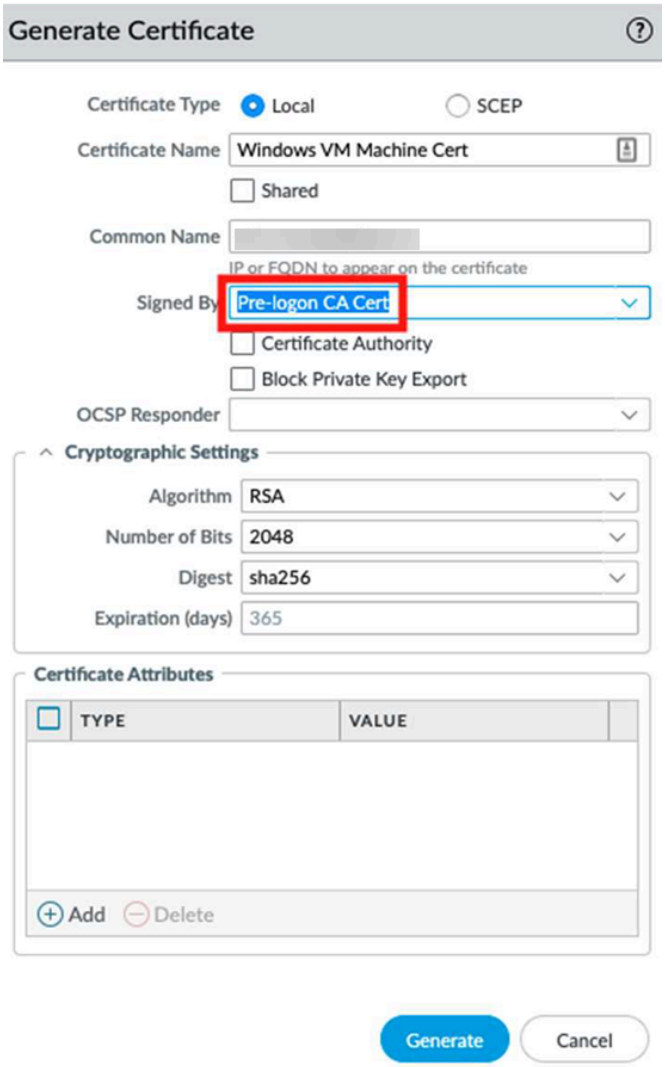


©2025 Palo Alto Networks, Inc.

STEP 2 | 在配置自签名 CA 后，将会生成计算机证书。

1. 在 **Certificate Name**（证书名称）和 **Common Name**（通用名称）中输入。
2. 在 **Signed By**（签名者）下拉列表中，选择您在第 1 步中创建的 **Pre-logon CA Cert** 证书。
3. 选择 **Generate**（生成）以生成稍后要安装在 Windows 计算机上的 **Windows VM** 计算机证书。

   此证书是登录前 CA 的子证书。

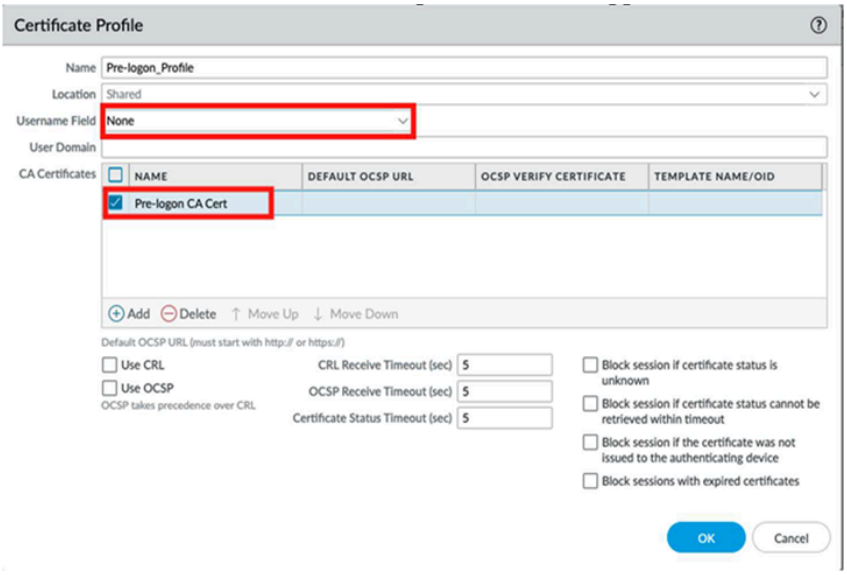


STEP 3 | 要创建一个包含预登录 CA 证书的证书配置文件，请转到 **Device**（设备） > **Certificate Management**（证书管理） > **Certificate Profile**（证书配置文件）。

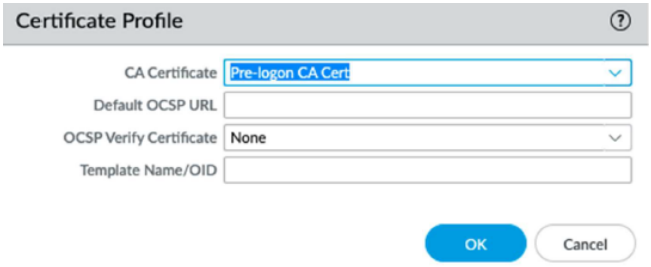
使用此 CA 来验证 GlobalProtect 客户端在登录前隧道初始化期间提供的计算机证书。

©2025 Palo Alto Networks, Inc.

STEP 4 | 创建并命名配置文件。确保 **Username Field**（用户名字段）为 **None**（无），以防止证书映射到用户。



STEP 5 | 在 **CA Certificates**（**CA** 证书）下方，选择 **Add**（添加），然后从下拉菜单中选择 **Pre-logon CA Cert**。



STEP 6 | 选择 **OK**（确定），然后再次选择 **OK**（确定）。

为预登录配置 **GlobalProtect** 门户

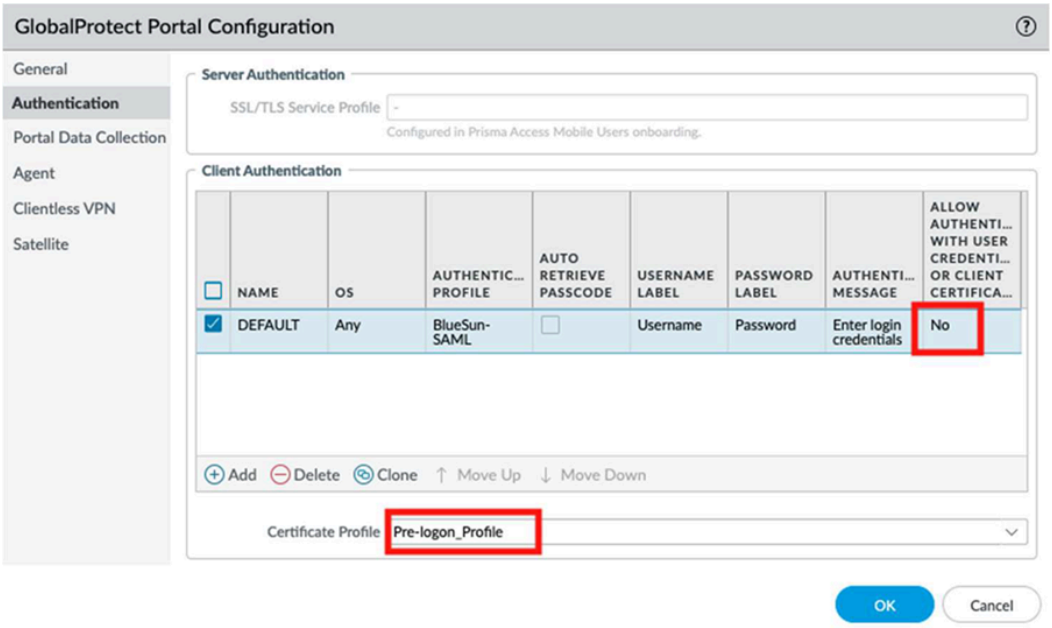
配置 GlobalProtect 门户以使用计算机证书对连接进行身份验证。

STEP 1 | 转到 **Network**（网络） > **GlobalProtect** > **Portals**（门户） > **GlobalProtect_External_Gateway** > **Authentication**（身份验证）。

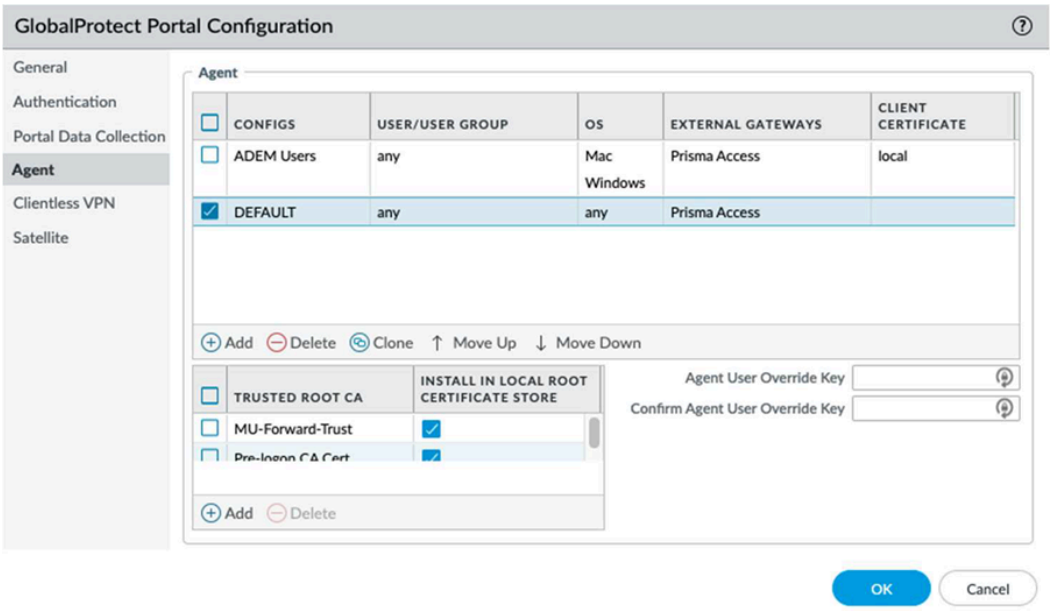
STEP 2 | 在 **Allow Authentication with User Credentials OR Client Certificate**（允许使用用户凭据或客户端证书进行身份验证）下方，选择 **No**（否），以仅强制实施基于证书的身份验证。

©2025 Palo Alto Networks, Inc.

STEP 3 | 对于 **Certificate Profile**（证书配置文件），选择创建的 **Pre-logon_Profile**，然后点击 **OK**（确定）。



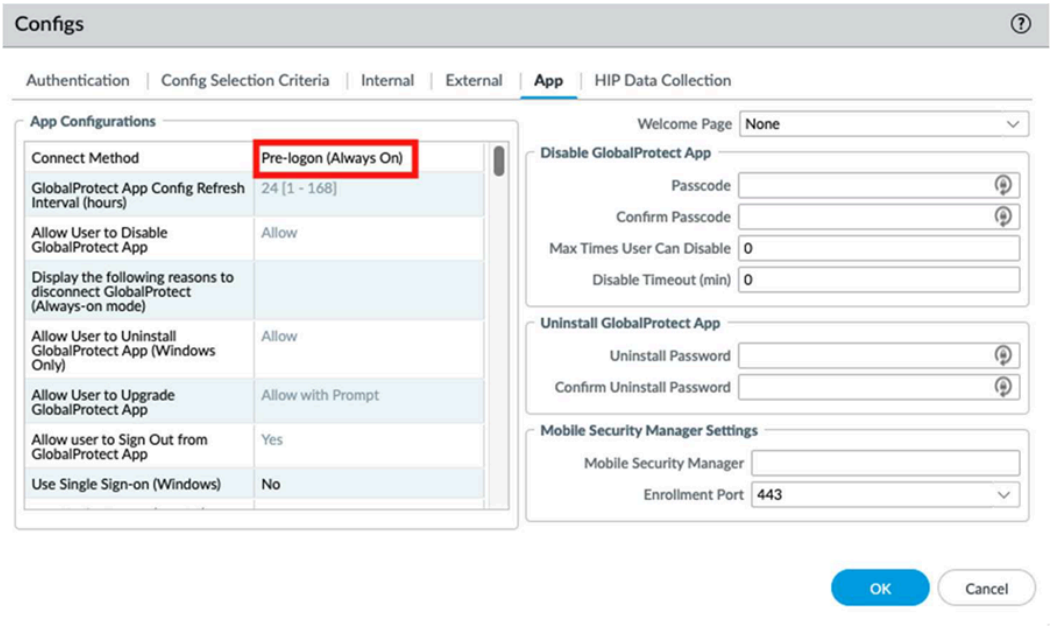
STEP 4 | 选择 **Agent**（代理），并打开已认证用户的代理配置。



STEP 5 | 选择 **App**（应用）选项卡。

©2025 Palo Alto Networks, Inc.

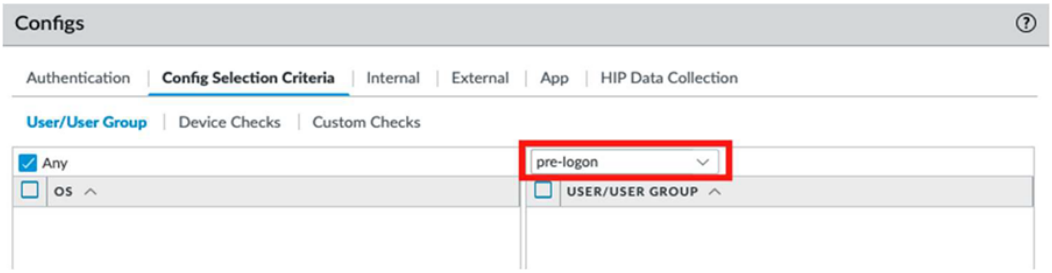
STEP 6 | 选择 **Pre-logon (Always On)**（预登录（始终开启）），然后选择 **OK**（确定）以返回到“Agent（代理）”区域。



STEP 7 | 在“Agent（代理）”区域中，选择 **Clone**（克隆）以克隆默认配置。将配置名称更改为 **Pre-logon**，以匹配用于计算机证书身份验证的连接方法。

STEP 8 | 选择新克隆的代理配置。

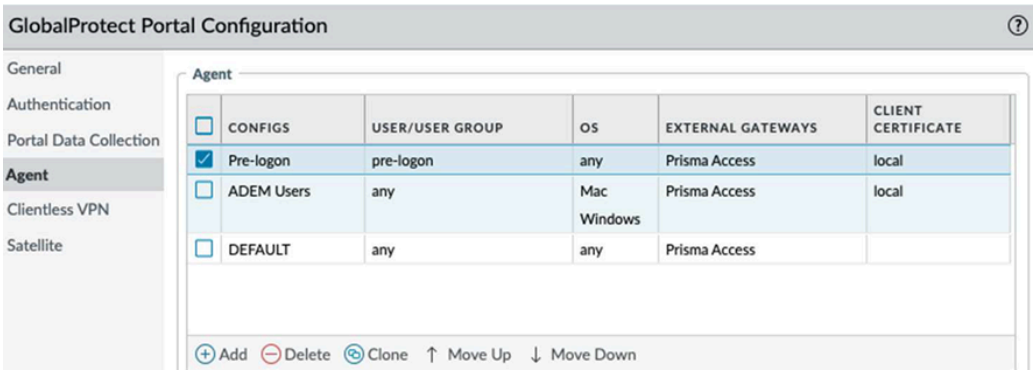
STEP 9 | 选择 **Config Selection Criteria**（配置选择标准）。在 **User/User Group**（用户/用户组）配置项下，从 **USER/USER Group**（用户/用户组）配置框上方的下拉菜单中选择 **pre-logon**（预登录），并确保配置设置为 **Any**（任意）。



STEP 10 | 根据需要配置应用程序设置，然后选择 **OK**（确定）。确保为预登录配置和当前配置都选择了预登录连接方法。

©2025 Palo Alto Networks, Inc.

STEP 11 | 将预登录代理配置移动到 **CONFIGS** 列表的顶部，以确保它首先与预登录条件相匹配。



STEP 12 | 单击确定以保存门户配置。

配置 **Prisma Access GlobalProtect** 网关

在 Panorama Managed Prisma Access 中配置 GlobalProtect 网关。

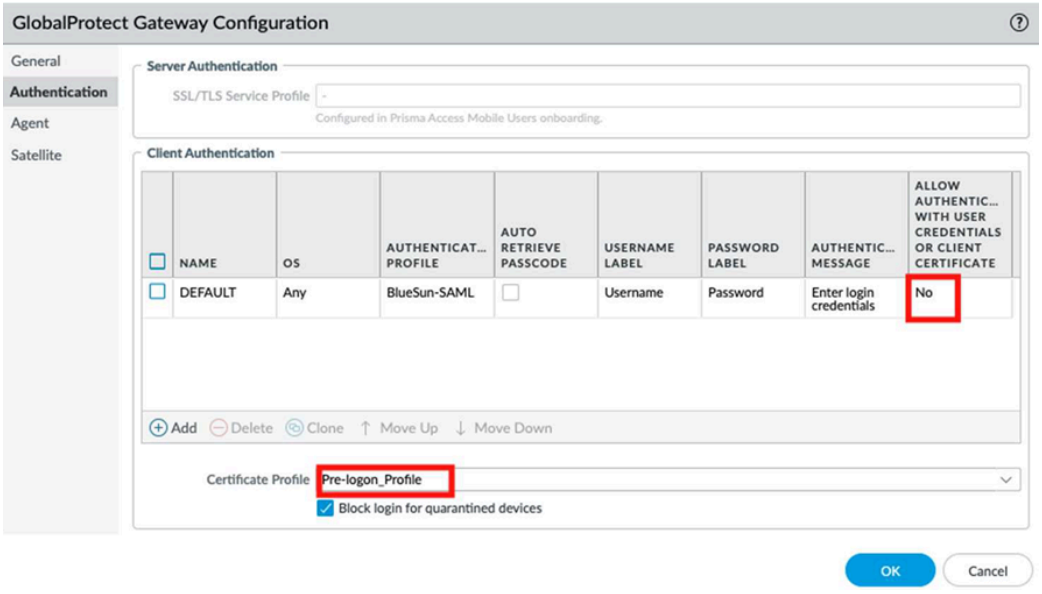
此配置仅强制实施基于证书的身份验证。

STEP 1 | 转到 **Network**（网络） > **GlobalProtect**（全球保护） > **Gateways**（网关） > **GlobalProtect_External_Gateway** > **Authentication**（身份验证）。

STEP 2 | 选择 **Default**（默认）身份验证方法。

如果您已经配置了客户端身份验证（例如 SAML），则选择已配置的，而不是选择 **Default**（默认）。

STEP 3 | 在 **Allow Authentication with User Credentials or Client Certificate**（允许使用用户凭据或客户端证书进行身份验证）下方，选择 **No**（否），然后选择 **OK**（确定）以保存配置。



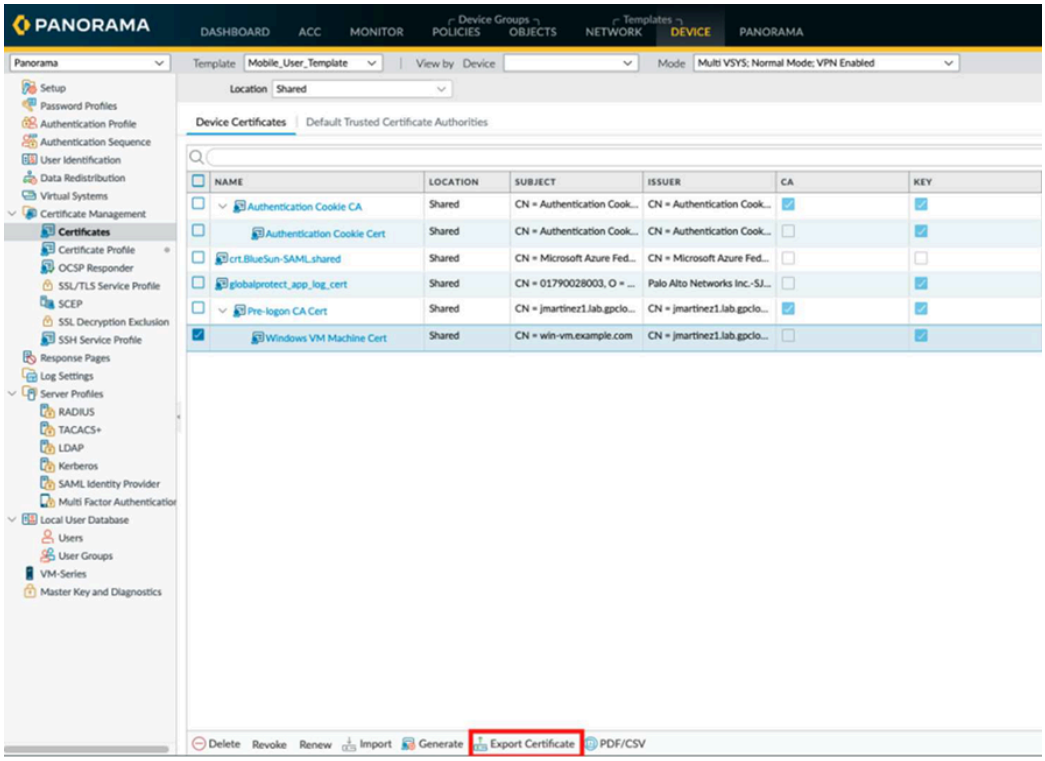
 ©2025 Palo Alto Networks, Inc.

安装计算机证书—Windows

在移动用户用于身份验证的端点上安装计算机证书。

STEP 1 | 转到 **Device**（设备） > **Certificate Management**（证书管理） > **Certificates**（证书）。

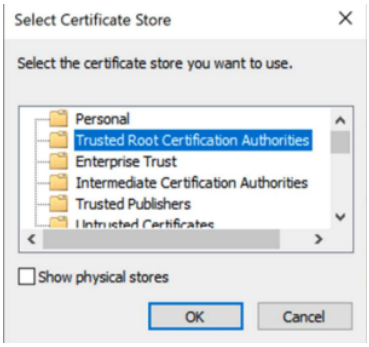
STEP 2 | 确保您仍在 Mobile_User_Template 中。选择 **Windows VM Machine Cert**（**Windows VM** 计算机证书），然后选择 **Export Certificate**（导出证书）以将其下载为带有密码短语的 PKCS12 文件。



STEP 3 | 将登录前 CA 证书导出为 base64 编码的证书。

STEP 4 | 将证书文件传输到 Windows 计算机。

STEP 5 | 在本地计算机的 **Trusted Root Certification Authorities**（受信任的根证书颁发机构）存储中安装登录前 CA 根证书。



STEP 6 | 在本地计算机存储位置安装预登录计算机证书。完成权限，然后选择 **Next**（下一步）以继续安装。

©2025 Palo Alto Networks, Inc.

STEP 7 | 验证证书的文件名，然后选择 **Next**（下一步）。

STEP 8 | 输入密码，也就是您在从 Panorama 导出证书时使用的密码，然后选择 **Next**（下一步）。

STEP 9 | 在 **Certificate Store**（证书存储）对话框中，选择 **Place all certificates in the following store**（将所有证书放在以下存储中），然后选择 **Browse**（浏览）。

STEP 10 | 选择 **Personal folder**（个人文件夹）以用于安装计算机证书，然后选择 **OK**（确定）。

STEP 11 | 选择 **Next**（下一步）以继续安装。

STEP 12 | 连接到 GlobalProtect 门户，并从主机中删除所有 Cookie。

STEP 13 | （可选）从您的计算机注销，然后查看 GlobalProtect 日志以验证登录前连接。

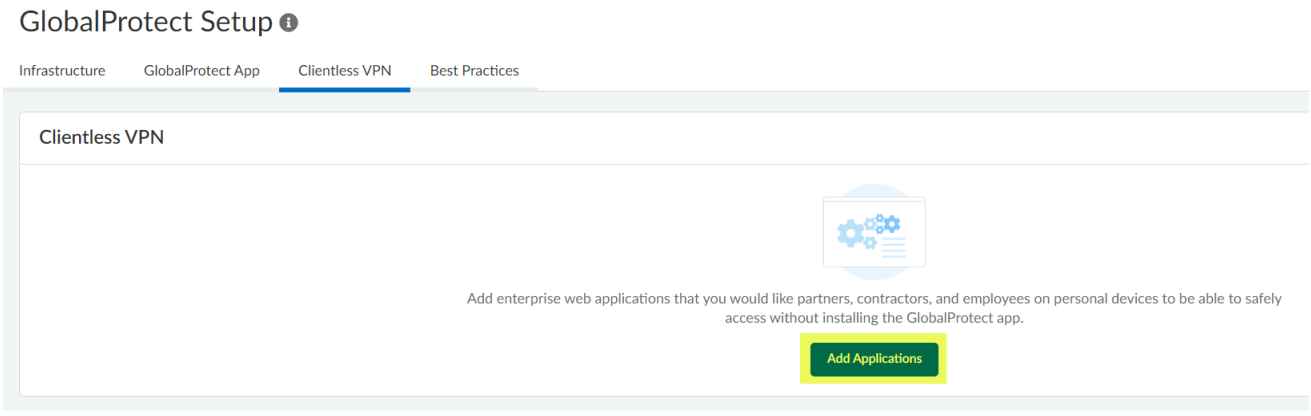
GlobalProtect — 无客户端 VPN

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

使用无客户端 VPN，可从支持 SSL 的 Web 浏览器实现对企业应用程序的安全远程访问。使用无客户端 VPN，最终用户无需在其端点上安装 GlobalProtect 应用程序，这在您需要允许合作伙伴或承包商访问应用程序并安全地启用非托管资产（包括个人端点）时非常有用。

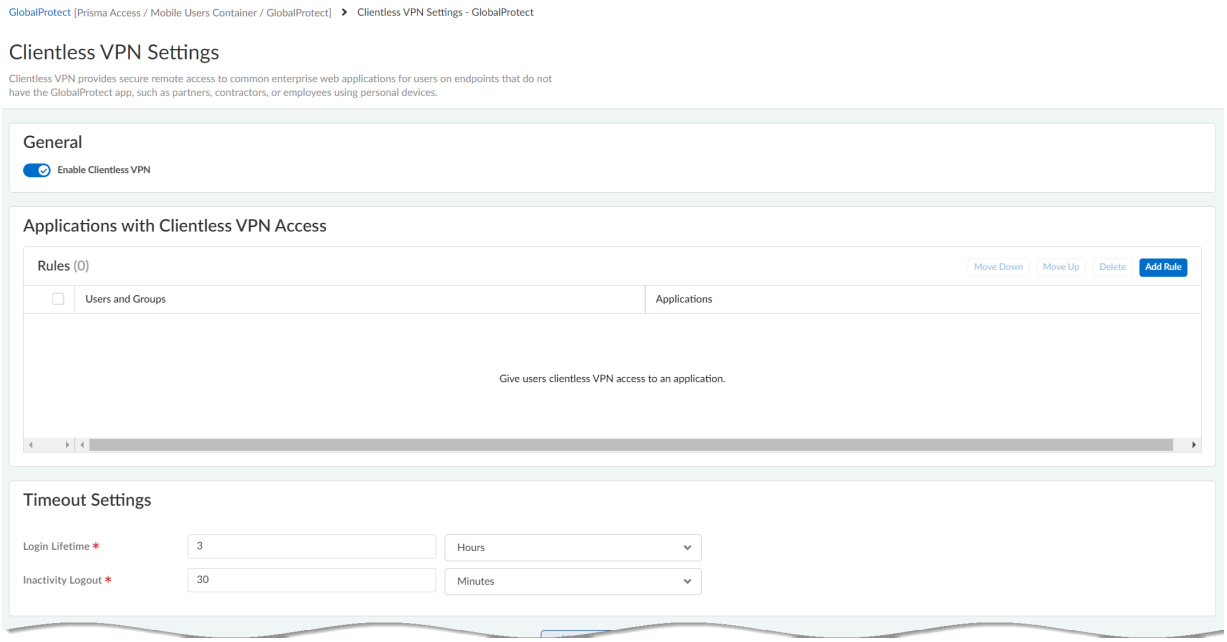
使用以下步骤为 Prisma Access 设置无客户端 VPN：

STEP 1 | 转到 **Settings**（设置） > **Prisma Access** 设置 > **GlobalProtect** > **GlobalProtect Setup**（**GlobalProtect** 设置） > **Clientless VPN**（无客户端 **VPN**），单击 **Add Applications**（添加应用程序）。



 ©2025 Palo Alto Networks, Inc.

STEP 2 | **Enable Clientless VPN**（启用无客户端 **VPN**）。



STEP 3 | 添加无客户端 VPN 规则。

指定可使用无客户端 VPN 的用户和应用程序。

STEP 4 | 如果用户需要通过代理服务器访问应用程序，请单击 **Add Proxy**（添加代理）。

只支持对代理的基本身份验证（用户名和密码）。您可以添加多个代理服务器配置，每组域配置一个。要添加的一些设置包括：

- **Domains**（域）— 添加代理服务器提供的域。您可以在域名开头使用通配符 **(*)** 来表示多个域。
- **Enable Proxy**（启用代理）— 分配代理服务器以提供对域的访问。
- **Server**（服务器）— 指定代理服务器的 IP 地址或主机名。
- **Port**（端口）— 指定与代理服务器通信的端口。
- **User and Password**（用户和密码）— 指定登录代理服务器所需的用户和密码凭据。再次指定密码以进行验证。

STEP 5 | 修改默认 **Crypto Settings**（加密设置），指定 Prisma Access 与使用无客户端 VPN 的应用程序之间的 SSL 会话的身份验证和加密算法。

©2025 Palo Alto Networks, Inc.

STEP 6 | 将域添加到 **Rewrite Exclude Domain List**（重写排除域列表）。

无客户端 VPN 充当反向代理，并修改发布的应用程序返回的 Web 页面。它会重写所有 URL 并向远程用户显示重写的页面，以便当用户访问这些 URL 时，请求都会通过 GlobalProtect 门户。在某些情况下，应用程序可能包含不需要通过门户访问的页面（例如，应用程序可能包含来自 yahoo.finance.com 的股票行情自动收录器）。您可以排除这些页面。您添加到 **Rewrite Exclude Domain List**（重写排除域列表）中的域将被排除在重写规则之外，并且无法重写。域名中不支持路径。域名的通配符 (*) 只能出现在名称的开头（例如，*.etrade.com）。

监控 GlobalProtect 移动用户

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证

Prisma Access (Managed by Strata Cloud Manager)

Prisma Access (Managed by Strata Cloud Manager) 用户可以使用 **Monitor**（监控） > **Users**（用户）。选择 **GlobalProtect** 或 **Explicit Proxy**（显式代理）连接方法。**Mobile Users**（移动用户）页面特定于您正在使用的连接方法。

Prisma Access (Managed by Panorama)

可在 Panorama 中的多个位置查看已登录用户的列表。可以查看不重复用户的数量、用户登录的位置，还有多个能提供更多额外信息的表格。了解 Prisma Access 如何计算“移动用户—GlobalProtect”部署中每个位置的用户数量也很重要。

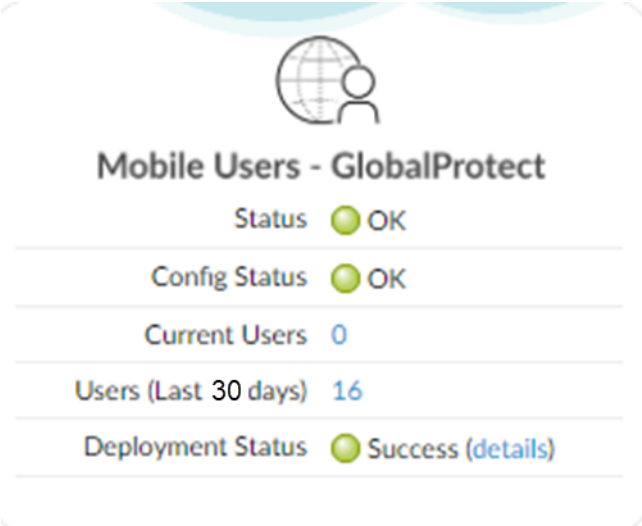
您可以从多个位置获取用户的详细视图：

- 要查看用户的总体概览并打开一个表格，以便你能够查看已登录用户并将其注销，请选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Status**（状态）。
- 要在地图视图中查看用户的图形化展示，并按地区和位置查看用户，请选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Service Stats**（服务统计数据） > **Mobile Users—GlobalProtect**（移动用户—全球保护）。
- 您还可以详细了解 Prisma Access 如何统计移动用户数量。

从“**Status**（状态）”选项卡查看 **GlobalProtect** 移动用户

要查看当前在所有位置已登录的唯一用户总数，请选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Status**（状态） > **Mobile Users—GlobalProtect**（移动用户—全球保护）。

 ©2025 Palo Alto Networks, Inc.



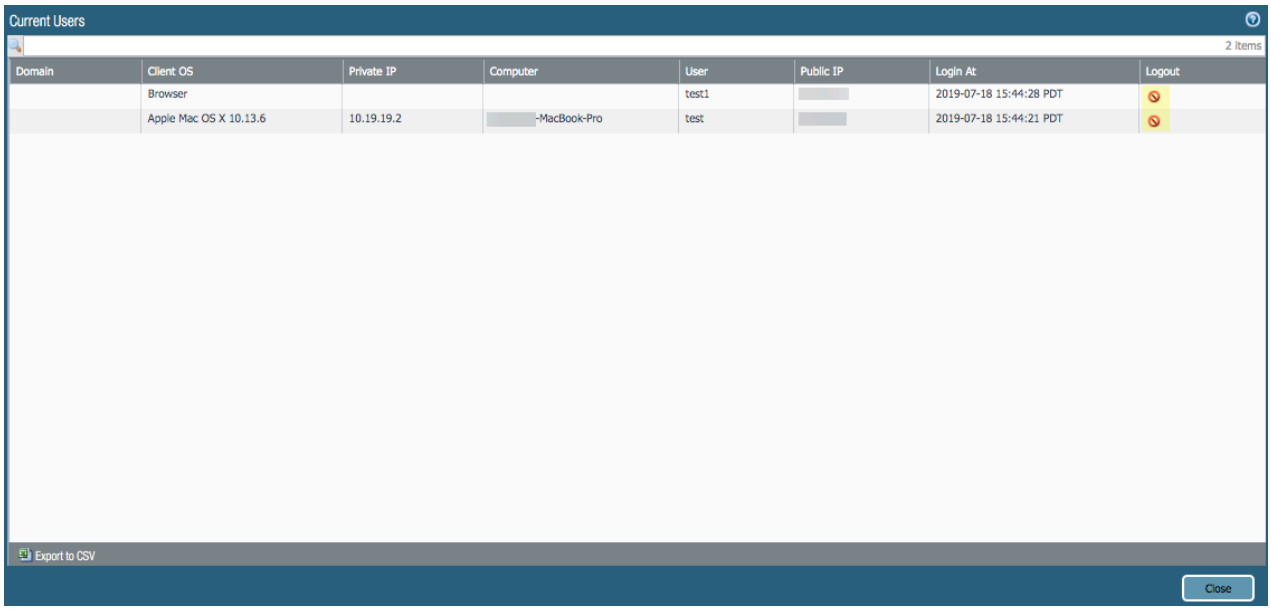
要查看当前已登录用户的更多详细信息，请单击 **Current Users**（当前用户） 旁边的超链接数字，以显示 **Current Users**（当前用户）表格。

在“*Status*（状态）”页面上显示的用户总数与弹出表格中显示的用户数量可能会有所不同；表格中显示的数量可能会更多。

可以从 **Current Users**（当前用户）表格中注销处于活动状态的用户；要执行此操作，选择该用户，然后单击 **Logout**（注销）。注意，要让 Prisma Access 将已注销的用户从 **Current Users**（当前用户） 页面中移除，您可能需要先关闭然后重新打开屏幕。

以下屏幕显示使用 GlobalProtect 应用程序和无客户端 VPN 登录的用户。屏幕显示用户的用户名、公共 IP 和上次登录时间。如果用户使用 GlobalProtect 应用程序登录，它还会显示用户的客户端操作系统、私有 IP 地址和计算机名称。

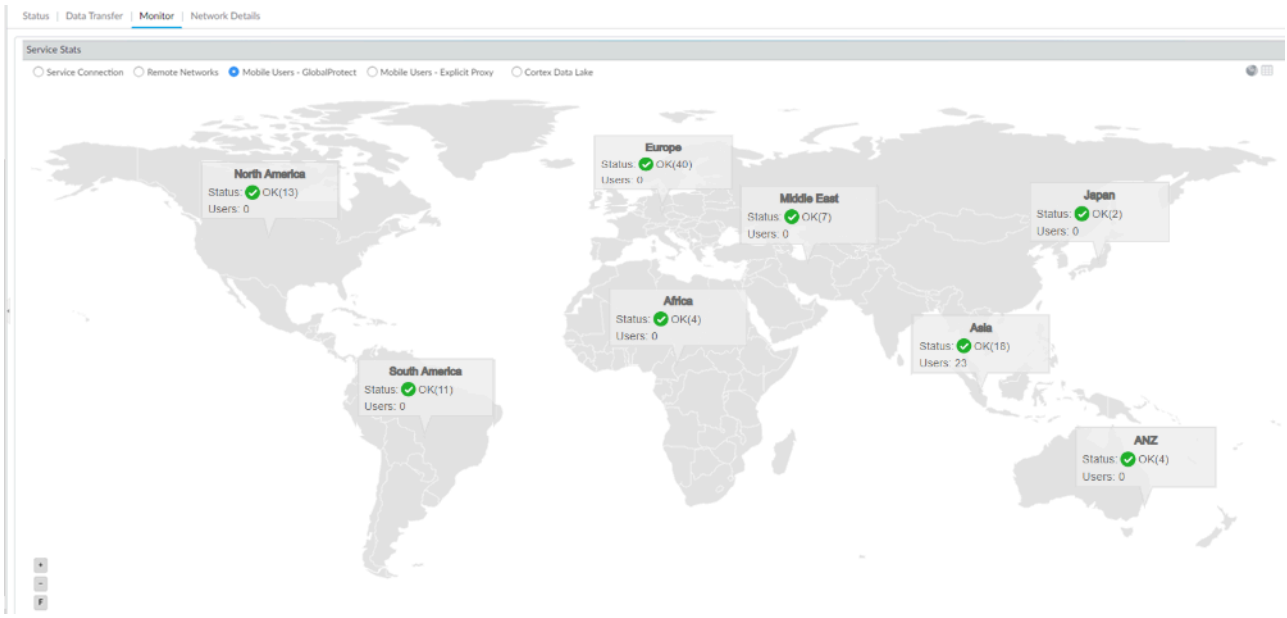
 ©2025 Palo Alto Networks, Inc.



从“**Monitor**（监控）”选项卡查看 **GlobalProtect** 移动用户

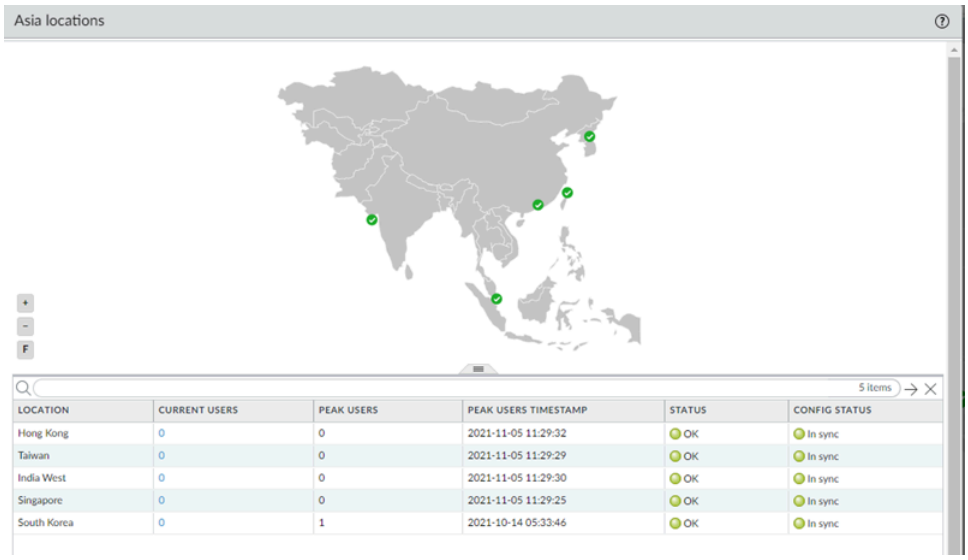
要查看每个地区已登录的不重复用户数量，请选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Service Stats**（服务统计数据） > **Mobile Users—GlobalProtect**（移动用户—**GlobalProtect**）。

 ©2025 Palo Alto Networks, Inc.



要查看某个区域内位置的详细信息，请单击该区域。

在全球地图视图页面上显示的用户数量与每个地区在表格中显示的用户数量可能会有所不同；表格中显示的数量可能会更多。



Prisma Access 如何统计 **GlobalProtect** 移动用户的数量

状态区域中显示的用户总数可能与关联表中显示的数量不同。以下部分描述了这些差异。

- **Status**（状态）选项卡（**Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Status**（状态））—在主页的 **Mobile Users—GlobalProtect**（移动用户—**GlobalProtect**）区域中显示的用户数量，该数量可能与您单击 **Current Users**（当前用户）超链接后出现的表格中的数量不同。在 **Mobile Users—GlobalProtect**（移动用户—全球保护）区域中显示的数量统计的是不重复用

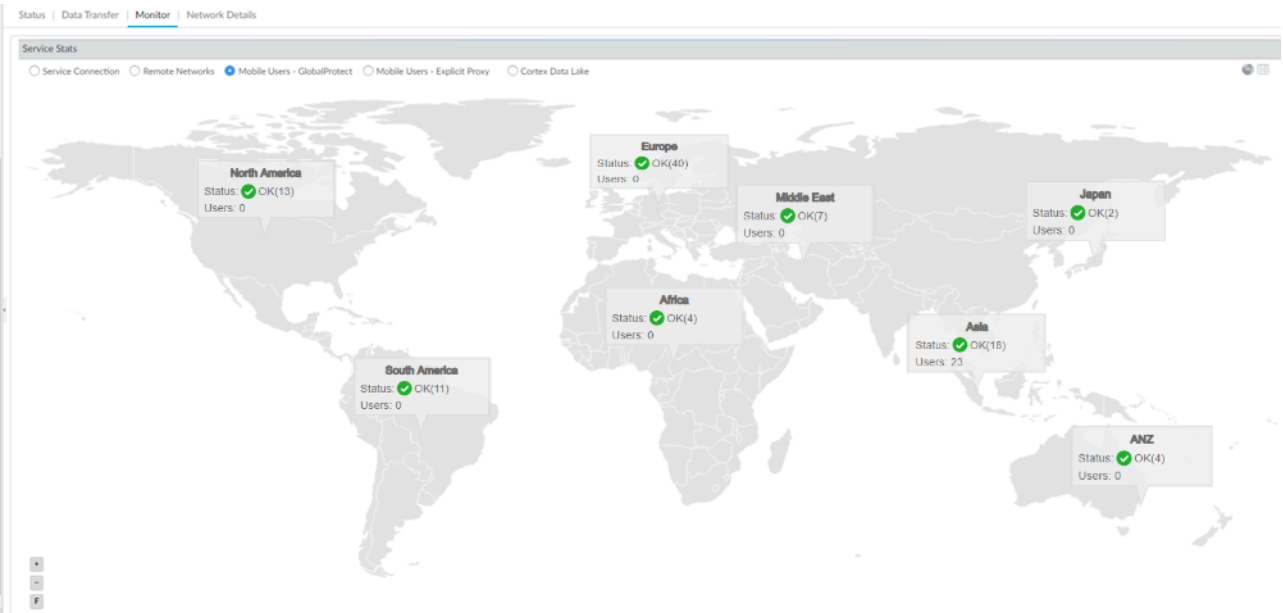
 ©2025 Palo Alto Networks, Inc.

户的数量；而 **Current Users**（当前用户）表格中的用户列表统计的是每次登录或连接的所有用户数量。如果单个用户登录到多个网关或连接到多个设备，则表中的数字可能会更大。

例如，有一个用户 **user1**（用户**1**） 登录到了位于 **United Kingdom**（英国）的两个网关上；出现这种情况可能是因为当大量用户登录到同一地点时，Prisma Access 会自动添加网关。在这种情况下，Prisma Access 在 **Mobile Users—GlobalProtect**（移动用户—**GlobalProtect**）区域中对 **user1**（用户**1**） 仅计为一次，但在 **Current Users**（当前用户） 表格中计为两次。

- **Monitor**（监控）选项卡（**Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Service Stats**（服务统计数据） > **Mobile Users—GlobalProtect**（移动用户—**GlobalProtect**））—选择一个地区后，可能会出现全球地图中显示的 **Users**（用户） 数量可能与表格中显示的数量不同的情况。登录到多个网关或连接多个设备的用户可能会在表格中出现多次。

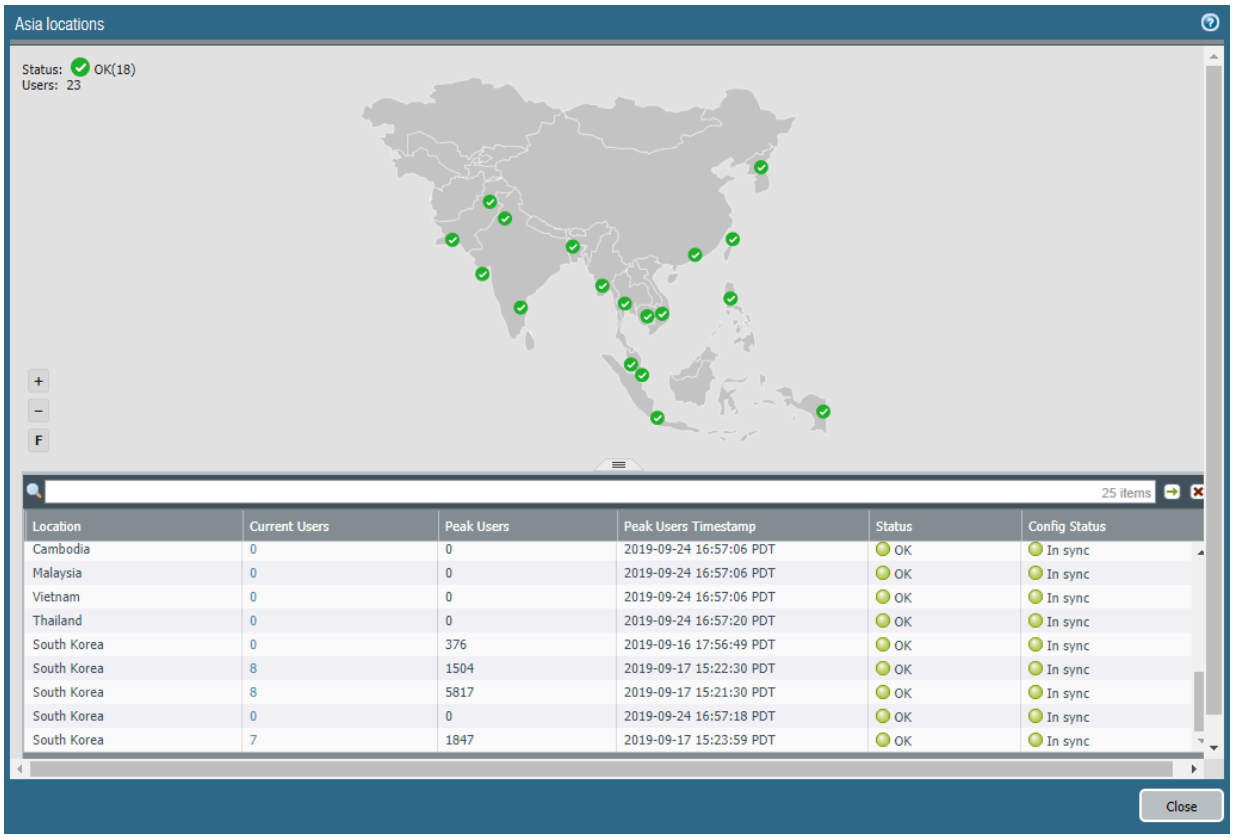
  以下屏幕截图提供了一个示例。如全球地图所示，**Asia**（亚洲）地区共有 23 位唯一用户登录。



  如果您选择 **Asia**（亚洲） 地区，Prisma Access 会在区域页面的左上角显示唯一用户的数量 (23)。但是，两个用户通过位于 **South Korea**（韩国）的多个设备（例如，智能手机和计算机）

 ©2025 Palo Alto Networks, Inc.

进行连接。由于用户有两个单独的连接，Prisma Access 在表中将它们计为两次，因此表中的总数为 25。



GlobalProtect 移动用户部署的 IP 地址池

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	• Prisma Access 许可证

©2025 Palo Alto Networks, Inc.

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	

确保您指定的IP地址池能够为组织中的移动用户提供足够的覆盖范围。请务必记住，每个唯一用户都可以使用多个设备同时连接到 Prisma Access，并且每个连接的设备都需要池中的唯一 IP 地址。该池中的地址不得与您内部使用的其他地址池重叠，也不得与在启用服务基础设施时分配的 IP 子网重叠。

我们建议池中的 IP 地址数量是将连接到 Prisma Access 的移动用户设备数量的 2 倍如果您的组织制定了自带设备 (BYOD) 策略，或者如果单个用户有多个用户帐户，请确保在分配 IP 池时考虑这些额外的设备和帐户。如果您的池空间有限，您可以指定一个较小的地址池；但是如果您的 IP 地址池达到其限制，则额外的移动用户设备将无法连接。

UI 会验证您输入有效的 IP 子网（例如，如果您输入的池的子网小于 /23，系统会提示您更改）。但并不检查您是否为您的部署分配了足够的 IP 地址。

如果您使用 *CLI* 配置位置，则此验证不可用。如果您使用 *CLI* 部署所有位置，我们建议您在全球池中为移动用户添加一个 */18* 地址。

Prisma Access 会检查您的配置，以确保您已指定以下最小 IP 地址池：

- 全球或区域地址池至少需要/23（512个IP地址）。
- 如果现有位置被转换为计算位置，则该位置最少需要 /23 子网（转换后）。
- 如果您在某个区域没有接入任何 Prisma Access 网关，则该区域不需要 IP 地址池。例如，如果您在美国东部、美国西北部和美国东北部位置指定网关，则只需为北美和南美地区指定一个 IP 地址池。相反，如果您在欧洲启用移动用户位置，而没有指定全球地址池或非洲、欧洲和中东的 IP 地址池，则您的部署将失败。
- GlobalProtect 移动用户首先消耗位置组中的 IP 地址，然后消耗特定于大区的 IP 地址，最后消耗全球 IP 地址。例如，如果您为位置组和全球指定了一个池，然后用尽了位置组池中的可用 IP 地址，则 Prisma Access 将从 **Worldwide**（全球）池中获取 IP 地址以在该位置组中使用。

  如果您指定多个 IP 地址池块，则 Prisma Access 将按照您在移动用户设置期间输入这些池的顺序来使用池。

“移动用户—GlobalProtect 部署”的静态 IP 地址分配

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	• Prisma Access 版本 5.2.1 • PAN-OS 数据平面版本 11.2.4 包含活动洞察、用户组和位置组支持 https://docs.paloaltonetworks.com/strata-cloud-manager/getting-started/activity-insights • GlobalProtect 版本 6.1.4

 ©2025 Palo Alto Networks, Inc.

在何处可以使用？	需要提供什么？
	这是一个有限供应的发布。要激活此功能，请在激活租户后联系您的*Palo Alto Networks*客户代表。

一些遗留网络使用基于IP地址的授权来限制用户对内部或外部资源的访问。Prisma Access 移动用户—GlobalProtect 部署为用户分配一个来自您在接入时分配的移动用户 IP 地址池的 IP 地址，并且此用户与 IP 地址的映射可以在后续登录中更改。为了保留用户与IP地址的映射，Prisma Access 允许您为用户分配静态IP地址。

此功能仅适用于新的 *Prisma Access* 部署。

要创建一个IP池配置文件，请使用以下一个或多个标准：

- 大区— 根据用户所在的大区分配IP地址。例如，您可以为特定大区创建一个 /30 子网。这些IP地址是该大区的静态地址。您可以通过为该大区指定的IP地址创建安全策略规则，基于大区对资源进行访问。
- 用户—通过在移动用户IP地址池中配置/30或/32地址，并使用匹配标准将该用户与IP地址关联，分配基于用户ID的IP地址。GlobalProtect 移动用户部署的 IP 地址池通过这种方式，您为特定用户分配一个静态IP地址，从而允许 Prisma Access 保持当前基于IP地址的安全策略规则，以控制用户对资源的访问。
- 用户组—根据用户组分配IP地址。如果用户属于配置的用户组，他们将从定义的IP池子网中获取IP地址。
- 一个位置组 — 根据在 IP 池配置文件中定义的位置组分配 IP 地址。

在分配静态IP地址时，请遵循以下指南：

- 如果您指定多个IP池，Prisma Access 将从上到下评估规则，并根据规则列表中的第一个匹配项分配IP地址。
- 如果您想使用用户 ID 或用户组作为匹配 IP 池的标准，请将您的部署与云身份引擎集成。Prisma Accesshttps://docs.paloaltonetworks.com/cloud-identity/cloud-identity-engine-getting-started
- 每个租户支持以下最大分配：2万用户 5000个用户组，每个用户组有5万用户 1万IP地址池配置 1万IP地址池
  -
  -
  -
  -
- 输入一个前缀长度在 /23 和 /32 之间。

 ©2025 Palo Alto Networks, Inc.

- 为您创建的每个移动用户客户端IP池配置文件：
  - 支持最多 10 个 IP 前缀。
  - 最多支持256个用户。
- 静态IP地址分配使用租约期和宽限期来指定用户与IP地址关联保持多长时间。Prisma Access租赁期是指在您分配用户到IP地址映射后，该映射有效的时间长度。
  - 默认租赁期为86400秒（24小时）。最短租赁期为3600秒（1小时）。

    最大租赁期限为7776000秒（90天）。

    宽限期是指在租赁期到期后，保留用户与IP地址映射的时间，而不将其分配给其他用户。
  - Prisma Access默认宽限期为14400秒（4小时）。

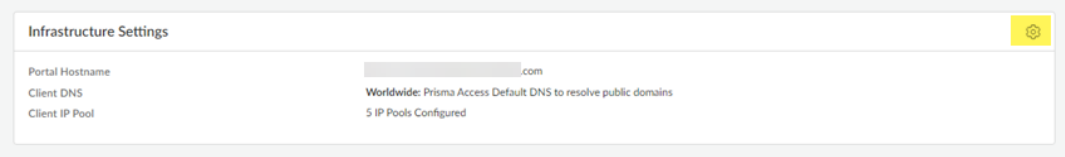
    最低宽限期为60秒。

    最大宽限期为7776000秒（90天）。

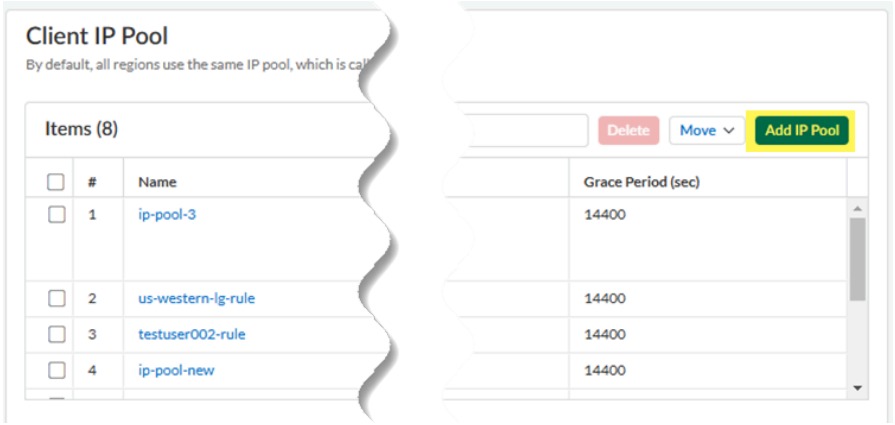
配置静态 **IP** 地址分配

要在 部署中配置静态 IP 地址分配，请完成以下步骤。

STEP 1 | 前往 Workflows Prisma Access 设置 GlobalProtect，然后单击齿轮以突出显示基础设施设置。 > >



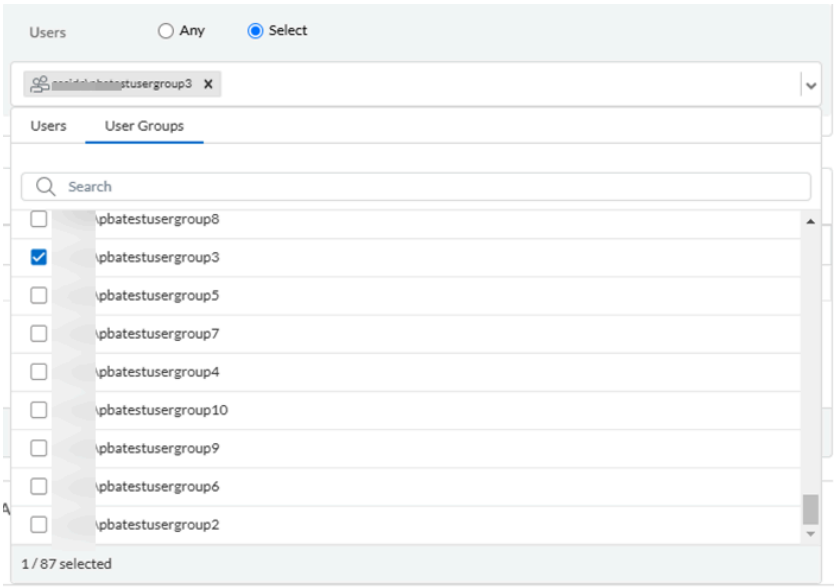
STEP 2 | 在客户端IP池区域，为静态IP地址添加IP池。



 ©2025 Palo Alto Networks, Inc.

STEP 3 | 将静态IP地址分配给大区、Prisma Access 位置组或用户。

1. 给IP地址池一个唯一的名称。
2. 选择一个或多个大区以允许在这些大区中使用该池，或选择“任何”以允许在所有大区中使用该池。
3. 选择一个或多个 Prisma Access 位置组，以允许在该位置组中使用池，或选择任何以允许在所有位置组中使用池。
4. 选择一个用户或用户组，或选择“任何”以允许该池被任何用户或用户组使用。
   - 要将一个或多个用户分配到 IP 地址池中，请在用户选项卡中选择用户。
   - 要将一个或多个用户组分配给IP地址池，请在用户组选项卡中选择用户。

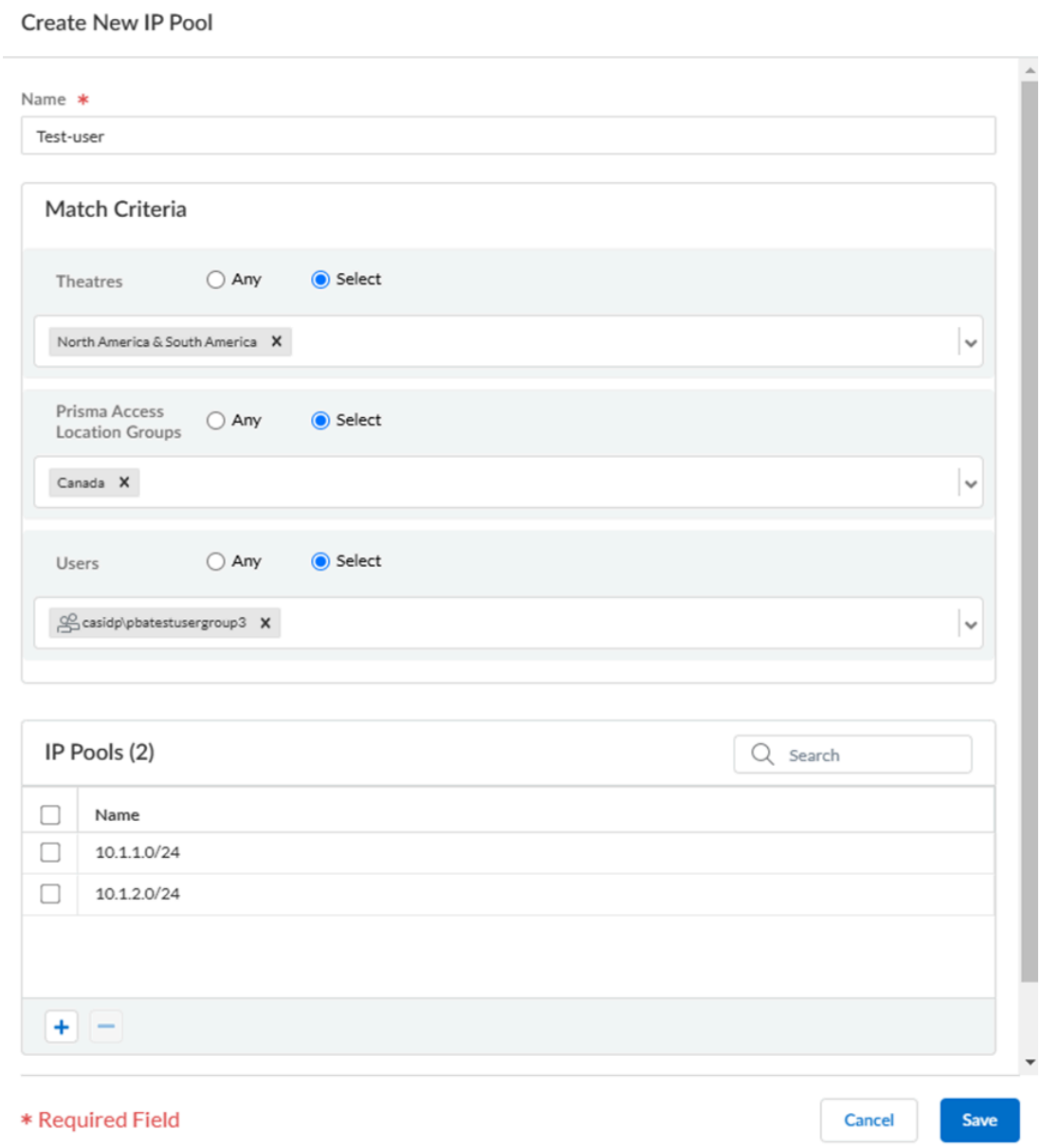


5. 在 **IP Pools**（**IP** 池）区域中，输入一个 IP 地址池。

   要将用户限制为单个*IP*地址，请指定*/30*或*/32 IP*地址；将用户分配到该地址。*Prisma Access*由于 */32* 仅提供一个 *IP* 地址，我们建议最小子网为 */30*，并将用户限制在该子网内。

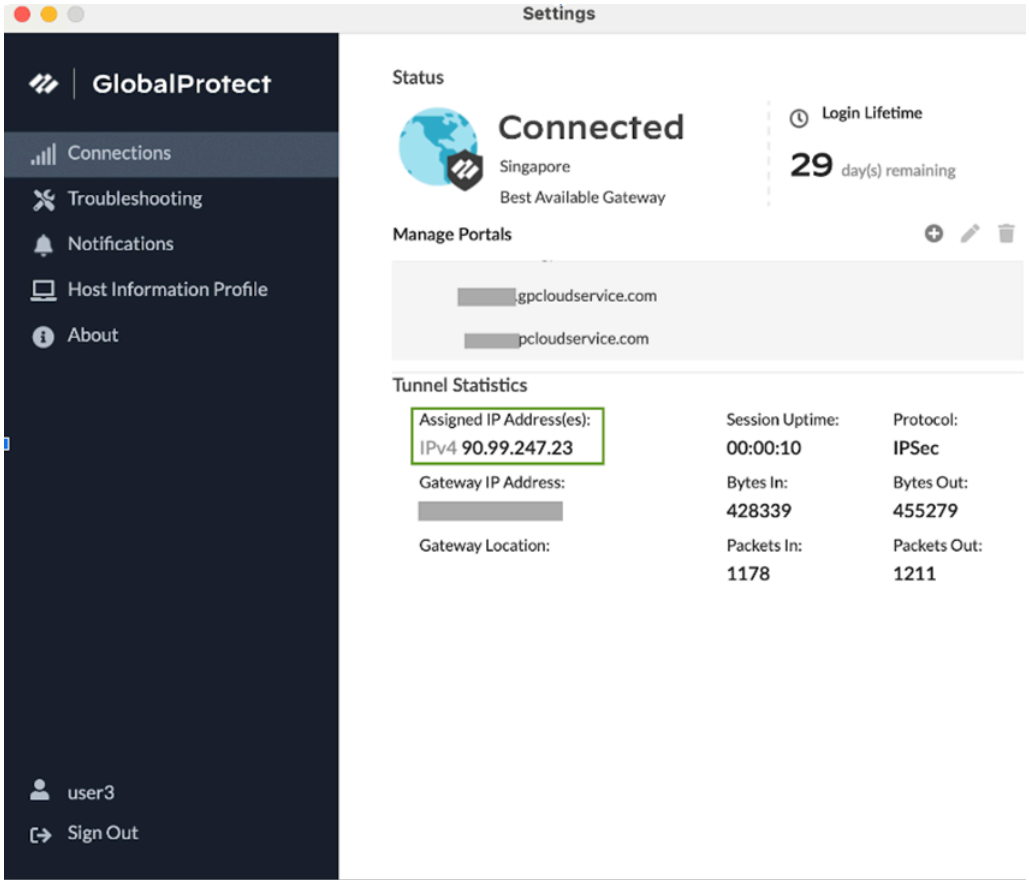
6. （可选）为用户到IP地址映射输入租赁期限和宽限期。
7. **Save**（保存）更改。

 ©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.

STEP 4 | 通过在客户端计算机上转到 GlobalProtect 设置，查看隧道统计信息，并验证分配的 IP 地址来验证您的更改。 >



GlobalProtect 应用程序如何为移动用户选择 Prisma Access 接入位置

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证

当移动用户连接到 Prisma Access 接入位置时，应用程序将使用以下选择过程来确定移动用户连接到的接入位置。

在移动用户接入过程中，可以启用希望 *Prisma Access* 覆盖的移动用户接入位置。如果在接入过程中没有选择该接入位置，则 *Prisma Access* 不会在部署中使用该接入位置。

- 如果移动用户在拥有 Prisma Access 接入位置的国家/地区进行连接，则该用户将连接到该国/地区中的位置。

©2025 Palo Alto Networks, Inc.

- 如果移动用户因任何原因无法连接到国内接入位置，Prisma Access 将根据区域，选择下列其中一个移动用户接入位置来连接用户。
  - 亚洲、澳大利亚和日本：香港、日本中部或日本南部
  - 非洲、欧洲和中东：荷兰中部
  - 北美和南美：美国西北部

  Palo Alto Networks 建议您在移动用户接入期间，在各个区域中至少启用其中一个接入位置，以提供冗余功能。如果您的移动用户要从某个没有 Prisma Access 接入位置的国家/地区连接到 Prisma Access，则必须启用先前列表中的至少一个备用接入位置。

  香港、日本中部、日本南部、荷兰中部和美国西北地区可以接受来自任何地方的客户端连接，被称为全球备用接入位置。除这些接入位置外，您还可以启用下列一个或多个兼具全球备用接入位置作用的接入位置：
  - 巴林
  - 法国北部
  - 爱尔兰
  - 南非西部
  - 韩国
- Palo Alto Networks 建议您启用多个计算接入位置，以实现冗余功能。
- 如果您将本地网关与 Prisma Access 接入位置配合使用，您可以在 Prisma Access 中指定优先级，以便让移动用户连接到特定的本地GlobalProtect网关或 Prisma Access 接入位置。有关详细信息，请参阅管理 Prisma Access 和本地网关的优先级。
- 移动用户进行连接时，即使您在接入期间于插件中选择了以下 Prisma Access 位置，GlobalProtect 应用程序在自动网关选择过程中也不会使用这些 Prisma Access 位置。然而，只要您在移动用户接入过程中允许他们手动选择这些接入，移动用户仍然可以手动选择其中一个接入位置，并将其设置为首选接入位置（网关）。
  - 澳大利亚：澳大利亚东部
  - 巴西：巴西东部和巴西中部
  - 法国：法国南部
  - 德国：德国北部和德国南部
  - 印度：印度南部
  - 墨西哥：墨西哥西部
  - 荷兰：荷兰南部
  - 巴基斯坦：巴基斯坦西部
  - 俄罗斯：俄罗斯西北部
  - 西班牙：西班牙东部

  可能必须将 ***Connect Method***（连接方法）更改为 ***On-Demand***（按需），才能让移动用户手动连接到网关。

 ©2025 Palo Alto Networks, Inc.

允许列出 GlobalProtect 移动用户

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证 ❑ Minimum Required Prisma Access Version：3.0 首选

了解如何为现有移动用户启用出口 IP 允许列表。

为了使您能够将 GlobalProtect—移动用户部署的公共（出口）IP 地址添加到您在组织内使用的任何 SaaS 应用程序允许列表中，Prisma Access 会提供 IP 地址并让您验证是否已将它们添加到允许列表中，然后您才能在您的环境中使用这些 IP 地址。如果您为现有 Prisma Access 部署启用出口 IP 允许列表，Prisma Access 会将已为您的位置分配的所有出口 IP 地址迁移到出口 IP 允许列表中。对于新的 Prisma 部署，请在载入 Global Protect 移动用户时启用出口 IP 允许列表。

将出口 IP 地址添加到组织的允许列表后，您将返回到 Prisma Access UI，确认 GlobalProtect 出口 IP 地址已列入允许列表，然后 **Push**（推送）您的更改。然后，Prisma Access 会释放这些出口 IP 地址并将其添加到您的部署中。如果 Prisma Access 由于自动缩放事件在初始配置后添加了更多 IP 地址，您需要确认新的出口 IP 地址已添加，然后 Prisma Access 才会将这些 IP 地址添加到您的部署中。

启用后，“出口 IP 允许列表”表将提供已确认或尚未确认的 IP 地址及其配置状态的相关信息。

- Strata Cloud Manager
- Panorama

允许列出 GlobalProtect 移动用户 (Strata Cloud Manager)

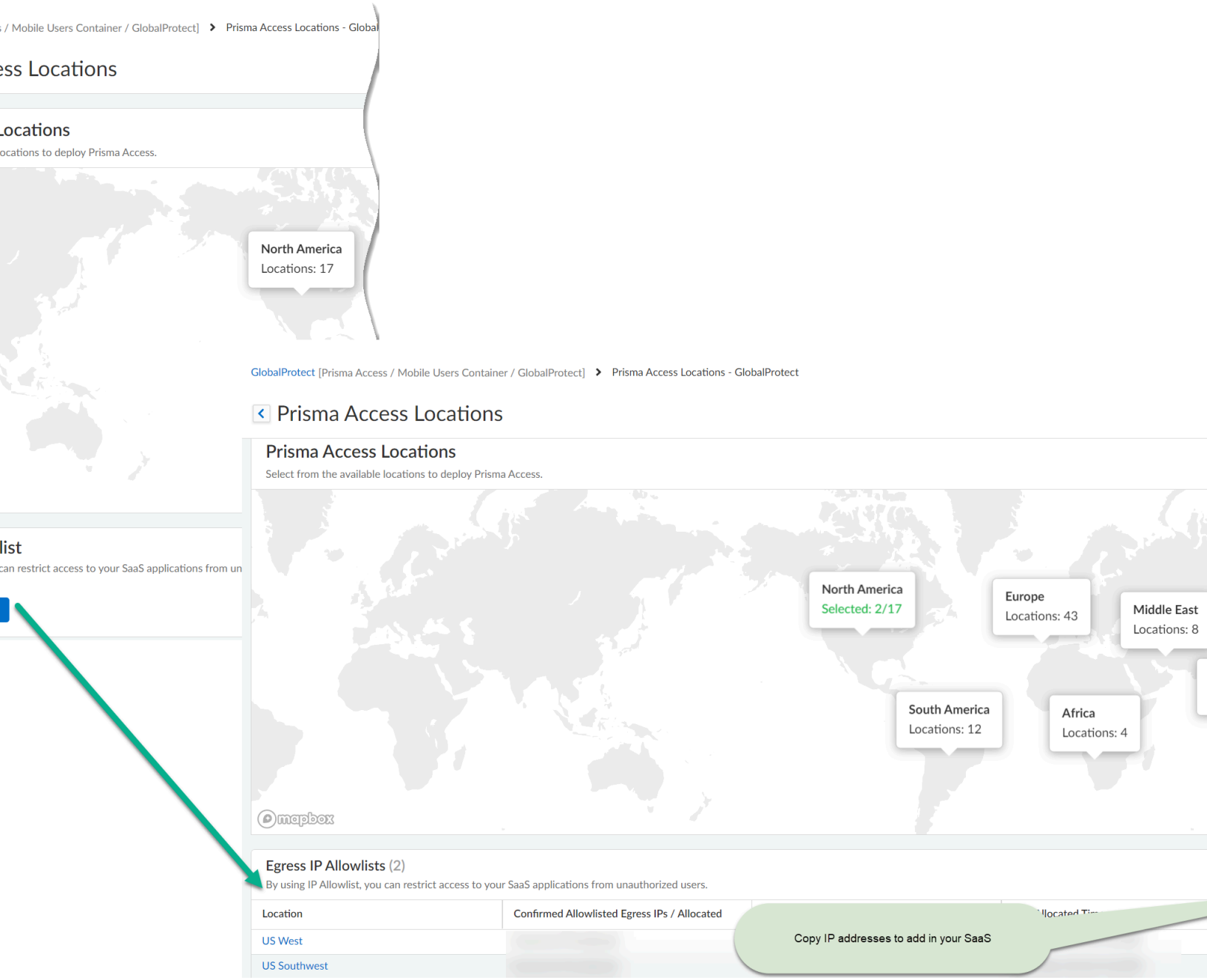
启用 Prisma Access 以显示 Prisma Access 流量的出口 IP 地址。在 SaaS 应用程序的 IP 允许列表中使用这些 IP 地址，以便仅限授权用户或来源使用。

STEP 1 | 转到 **Workflows**（工作流） > **Prisma Access** 设置 > **GlobalProtect** > **Infrastructure**（基础架构），然后编辑 **Prisma Access** 位置设置。

 ©2025 Palo Alto Networks, Inc.

STEP 2 | 显示 Prisma Access 位置的 IP 地址。

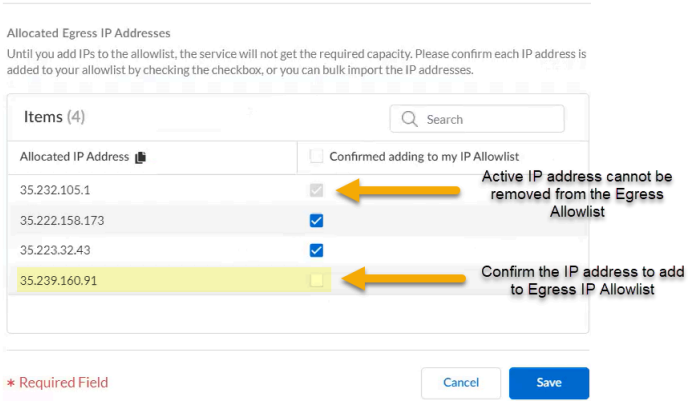
1. 启用出口 IP 允许列表，以显示加入的 Prisma Access 位置的 IP 地址。
2. 复制分配的 IP 地址并将其添加到 SaaS 应用程序的允许列表中。
3. 选择 **Migrate**（迁移）以确认分配给 Prisma Access 中加入位置的 IP 地址。



 ©2025 Palo Alto Networks, Inc.

STEP 3 | 针对新加入的位置或在自动缩放事件期间检索 IP 地址。

1. 选择 **Location**（位置）名称以查找分配给该位置的新出口 IP 地址。
2. 选择 **Confirmed adding to my IP Allowlist**（确认添加到我的 **IP** 允许列表中），以便在 Prisma Access 中确认这些 IP 地址之前将其添加到 SaaS 应用程序的允许列表中。



如果您有 IPv6 地址，请选择 **Confirmed adding to my IPv6 Allowlist**（确认添加到我的 **IPv6** 允许列表中）。



STEP 4 | 将更改推送到 Prisma Access。

分配的出口 **IP** 地址的状态

出口 IP 允许列表中的状态列指示是否为您的部署配置了分配到这些位置的所有 IP 地址。继续阅读以了解每种状态。

已配置 — 您已将出口 IP 地址添加到 SaaS 应用程序的允许列表中，在 Prisma Access 中确认了这些 IP 地址，并推送更改以使其完全配置。

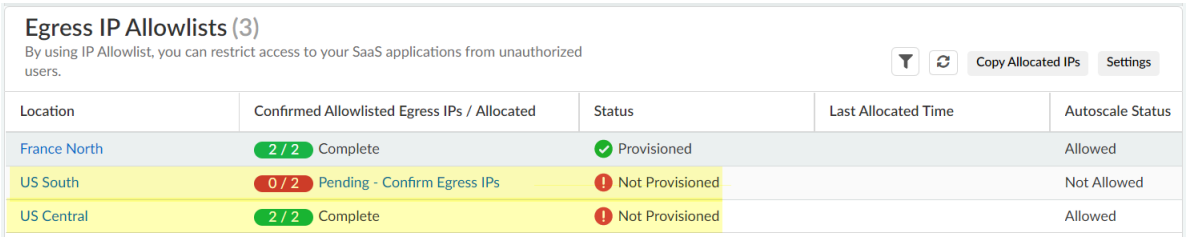
已部分配置 — 您已添加第一组出口 IP 地址，在 Prisma Access 中确认了这些 IP 地址并推送了您的更改。但是，Prisma Access 在自动缩放事件期间添加了另一组 IP 地址，并且未在 Prisma Access 中确认这些 IP 地址。

未配置 — Prisma Access 已为该位置分配了 IP 地址，并且您已将出口 IP 地址添加到 SaaS 应用程序的允许列表中并在 Prisma Access 中确认了这些 IP 地址，但您尚未加入此位置。

无法配置 — 您已加入此位置，但尚未在 Prisma Access 中确认并推送更改。

“出口 IP 允许列表”表还指示在 Prisma Access 中已确认和尚未确认的 IP 地址数量。例如，1/2 表示，分配给该位置的 2 个 IP 地址中有 1 个已在 Prisma Access 中得到确认。

©2025 Palo Alto Networks, Inc.



允许列出 GlobalProtect 移动用户 (Panorama)

为了使您能够将 GlobalProtect—移动用户部署的公共（出口）IP 地址添加到您在组织内使用的任何 SaaS 应用程序允许列表中，Prisma Access 会提供 IP 地址并让您验证是否已将它们添加到允许列表中，然后您才能在您的环境中使用这些 IP 地址。

这种出口 IP 地址分配方法具有以下优点：

- 它确保 Prisma Access 仅配置您列入允许列表的 IP 地址。
- 它可以防止移动用户尝试从组织网络阻止的 IP 地址连接到 Prisma Access。直到您确认将 IP 地址列入允许列表后，Prisma Access 才会将 IP 地址发布到您的部署。
- 它提供了一种无需使用 API 即可检索当前出口 IP 地址的方法。

Prisma Access 在以下情况下分配出口 IP 地址：

- 当您在移动用户登录期间加入您的位置时。

  Prisma Access 为您加入的每个位置分配两个网关 IP 地址。

  如果您加入某个位置，并且同一计算地点中的其他位置正在经历自动缩放事件，则 *Prisma Access* 可能会为新位置分配两个以上的 *IP* 地址。在这种情况下，请确保将所有这些 *IP* 地址添加到允许列表中，并确认所有地址 ***Added to My Allow List***（已添加到我的允许列表中）。

©2025 Palo Alto Networks, Inc.

- 大型缩放事件期间。

  如果移动用户数量超出了两个预分配 IP 地址的容量，则 Prisma Access 会另外分配一组 IP 地址（包含两个 IP 地址）。

  自动缩放事件会影响计算地点中加入的所有位置。当某个位置发生自动缩放事件并且您尚未确认将这些地址添加到允许列表中时，该计算地点中的所有位置都将显示 **Not Allowed**（不允许）的 **Autoscale Status**（自动缩放状态）。

  Autoscale Status（自动缩放状态）显示 *Prisma Access* 中的自动缩放状态。

  - ***Allowed***（允许）— 您已将 *IP* 地址添加到允许列表中。如果大量移动用户登录到单个位置并触发自动缩放事件，*Prisma Access* 会将允许列表中的 *IP* 地址用于自动缩放事件。
  - ***Not Allowed***（不允许）— 您尚未在 *Prisma Access UI* 中指定将所有 *IP* 地址添加到允许列表中，或者在将更改标记为“已添加”后尚未提交并推送更改。即使 *Prisma Access* 触发自动缩放事件，*Prisma Access* 也不会配置更多 *IP* 地址来增加该位置的容量。

    每次添加位置时，或者每次 *Prisma Access* 由于自动缩放事件而添加 *IP* 地址时，您都需要刷新包含 ***Egress IP Allow List***（出口 *IP* 允许列表）表的页面，指定 ***Added to My Allow List***（已添加到我的允许列表中）以将 *IP* 地址标记为已添加到组织的允许列表，然后 ***Commit and Push***（提交并推送）更改。

  要随时了解 *Prisma Access* 因自动缩放事件而添加的任何 *IP* 地址，您可以设置一个 *URL*，*Prisma Access* 将通过该 *URL* 通知您 *IP* 地址的更改。

  您无需启用此功能；您可以选择是否让 Prisma Access 释放 IP 地址，直至您确认已在 UI 中将这些 IP 地址列入允许列表。

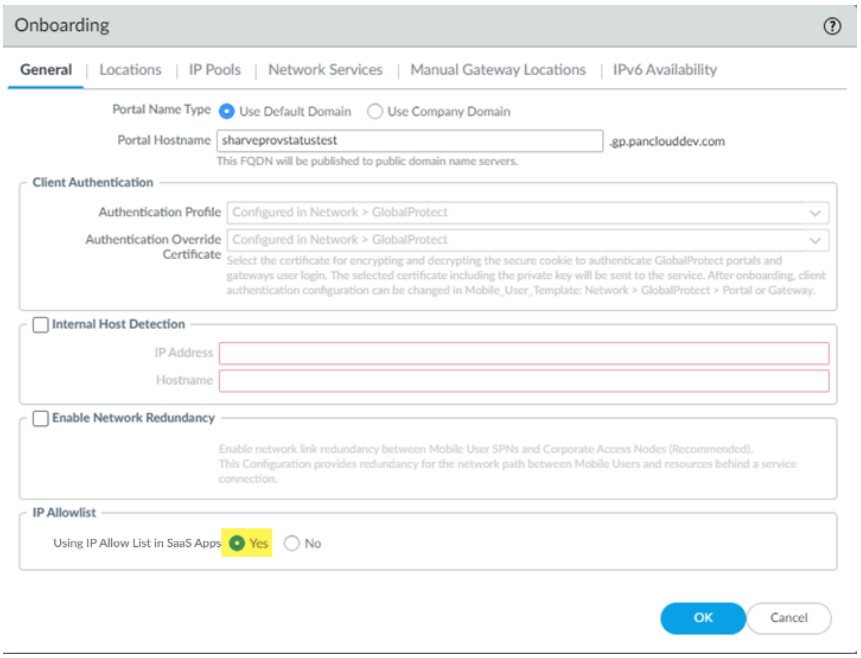
  为了防止在允许列表中添加公共（出口）GlobalProtect IP 地址之前 Prisma Access 将这些地址配置到您的部署，在移动用户 — GlobalProtect 登录期间，在 **Using IP Allow List in SaaS Apps**（在 **SaaS** 应用程序中使用 **IP** 允许列表）设置中指定 **Yes**（是）。通过完成以下任务确认您已在 Prisma Access UI 中添加这些 IP 地址。

STEP 1 | 选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Mobile Users**—**GlobalProtect**（移动用户 — **GlobalProtect**）。

STEP 2 | 选择您的 **Hostname**（主机名）并对其进行 **Configure**（配置）（适用于现有部署），或首次 **Configure**（配置）您的部署（适用于新部署）。

 ©2025 Palo Alto Networks, Inc.

STEP 3 | 将 **Using IP Allow List in SaaS Apps**（在 **SaaS** 应用程序中使用 **IP** 允许列表）指定为 **Yes**（是）。



STEP 4 | 继续您的 Prisma Access 登录过程，包括选择要在移动用户 — GlobalProtect 部署中使用的位置，然后 **Commit and Push**（提交并推送）更改。

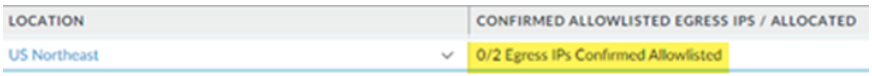
这些更改可能需要一分钟时间才能反映在 UI 中。如果您在提交并推送更改之前查看 **Egress IP Allow List**（出口 **IP** 允许列表），它会显示 **0/0 Egress IPs Confirmed Allow Listed**（**0/0** 个出口 **IP** 已确认列入允许列表）的状态，因为 Prisma Access 尚未为您的部署分配任何出口 IP 地址。

©2025 Palo Alto Networks, Inc.

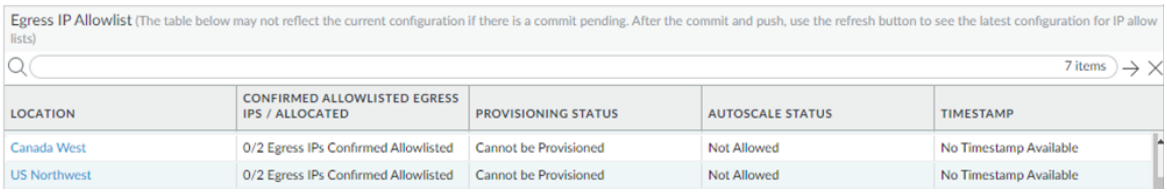
STEP 5 | 查看 **Egress IP Allow List**（出口 **IP** 允许列表）表，并记下需要添加到允许列表中的出口 IP 地址。

您可以在 **Egress IP Allow List**（出口 **IP** 允许列表）表的 **Confirmed Allow Listed Egress IPs / Allocated**（已确认列入允许列表的出口 **IP**/已分配）字段中查看出口 IP 地址。第一个数字表示 IP 地址是否已确认添加到您的允许列表中。

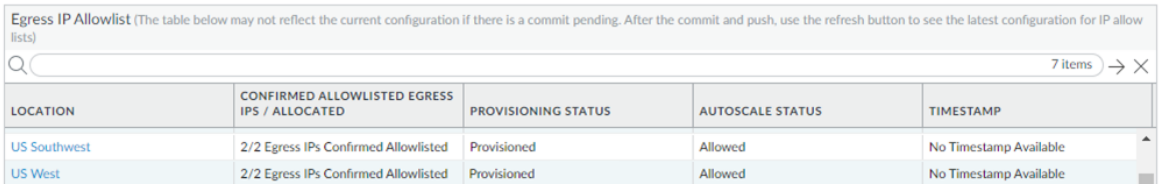
以下示例显示了美国东北部位置的 IP 地址。`0/2 Egress IPs Confirmed Allow Listed`（`0/2` 个出口 `IP` 已确认列入允许列表）的描述表示两个出口 IP 地址中的 0 个 IP 地址已被标记为添加到您的允许列表中，您需要添加这些 IP 地址。



如果您有新的 Prisma Access 部署，或者如果您添加了位置或发生了自动缩放事件，则该表显示没有任何出口 IP 地址添加到组织的允许列表中。

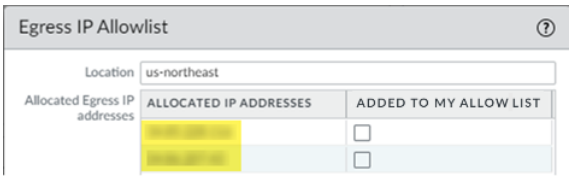


如果您有现有的 Prisma Access 部署，则该表显示 **Provisioned**（已配置）的 **Provisioning Status**（配置状态）以及 **Allowed**（允许）的 **Autoscale Status**（自动缩放状态），这表明 Prisma Access 将出口 IP 地址标记为已添加。



Prisma Access 将为每个新添加的位置分配两个地址。如果现有位置之前在大量移动用户同时登录到单个位置时发生过自动缩放事件，则 Prisma Access 会以 2 的倍数分配额外的出口 IP 地址，现有位置可能有四个或更多地址。

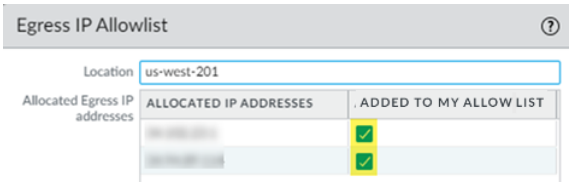
STEP 6 | 通过选择表中的 **Location**（位置）名称，找到需要添加到组织允许列表中的新出口 IP 地址。



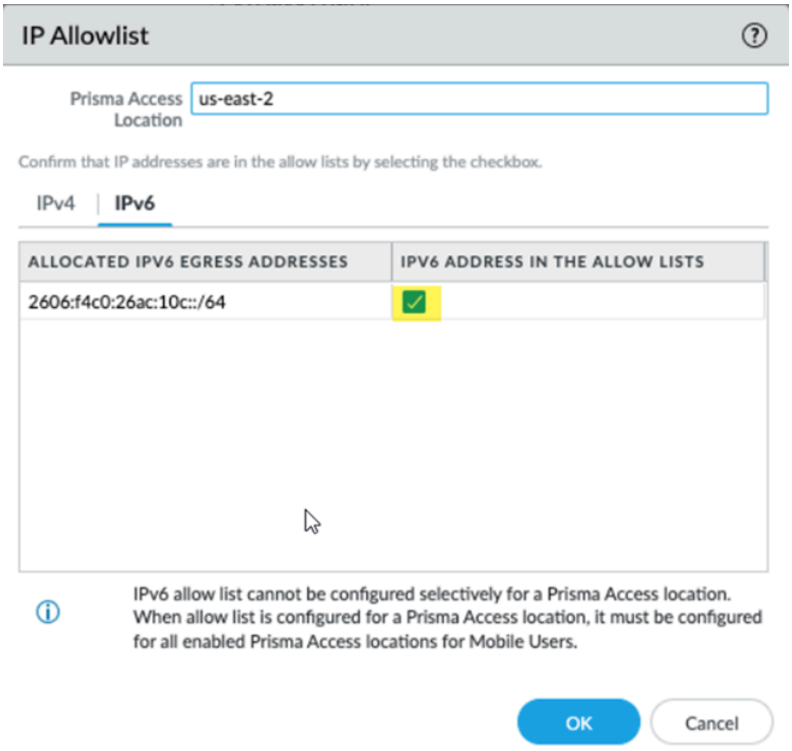
STEP 7 | 将这些出口 IP 地址添加到组织的允许列表中。

 ©2025 Palo Alto Networks, Inc.

STEP 8 | 将出口 IP 地址列入允许列表后，返回出口 IP 区域，并通过选择 **Added to My Allow List**（已添加到我的允许列表中）表明您已将这些 IP 地址添加到允许列表中。

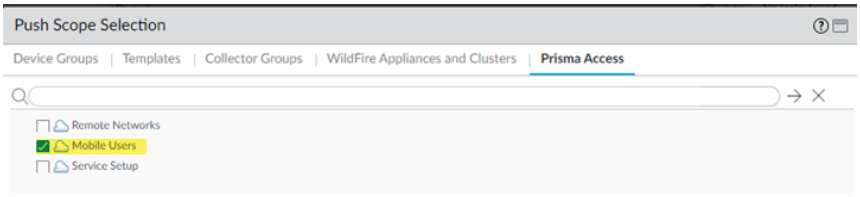


如果您有 IPv6 地址，请选择 **IPv6 Address in the Allow Lists**（允许列表中的 **IPv6** 地址）。



STEP 9 | 提交并推送您的更改，使其在 Prisma Access 中处于活动状态。

1. 选择 **Commit**（提交） > **Commit and Push**（提交并推送）和推送范围中的 **Edit Selections**（编辑选择）。
2. 选择 **Prisma Access**，然后确保选择了 **Mobile Users**（移动用户）。

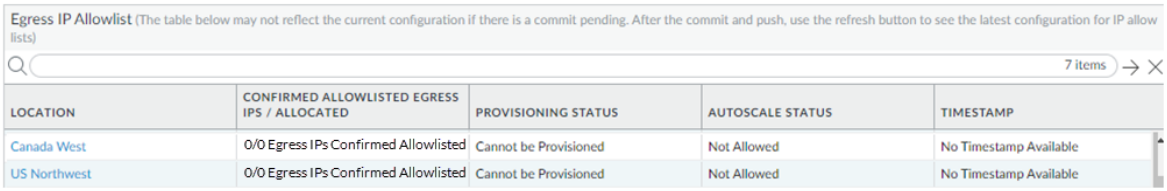


3. 单击 **OK**（确定）保存对推送范围所作的更改。
4. **Commit**（提交）并 **Push**（推送）更改。

如果您在提交并推送更改之前查看 **Egress IP Allow List**（出口 **IP** 允许列表）表，“已确认”列会显示 **0/0 Egress IPs Confirmed Allow Listed**（**0/0** 个出口 **IP** 已确认列入允许列表）的状态，

 ©2025 Palo Alto Networks, Inc.

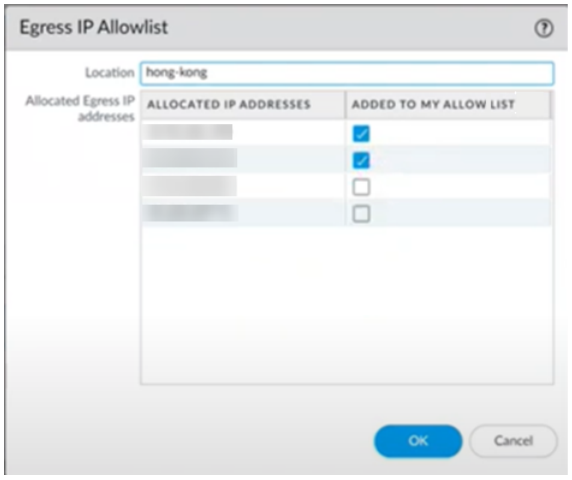
因为在您 **Commit and Push**（提交并推送）之前 Prisma Access 尚未为您的部署分配任何出口 IP 地址。



Egress IP Allow List（出口 **IP** 允许列表）表包含以下附加字段：

字段	说明
地点	已加入的移动用户位置。
已确认列入允许列表的出口 **IP /**已分配	已确认列入允许列表的出口 IP 地址的数量，以及已分配的出口 IP 地址的数量。
配置状态	出口 IP 地址的允许列出状态。 • **Provisioned**（已配置）— 您已将出口 IP 地址添加到组织的允许列表中，通过选中 **Added to My Allow List**（已添加到我的允许列表中）确认已将这些 IP 地址添加到 Prisma Access UI 中，并且已提交并推送更改以使其完全配置。 • **Not Provisioned**（未配置）— Prisma Access 已为该位置分配 IP 地址，并且您已将出口 IP 地址添加到组织的允许列表中并确认在 Prisma Access UI 中添加了这些 IP 地址，但您尚未加入此位置。 • **Cannot Be Provisioned**（无法配置）— 您已加入此位置，但尚未选中 **Added to My Allow List**（已添加到我的允许列表中）并提交和推送更改。 在 Prisma Access 中指定已将这些出口 IP 添加到组织的允许列表并且 **Commit and Push**（提交并推送）更改之前，Prisma Access 不会向您的部署配置这些 IP 地址。 • **Provisioned with partial capacity**（已配置部分容量）— 您已添加第一组出口 IP 地址，确认已将这些 IP 地址添加到 Prisma Access UI 中，并且已提交和推送更改。但是，Prisma Access 在自动缩放事件期间添加了另一组 IP

©2025 Palo Alto Networks, Inc.

字段	说明
	地址，并且尚未指定将这些 IP 地址添加到 Prisma Access UI 中的允许列表。 以下屏幕截图显示了标记为 **Provisioned with partial capacity**（已配置部分容量）的部署的示例。两个 IP 地址已标记为 **Added to My Allow List**（已添加到我的允许列表中）；但是，Prisma Access 已将另外两个 IP 地址添加到此位置，并且这些位置尚未添加到 UI 中。 
自动缩放状态	显示 Prisma Access 中自动缩放的状态。 • **Allowed**（允许）— 您已将 IP 地址添加到允许列表中。如果大量移动用户登录到单个位置并触发自动缩放事件，Prisma Access 会将允许列表中的 IP 地址用于自动缩放事件。 • **Not Allowed**（不允许）— 您尚未在 Prisma Access UI 中指定将所有 IP 地址添加到允许列表中，或者在将更改标记为“已添加”后尚未提交并推送更改。即使 Prisma Access 触发自动缩放事件，Prisma Access 也不会配置更多 IP 地址来增加该位置的容量。 每次添加位置时，或者每次 Prisma Access 由于自动缩放事件而添加 IP 地址时，您都需要刷新包含 **Egress IP Allow List**（出口 IP 允许列表）表的页面，指定 **Added to My Allow List**（已添加到我的允许列表中）以将 IP 地址标记为已添加到组织的允许列表，然后 **Commit and Push**（提交并推送）更改。

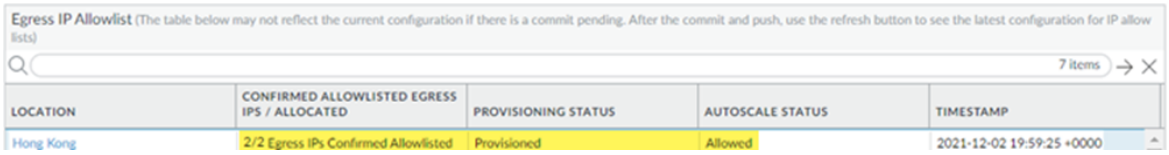
 ©2025 Palo Alto Networks, Inc.

字段	说明
	要随时了解 *Prisma Access* 因自动缩放事件而添加的任何 *IP* 地址，您可以设置一个 *URL*，*Prisma Access* 将通过该 *URL* 通知您 *IP* 地址的更改。
时间戳	以协调世界时 (UTC) 为此地区分配 IP 的最后已知时间。

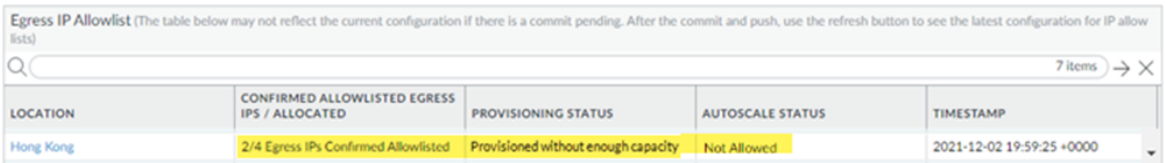
Commit and Push（提交并推送）后，“已确认”列将显示 **0/2 Egress IPs Confirmed Allow Listed**（**0/2** 个出口 **IP** 已确认列入允许列表）的状态，因为您尚未确认在 Prisma Access UI 中将这些 IP 地址列入允许列表。

当您加入移动用户位置时，Prisma Access 会为您提供两个出口 IP 地址 — 一个活动 IP 地址和一个用于自动缩放事件的地址。以下提供了 Prisma Access 在自动缩放事件后如何分配和配置出口 IP 地址的示例。

自动缩放事件 — 如果大量移动用户同时登录到某个移动用户位置，该事件可能会导致 Prisma Access 分配另外两个出口 IP 地址来容纳大量用户。在将前两个出口 IP 地址列入允许列表后，自动缩放事件之前的状态显示这两个出口 IP 地址已列入允许列表，其确认状态为 **2/2 Egress IPs Confirmed Allow Listed**（**2/2** 个出口 **IP** 已确认列入允许列表），配置状态为 **Provisioned**（已配置），自动缩放状态为 **Allowed**（允许），如以下屏幕截图中的香港位置所示。

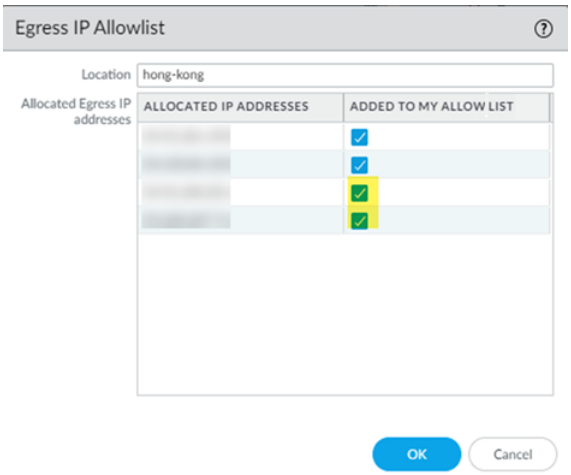


如果大量移动用户同时登录到香港位置，Prisma Access 会将备用出口 IP 地址设为活动状态，并分配另外两个 IP 地址，将其中一个 IP 地址设为活动状态。发生自动缩放事件时，出口 IP 地址已分配但尚未配置，确认状态为 **2/4 Egress IPs Confirmed Allow Listed**（**2/4** 个出口 **IP** 已确认列入允许列表），配置状态显示 **Provisioned without enough capacity**（已配置但容量不足）。此外，自动缩放状态显示 **Not Allowed**（不允许），这意味着如果发生自动缩放事件，Prisma Access 将不会为您的部署配置额外的出口 IP 地址。

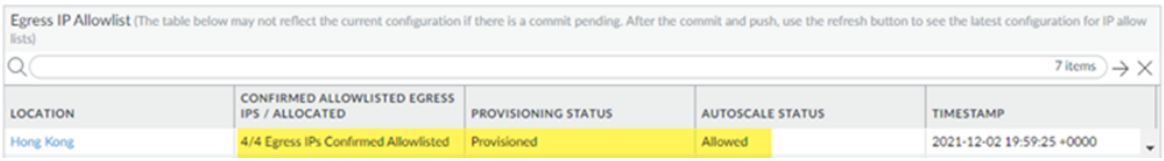


将新的出口 IP 地址添加到允许列表后，选择位置名称；然后，为添加的两个 IP 地址选择 **Added to My Allow List**（已添加到我的允许列表中），然后 **Commit and Push**（提交并推送）更改。

 ©2025 Palo Alto Networks, Inc.



完成后，香港位置显示所有四个出口 IP 地址均已确认和配置，并且自动缩放处于活动状态。



GlobalProtect 应用程序升级

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证

Prisma Access 托管组织中 macOS 和 Windows 用户可从 Prisma Access 门户下载的 GlobalProtect 应用版本。Prisma Access 提供了多个版本的 GlobalProtect 应用，并且您可以选择将其中一个版本设为活动版本。您还可以管理移动用户对 GlobalProtect 应用的访问，或执行分阶段升级。

- 选择适用于 Prisma Access 的活动 GlobalProtect 应用程序版本
- 允许用户升级 GlobalProtect 应用程序
- 错开GlobalProtect应用程序更新

选择适用于 Prisma Access 的活动 GlobalProtect 应用程序版本

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证

 ©2025 Palo Alto Networks, Inc.

Prisma Access 在您的组织中管理 Windows 和 macOS 用户的 GlobalProtect 应用程序版本。Prisma Access 虽然托管了多个 GlobalProtect 应用程序版本，但只有一个托管版本是活动的。当移动用户登录 Prisma Access 门户时，活动版本是可供移动用户下载和安装在他们的 Windows 和 macOS 设备上的版本。

您可以在多租户部署中选择多个 GlobalProtect 版本。您应用的 GlobalProtect 应用程序版本设置是按租户设置的，而不是全局设置；您可以按租户控制应用程序版本。

某些功能要求用户使用足够新的 GlobalProtect 版本，例如 IP 优化。继续阅读以了解在 Prisma Access 中如何选择活动的 GlobalProtect 应用程序版本。

- Strata Cloud Manager
- Panorama

选择适用于 **Prisma Access (Managed by Strata Cloud Manager)** 的活动 **GlobalProtect** 应用程序版本

完成以下步骤，您可以从服务设置页面将当前活动版本替换为另一个托管版本。

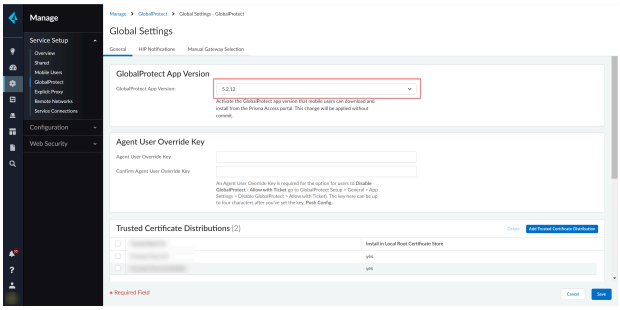
STEP 1 | 选择 **Workflows**（工作流） > **Prisma Access** 设置 > **Mobile Users**（移动用户），然后找到 **GlobalProtect Connection**（**GlobalProtect** 连接）面板。

STEP 2 | 如果尚未启用 GlobalProtect，请选择 **GlobalProtect Setup**（**GlobalProtect** 设置）或 **Enable**（启用） > **GlobalProtect Setup**（**GlobalProtect** 设置）。

STEP 3 | 选择 **GlobalProtect App**（**GlobalProtect** 应用程序）选项卡，然后编辑 **Global App Settings**（全局应用程序设置）。

STEP 4 | 在 **Global Settings**（全局设置）页面的 **General**（常规）选项卡上，选择您希望允许移动用户从 Prisma Access 门户网站下载和安装的 **GlobalProtect App Version**（**GlobalProtect** 应用程序版本）。

下拉列表中指明了活动版本。



选择适用于 **Prisma Access (Managed by Panorama)** 的活动 **GlobalProtect** 应用程序版本

如果您当前使用的版本已过期，Prisma Access 会通知您并请求您激活支持的版本。

完成以下步骤，您可以从服务设置页面将当前活动版本替换为另一个托管版本。

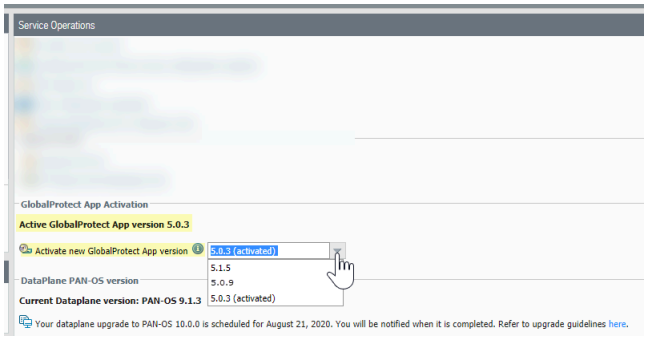
如果您正在 FedRAMP 环境中使用 *Prisma Access*，则必须使用 *FIPS* 认证版本的 *GlobalProtect*，即 *5.1.4* 版本。如果您从 5.1.4 更改默认的 GlobalProtect 版本，则无法从 *Panorama UI* 中选择版本 *5.1.4*，并且必须向 *Palo Alto Networks* 技术支持部门提交支持案例才能将其添加回来。

 ©2025 Palo Alto Networks, Inc.

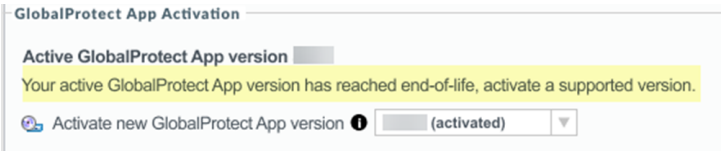
STEP 1 | 在 Panorama 中，选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Service Setup**（服务设置）。

STEP 2 | 选择 **Activate new GlobalProtect App version**（激活新版本的 **GlobalProtect** 应用程序）。

下拉列表中指明了活动版本。



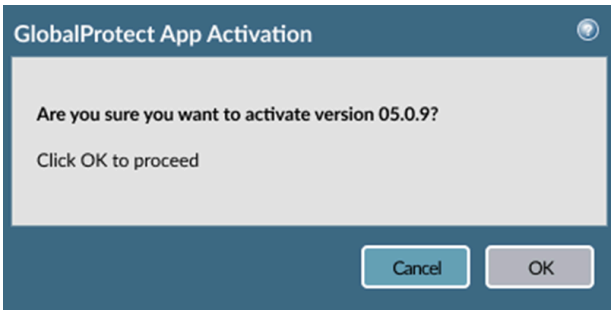
如果您当前的 *GlobalProtect* 版本已过期 *(EoL)*，服务设置页面的此区域将显示一条消息；如果您收到此消息，请继续下一步以升级您的 *GlobalProtect* 应用程序版本。



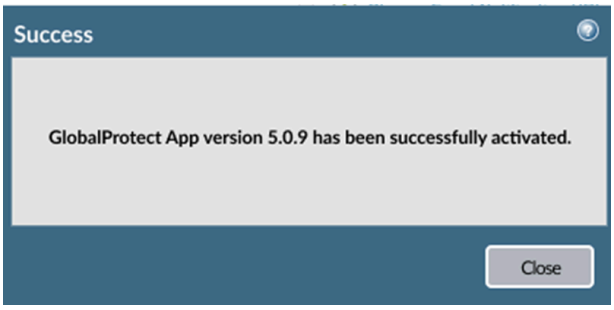
 ©2025 Palo Alto Networks, Inc.

STEP 3 | 选择需要升级到的版本并单击 **OK**（确定）。

此时将显示一个窗口来验证您的选择。



应用程序激活后，您会收到一条成功消息。



STEP 4 | 查看系统状态页面以验证 **Active GlobalProtect App version**（活动的 **GlobalProtect** 应用程序版本）。

允许用户升级 GlobalProtect 应用程序

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证

了解如何控制移动用户对适用于 Prisma Access GlobalProtect 部署的 GlobalProtect 应用程序版本的访问。

- Strata Cloud Manager
- Panorama

允许用户升级 GlobalProtect 应用程序 (Strata Cloud Manager)

您可以管理移动用户对 Prisma Access 托管的活动 GlobalProtect 应用程序版本的访问。要在 Prisma Access (Managed by Strata Cloud Manager) 中执行此操作，请配置 **Upgrade Global Protect**（升级 **Global Protect**）设置。对于 Prisma Access (Managed by Strata Cloud Manager)，请完成以下步骤。

STEP 1 | 选择 **Workflows**（工作流） > **Prisma Access** 设置 > **Mobile Users**（移动用户），然后找到 **GlobalProtect Connection**（**GlobalProtect** 连接）面板。

©2025 Palo Alto Networks, Inc.

STEP 2 | 如果尚未启用 GlobalProtect，请选择 **GlobalProtect Setup**（**GlobalProtect** 设置）或 **Enable**（启用） > **GlobalProtect Setup**（**GlobalProtect** 设置）。

STEP 3 | 选择 **GlobalProtect App**（**GlobalProtect** 应用程序）选项卡，然后选择 **Add App Settings**（添加应用程序设置）。

STEP 4 | 在 **App Configuration**（应用程序配置）区域中，在 **Upgrade GlobalProtect App**（升级 **GlobalProtect** 应用程序）中选择一个选项，以指定移动用户是否可以将其 GlobalProtect 应用程序版本升级到 Prisma Access 上托管的活动版本，如果可以升级，他们是否可以选择何时升级：

- **Allow when user accepts the upgrade Prompt**（当用户接受升级提示时允许）（默认）— 当新版本激活时提示用户，并且允许用户在方便时升级其软件。
- **Disallow**（不允许）— 防止用户升级应用程序软件。
- **Allow Manually**（手动允许）— 允许用户通过选择 GlobalProtect 应用程序中的 **Check Version**（检查版本）来手动检查并启动升级。
- **Allow Transparently**（透明允许）— 只要门户上有可用的新版本，便自动升级应用程序软件。
- **Allow when the user is in the corporate network**（当用户在公司网络中时允许）— 每当门户上有新版本可用时，自动升级应用程序软件，但需要等到端点在内部连接到公司网络。这可以防止由低带宽连接升级引起的延迟。

允许用户升级 **GlobalProtect** 应用程序 **(Panorama)**

您可以管理移动用户对 Prisma Access 托管的活动 GlobalProtect 应用程序版本的访问。要在 Prisma Access (Managed by Strata Cloud Manager) 中执行此操作，请配置 **Upgrade Global Protect**（升级 **Global Protect**）设置。对于 Prisma Access (Managed by Panorama)，请完成以下步骤。

STEP 1 | 选择 **Network**（网络） > **GlobalProtect** > **Portals**（门户）。

STEP 2 | 从 **Template**（模板）下拉列表中选择 **Mobile_User_Template** 模板。

STEP 3 | 选择 **GlobalProtect_Portal** 以编辑 Prisma Access 门户配置。

STEP 4 | 选择 **Agent**（代理）选项卡，并选择应用程序配置。

STEP 5 | 选择 **App**（应用）选项卡。

STEP 6 | 在 **App Configuration**（应用程序配置）区域中，在 **Allow User to Upgrade GlobalProtect App**（允许用户升级 **GlobalProtect** 应用程序）中选择一个选项，以指定移动用户是否可以将其 GlobalProtect 应用程序版本升级到 Prisma Access 上托管的活动版本，如果可以升级，他们是否可以选择何时升级：

- **Allow with Prompt**（提示时允许）（默认）— 当新版本激活时，系统会提示用户，并允许用户在方便时升级其软件。
- **Disallow**（不允许）— 防止用户升级应用程序软件。
- **Allow Manually**（手动允许）— 允许用户通过选择 GlobalProtect 应用程序中的 **Check Version**（检查版本）来手动检查并启动升级。

 ©2025 Palo Alto Networks, Inc.

- **Allow Transparently**（透明允许）— 只要门户上有可用的新版本，便自动升级应用程序软件。
- **Internal**（内部）— 当门户上有新版本可用时自动升级应用程序软件，但需要等到端点在内部连接到公司网络。这可以防止由低带宽连接升级引起的延迟。

错开GlobalProtect应用程序更新

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	• Prisma Access 许可证

如果您管理一个大型组织，您可能希望分阶段将移动用户更新到最新版本的GlobalProtect应用程序。例如，您可以在向组织中的每个人推出更新之前，分配一个较小的组来更新其GlobalProtect应用程序。为此，请完成以下任务。

STEP 1 | 如果您尚未创建用户组，请为要向其推出 GlobalProtect 应用程序更新的第一组用户创建用户组。

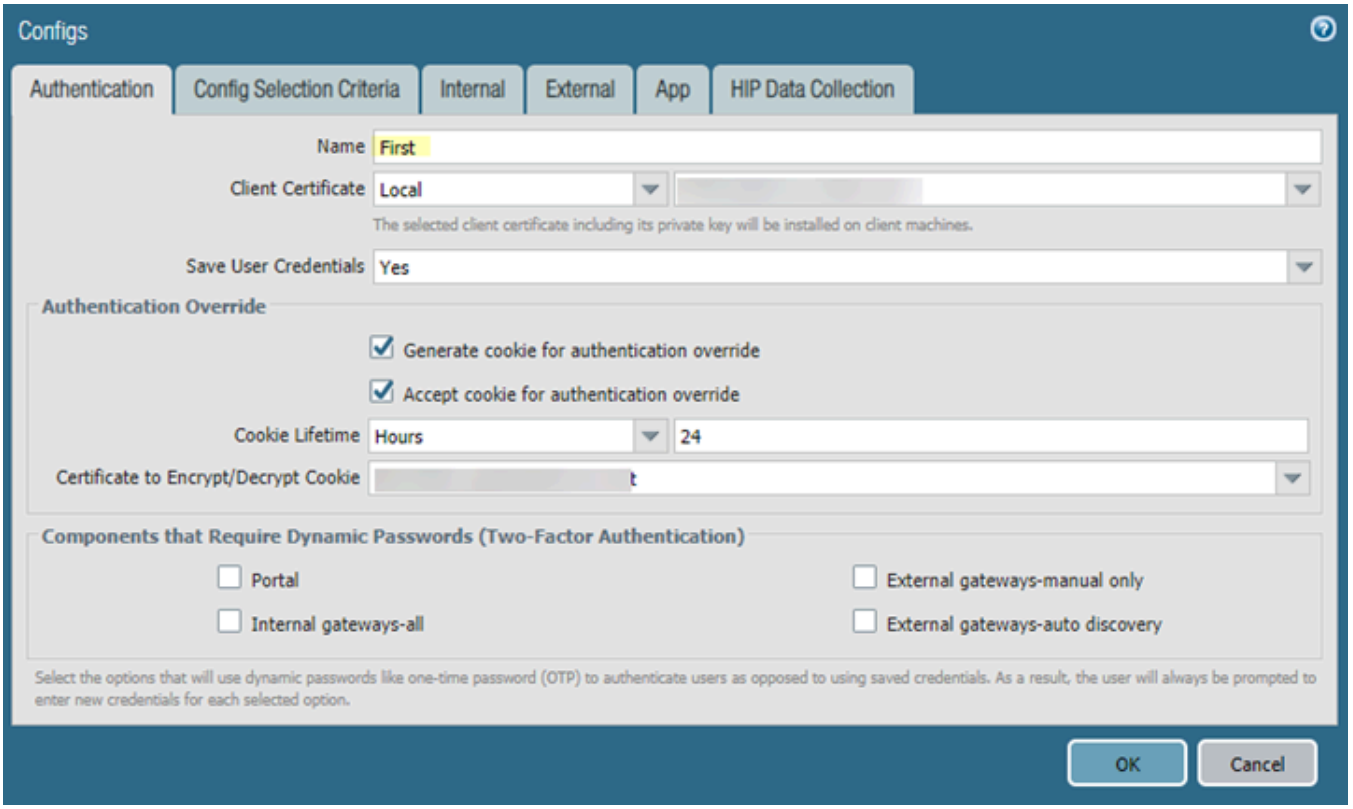
可以使用User-ID将用户映射到组，或选择设备本地用户数据库用户组手动创建组。https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/user-id/map-users-to-groups > >

 ©2025 Palo Alto Networks, Inc.

STEP 2 | 创建新的GlobalProtect代理配置以供第一组用户使用。https://docs.paloaltonetworks.com/globalprotect/10-1/globalprotect-admin/globalprotect-portals/define-the-globalprotect-client-authentication-configurations/define-the-globalprotect-app-configurations

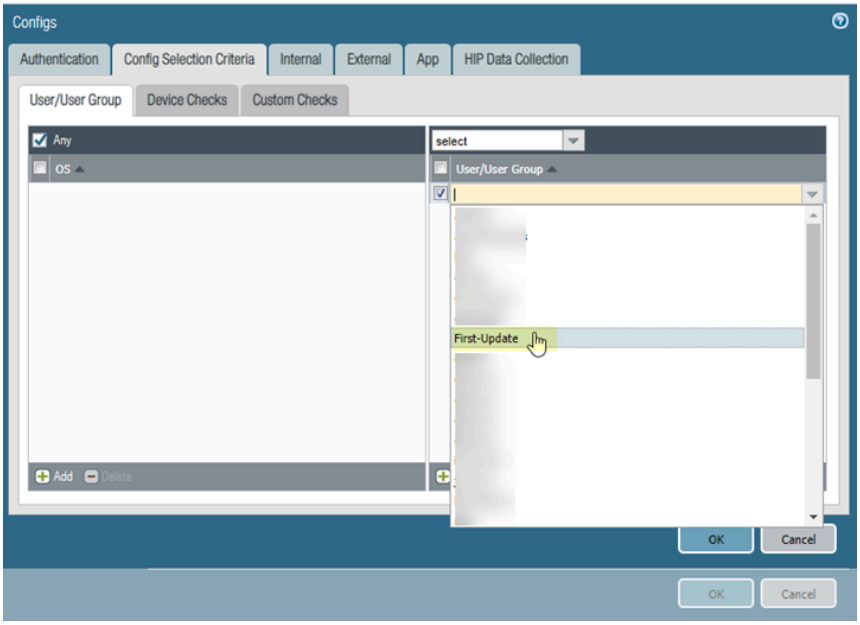
1. 在 Panorama 中，选择 **Network**（网络） > **GlobalProtect** > **Portals**（门户）。
2. 从 **Template**（模板）下拉列表中选择 **Mobile_User_Template** 模板。
3. 选择 **GlobalProtect_Portal** 以编辑 Prisma Access 门户配置。
4. 选择 **Agent**（代理）选项卡。
5. 选择DEFAULT配置并克隆它。

   您也可以添加新配置;但克隆现有配置会复制新配置所需的信息。
6. 输入该配置的 **Name**（名称）。



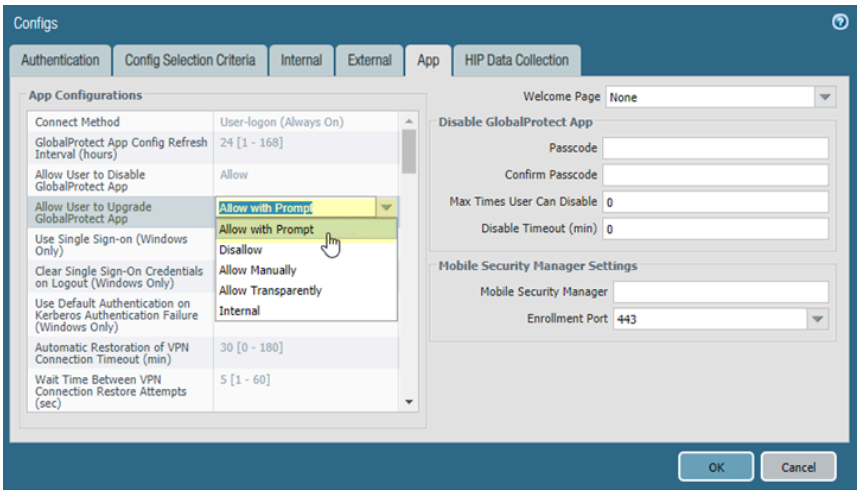
7. 选择 **Config Selection Criteria**（配置选择条件）选项卡。
8. 在“用户/用户组”区域中，选择在步骤中创建的用户。1

 ©2025 Palo Alto Networks, Inc.



9. 选择 **App**（应用）选项卡。
10. 将“允许用户升级GlobalProtect应用程序”更改为“允许并提示”或“允许并不提示”。

    当激活新版本时，“允许并提示”会提示用户，并允许他们在方便时升级其软件;“允许并提示”会在门户网站上出现新版本时自动升级应用程序软件。

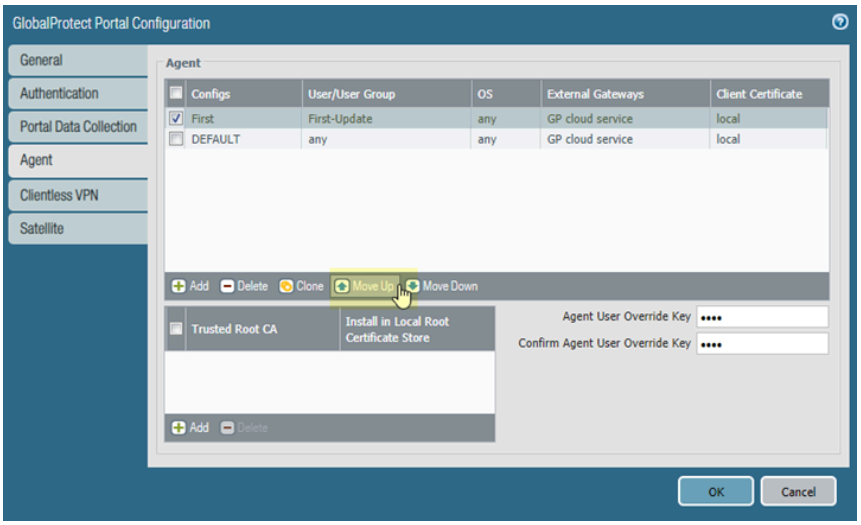


11. 单击 **OK**（确定）保存更改。

 ©2025 Palo Alto Networks, Inc.

STEP 3 | 选择“上移”可将您的配置移到默认配置之上。

应用进行连接时，门户会将数据包中的源信息与已定义的代理配置进行比较。与安全规则评估相同，门户从列表的顶部开始查找匹配项。在其找到匹配项后，会将对应的配置提交给应用程序。



STEP 4 | 对DEFAULT配置重复这些步骤，但将“允许用户升级GlobalProtect应用程序”更改为“不允许”，以防止用户更新到最新的GlobalProtect应用程序软件。

STEP 5 | 当您希望让其他用户更新其应用程序时，请将“默认”配置中的“允许用户升级GlobalProtect应用程序”更改为允许该选项（“允许并提示”或“允许并不提示”）。

将 Prisma 访问与本地 GlobalProtect 网关集成

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager)	• Prisma Access 许可证

利用 Prisma Access，您能够将 Palo Alto Networks 安全平台扩展到您的远程网络位置以及移动用户，无需构建您自己的全球安全基础设施，也无需扩展您的运营能力。如果您已经在具备基础设施管理功能的区域中部署了 GlobalProtect 网关，您可以通过配置 Prisma Access，以便在适当的时候将移动用户引导至您现有的外部网关，从而充分利用这项（已有的）投入。

您可以管理 Prisma Access 网关和本地网关的优先级，这样便可以为本地网关和 Prisma Access 网关指定优先级。管理员无法规定移动用户必须连接到哪个特定 Prisma Access 网关。但管理员可以允许移动用户使用 GlobalProtect 应用程序手动选择特定的 Prisma Access 网关。

不能将自己的门户与 *Prisma Access* 一起使用。只能使用在为移动用户配置 *Prisma Access* 时部署的门户。

- Strata Cloud Manager

 ©2025 Palo Alto Networks, Inc.

- Panorama

将 Prisma Access 与本地 GlobalProtect 网关集成 (Prisma Access (Managed by Strata Cloud Manager))

 ©2025 Palo Alto Networks, Inc.

STEP 1 | 将您的本地网关添加到代理配置中的网关列表。

1. 转到 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **GlobalProtect**，然后选择 **GlobalProtect App**（**GlobalProtect** 应用程序）。
2. 添加应用程序设置。



3. 添加外部网关。



如果您添加新的代理配置，并且希望将 *Prisma Access* 网关添加到该配置的外部网关列表中，则必须将 ***Name***（名称）设置为 ***GP cloud service***（***GP*** 云服务），将 ***Address***（地址）设置为 ***gpcloudservice.com***。完全按照显示的内容输入这些值，并且不能将这些值中的任何一个用于非 *Prisma Access* 网关。

4. 在 **Name**（名称）中输入网关名称，在 **Address**（地址）字段中指定网关的 **FQDN** 或 **IP** 地址；该值必须与网关证书中的通用名称 (CN) 完全匹配。
5. （可选）如果您希望移动用户仅在相应区域内连接到网关，请依次选择 **Add**（添加）、**Source Region**（源区域）以添加要将网关限制到的源区域。例如，如果您在法国有一个网关，您会选择 FR（法国）。如果您在瑞典有一个网关，您会选择 (SE) 瑞典。

   这样做的一个好处是，用户届时将能够访问一个网关，通过该网关他们可以使用自己的母语来访问互联网资源。
6. （可选）在网关配置中指定优先级。

   可以将本地网关设置为更高的优先级或更低的优先级。

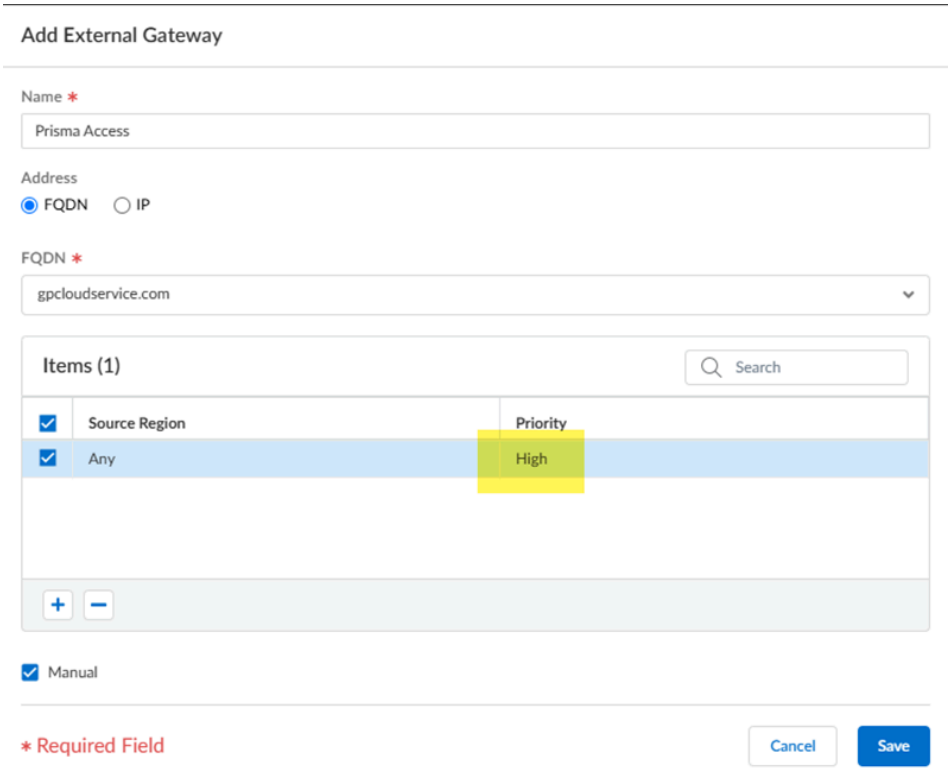
   - 要将本地网关设置为比默认 Prisma Access 网关优先级更低的级别，请将 **Priority**（优先级）设置为 **High**（高）或 **Medium**（中）。

     如果添加了更多网关，并且要为每个网关设置不同的优先级，则可以将 **Priority**（优先级）设置为 **High**（高）、**Medium**（中）、**Low**（低）或 **Lowest**（最低）。

 ©2025 Palo Alto Networks, Inc.

- 要将本地网关设置为比默认网关更高的优先级，请将 **Priority**（优先级）设置为 **Highest**（最高）。

  如果要将本地网关设置为更高的优先级，还必须编辑默认的 **Prisma Access** 网关，并将其优先级设置为低于 **Highest**（最高）的优先级。

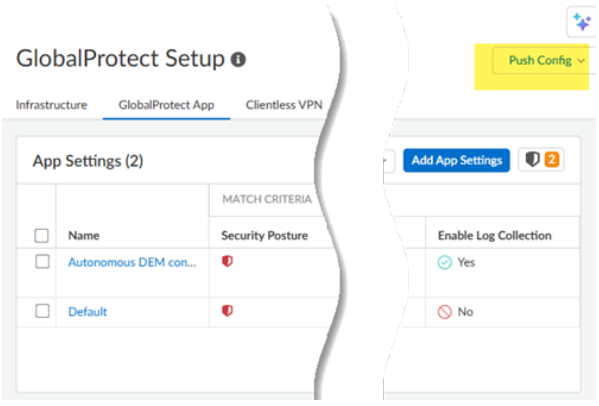


7. 选择 **Manual**（手动）。

   选中此复选框允许 GlobalProtect 用户在其 GlobalProtect 应用程序中手动选择此外部网关。

STEP 2 | **Save**（保存）更改。

STEP 3 | **Push Config**（推送配置）。



 ©2025 Palo Alto Networks, Inc.

将 Prisma Access 与本地 GlobalProtect 网关集成 (Prisma Access (Managed by Panorama))

要配置其中一个混合 Prisma Access 部署，必须编辑 Mobile_User_Template 中的 GlobalProtect_Portal 配置，以将本地网关添加到相应的区域。

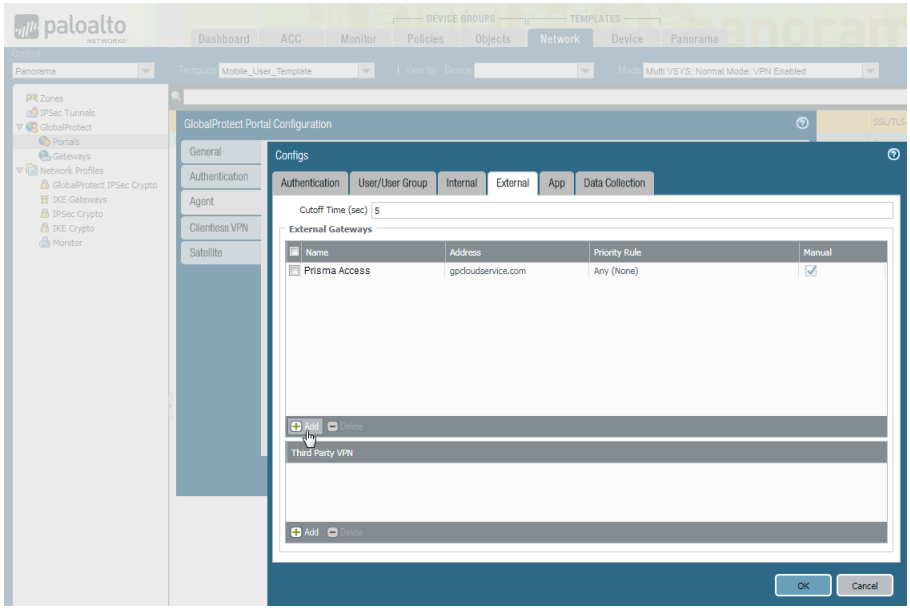
STEP 1 | 编辑 Prisma Access 门户配置。

1. 要将现有网关添加到可用网关列表中，请选择网络 **Network**（网络） > **GlobalProtect** > **Portals**（门户）
2. 从 **Template**（模板）下拉列表中选择 **Mobile_User_Template** 模板。
3. 选择 **GlobalProtect_Portal** 以编辑 Prisma Access 门户配置。

 ©2025 Palo Alto Networks, Inc.

STEP 2 | 将您的本地网关添加到代理配置中的网关列表。

1. 选择 **Agent**（代理）选项卡，然后选择 **DEFAULT**（默认）代理配置，或者选择 **Add**（添加）以添加一个新配置。
2. 选择 **External**（外部）选项卡，然后选择 **Add**（添加）以添加您的本地网关。



如果您添加新的代理配置，并且希望将 *Prisma Access* 网关添加到该配置的外部网关列表中，则必须将 ***Name***（名称）设置为 ***GP cloud service***（***GP*** 云服务），将 ***Address***（地址）设置为 ***gpcloudservice.com***。您必须完全按照显示的内容输入这些值，并且不能将这些值中的任何一个用于非 *Prisma Access* 网关。

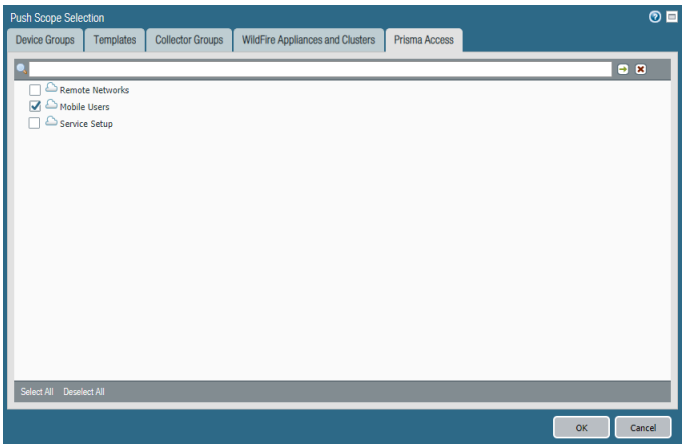
3. 在 **Name**（名称）中输入网关名称，在 **Address**（地址）字段中指定网关的 **FQDN** 或 **IP** 地址；该值必须与网关证书中的通用名称 (CN) 完全匹配。
4. （可选）如果您希望移动用户仅在相应区域内连接到网关，请依次选择 **Add**（添加）、**Source Region**（源区域）以添加要将网关限制到的源区域。例如，如果您在法国有一个网关，您会选择 FR（法国）。如果您在瑞典有一个网关，您会选择 (SE) 瑞典。

   这样做的一个好处是，用户届时将能够访问一个网关，通过该网关他们可以使用自己的母语来访问互联网资源。
5. （可选）网关的优先级。
6. 根据需要配置其他代理设置，以完成代理配置。
7. 单击确定以保存门户配置。

©2025 Palo Alto Networks, Inc.

STEP 3 | 将所有更改提交到 Panorama 并将配置更改推送到 Prisma Access。

1. 单击 **Commit**（提交） > **Commit to Panorama**（提交到 **Panorama**）。
2. 单击 **Commit**（提交） > **Push to Devices**（推送到设备），然后单击 **Edit Selections**（编辑选择）。
3. 在 **Prisma Access** 选项卡上，确保选择了 **Prisma Access for users**，然后单击 **OK**（确定）。



4. 单击 **Push**（推送）。

设置 Prisma Access 的优先级和本地网关

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	• Prisma Access 许可证

您可以选择一个物理上离您的移动用户最近的本地网关，并允许用户连接到不同的网关（无论是本地还是云）以确保移动用户在更改位置时的安全访问。您还可以为与您的移动用户位于同一国家或同一语言区域的网关指定优先级。

如果您要求用户连接到特定的 Prisma Access 网关，您可以允许移动用户手动选择特定的 Prisma Access 网关。移动用户使用安装在终端上的 GlobalProtect 应用程序选择 Prisma Access 的一个网关。

完成以下工作流程以配置 Prisma Access 中的网关优先级。

- 为本地和网关设置相等的 Prisma Access 网关优先级
- 为本地网关设置更高的网关优先级
- 为多个本地网关设置更高的优先级
- 配置 Prisma Access 优先级和本地网关

为本地和网关设置相等的 **Prisma Access** 网关优先级

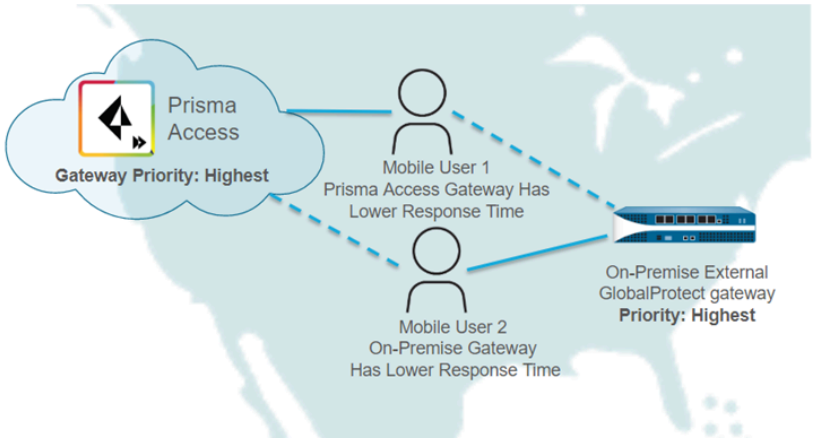
为了确保您的移动员工无论身在何处都能安全访问，您可以为本地 GlobalProtect 网关和 Prisma Access 网关设置相等的优先级。GlobalProtect 应用程序在多个网关配置中使用网关优先级来确定首选网关。

 ©2025 Palo Alto Networks, Inc.

如果您的移动用户通常更接近本地网关，则可以使用此配置。当用户更改位置时，GlobalProtect 应用程序会根据最高优先级和最低响应时间选择另一个网关（本地或 Prisma Access 网关）。

下图显示了北美两个移动用户的示例配置。Prisma Access您将网关优先级设置为最高，适用于所有网关和本地网关。

在这个例子中，用户1的GlobalProtect应用程序确定Prisma Access网关的响应时间低于本地网关，而用户2的GlobalProtect应用程序确定本地网关的响应时间较低。由于所有网关具有相同的优先级，用户1连接到 Prisma Access 网关，用户2根据较低的响应时间连接到本地网关。



为本地网关设置更高的网关优先级

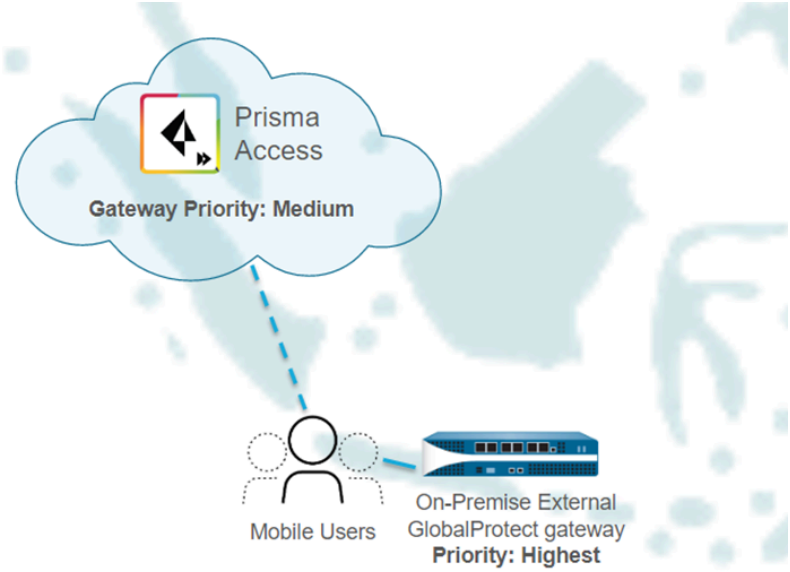
在您希望引导移动用户使用本地网关而不是 Prisma Access 网关的情况下，请指定具有源区域和比 Prisma Access 网关更高优先级的本地网关。

下图显示了印度尼西亚移动用户的示例配置。为了避免移动用户连接到新加坡最近的 Prisma Access 网关，您将印度尼西亚本地网关的优先级设置为 **Highest**（最高），并将 Prisma Access 网关的优先级设置为 **Medium**（中等）。

此示例还指定了本地网关的源区域为印度尼西亚。我们建议指定源区域，原因如下：

- 指定本地网关的源区域允许该区域的用户访问该网关，并防止该区域外的用户连接到该网关。在这个例子中，只有来自印度尼西亚的移动用户可以连接到源区域为印度尼西亚的本地网关，而更高的优先级意味着本地网关优先于其他 Prisma Access 网关。
- 如果您为印度尼西亚的本地网关设置了任何源区域，您组织中的每个移动用户都将更喜欢印度尼西亚的本地网关，因为它具有更高的优先级和全球可访问性。此配置意味着移动用户可能永远无法连接到 Prisma Access 网关。

©2025 Palo Alto Networks, Inc.



为多个本地网关设置更高的优先级

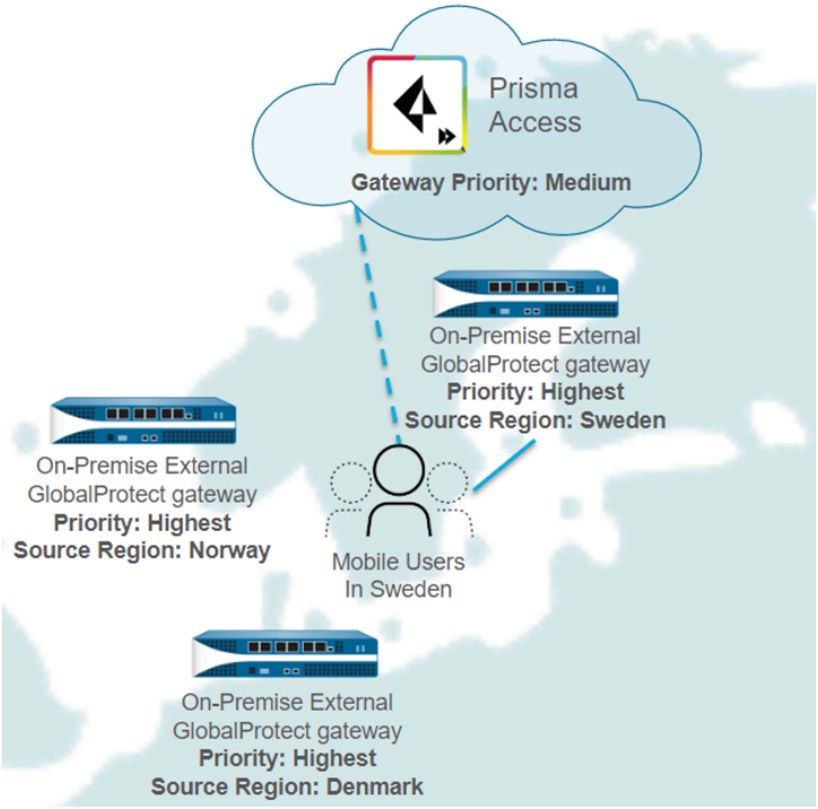
为了确保互联网流量保持在特定语言区域，您可以在多个源区域配置多个网关，将本地网关的优先级设置为最高，将网关的优先级设置为中等。Prisma Access

下图显示了斯堪的纳维亚地区移动用户的示例配置。使用此配置，当移动用户访问互联网网站时，网站使用特定于其语言的字符编码集。

在此示例中，您配置了源区域位于丹麦、挪威和瑞典的本地网关。您将这些网关的优先级设置为最高，并将其他网关的优先级设置为中等。Prisma Access指定本地网关的源区域允许该区域的用户访问这些网关，并防止该区域外的用户连接到这些网关。

在这个例子中，瑞典的移动用户使用的GlobalProtect应用程序选择了瑞典的本地网关，因为源区域和更高的网关优先级。

 ©2025 Palo Alto Networks, Inc.



配置 **Prisma Access** 优先级和本地网关

使用此工作流程配置使用本地网关的 Prisma Access 部署的优先级。

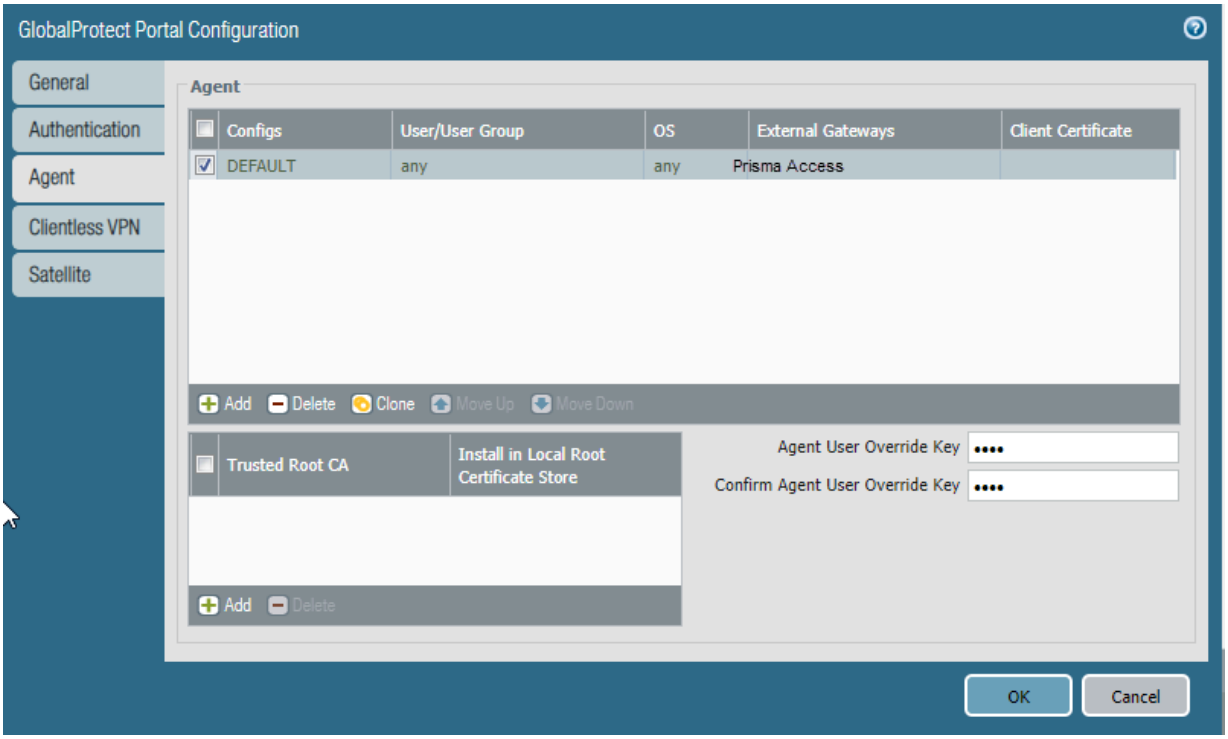
STEP 1 | 登录 Prisma Access。

STEP 2 | 在 Mobile_User_Template 模板中选择网络 GlobalProtect 门户。 > >

STEP 3 | 点击名称字段中的门户名称。

 ©2025 Palo Alto Networks, Inc.

STEP 4 | 点击代理选项卡。



STEP 5 | 单击代理的名称进行配置。

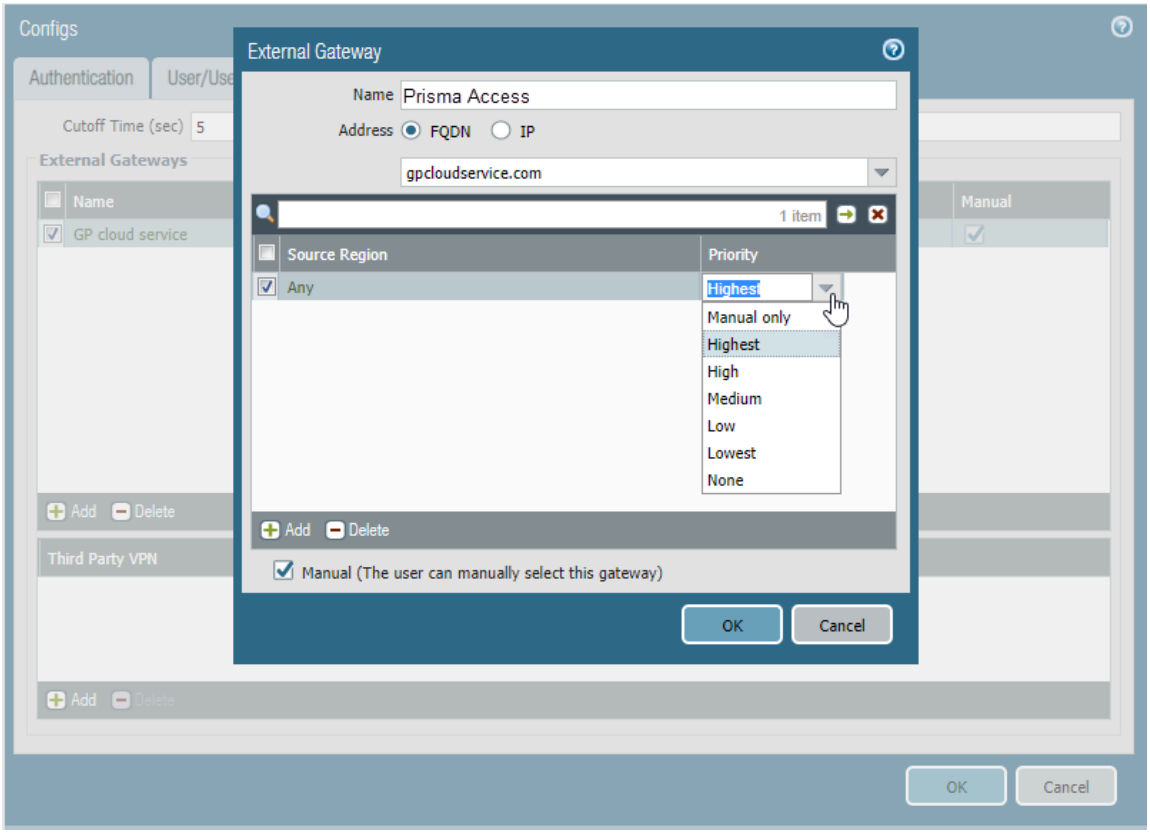
默认代理名为DEFAULT。

STEP 6 | 点击外部标签。

 ©2025 Palo Alto Networks, Inc.

STEP 7 | 设置 Prisma Access 网关的优先级。

1. 点击 **GP** 云服务。
2. 设置您首选配置的优先级。
   - 要为本地和 Prisma Access 网关设置相等的网关优先级，请将优先级从无更改为最高。
   - 要为本地网关设置更高的网关优先级或为多个本地网关设置更高的优先级，请将优先级从无更改为中。为本地网关设置更高的网关优先级为多个本地网关设置更高的优先级



3. 确保选中手动复选框。

   检查手动复选框可确保移动用户在需要时可以选择特定的 Prisma Access 网关。

   请不要为 *Prisma Access* 网关添加源区域；您指定的任何区域都不会应用于配置。

 ©2025 Palo Alto Networks, Inc.

4. 单击 **OK**（确定）。

 ©2025 Palo Alto Networks, Inc.

STEP 8 | 将一个或多个本地外部网关添加到您的配置中。

1. 为网关输入描述性 **Name**（名称）。

   此处所输入的名称应与配置网关时所定义的名称匹配，同时还应包含足够的描述性信息，以便用户了解其所连接至的网关的位置。

2. 输入在“地址”字段中配置网关的接口的 FQDN 或 IP 地址。

   您可以配置 IPv4 地址。指定的地址必须与网关服务器证书中的公用名 (CN) 完全匹配。

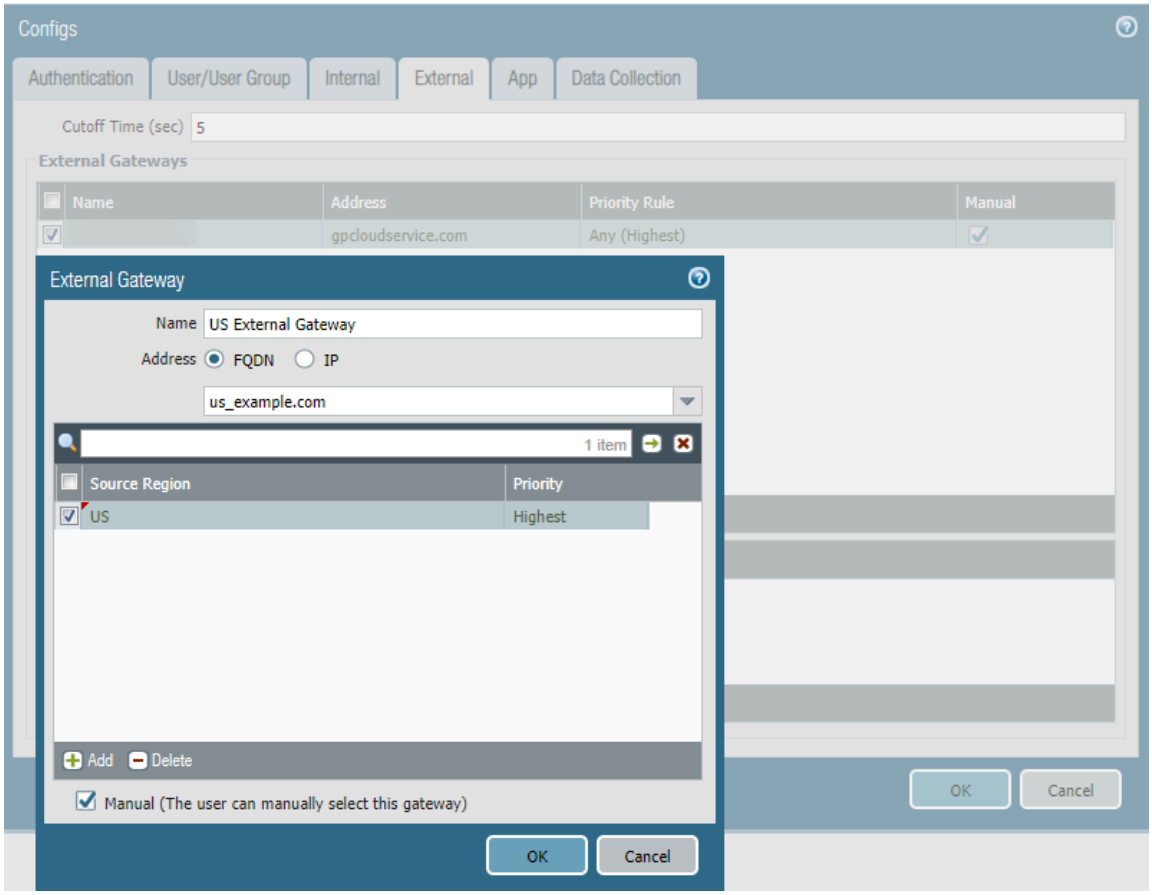
3. 为本地网关添加一个或多个 **Source Regions**（源区域），或者选择 **Any**（任何），使网关可供所有区域使用。

   如果您将本地外部网关的优先级设置得高于 *Prisma Access* 网关，我们建议您为外部网关指定源区域。如果您为区域指定任何，*GlobalProtect* 应用程序可能永远不会选择 *Prisma Access* 网关，而是会选择本地网关，因为本地网关的优先级更高。

4. 如果允许用户能手动切换至网关，则请选中 **Manual**（手动）复选框。

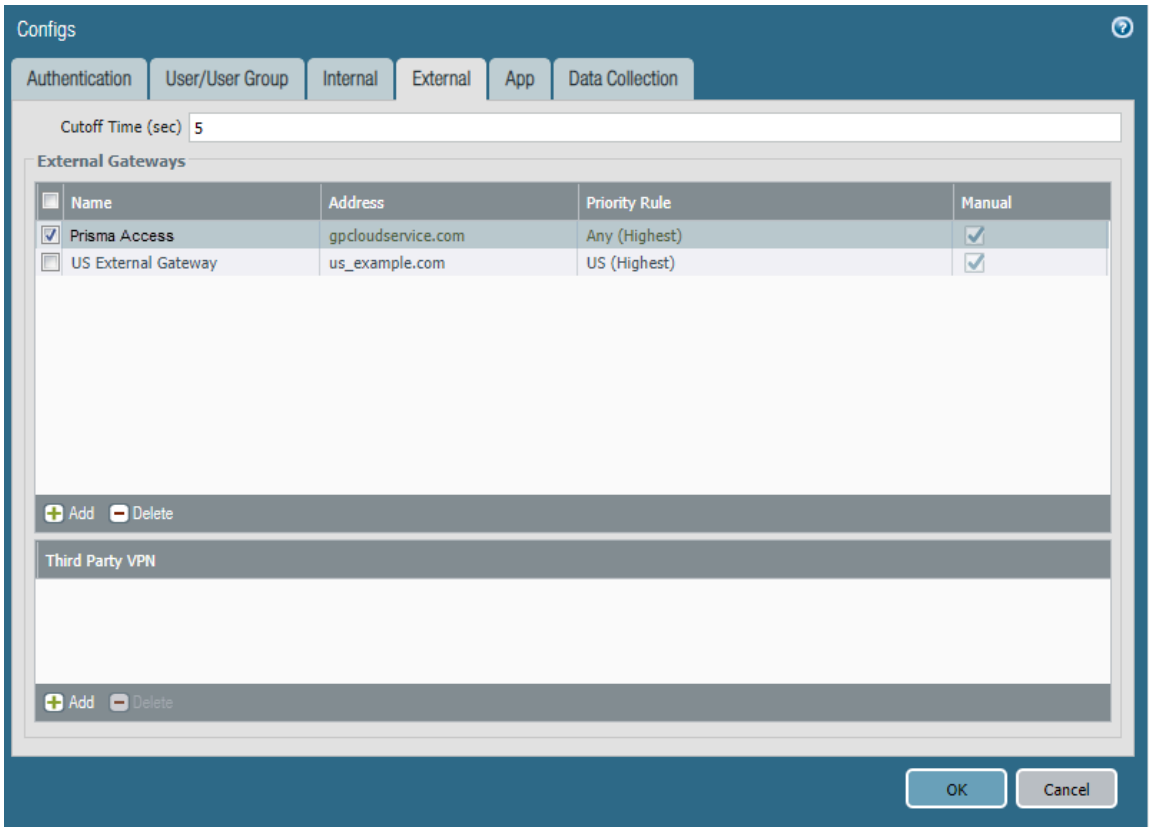
5. 将本地网关的优先级设置为最高（默认）。

 ©2025 Palo Alto Networks, Inc.



6. 单击 **OK**（确定）。

©2025 Palo Alto Networks, Inc.



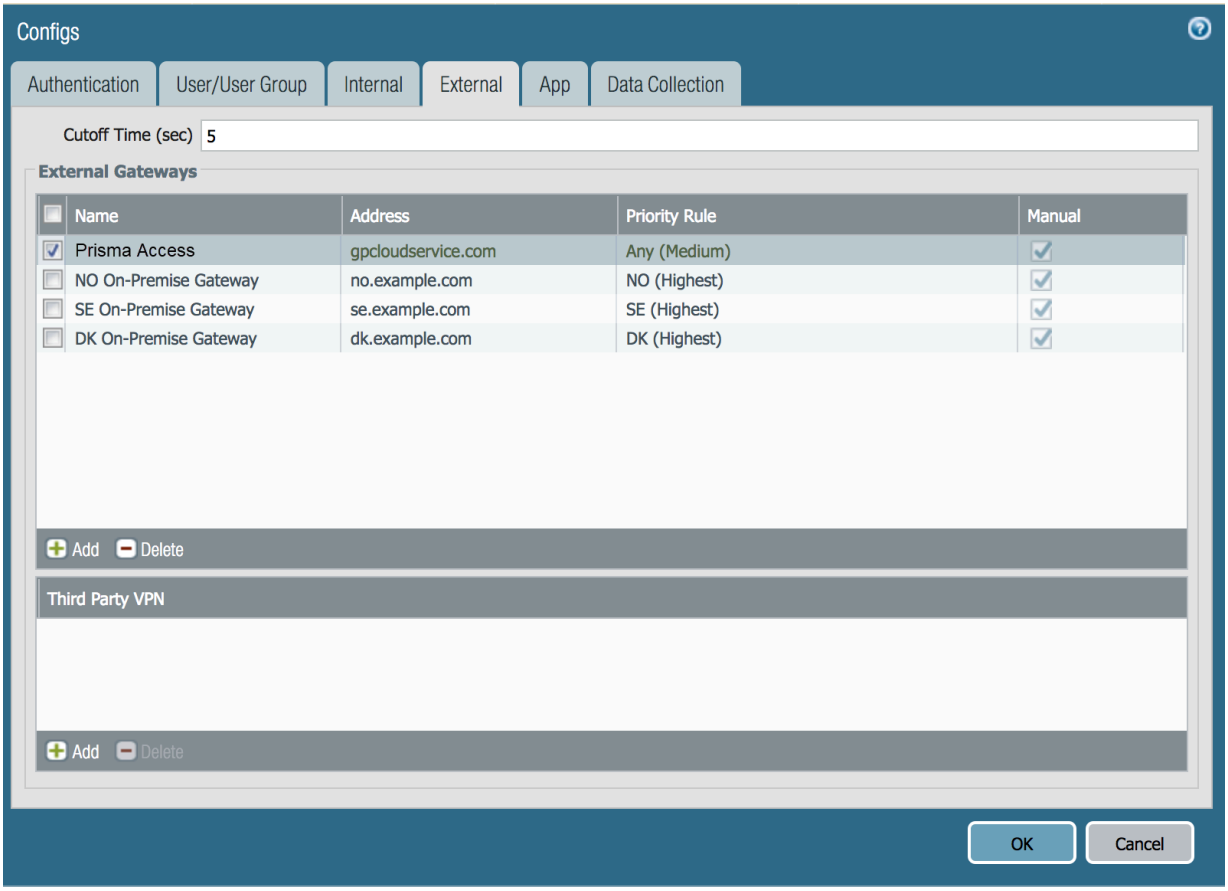
©2025 Palo Alto Networks, Inc.

STEP 9 | （可选）通过重复步骤 8 来设置其他网关的优先级。

确保指定正确的源区域。

下图显示了一个示例配置，其中有多个网关，其源区域位于挪威、瑞典和丹麦。请注意，手动复选框已被选中，这表示移动用户可以手动选择这些网关中的任何一个。

©2025 Palo Alto Networks, Inc.



©2025 Palo Alto Networks, Inc.

移动用户：显式代理

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证

Prisma Access 是 Palo Alto Networks 推出的是一款安全服务边缘 (SSE) 解决方案，它提供了一流的云安全 Web 网关（SWG）功能，包括高级 URL 过滤、SSL 解密、SaaS 应用程序控制以及高级威胁防护。Prisma Access 通过一个由 Palo Alto Networks 全面管理、全面覆盖且始终在线的云原生基础设施，将新一代安全部署付诸实践。移动用户和远程站点可以根据公司策略安全地访问互联网 和 SaaS 应用程序。Prisma Access 提供灵活的连接选项：PAC 文件、代理、无代理和站点到站点 IPSEC，以确保任何传统或替代云代理架构只需进行极少的网络更改便可以迁移到 Prisma Access。

显式代理

Prisma Access 提供完整的云安全 Web 网关 (SWG) 功能，包括基于云的显式代理连接方法。如果您组织的现有网络已经使用显式代理并在您的客户端端点上部署 PAC 文件，您可以顺利地从基于代理的旧 SWG 解决方案迁移到 Prisma Access，保护移动用户的出站互联网流量。如果您是出于合规性目的而需要使用代理，也可以使用显式代理。显式代理使用移动用户许可证。

如果使用多个 PAC 文件来定义如何为不同的用户或系统定向 Web 流量，Prisma Access 使您能够将这些 PAC 文件与转发配置文件相关联，以便您可以一次使用多个 PAC 文件。此外，转发配置文件使您能够配置简单的转发规则来定义 Web 流量的方向，而不是编写 PAC 文件。

- 支持的位置
- 安装了 GlobalProtect 应用程序的显式代理
  - 代理模式下的 GlobalProtect
  - 隧道和代理模式下的 GlobalProtect
- 带有 PAC 文件的显式代理
  - 设置了 SAML
  - 设置了 Kerberos
- 转发配置文件
  - 多 PAC 文件支持
  - 转发规则
  - 使用 GlobalProtect 转发配置文件

Prisma Access 显式代理功能

©2025 Palo Alto Networks, Inc.

功能	说明
App-ID	可持续对所有应用程序进行分类，无论其使用何种端口、是否采用 TLS/SSL 加密，也无论攻击者采用何种规避检测的手段。传统解决方案在进行应用程序分类之前，依赖第 3 层和第 4 层作为首要控制层，与之不同的是，Prisma Access 将 App-ID 与其他第 7 层控制机制（如 User-ID）结合使用。
User-ID	可与广泛的用户身份存储库集成，这样一来，无论用户和用户组在什么位置，都会应用您制定的策略。
SSL 解密	检查策略并将其应用于 TLS/SSL 加密的流量。为了保护隐私和合规性，您可以根据 URL、源、目标、用户、用户组和端口灵活启用或禁用解密。
基于 AI/ML 的检测	提供内联、无特征码的攻击检测手段以及零日漏洞利用防护。与计划更新相比，Prisma Access 能够自适应，并提供即时的实时防护。可以即时阻止高达 95% 的未知威胁，特征码传递时间不到 10 秒，将受感染的系统减少 99.5%。
DNS 安全	应用实时保护和内联机器学习来中断 C2 回调和其他采用 DNS 的攻击手段。原生集成到 Prisma Access，Advanced DNS Security 提供自动保护功能，可防止攻击者绕过安全措施，并且无需独立工具，也无需更改 DNS 路由。
高级 URL 筛选	针对基于网络的威胁（如网络钓鱼、恶意软件和 C2 攻击）提供卓越的防护。将强大的数据库防护与由机器学习驱动的网络安全引擎相结合，能够实时对新的恶意 URL 进行分类并予以拦截。行业领先的网络钓鱼防护功能可应对最常见的安全漏洞成因，您可以通过细粒度的控制和策略设置重新掌控网络流量。这些设置可基于用户、风险评级和内容类别自动执行安全操作。
高级威胁防护	通过行业领先的威胁预防功能，阻止零日威胁、已知漏洞、恶意软件、间谍软件和恶意命令和控制 (C2)。与传统入侵防御系统相比，未知注入攻击防范次数增加 60%，抵御的高度规避的 C2 流量增加 48%。
Advanced WildFire	利用业界最大的威胁情报和恶意软件防护引擎，将自动阻止已知、未知和高度规避的恶意软件的速度提高 60 倍，确保文件安全。
NG-CASB*	获得主动的 SaaS 可见性、防止错误配置和实时数据保护，以实现一流的 SaaS 安全性。
数据丢失防护 (DLP)*	包含一组工具和进程，允许您保护敏感信息免遭未经授权访问、滥用、提取和共享。Prisma Access 上的 DLP 使您能够强制实施数据安全策略，并防止在移动用户和远程网络中丢失敏感数据。
远程浏览器隔离设置	通过 CloudBlades，利用现有 NGFW URL 分类和 URL 重写功能，与第三方 RBI 云进行集成，从而将选定的/所有发往互联网的流量转发至 RBI 云。这种能力可提供无缝的用户体验，同时将某些流量（未知

 ©2025 Palo Alto Networks, Inc.

功能	说明
	或高风险类别）转发至 RBI 进行额外检查，而其余流量则可由 Prisma Access 进行检查，并直接出口至互联网。
报告	包括详细的、可定制的 SaaS 应用程序使用情况报告（作为标准），该报告可以让您深入了解网络上所有 SaaS 流量（批准的和未批准的）。还可以根据自身需求创建自定义报告，并且能够轻松安排报告的生成时间、下载报告，以及与组织内的其他人员共享报告。
用户身份验证	支持所有现有的 PAN-OS 身份验证方法，包括 Kerberos、RADIUS、SAML、LDAP、客户端证书和本地用户数据库。仅使用 PAC 时，支持 Kerberos 和 SAML。
站点到站点 IPsec VPN	支持基于 IPv4 和 IKEv1/IKEv2 的站点到站点隧道，以确保兼容性。对于多个连接站点，ECMP 路由可在可用的互联网连接上平衡会话，从而提供额外的冗余性并提高成本效益。
记录	展示总体流量、应用程序、用户、威胁、URL 和数据过滤日志，以便通过基于云的 Strata Logging Service 对数据进行整理。
转发配置文件	允许为不同的用户组或系统使用多个 PAC 文件。还支持创建转发规则以定义 Web 流量方向，从而以更简单的方式创建和维护 PAC 文件。

* 需要附加许可证。

有关产品特性和功能的详细说明，请参阅Prisma Access 数据表。

显式代理配置准则

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证

系统要求和支持的功能

以下是可用于显式代理的不同连接方法的系统要求和支持的功能。

	无客户端 **SAML**	无客户端 **Kerberos**	客户端上的代理模式（需要 **GP 6.2** 或更高版本）	远程网络的代理模式
应用程序和操作系统支持				

©2025 Palo Alto Networks, Inc.

流量类型	仅限互联网和公共 SaaS 流量	仅限互联网和公共 SaaS 流量	仅限互联网和公共 SaaS 流量	仅限互联网和公共 SaaS 流量
协议支持	代理感知 HTTP 或 HTTPS	代理感知 HTTP 或 HTTPS	代理感知 HTTP 或 HTTPS	代理感知 HTTP 或 HTTPS
到 **Prisma Access** 的传输通道	HTTP 连接	HTTP 连接	TLS 内的 HTTP 连接	从分支机构到远程网络安全处理节点 (SPN) 的 IPSec 内部 HTTP 连接
支持的环境	Windows、Mac、Linux、ChromeOS、VDI	Windows、Mac、Linux、ChromeOS、VDI	Windows 和 Mac	Windows、Mac、Linux、ChromeOS、VDI
应用程序支持	代理感知 HTTP(s) 应用程序	任何遵循 PAC 文件或系统代理设置且支持 Kerberos 的应用程序	代理感知 HTTP(s) 应用程序	代理感知 HTTP(s) 应用程序
浏览器支持	Chrome#、Edge、Firefox 版本 115 或更高版本	Chrome#、Edge、Firefox 版本 115 或更高版本	Chrome#、Edge、Firefox 版本 115 或更高版本*	Chrome#、Edge、Firefox 版本 115 或更高版本
O365 支持†	浏览器和客户端应用程序	浏览器和客户端应用程序	浏览器和客户端应用程序	浏览器和客户端应用程序
标识				
User-ID‡	解密和非 HTTP CORS 流量	所有支持的流量	所有支持的流量	取决于您使用的是 SAML 还是 Kerberos：解密/非 CORS X-Authenticated-User 流量
支持的身份验证	SAML（任何 SAML 2.0 IdP 或通过 CIE）	Kerberos	GlobalProtect 支持的所有身份验证	SAML、Kerberos、基于 X-Authenticated-User
跳过身份验证	按域名和按源 IP	按域名和按源 IP	按域	按域名和按源 IP
用户组目录	CIE 支持的所有目录	CIE 支持的所有目录	CIE 支持的所有目录	CIE 支持的所有目录

©2025 Palo Alto Networks, Inc.

许可证	每用户的移动用户单位	每用户的移动用户单位	每用户的移动用户单位	每位用户或无界面设备的移动用户单元，以及用于远程网络带宽的 NET 单元。
管理				
多租户 **Panorama**	在首个租户上受支持	在首个租户上受支持	在首个租户上受支持	在首个租户上受支持
多租户云管理	支持	支持	支持	支持
安全服务				
SaaS Inline	支持	支持	支持	支持
DLP	支持	支持	支持	支持
DNS 安全§	支持	支持	支持	支持
高级 **URL** 筛选	支持	支持	支持	支持
Advanced WildFire	支持	支持	支持	支持
高级威胁防护	支持	支持	支持	支持
远程浏览器隔离	支持	支持	支持	支持
私有 **IP** 可见性和管控	不支持	不支持	支持已知站点或分支	支持
出口 **NAT**	支持	支持	支持	支持
私有应用程序访问权限	不支持	不支持	通过服务连接支持	不支持
所有 **TCP** 流量	不支持	不支持	支持（通过 GlobalProtect 版本 6.3.1）	不支持
ZTNA 连接器	不支持	不支持	支持	不支持
Colo Connect	不支持	不支持	支持	不支持
服务连接	支持	支持	支持	支持

©2025 Palo Alto Networks, Inc.

HIP 支持（隧道和代理模式）	不支持	不支持	支持	不支持

对于 Chrome 浏览器，如果启用了解密，请按照下面列出的说明禁用 TLS 1.3 Kyber：

1. 打开 Chrome 浏览器。
2. 在地址栏中输入 `chrome://flags/#enable-tls13-kyber` 并禁用 TLS 1.3 Kyber。
3. 单击 **Relaunch**（重新启动）。

* 对于客户端上的代理模式，Firefox 需要一个通过移动设备管理推送的手动策略规则，指示其遵守系统代理

† 显式代理仅支持 HTTP 流量，不支持 UDP。使用 SAML，显式代理不会为客户端应用程序流提供 User-ID。对于客户端代理，您需要使用 PAC 文件将客户端应用程序身份验证流发送到云端代理。

‡ 没有可用于绕过身份验证的 User-ID。

§ 不能将 DNS 安全配置文件应用于显式代理流。可以采取阻止域名的措施。

应用程序支持注意事项

1. 显式代理不支持需要 IP 亲和性的应用程序。对于给定的用户会话，应用程序必须支持来自多个 IP 的流量。
2. 显式代理将解密的 HTTP/2 流降级为 HTTP/1。
3. 显式代理不会获取本地外部动态列表。
4. 仅限无客户端 SAML：
   1. 配置 SSL 解密策略，以允许基于无客户端 PAC 的显式代理在使用 SAML 身份验证时，按域绕过身份验证。

      Prisma Access 需要解密才能读取 *Prisma Access* 在移动用户浏览器上设置的身份验证状态 *cookie*。若未能实施解密，就会使显式代理被滥用作开放代理，攻击者可利用它作为转发服务来发动拒绝服务攻击。
   2. 在流量日志中，显式代理会将未解密的日志以及 HTTP-CORS 移动用户流量日志显示为经过 SWG 认证的用户。
   3. 请注意下列浏览器要求和使用指南：
      - 如果您使用显式代理，请不要在浏览器中禁用 Cookie；否则将无法浏览任何网页。
      - 如果您在 Microsoft Edge 中使用显式代理，请确保将 **Settings**（设置） > **Privacy, Search, and Services**（隐私、搜索和服务） > **Tracking prevention**（防止跟踪）设置为 **Basic**（基本）。

连接要求

如果移动用户使用显式代理从远程站点、总部或数据中心位置进行连接，则移动用户端点必须能够访问并路由到 IdP、ACS FQDN、显式代理 URL 以及 Prisma Access 托管的 PAC 文件的 URL。

PAC 文件要求和指南— 设置要与显式代理一起使用的 PAC 文件时，请务必遵循PAC 文件指南。

 ©2025 Palo Alto Networks, Inc.

代理链指南 — 如果您使用从第三方代理到显式代理的代理链，请在第三方代理中指定 **Explicit Proxy URL**（显式代理 **URL**），以将流量转发到显式代理

本地支持 — 显式代理是一种基于云的代理解决方案，而不是本地产品。对于本地代理解决方案，请配置 PAN-OS Web 代理。

代理模式下的 GlobalProtect

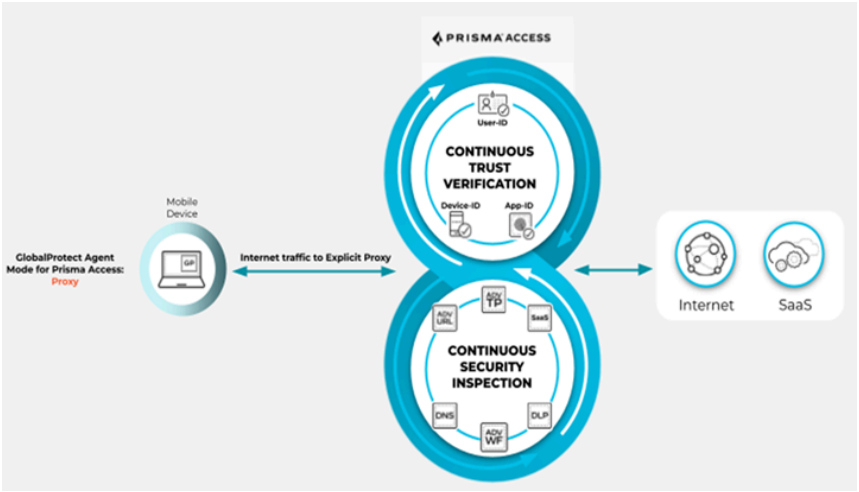
在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager) 如果您想在 Prisma Access 环境中使用此功能，请与客户团队联系以了解更多信息。	• Prisma Access 5.2 • 适用于 Windows 或 macOS 的 GlobalProtect 应用程序版本 6.2 • 内容发布版本 8700-7994 • Prisma Access 移动用户许可证

使用代理模式时，GlobalProtect 应用程序提供始终在线的互联网安全性。在此模式下，GlobalProtect 应用程序根据 PAC 文件（该文件托管在 Prisma Access 中或您的环境中）的转发规则和逻辑将流量代理到 Prisma Access。如果您拥有现有（旧版）代理架构，或者出于监管或合规性原因需要维护代理架构，此功能将非常有用。

基于客户端的代理功能有助于实现 GlobalProtect 应用程序与第三方 VPN 的共存和互操作性，您可以通过 GlobalProtect 应用程序保护移动用户流向显式代理的互联网流量，并使用您选择的第三方 VPN 来保护私有应用程序访问。

您需要 *Strata Cloud Manager* 以及 *GlobalProtect* 代理版本 *6.3.0*，*GlobalProtect* 代理通道才能支持所有 *IPv4 TCP* 连接，包括非代理感知流量。为了确保无缝功能，在端点上配置的 *DNS* 必须能够解析目标 *FQDN*。

在这种情况下，GlobalProtect 应用程序根据您定义的 PAC 文件规则将互联网流量发送到 Prisma Access，而端点使用 IPSec/TLS 隧道通过第三方 VPN 路由对私有应用程序的访问。



- Strata Cloud Manager

 ©2025 Palo Alto Networks, Inc.

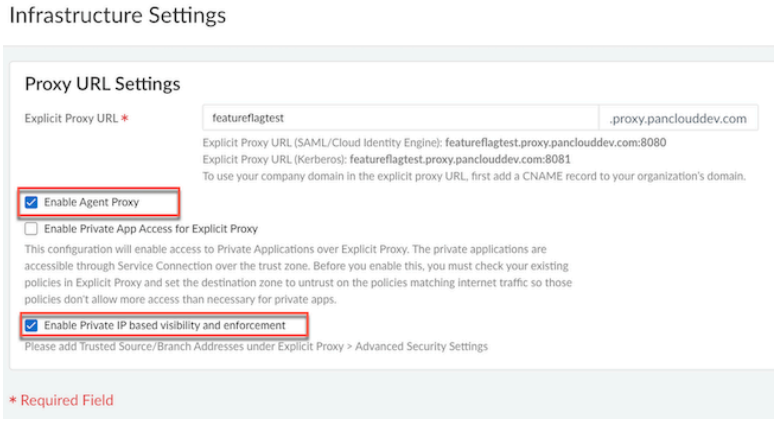
- Panorama

代理模式下的 GlobalProtect (Strata Cloud Manager)

©2025 Palo Alto Networks, Inc.

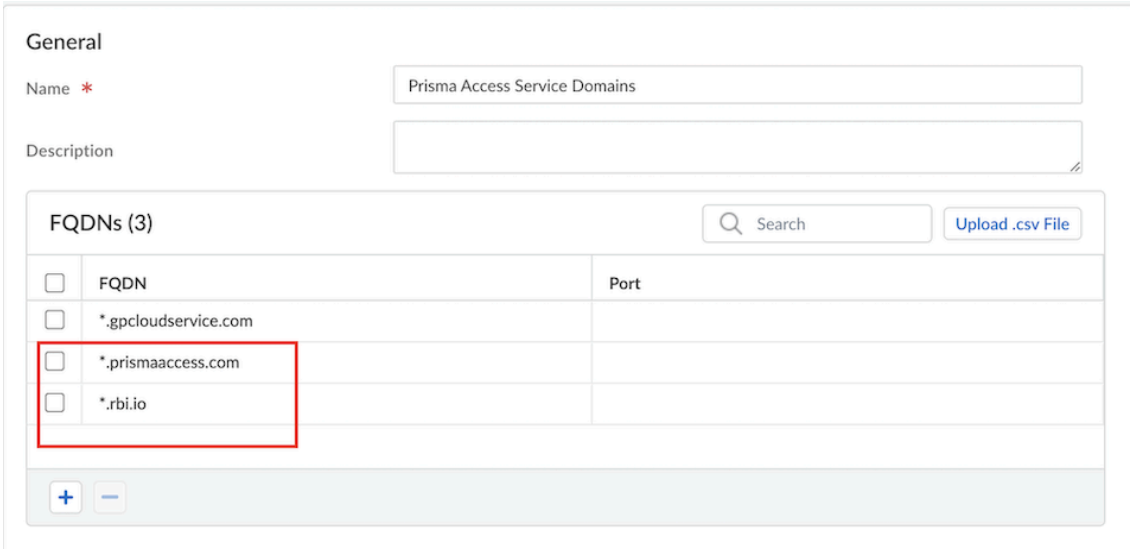
STEP 1 | 在 Prisma Access 上为移动用户启用基于客户端的代理功能。

1. 启用显式代理。
   1. 选择 **Workflows**（工作流） > **Prisma Access** 设置 > **Mobile Users**（移动用户），然后单击 **Explicit Proxy Setup**（显式代理设置）。
   2. 在“基础架构设置”区域中，单击 **Setup Proxy Settings**（设置代理设置），指定 **Explicit Proxy URL**（显式代理 URL）。
2. 选择 **Enable Agent Proxy**（启用客户端代理），也可以选择 **Enable Private IP based visibility and enforcement**（启用基于私有 IP 的可见性和强制执行），然后单击 **Save**（保存）。



3. 选择您想要支持移动用户的 Prisma Access 地点。

   为了获得最佳用户体验，如果要限制地点数量，请选择离最终用户最近的地点。如果某个地点在您的移动用户居住的国家/地区不可用，请选择离该移动用户最近的地点。
4. 创建转发配置文件以定义要通过显式代理发送的流量。配置转发配置文件时，请绕过 *.prismaaccess.com 和 *.gpcloudservice.com 域。



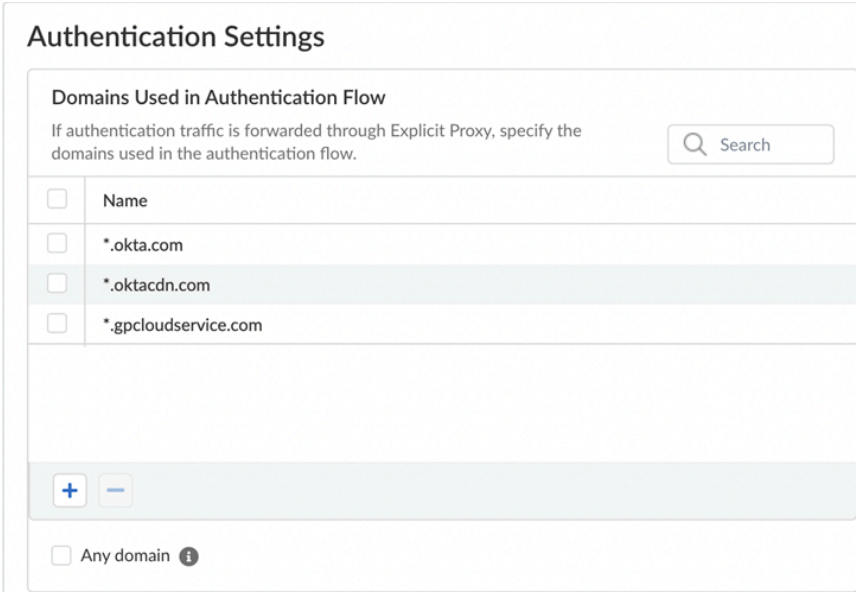
5. 将转发配置文件附加到 GlobalProtect 应用程序配置中。

 ©2025 Palo Alto Networks, Inc.

6. 选择 **Workflows**（工作流） > 设置 > **Explicit Proxy**（显式代理） > **Advanced Security Settings**（高级安全设置） > **Authentication Settings**（身份验证设置），添加需要绕过的域名。

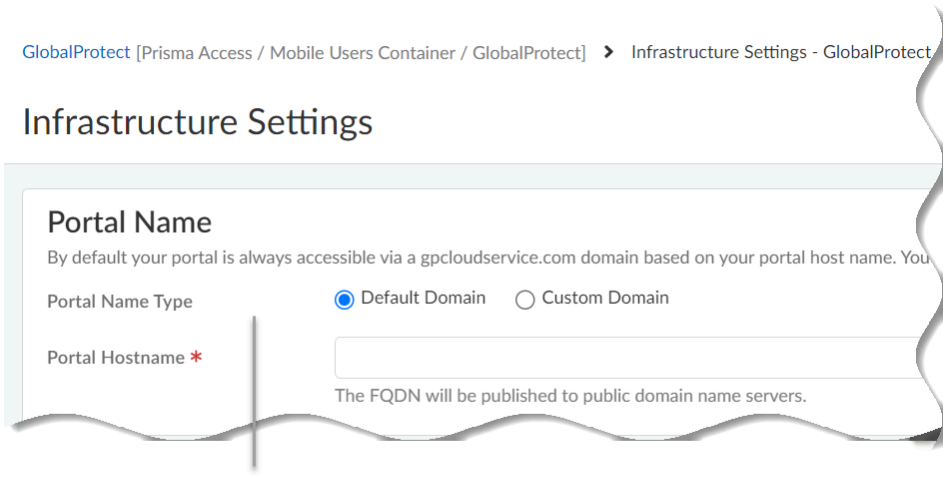
   向代理提出的所有请求都经过身份验证。但是，如果您通过代理传递 IdP 流程，则需要绕过 IdP 才能成功进行身份验证。

   在此示例中，我们将绕过 GlobalProtect 门户和 Okta，但请根据您使用的 IdP 对其进行自定义。



STEP 2 | 设置 GlobalProtect 门户、身份验证，并为 GlobalProtect 应用程序配置代理模式。

1. 选择 **Workflows**（工作流） > **Prisma Access** 设置 > **GlobalProtect** > **Infrastructure**（基础架构） > **Infrastructure Settings**（基础架构设置），并指定 **Portal Name**（门户名称）。



GlobalProtect Infrastructure Settings

- **Default Domain**（默认域）— 如果选择此选项，则门户主机名将使用默认域名：`.gpcloudservice.com`。在这种情况下，只需输入 **Portal Hostname**（门户主

 ©2025 Palo Alto Networks, Inc.

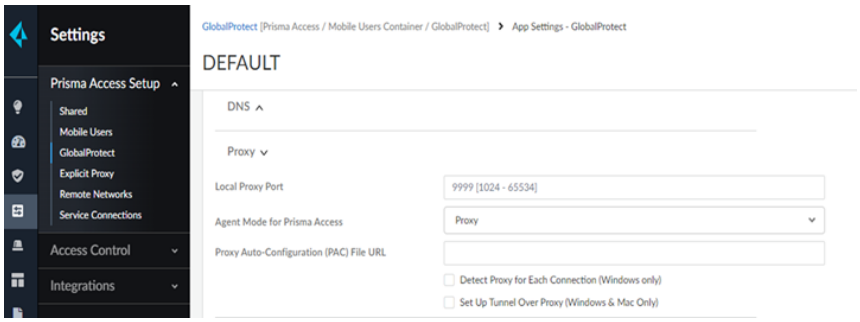
机名）以附加到默认域名即可。适用于用户的 Prisma Access 将自动创建必要的证书并将主机名发布到公共 DNS 服务器。

- **Custom Domain**（自定义域）— 如果您希望门户主机名中的域名与您的公司域名匹配（例如，myportal.mydomain.com），您还可以自定义门户地址。

2. 让移动用户能够对 Prisma Access 进行身份验证。
3. 在 GlobalProtect 应用程序设置中为 Prisma Access 启用 GlobalProtect 代理模式，以将互联网流量发送到基于客户端的代理。

   GlobalProtect 连接方法不适用于代理模式，因为它始终处于开启状态。

   - 选择 **Workflows**（工作流） > **Prisma Access** 设置 > **GlobalProtect**。
   - 在 **GlobalProtect App**（**GlobalProtect** 应用程序）选项卡上，单击 **Default**（默认）以自定义应用程序设置，或单击 **Add App Settings**（添加应用程序设置）以添加新配置。
   - 在 **App Configuration**（应用程序配置）部分中单击 **Show Advanced Options**（显示高级选项）。
   - 将 **Prisma Access** 的客户端模式设置为 **Proxy**（代理），以指示 GlobalProtect 应用程序将互联网流量发送到 Prisma Access 上的显式代理。
   - （可选）配置本地代理端口。端口范围为 1024 到 65534，默认端口为 9999。如果默认端口不可用，GlobalProtect 将尝试连接 9999 到 10009 范围内的其他 10 个端口，并使用可用的端口。您也可以在该范围内选择自己的端口号。
   - （可选）如果要将代理设置的新的 PAC URL 推送到端点，请配置 PAC 自动配置 (PAC) 文件 URL。用户连接后，PAC URL 会推送到端点。当用户断开 GlobalProtect 应用程序的连接时，端点代理配置将自动禁用并恢复为之前的设置。
   - （可选）如果希望用户检查门户是否有任何新设置，请启用允许用户重新发现网络。
   - （可选）配置 GlobalProtect 应用程序配置刷新间隔（小时）。默认情况下，GlobalProtect 客户端每 24 小时刷新一次缓存的门户配置。您可以根据业务需求更改刷新间隔。
   - 禁用 **Set Up Tunnel Over Proxy (Windows & Mac Only)**（设置代理上的隧道（仅限 **Windows** 和 **Mac**））。



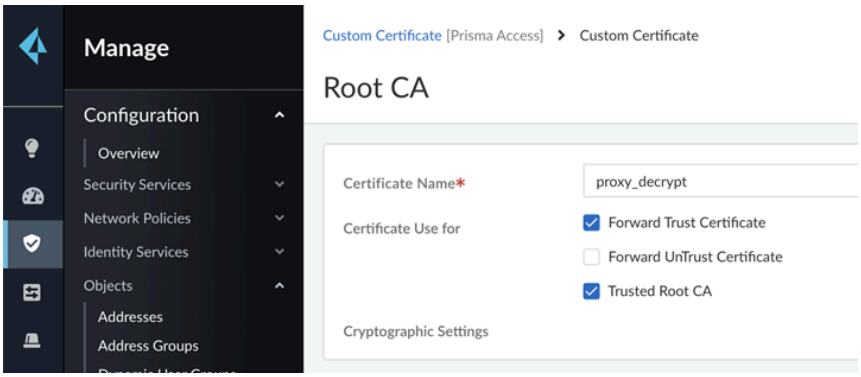
4. 要启用始终在线的互联网安全性，请在 **Workflows**（工作流） > **Prisma Access** 设置 > **GlobalProtect** > **GlobalProtect App**（**GlobalProtect** 应用程序） > **Add App Settings**（添加应用程序设置）页面上配置以下设置：

 ©2025 Palo Alto Networks, Inc.

1. 将禁用 GlobalProtect 设置为 **Disallow**（不允许）、**Allow with Passcode**（使用密码允许）或 **Allow with Ticket**（具有支持工单时允许）。
2. 禁用允许用户从 GlobalProtect 应用程序注销。

STEP 3 | 为显式代理流量配置解密策略。

- 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW** 和 > **Security Services**（安全服务） > **Decryption**（解密）。
- 如果启用解密，请确保将解密证书设置为受信任的根 CA。



STEP 4 | 为显式代理流量配置安全策略规则。

- 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW** 和 **Prisma Access** > **Security Services**（安全服务） > **Security Policy**（安全策略）。
- 遵循互联网网关安全策略最佳实践。

STEP 5 | （可选）在非默认路由网络中以代理模式配置 GlobalProtect 应用程序。

- （可选）在内部托管 PAC 文件并在 PAC 文件中将 Prisma Access 显式代理 FQDN 添加为代理，或者将 PAC 文件托管在转发配置文件中，并在网络中添加 PAC 服务 IP 地址的路由。
- 在 PAC 文件中，将 IdP URL 和 Prisma Access 门户 URL 转发到显式代理。
- 在显式代理上，从身份验证设置中排除 IdP 和门户 URL。将 IdP 和门户 URL 添加到在身份验证流程中使用的域。
- 在外围设备上设置指向显式代理 FQDN 或 IP 地址的路由，以允许用户通过显式代理访问互联网。
- （可选）如果用户无法解析分支网络中的公共域，则添加 DNS 记录以将 Prisma Access 显式代理 FQDN 解析为内部 IP 地址，并将内部 IP 地址的目标 NAT 添加到显式代理 FQDN 或 IP 地址。

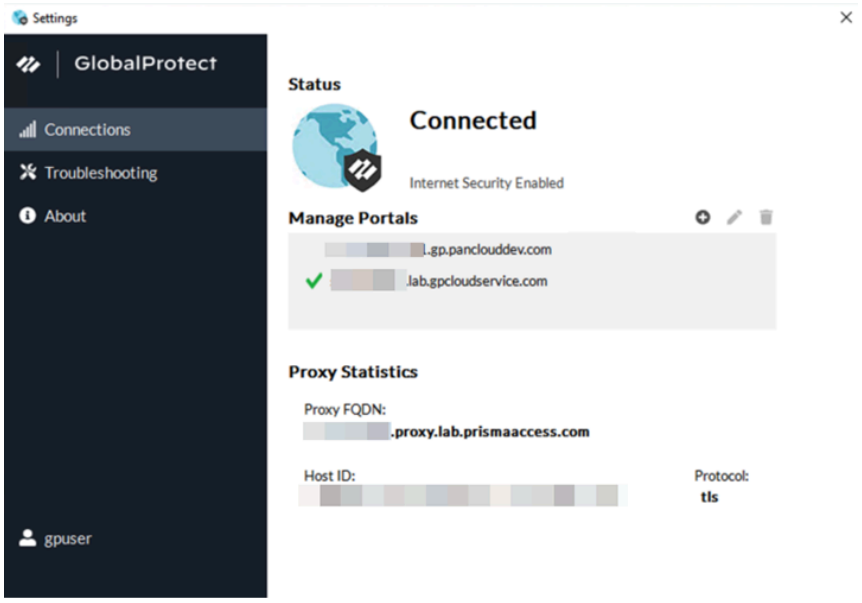
STEP 6 | 单击 **Save**（保存）并 **Push Config**（推送配置）到 **GlobalProtect** 和 **Explicit Proxy**（显式代理）。

 ©2025 Palo Alto Networks, Inc.

STEP 7 | 验证客户端代理部署并排除故障。

1. 在 GlobalProtect 应用程序 **Settings**（设置）下的 **Connections**（连接）选项卡上验证有关网络连接的信息。

   1. 打开 GlobalProtect 应用程序。
   2. 选择 **Settings**（设置）以打开 GlobalProtect 设置面板，然后选择 **Connections**（连接）。



2. 查看并收集 GlobalProtect 日志。

   查看 PangPS 日志，以验证 GlobalProtect 门户上的代理模式配置。

   可以通过在 PangPS 日志中查找以下事件来验证是否已配置代理模式：

   `OnProxyAgentMode`：仅代理模式

   要在 中查看 GlobalProtect 日志，请选择 **Incidents & Alerts**（事件和警报） > **Log Viewer**（日志查看器），并且选择：

   - **GlobalProtect**（用于身份验证日志）
   - **Traffic**（流量）和 **Decryption**（解密）（用于用户访问日志）

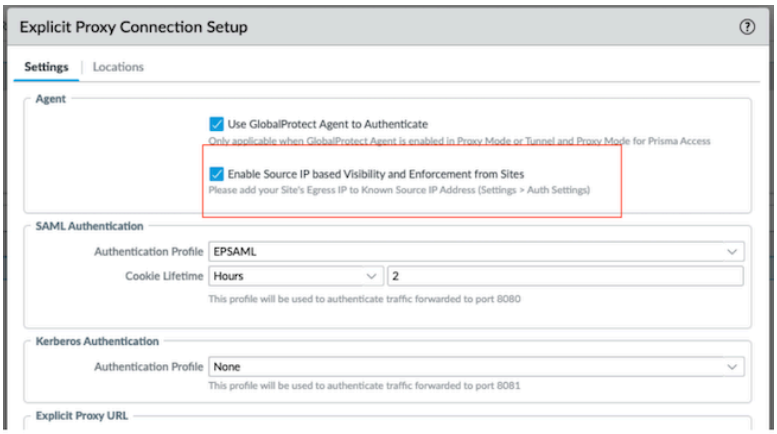
代理模式下的 GlobalProtect (Panorama)

如果将单租户 *Prisma Access (Managed by Panorama)* 部署转换为多租户，则只有第一个租户（您迁移的租户）支持此功能。此外，在第一个租户中，您必须在预定义的 *Explicit_Proxy_Device_Group* 中设置策略规则，而不是在自定义设备组中设置策略规则。在第一个租户之后为多租户部署创建的任何后续租户均不支持此功能。

©2025 Palo Alto Networks, Inc.

STEP 1 | 为移动用户启用基于客户端的代理功能。

1. 启用显式代理。
   1. 选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Mobile Users**—**Explicit Proxy**（移动用户—显式代理）。
   2. **Configure**（配置）显式代理设置以指定 **Explicit Proxy URL**（显式代理 **URL**）。
2. 选择 **Use GlobalProtect app to Authenticate**（使用 **GlobalProtect** 应用程序进行身份验证），以启用基于客户端的代理功能，也可以选择 **Enable Source IP based Visibility and Enforcement from Sites**（从站点启用基于源 **IP** 的可见性和和强制执行）。



3. 输入 **PAC (Proxy Auto-Configuration) File**（**PAC**（代理自动配置）文件） URL。确保在 PAC 文件中输入端口 8080。
   - 确保在 PAC 文件中输入端口 8080。
   - PAC 文件中的代理语句必须使用您在上方配置的 Prisma Access FQDN。
   - 必须将 PAC 文件配置为绕过第三方 VPN 流量。

   示例 PAC 文件：

```
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. 为您配置的显式代理设置选择 **Connection Name**（连接名称）。
5. 选择要为移动用户部署显式代理的 **Locations**（地点）和区域。

   Prisma Access 会将代理节点添加到您选择的每个地点。显式代理支持所有 Prisma Access 地点的子集。为了获得最佳用户体验，如果要限制地点数量，请选择离最终用户最近的地

 ©2025 Palo Alto Networks, Inc.

点。如果某个地点在您的移动用户居住的国家/地区不可用，请选择离该移动用户最近的地点。

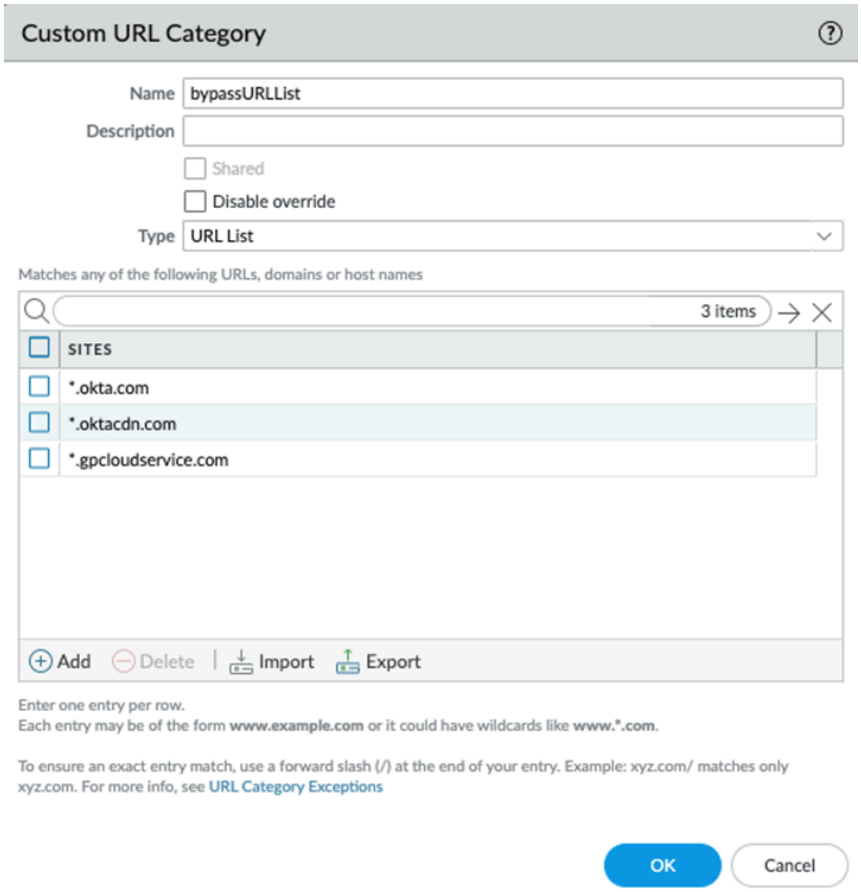
 ©2025 Palo Alto Networks, Inc.

STEP 2 | 绕过身份提供程序 (IDP)。

向代理提出的请求都经过身份验证。但是，如果您通过代理传递 IDP 流程，则需要绕过 IDP 才能成功进行身份验证。

在此示例中，我们将绕过 GlobalProtect 门户和 Okta，但请根据您使用的 IDP 对其进行自定义。

1. 选择 **Explicit_Proxy_Device_Group** 后，选择 **Object**（对象） > **Custom Objects**（自定义对象） > **URL Category**（**URL** 类别），然后创建自定义 URL 类别。
2. 在自定义 URL 类别中，添加需要绕过 EP 身份验证的所有 FQDN 域名。



3. 选择 **Cloud Services**（云服务） > **Configuration**（配置） > **Mobile Users**（移动用户） > **Explicit Proxy**（显式代理） > **Settings**（设置） > **Authentication Settings**（身份验证设置），并附加自定义 URL 类别。



4. 提交并推送到 **Explicit_Proxy_Device_Group**。

 ©2025 Palo Alto Networks, Inc.

STEP 3 | 配置 GlobalProtect 门户。

在代理模式下，您设置的连接方法不会改变代理功能的行为。即使您设置了按需连接方法，所有互联网绑定流量仍将通过代理进行传输，以确保始终在线的互联网安全。

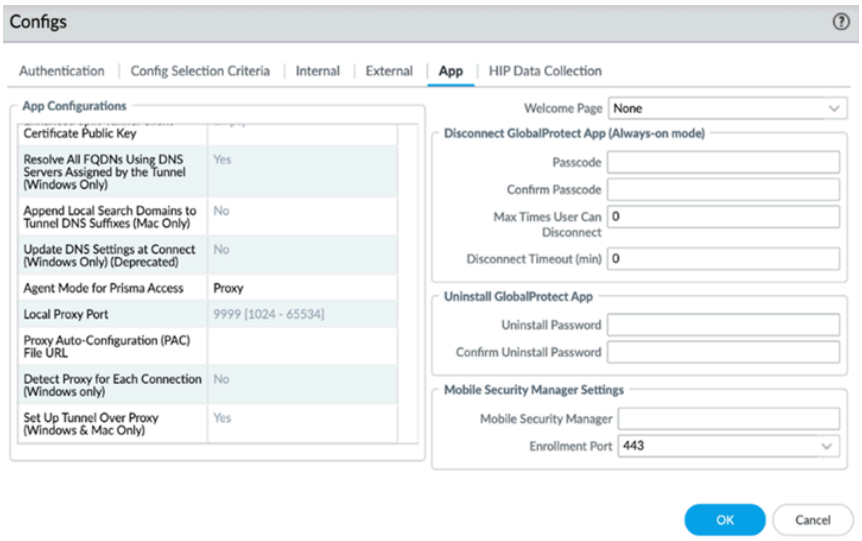
1. 在“加入”部分中，单击 **Configure**（配置）。
2. 在 **General**（常规）选项卡上，指定 **Portal Name Type**（门户名称类型）：

   Use Default Domain（使用默认域）— 如果选择此选项，则门户主机名将使用默认域名：.gpcloudservice.com。在这种情况下，只需输入门户主机名以附加到默认域名即可。Prisma Access 将自动创建必要的证书并将主机名发布到公共 DNS 服务器。

   Use Company Domain（使用公司域）— 如果您希望门户主机名中的域名与您的公司域名相匹配（例如，myportal.mydomain.com），请选择此选项。
3. 选择一个用于指定 Prisma Access 应如何对移动用户进行身份验证的 **Authentication Profile**（身份验证配置文件），或创建一个新的配置文件。
4. （可选）选择 **Authentication Override Certificate**（身份验证覆盖证书），以加密移动用户用于向门户和网关进行身份验证的安全 Cookie。

STEP 4 | 在 GlobalProtect 上启用代理模式。

1. 选择 **Network**（网络）> **GlobalProtect Portals**（**GlobalProtect** 门户）。
2. 选择正向其添加代理配置的门户配置，然后选择 **Agent**（代理）选项卡。
3. 在 **Agent**（客户端）选项卡上，选择 **App**（应用程序）。
4. 在应用配置区域中，将 **Prisma Access** 的客户端模式设置为 **Proxy**（代理），以将互联网流量发送到基于 GlobalProtect 客户端的代理



 ©2025 Palo Alto Networks, Inc.

STEP 5 | 执行可选配置。

1. （可选）配置本地代理端口。端口范围为 1024 到 65534，默认端口为 9999。如果默认端口不可用，GlobalProtect 将尝试连接 9999 到 10009 范围内的其他 10 个端口，并使用可用的端口。您也可以在该范围内选择自己的端口号。
2. （可选）如果要将代理设置的自定义 PAC URL 推送到端点，请配置 PAC 自动配置 (PAC) 文件 URL。用户连接后，PAC URL 会推送到端点。当用户断开 GlobalProtect 应用程序的连接时，端点代理配置将自动禁用并恢复为之前的设置。
3. （可选）如果希望用户检查门户是否有任何新设置，请启用允许用户重新发现网络。
4. （可选）配置 GlobalProtect 应用程序配置刷新间隔（小时）。默认情况下，GlobalProtect 客户端每 24 小时刷新一次缓存的门户配置。您可以根据业务需求更改刷新间隔。

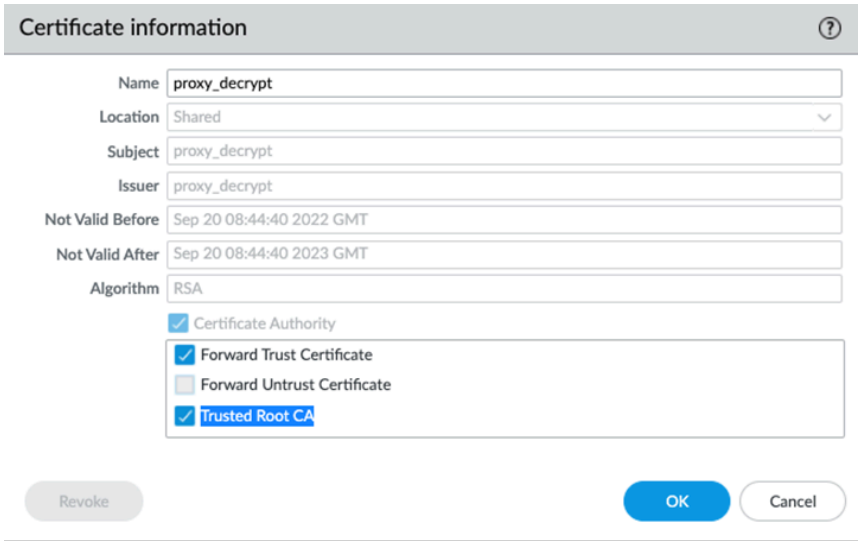
STEP 6 | 通过配置以下设置启用始终在线的互联网安全性：

1. 将允许用户禁用 GlobalProtect 设置为 **Disallow**（不允许）、**Allow with Passcode**（使用密码允许）或 **Allow with Ticket**（具有支持工单时允许）。
2. 将允许用户从 GlobalProtect 应用程序注销设置为 **No**（否）。

STEP 7 | （可选）为显式代理流量配置解密策略。

如果启用解密，请确保解密证书也设置为可信的根 CA。

1. 选择 **Device**（设备） > **Certificate Management**（证书管理） > **Certificates**（证书），并创建可信的根 CA 证书和转发信任证书。



2. 在 **Explicit_Proxy_Device Group** 组下创建具有 SSL 转发代理的解密规则。

STEP 8 | 为显式代理流量配置安全策略规则。

1. 选择 **Policies**（策略） > **Security**（安全）。
2. 将 **Device Group**（设备组）设置为 **Explicit_Proxy_Device_Group**。
3. 遵循互联网网关安全策略最佳实践。

©2025 Palo Alto Networks, Inc.

STEP 9 | （可选）在非默认路由网络中以代理模式配置 GlobalProtect 应用程序。

- （可选）在内部托管 PAC 文件并在 PAC 文件中将 Prisma Access 显式代理 FQDN 添加为代理，或者将 PAC 文件托管在转发配置文件中，并在网络中添加 PAC 服务 IP 地址的路由。
- 在 PAC 文件中，将 IDP URL 和 Prisma Access 门户 URL 转发到显式代理。
- 在显式代理上，从身份验证设置中排除 IDP 和门户 URL。将 IDP 和门户 URL 添加到在身份验证流程中使用的域。
- 在外围设备上设置指向显式代理 FQDN 或 IP 地址的路由，以允许用户通过显式代理访问互联网。
- （可选）如果用户无法解析分支网络中的公共域，则添加 DNS 记录以将 Prisma Access 显式代理 FQDN 解析为内部 IP 地址，并将内部 IP 地址的目标 NAT 添加到显式代理 FQDN 或 IP 地址。

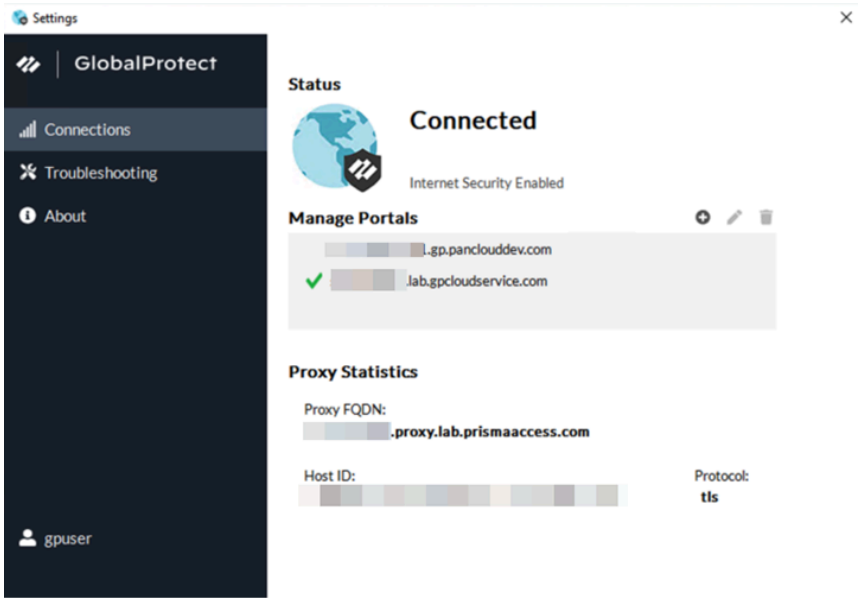
STEP 10 | 将更改 **Commit**（提交）到 Panorama，将配置更改 **Commit and Push**（提交并推送）给 Prisma Access **Mobile Users**（移动用户）和 **Explicit Proxy**（显式代理）。

 ©2025 Palo Alto Networks, Inc.

STEP 11 | 验证客户端代理部署并排除故障。

1. 在 GlobalProtect 应用程序 **Settings**（设置）下的 **Connections**（连接）选项卡上验证有关网络连接的信息。

   1. 打开 GlobalProtect 应用程序。
   2. 选择 **Settings**（设置）以打开 GlobalProtect 设置面板，然后选择 **Connections**（连接）。



2. 查看并收集 GlobalProtect 日志

   查看 PangPS 日志，以验证 GlobalProtect 门户上的代理模式配置。

   可以通过在 PangPS 日志中查找以下事件来验证是否已配置代理模式：

   `OnProxyAgentMode`：仅代理模式

   要在 Panorama 中查看 GlobalProtect 日志，请选择 **Monitor**（监控） > **Logs**（日志）和：

   - **GlobalProtect**（用于身份验证日志）
   - **Traffic**（流量）和 **Decryption**（解密）（用于用户访问日志）

隧道和代理模式下的 GlobalProtect

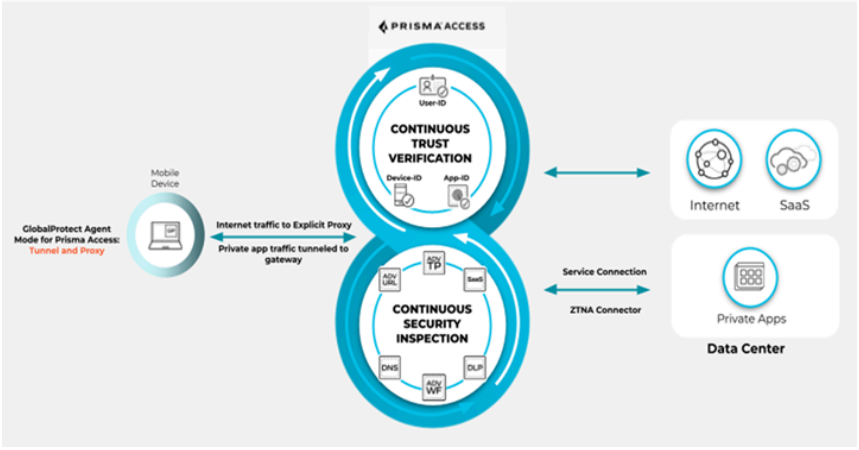
在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager) 如果您想在 Prisma Access 环境中使用此功能，请与客户团队联系以了解更多信息。	• Prisma Access 5.2 • 适用于 Windows 或 macOS 的 GlobalProtect 应用程序版本 6.2 • 内容发布版本 8700-7994 • Prisma Access 移动用户许可证

 ©2025 Palo Alto Networks, Inc.

在 **Tunnel and Proxy**（隧道和代理）模式下，GlobalProtect 应用程序会根据您在 PAC 文件中定义的规则将互联网绑定流量发送到显式代理。对于剩余流量，它使用在 PAC 文件中定义的拆分隧道规则和逻辑来确定哪些流量通过隧道发送，哪些流量可以绕过隧道。如果未定义拆分通道规则，该应用程序将通过隧道发送所有剩余流量。

在隧道和代理模式下运行 *GlobalProtect* 应用程序时，只有通过 *GlobalProtect* 隧道的流量才支持主机信息配置文件 *(HIP)* 功能。

您需要 *Strata Cloud Manager* 及 *GlobalProtect* 代理版本 *6.3.0*，*GlobalProtect* 代理通道才能支持所有 *IPv4 TCP* 连接，包括非代理感知流量。为了确保无缝功能，在端点上配置的 *DNS* 必须能够解析目标 *FQDN*。



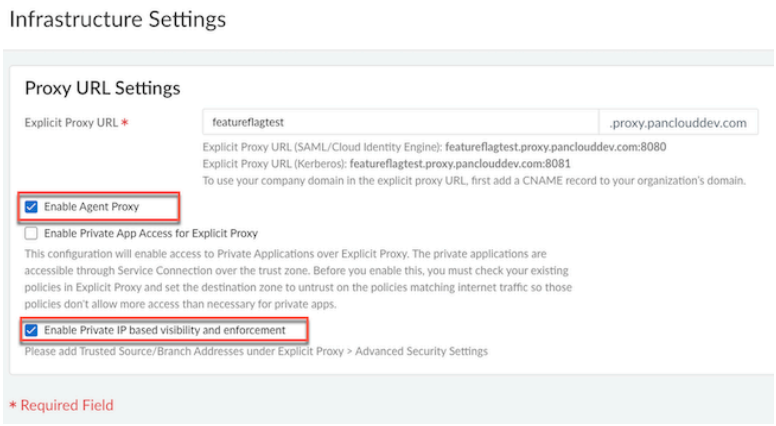
- Strata Cloud Manager
- Panorama

隧道和代理模式下的 GlobalProtect (Strata Cloud Manager)

 ©2025 Palo Alto Networks, Inc.

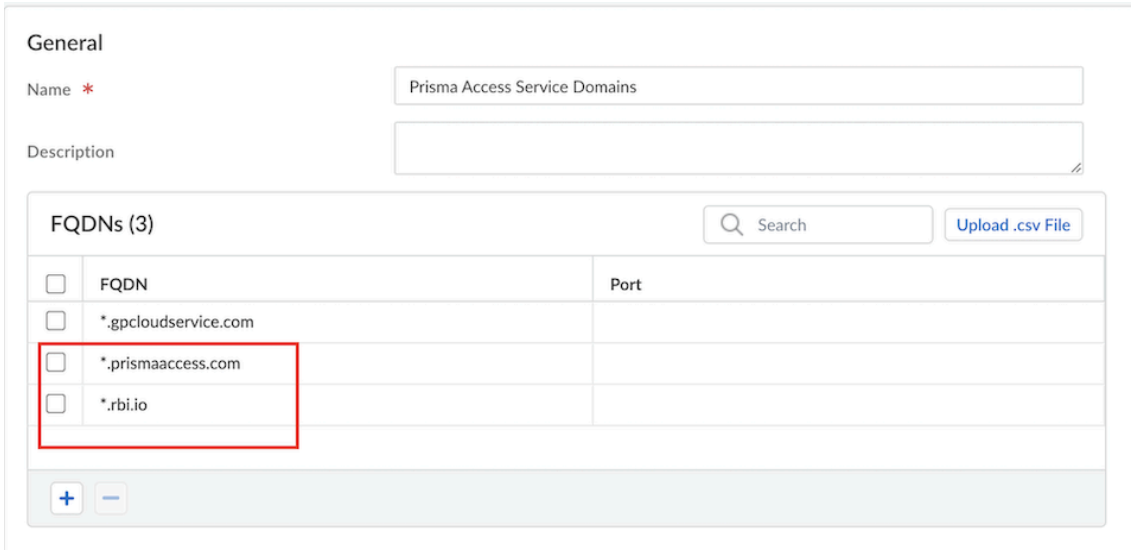
STEP 1 | 在 Prisma Access 上为移动用户启用基于客户端的代理功能。

1. 启用显式代理。
   1. 选择 **Workflows**（工作流） > **Prisma Access** 设置 > **Explicit Proxy**（显式代理）。
   2. 在“基础架构设置”区域中，单击 **Setup Proxy Settings**（设置代理设置），指定 **Explicit Proxy URL**（显式代理 **URL**）。
2. 选择 **Enable Agent Proxy**（启用客户端代理），也可以选择 **Enable Private IP based visibility and enforcement**（启用基于私有 **IP** 的可见性和强制执行），然后单击 **Save**（保存）。



3. 选择您想要支持移动用户的 Prisma Access 地点。

   为了获得最佳用户体验，如果要限制地点数量，请选择离最终用户最近的地点。如果某个地点在您的移动用户居住的国家/地区不可用，请选择离该移动用户最近的地点。
4. 创建转发配置文件以定义要通过显式代理发送的流量。配置转发配置文件时，请绕过 *.prismaaccess.com 和 *.gpcloudservice.com 域。

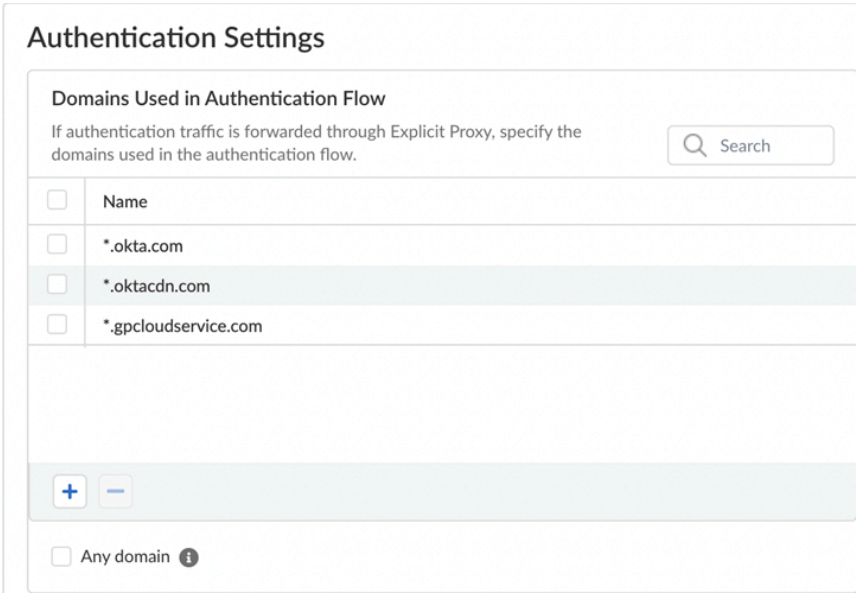


5. 将转发配置文件附加到 GlobalProtect 应用程序配置中。
6. 选择 **Workflows**（工作流） > 设置 > **Explicit Proxy**（显式代理） > **Advanced Security Settings**（高级安全设置） > **Authentication Settings**（身份验证设置），添加需要绕过的域名。

 ©2025 Palo Alto Networks, Inc.

向代理提出的所有请求都经过身份验证。但是，如果您通过代理传递 IdP 流程，则需要绕过 IdP 才能成功进行身份验证。

在此示例中，我们将绕过 GlobalProtect 门户和 Okta，但请根据您使用的 IdP 对其进行自定义。

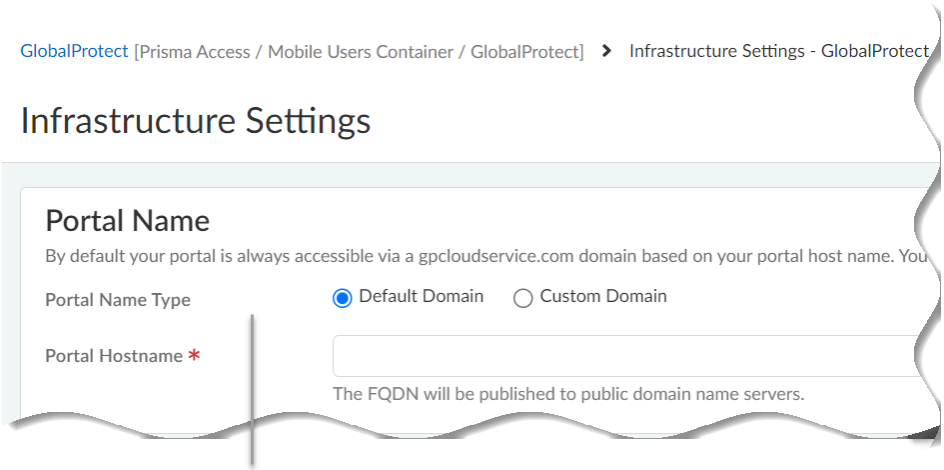


 ©2025 Palo Alto Networks, Inc.

STEP 2 | 为 Prisma Access 上的 GlobalProtect 应用程序配置隧道和代理模式。

在隧道和代理模式下，您设置的连接方法仅适用于通过 *GlobalProtect* 隧道传输的流量。基于客户端的代理功能将提供始终在线的互联网安全性。即使您设置了按需连接方法，当用户断开 *GlobalProtect* 应用程序的连接时，所有互联网绑定流量仍将通过代理进行传输，以确保始终在线的互联网安全性。

1. 选择 **Workflows**（工作流） > **Prisma Access** 设置 > **GlobalProtect** > **Infrastructure**（基础架构） > **Infrastructure Settings**（基础架构设置），并指定 **Portal Name**（门户名称）。



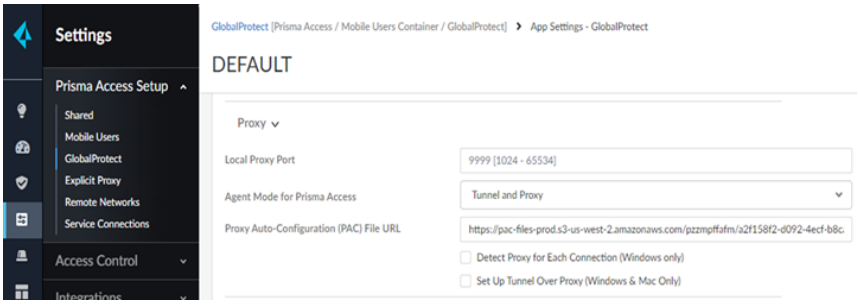
GlobalProtect Infrastructure Settings

   - **Default Domain**（默认域）— 如果选择此选项，则门户主机名将使用默认域名：`.gpcloudservice.com`。在这种情况下，只需输入 **Portal Hostname**（门户主机名）以附加到默认域名即可。适用于用户的 Prisma Access 将自动创建必要的证书并将主机名发布到公共 DNS 服务器。
   - **Custom Domain**（自定义域）— 如果您希望门户主机名中的域名与您的公司域名相匹配（例如，myportal.mydomain.com），您还可以自定义门户地址。
2. 让移动用户能够对 Prisma Access 进行身份验证。
3. 在 GlobalProtect 应用程序设置中为 Prisma Access 启用 GlobalProtect 隧道和代理模式，以将互联网流量发送到基于客户端的代理。
   - 选择 **Workflows**（工作流） > **Prisma Access** 设置 > **GlobalProtect**。
   - 在 **GlobalProtect App**（**GlobalProtect** 应用程序）选项卡上，单击 **Default**（默认）以自定义应用程序设置，或单击 **Add App Settings**（添加应用程序设置）以添加新配置。
   - 在 **App Configuration**（应用程序配置）部分中单击 **Show Advanced Options**（显示高级选项）。
   - 在 **Proxy**（代理）部分中，将 **Prisma Access** 的客户端模式设置为 **Tunnel and Proxy**（隧道和代理），以指示 GlobalProtect 应用程序将互联网流量发送到 Prisma Access 上的显式代理，并将私有应用程序流量发送到 VPN。在 Prisma

 ©2025 Palo Alto Networks, Inc.

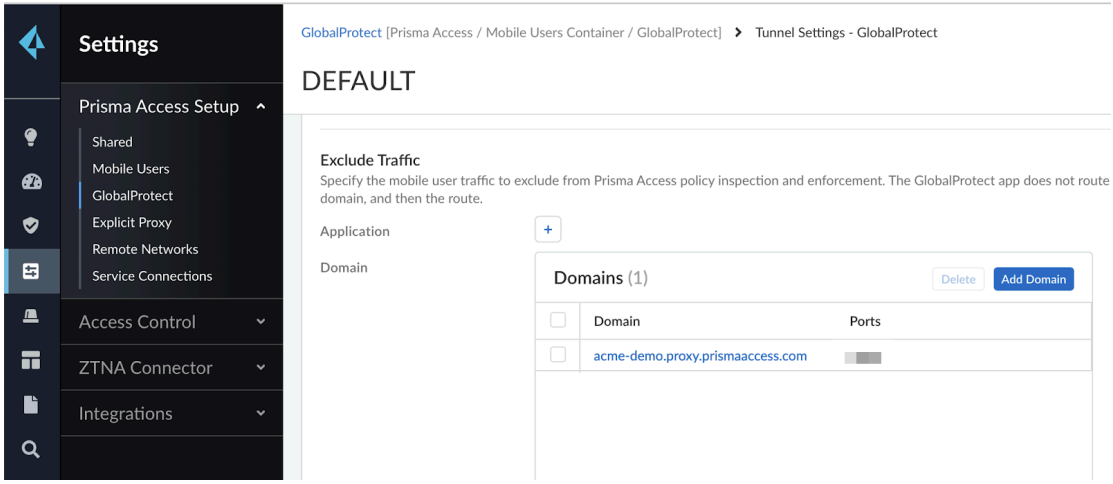
Access 上配置 **Tunnel and Proxy**（隧道和代理） 模式后，即使用户断开连接或禁用 GlobalProtect 应用程序， 也可以通过 Prisma Access 安全地访问互联网。

- （可选）配置本地代理端口。端口范围为 1024 到 65534，默认端口为 9999。如果默认端口不可用，GlobalProtect 将尝试连接 9999 到 10009 范围内的其他 10 个端口，并使用可用的端口。您也可以在该范围内选择自己的端口号。
- （可选）如果要将代理设置的新的 PAC URL 推送到端点，请配置 PAC 自动配置 (PAC) 文件 URL。用户连接后，PAC URL 会推送到端点。当用户断开 GlobalProtect 应用程序的连接时，端点代理配置将自动禁用并恢复为之前的设置。
- （可选）如果希望用户检查门户是否有任何新设置，请启用允许用户重新发现网络。
- （可选）配置 GlobalProtect 应用程序配置刷新间隔（小时）。默认情况下，GlobalProtect 客户端每 24 小时刷新一次缓存的门户配置。您可以根据业务需求更改刷新间隔。
- 禁用 **Set Up Tunnel Over Proxy (Windows & Mac Only)**（设置代理上的隧道（仅限 **Windows** 和 **Mac**））。



4. 在 **Split Tunnel**（拆分隧道）配置中，排除显式代理 FQDN 和 PAC 文件 FQDN。
   - 选择 **Workflows**（工作流） > **Prisma Access** 设置 > **GlobalProtect**。
   - 在 **GlobalProtect App**（**GlobalProtect** 应用程序）选项卡上，单击 **Default**（默认）以自定义隧道设置，或单击 **Add Tunnel Settings**（添加隧道设置）以添加新配置。
   - 在 **Exclude Traffic**（排除流量）下，单击 **Add Domain**（添加域名）。

 ©2025 Palo Alto Networks, Inc.



将图像中的 *FQDN* 替换为您的代理 *FQDN*。

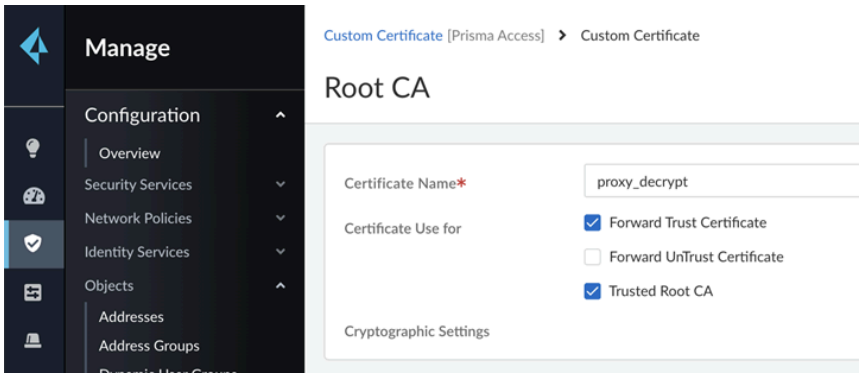
STEP 3 | 要启用始终在线的安全性，请在 **Workflows**（工作流） > **Prisma Access** 设置 > **GlobalProtect** > **GlobalProtect App**（**GlobalProtect** 应用程序） > **Add App Settings**（添加应用程序设置）页面上配置以下设置：

1. 将禁用 GlobalProtect 设置为 **Disallow**（不允许）、**Allow with Passcode**（使用密码允许）或 **Allow with Ticket**（具有支持工单时允许）。
2. 禁用允许用户从 GlobalProtect 应用程序注销。

 ©2025 Palo Alto Networks, Inc.

STEP 4 | 为显式代理流量配置解密策略。

- 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW** 和 > **Security Services**（安全服务） > **Decryption**（解密）。
- 如果启用解密，请确保将解密证书设置为受信任的根 CA。



STEP 5 | 为显式代理流量配置安全策略规则。

- 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW** 和 **Prisma Access** > **Security Services**（安全服务） > **Security Policy**（安全策略）。
- 遵循互联网网关安全策略最佳实践。

STEP 6 | （可选）在非默认路由网络中以代理和隧道模式配置 GlobalProtect 应用程序。

- （可选）在内部托管 PAC 文件并在 PAC 文件中将 Prisma Access 显式代理 FQDN 添加为代理，或者将 PAC 文件托管在转发配置文件中，并在网络中添加 PAC 服务 IP 地址的路由。
- 将门户和网关 FQDN 以及 IdP URL 的身份验证请求转发到互联网。
- 在外围设备上设置指向显式代理 FQDN 或 IP 地址的路由，以允许用户通过显式代理访问互联网。
- （可选）如果用户无法解析分支网络中的公共域，则添加 DNS 记录以将 Prisma Access 显式代理 FQDN 解析为内部 IP 地址，并将内部 IP 地址的目标 NAT 添加到显式代理 FQDN 或 IP 地址。
- 要使用户能够在办公室直接访问私有应用程序：
  - 直接访问：启用内部主机检测并保持内部网关列表为空。

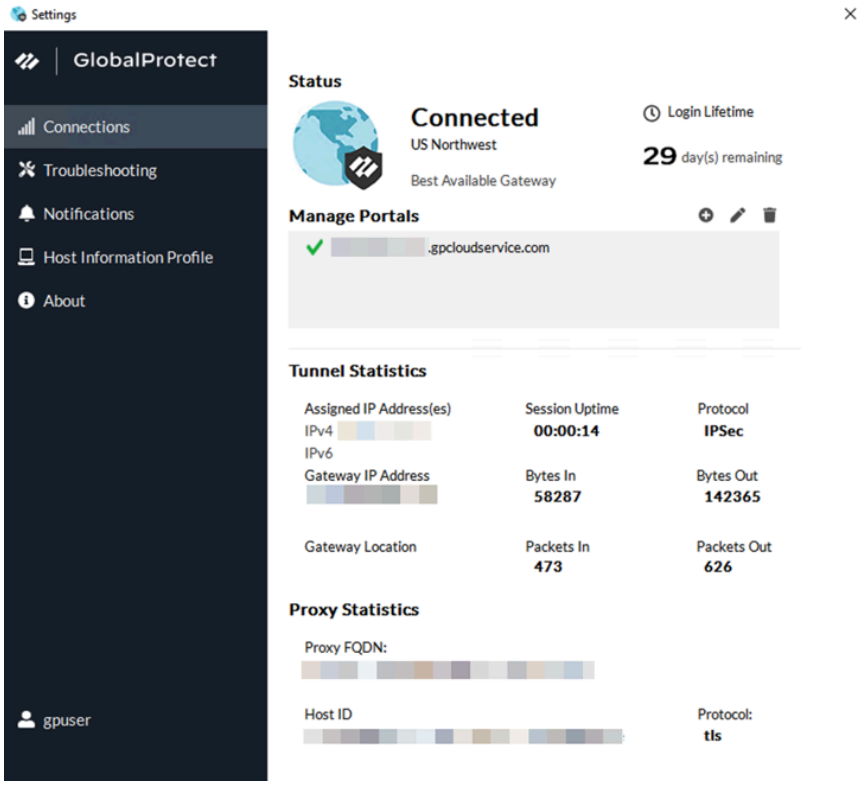
STEP 7 | 单击 **Save**（保存）并 **Push Config**（推送配置）到 **GlobalProtect** 和 **Explicit Proxy**（显式代理）。

 ©2025 Palo Alto Networks, Inc.

STEP 8 | 验证客户端代理部署并排除故障。

1. 在 GlobalProtect 应用程序 **Settings**（设置）下的 **Connections**（连接）选项卡上验证有关网络连接的信息。

   1. 打开 GlobalProtect 应用程序。
   2. 选择 **Settings**（设置）以打开 GlobalProtect 设置面板，然后选择 **Connections**（连接）。



2. 查看并收集 GlobalProtect 日志。

   查看 PangPS 日志，以验证 GlobalProtect 门户上的代理模式配置。

   可以通过在 PangPS 日志中查找以下事件来验证是否已配置代理模式：

   `OnProxyAgentMode`：混合模式

   要在 中查看 GlobalProtect 日志，请选择 **Incidents & Alerts**（事件和警报） > **Log Viewer**（日志查看器），并且选择：

   - **GlobalProtect**（用于身份验证日志）
   - **Traffic**（流量）和 **Decryption**（解密）（用于用户访问日志）

使用始终在线连接方法断开连接并禁用隧道和代理模式

从 GlobalProtect 版本 6.3.1 开始，当为 GlobalProtect 应用程序配置 **Tunnel and Proxy**（隧道和代理）模式以及 **Always-On**（始终在线）模式作为连接方法，并且想要断开隧道和代理模式时，必须执行以下步骤：

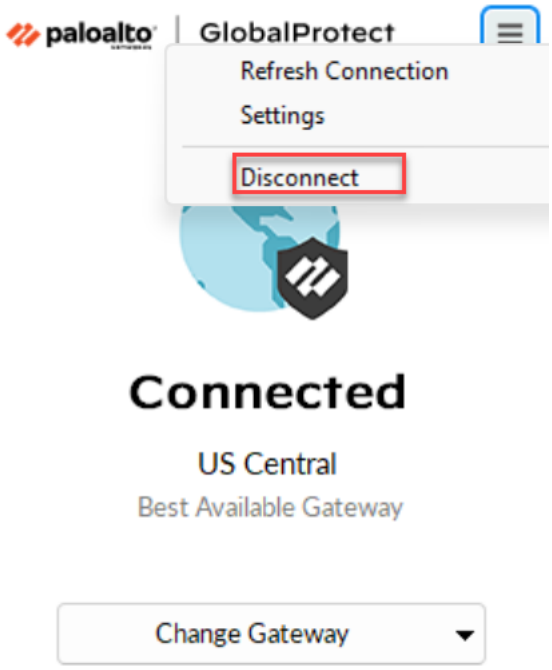
1. 断开 GlobalProtect 应用程序以断开隧道 (VPN) 连接。断开应用程序时，隧道 (VPN) 连接将断开，但该应用程序仍将通过代理模式连接。

 ©2025 Palo Alto Networks, Inc.

2. 禁用 GlobalProtect 应用程序以同时断开隧道和代理模式。禁用该应用程序时，隧道和代理模式都将断开连接，并且该应用程序将不再连接。

要断开连接并禁用配置了 **Tunnel and Proxy**（隧道和代理）（混合模式）和 **Always-On**（始终在线）连接方法的 GlobalProtect 应用程序，您必须：

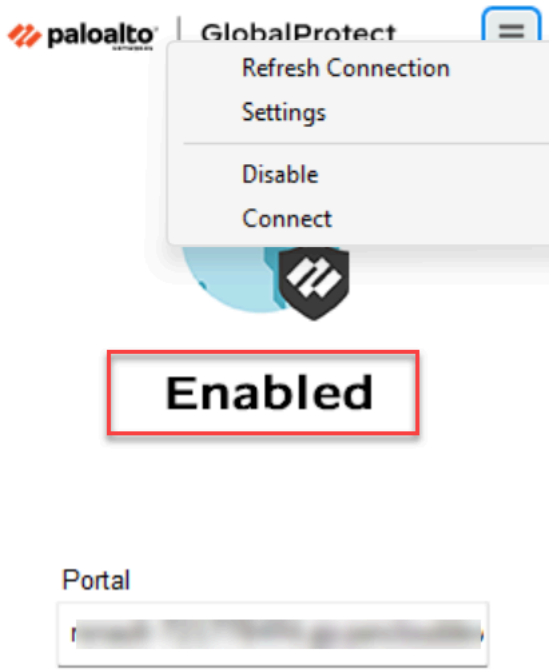
1. 使用汉堡菜单中的 **Disconnect**（断开连接）选项断开 GlobalProtect 应用程序的连接。断开该应用程序的连接时，隧道 (VPN) 连接也会断开。



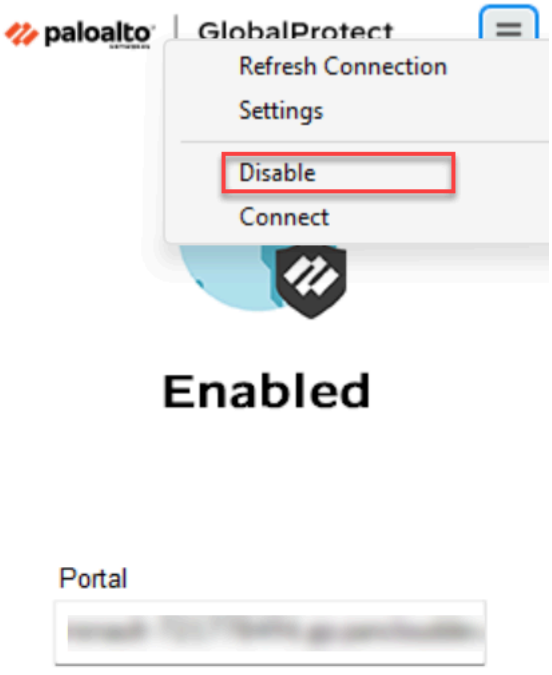
断开该应用程序后，VPN 连接将断开，但代理模式仍处于启用状态。该应用程序仍将通过代理模式连接，并且应用程序显示的状态为 **Enabled**（已启用）。

如果您想重新连接隧道 *(VPN)* 连接，可以使用汉堡菜单中的 ***Connect***（连接）选项。

©2025 Palo Alto Networks, Inc.

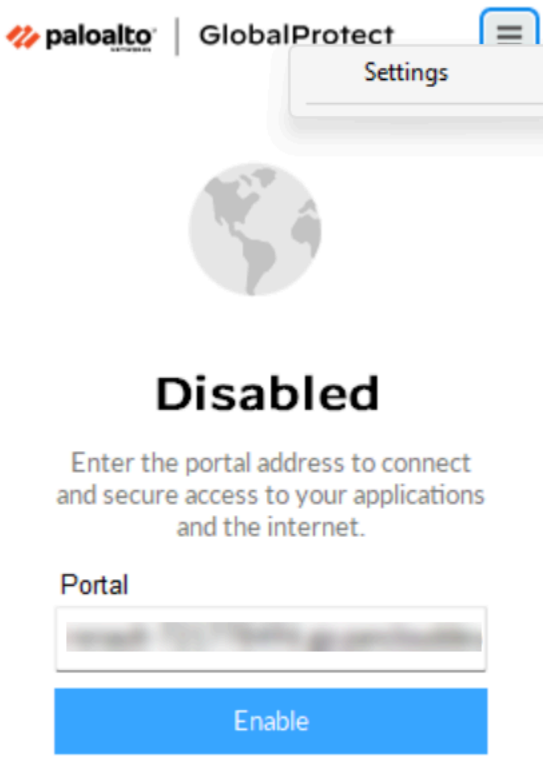


2. 使用汉堡菜单中的 **Disable**（禁用）选项禁用 GlobalProtect 应用程序。禁用该应用程序后，隧道和代理连接都会断开。



该应用程序将被禁用，并且显示的状态为 **Disabled**（已禁用）。

 ©2025 Palo Alto Networks, Inc.



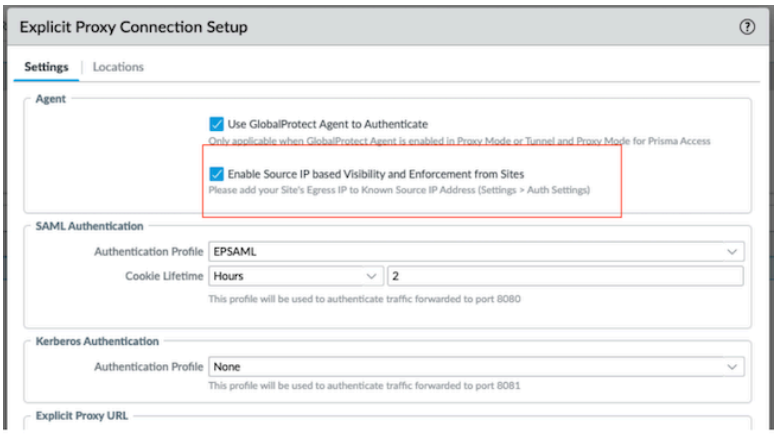
隧道和代理模式下的 GlobalProtect (Panorama)

如果将单租户 *Prisma Access (Managed by Panorama)* 部署转换为多租户，则只有第一个租户（您迁移的租户）支持此功能。此外，在第一个租户中，您必须在预定义的 *Explicit_Proxy_Device_Group* 中设置策略规则，而不是在自定义设备组中设置策略规则。在第一个租户之后为多租户部署创建的任何后续租户均不支持此功能。

©2025 Palo Alto Networks, Inc.

STEP 1 | 为移动用户启用基于客户端的代理功能。

1. 启用显式代理。
   1. 选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Mobile Users**—**Explicit Proxy**（移动用户—显式代理）。
   2. **Configure**（配置）显式代理设置以指定 **Explicit Proxy URL**（显式代理 **URL**）。
2. 选择 **Use GlobalProtect app to Authenticate**（使用 **GlobalProtect** 应用程序进行身份验证），以启用基于客户端的代理功能，也可以选择 **Enable Source IP based Visibility and Enforcement from Sites**（从站点启用基于源 **IP** 的可见性和和强制执行）。



3. 输入 **PAC (Proxy Auto-Configuration) File**（**PAC**（代理自动配置）文件） URL。确保在 PAC 文件中输入端口 8080。
   - PAC 文件中的代理语句必须使用您在上方配置的 Prisma Access FQDN。
   - 必须配置 PAC 文件以排除 GlobalProtect 网关 (*.gp.gpcoudservice.com)。
4. 为您配置的显式代理设置选择 **Connection Name**（连接名称）。
5. 选择要为移动用户部署显式代理的 **Locations**（地点）和区域。

   Prisma Access 会将代理节点添加到您选择的每个地点。显式代理支持所有 Prisma Access 地点的子集。为了获得最佳用户体验，如果要限制地点数量，请选择离最终用户最近的地点。如果某个地点在您的移动用户居住的国家/地区不可用，请选择离该移动用户最近的地点。

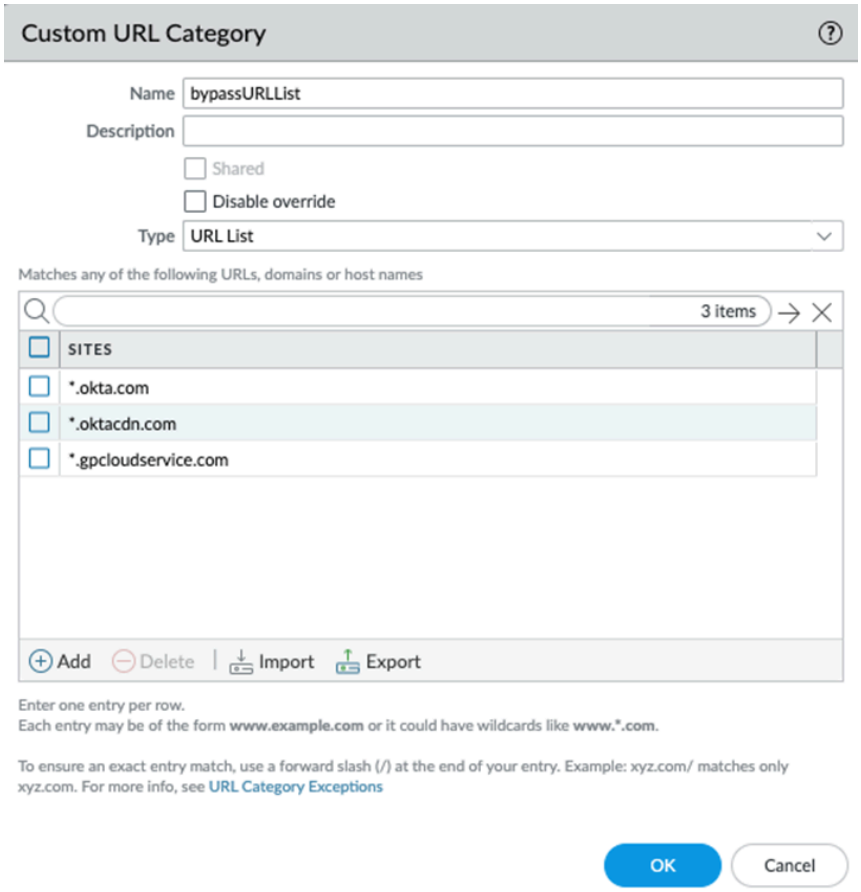
©2025 Palo Alto Networks, Inc.

STEP 2 | 绕过身份提供程序 (IDP)。

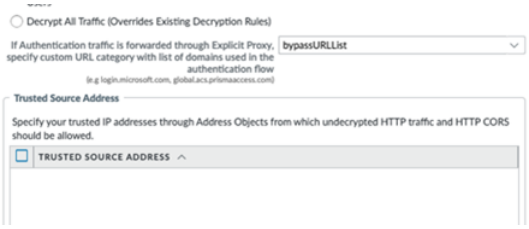
向代理提出的请求都经过身份验证。但是，如果您通过代理传递 IDP 流程，则需要绕过 IDP 才能成功进行身份验证。

在此示例中，我们将绕过 GlobalProtect 门户和 Okta，但请根据您使用的 IDP 对其进行自定义。

1. 选择 **Explicit_Proxy_Device_Group** 后，选择 **Object**（对象） > **Custom Objects**（自定义对象） > **URL Category**（**URL** 类别），然后创建自定义 URL 类别。
2. 在自定义 URL 类别中，添加需要绕过 EP 身份验证的所有 FQDN 域名。



3. 选择 **Cloud Services**（云服务） > **Configuration**（配置） > **Mobile Users**（移动用户） > **Explicit Proxy**（显式代理） > **Settings**（设置） > **Authentication Settings**（身份验证设置），并附加自定义 URL 类别。



4. 提交并推送到 **Explicit_Proxy_Device_Group**。

 ©2025 Palo Alto Networks, Inc.

STEP 3 | 配置 GlobalProtect 门户。

在隧道和代理模式下，您设置的连接方法仅适用于通过 *GlobalProtect* 隧道传输的流量。基于客户端的代理功能将提供始终在线的互联网安全性。即使您设置了按需连接方法，当用户断开 *GlobalProtect* 应用程序的连接时，所有互联网绑定流量仍将通过代理进行传输，以确保始终在线的互联网安全性。

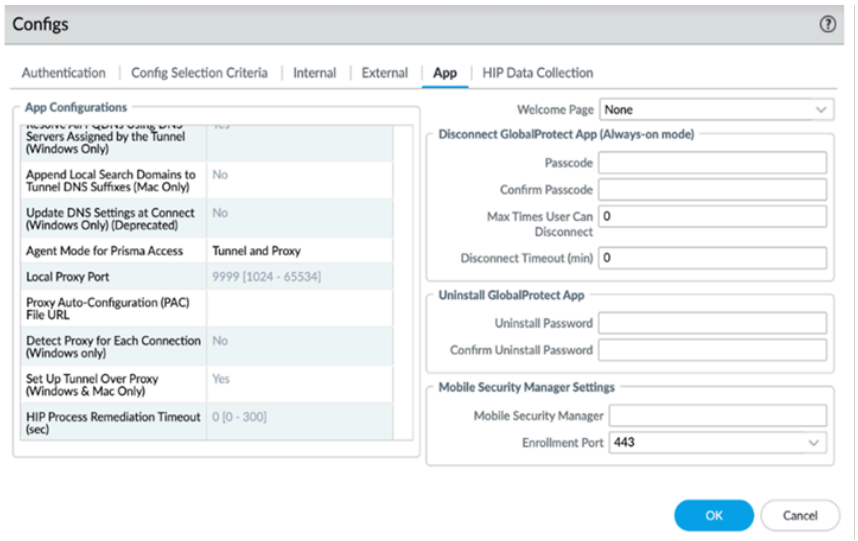
1. 在“加入”部分中，单击 **Configure**（配置）。
2. 在 **General**（常规）选项卡上，指定 **Portal Name Type**（门户名称类型）：

   Use Default Domain（使用默认域）— 如果选择此选项，则门户主机名将使用默认域名：.gpcloudservice.com。在这种情况下，只需输入门户主机名以附加到默认域名即可。Prisma Access 将自动创建必要的证书并将主机名发布到公共 DNS 服务器。

   Use Company Domain（使用公司域）— 如果您希望门户主机名中的域名与您的公司域名相匹配（例如，myportal.mydomain.com），请选择此选项。
3. 选择一个用于指定 Prisma Access 应如何对移动用户进行身份验证的 **Authentication Profile**（身份验证配置文件），或创建一个新的配置文件。
4. （可选）选择 **Authentication Override Certificate**（身份验证覆盖证书），以加密移动用户用于向门户和网关进行身份验证的安全 Cookie。
   1. 在 GlobalProtect 上启用隧道和代理模式。
      1. 选择 **Network**（网络） > **GlobalProtect Portals**（**GlobalProtect** 门户）。
      2. 选择正向其添加代理配置的门户配置，然后选择 **Agent**（代理）选项卡。
      3. 在 **Agent**（客户端）选项卡上，选择 **App**（应用程序）。
      4. 在 App Configurations（应用配置）区域中，将 **Agent Mode for Prisma Access**（**Prisma Access** 的客户端模式）设置为 **Tunnel and Proxy**（隧道和代理），

 ©2025 Palo Alto Networks, Inc.

以将互联网流量发送到 Prisma Access 显式代理，并将私有应用程序流量发送到 VPN。



2. 执行可选配置。
   1. （可选）配置本地代理端口。端口范围为 1024 到 65534，默认端口为 9999。如果默认端口不可用，GlobalProtect 将尝试连接 9999 到 10009 范围内的其他 10 个端口，并使用可用的端口。您也可以在该范围内选择自己的端口号。
   2. （可选）如果要将代理设置的自定义 PAC URL 推送到端点，请配置 PAC 自动配置 (PAC) 文件 URL。用户连接后，PAC URL 会推送到端点。当用户断开 GlobalProtect 应用程序的连接时，端点代理配置将自动禁用并恢复为之前的设置。
   3. （可选）如果希望用户检查门户是否有任何新设置，请启用允许用户重新发现网络。
   4. （可选）配置 GlobalProtect 应用程序配置刷新间隔（小时）。默认情况下，GlobalProtect 客户端每 24 小时刷新一次缓存的门户配置。您可以根据业务需求更改刷新间隔。
3. 在拆分隧道配置中，排除显式代理 FQDN 和 PAC 文件 FQDN。

STEP 4 | 通过配置以下设置启用始终在线的互联网安全性：

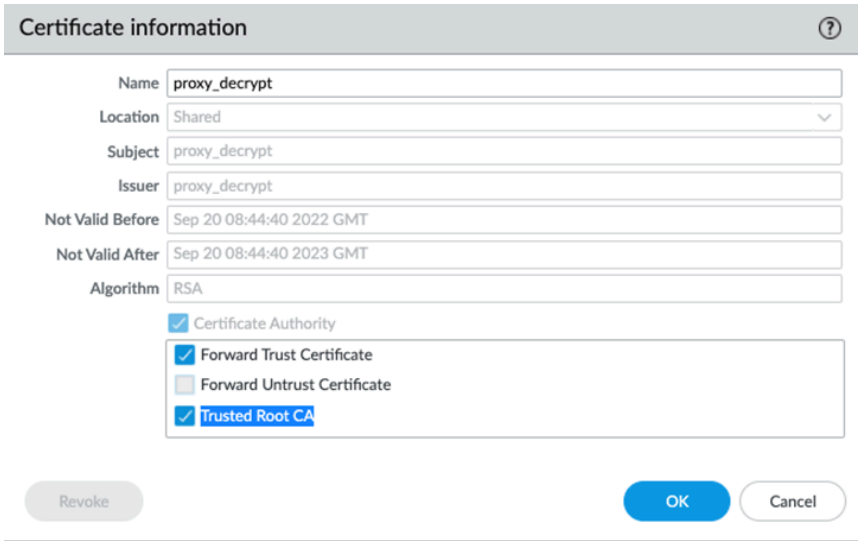
1. 将允许用户禁用 GlobalProtect 设置为 **Disallow**（不允许）、**Allow with Passcode**（使用密码允许）或 **Allow with Ticket**（具有支持工单时允许）。
2. 将允许用户从 GlobalProtect 应用程序注销设置为 **No**（否）。

©2025 Palo Alto Networks, Inc.

STEP 5 | （可选）为显式代理流量配置解密策略。

如果启用解密，请确保解密证书也设置为可信的根 CA。

1. 选择 **Device**（设备） > **Certificate Management**（证书管理） > **Certificates**（证书），并创建可信的根 CA 证书和转发信任证书。



2. 在 **Explicit_Proxy_Device Group** 组下创建具有 SSL 转发代理的解密规则。

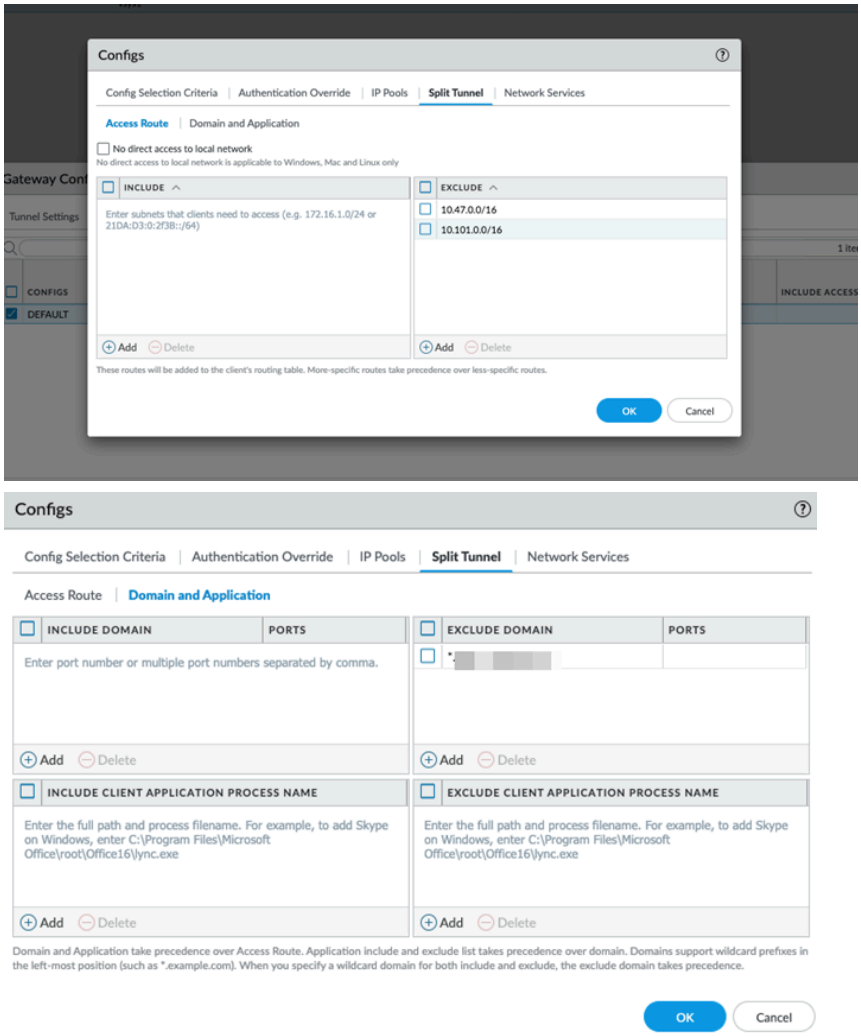
STEP 6 | 为显式代理流量配置安全策略规则。

- 选择 **Manage**（管理） > **Security Services**（安全服务） > **Security Policy**（安全策略） > 。
- 遵循互联网网关安全策略最佳实践。

 ©2025 Palo Alto Networks, Inc.

STEP 7 | 在 Panorama 上配置拆分隧道。

1. 选择 **Network**（网络） > **Mobile User Template**（移动用户模板） > **Gateways**（网关） > **GlobalProtect_ExternalGateway** > **Agent**（客户端） > **Client Settings**（客户端设置） > **Split**（拆分）。
2. 根据路由和域配置隧道。



 ©2025 Palo Alto Networks, Inc.

STEP 8 | （可选）在非默认路由网络中以隧道和代理模式配置 GlobalProtect 应用程序。

- （可选）在内部托管 PAC 文件并在 PAC 文件中将 Prisma Access 显式代理 FQDN 添加为代理，或者将 PAC 文件托管在转发配置文件中，并在网络中添加 PAC 服务 IP 地址的路由。
- 验证 GlobalProtect 门户 URL 和 IDP URL 是否转发到 Prisma Access 显式代理。
- 在外围设备上设置指向显式代理 FQDN 或 IP 地址的路由，以允许用户通过显式代理访问互联网。
- （可选）如果用户无法解析分支网络中的公共域，则添加 DNS 记录以将 Prisma Access 显式代理 FQDN 解析为内部 IP 地址，并将内部 IP 地址的目标 NAT 添加到显式代理 FQDN 或 IP 地址。
- 要使用户能够在办公室直接访问私有应用程序：
  - 直接访问 — 启用内部主机检测并保持内部网关列表为空。

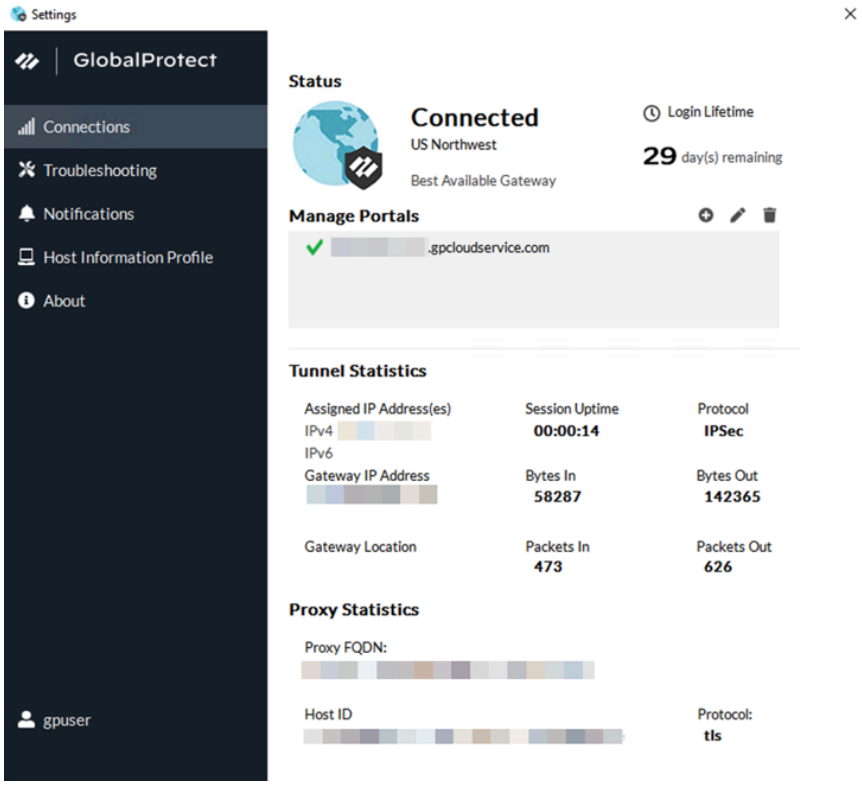
STEP 9 | 将更改 **Commit**（提交）到 Panorama，将配置更改 **Commit and Push**（提交并推送）给 Prisma Access **Mobile Users**（移动用户）和 **Explicit Proxy**（显式代理）。

 ©2025 Palo Alto Networks, Inc.

STEP 10 | 验证客户端代理部署并排除故障。

1. 在 GlobalProtect 应用程序 **Settings**（设置）下的 **Connections**（连接）选项卡上验证有关网络连接的信息。

   1. 打开 GlobalProtect 应用程序。
   2. 选择 **Settings**（设置）以打开 GlobalProtect 设置面板，然后选择 **Connections**（连接）。



2. 查看并收集 GlobalProtect 日志

   查看 PangPS 日志，以验证 GlobalProtect 门户上的代理模式配置。

   可以通过在 PangPS 日志中查找以下事件来验证是否已配置代理模式：

   `OnProxyAgentMode`：混合模式

   要在 Panorama 中查看 GlobalProtect 日志，请选择 **Monitor**（监控） > **Logs**（日志）和：

   - **GlobalProtect**（用于身份验证日志）
   - **Traffic**（流量）和 **Decryption**（解密）（用于用户访问日志）

使用始终在线连接方法断开连接并禁用隧道和代理模式

从 GlobalProtect 版本 6.3.1 开始，当为 GlobalProtect 应用程序配置 **Tunnel and Proxy**（隧道和代理）模式以及 **Always-On**（始终在线）模式作为连接方法，并且想要断开隧道和代理模式时，必须执行以下步骤：

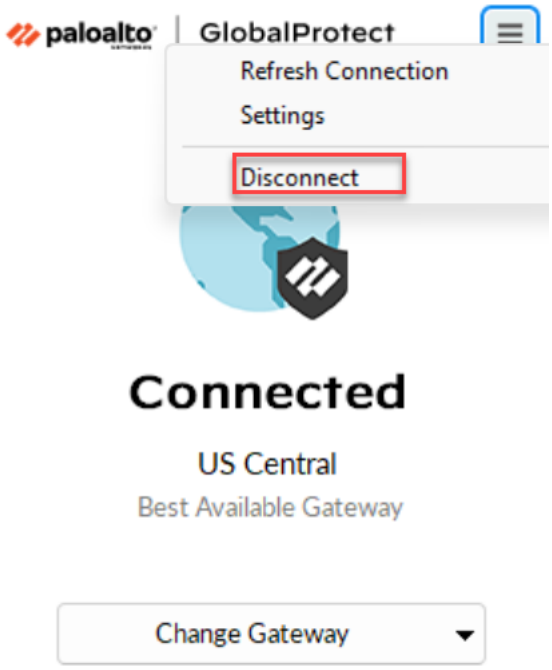
1. 断开 GlobalProtect 应用程序以断开隧道 (VPN) 连接。断开应用程序时，隧道 (VPN) 连接将断开，但该应用程序仍将通过代理模式连接。

 ©2025 Palo Alto Networks, Inc.

2. 禁用 GlobalProtect 应用程序以同时断开隧道和代理模式。禁用该应用程序时，隧道和代理模式都将断开连接，并且该应用程序将不再连接。

要断开连接并禁用配置了 **Tunnel and Proxy**（隧道和代理）（混合模式）和 **Always-On**（始终在线）连接方法的 GlobalProtect 应用程序，您必须：

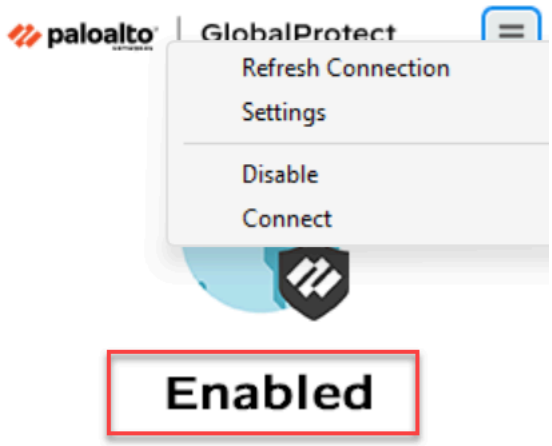
1. 使用汉堡菜单中的 **Disconnect**（断开连接）选项断开 GlobalProtect 应用程序的连接。断开该应用程序的连接时，隧道 (VPN) 连接也会断开。

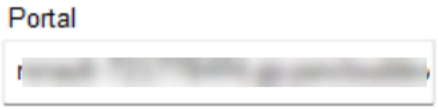


断开该应用程序后，VPN 连接将断开，但代理模式仍处于启用状态。该应用程序仍将通过代理模式连接，并且应用程序显示的状态为 **Enabled**（已启用）。

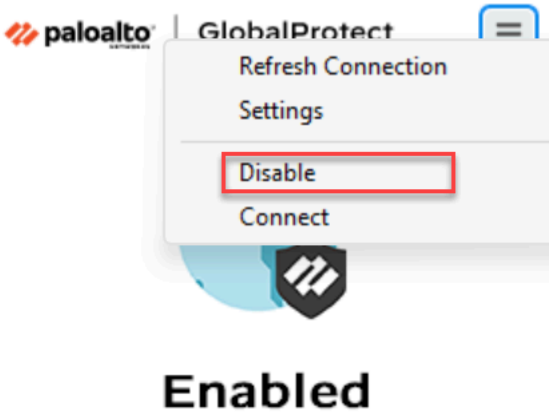
如果您想重新连接隧道 *(VPN)* 连接，可以使用汉堡菜单中的 ***Connect***（连接）选项。

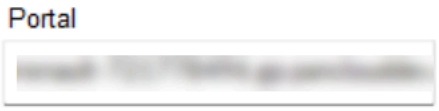
©2025 Palo Alto Networks, Inc.





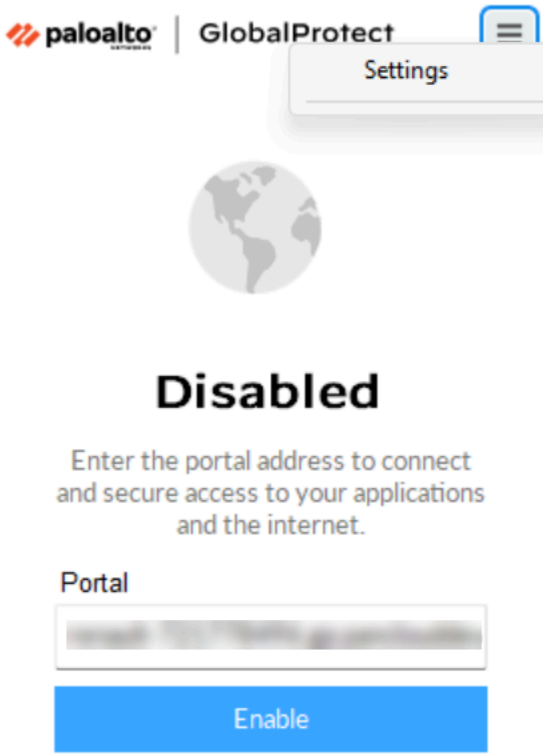
2. 使用汉堡菜单中的 **Disable**（禁用）选项禁用 GlobalProtect 应用程序。禁用该应用程序后，隧道和代理连接都会断开。





该应用程序将被禁用，并且显示的状态为 **Disabled**（已禁用）。

 ©2025 Palo Alto Networks, Inc.



基于代理的代理流量的专用 IP 地址可见性和实施

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager)	• Prisma Access 5.2 • 适用于 Windows 或 macOS 的 GlobalProtect 应用程序版本 6.3.1 • Prisma Access 数据平面 10.2.4 • Prisma Access 移动用户许可证 • Panorama 插件版本 5.2.0

通过分支机构的 GlobalProtect 代理连接到 Prisma Access 显式代理的用户可以利用端点的专用 IP 地址进行日志记录或应用基于 IP 地址的强制执行。

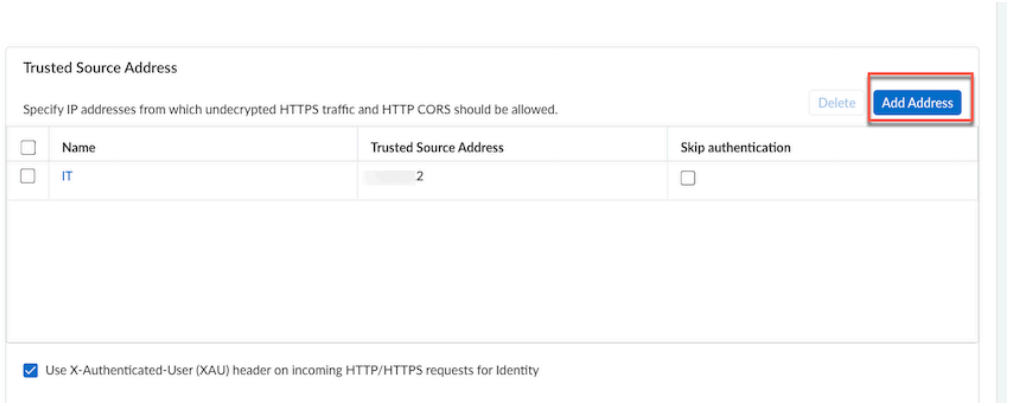
- Strata Cloud Manager
- Panorama

基于客户端的代理流量的专用 IP 地址可见性和强制执行 (Strata Cloud Manager)

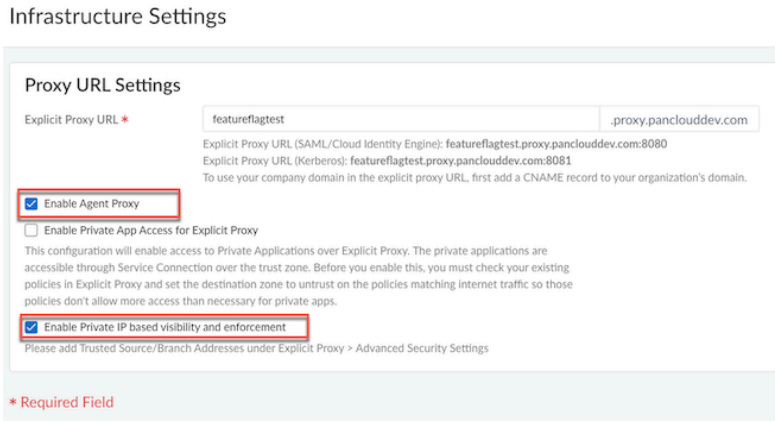
STEP 1 | 为移动用户启用基于客户端的代理功能（代理模式或隧道和代理模式）。

 ©2025 Palo Alto Networks, Inc.

STEP 2 | 导航到 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Explicit Proxy**（显式代理） > **Advanced Security Settings**（高级安全设置），然后单击设置图标。在 **Trusted Source Address**（可信源地址）下，添加分支传出 IP 地址。



STEP 3 | 导航到 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Explicit Proxy**（显式代理） > **Infrastructure Settings**（基础架构设置）。在 **Proxy URL Settings**（代理 **URL** 设置）下，启用 **Enable Source IP based visibility and enforcement**（启用基于源 **IP** 的可见性和强制执行），然后单击 **Save**（保存）。



STEP 4 | （可选）使用端点的源 IP 地址配置安全规则。

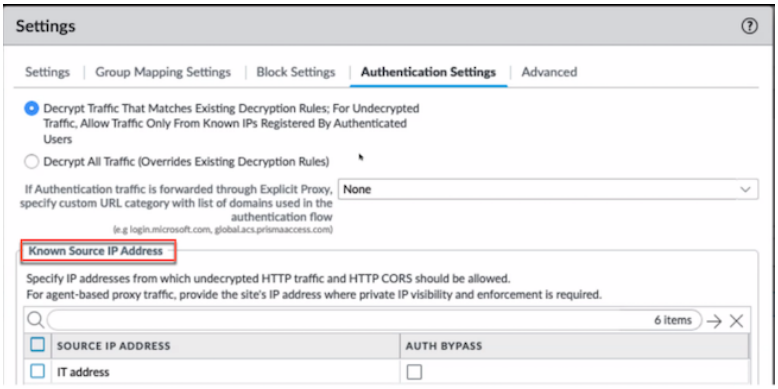
STEP 5 | **Push Config**（推送配置）到 **Explicit Proxy**（显式代理）。

基于客户端的代理流量的专用 IP 地址可见性和强制执行 (Panorama)

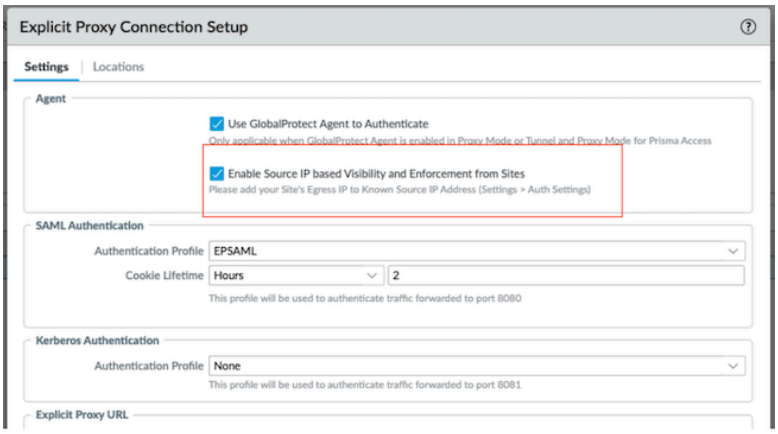
STEP 1 | 为移动用户启用基于客户端的代理功能（代理模式和隧道和代理模式）。

©2025 Palo Alto Networks, Inc.

STEP 2 | 导航到 **Cloud Services**（云服务） > **Configuration**（配置） > **Mobile Users**（移动用户） > **Explicit Proxy**（显式代理） > **Settings**（设置） > **Authentication Settings**（身份验证设置），在 **Known Source IP Address**（已知源 **IP** 地址）下添加分支传出 IP 地址。



STEP 3 | 导航到 **Cloud Services**（云服务） > **Configuration**（配置） > **Mobile Users-Explicit Proxy**（移动用户-显式代理）。在 **Agent**（客户端）下，启用 **Enable Source IP based Visibility and Enforcement from Sites**（从站点启用基于源 **IP** 的可见性和强制执行），然后单击 **OK**（确定）。



STEP 4 | （可选）使用端点的源 IP 地址配置安全规则。

STEP 5 | 提交并推送到 **Explicit_Proxy_Device_Group**。

用于显式代理的 SAML 身份验证

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	Prisma Access 许可证

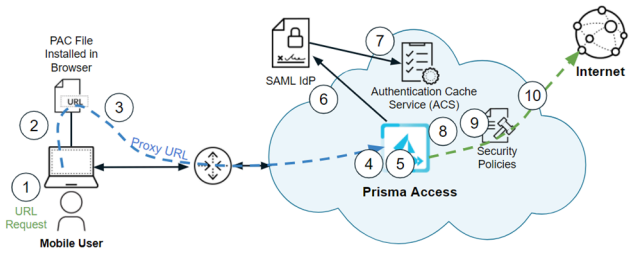
了解采用 SAML 的显式代理的工作方式以及如何配置 SAML。

- 采用 SAML 的显式代理如何处理流量
- 为显式代理配置 SAML

 ©2025 Palo Alto Networks, Inc.

采用 SAML 的显式代理如何处理流量

以下是采用 SAML 的显式代理的工作方式。请继续以查看流量的走向：



STEP 1 | 移动用户使用网络浏览器输入 URL 或 IP 地址，从而浏览互联网或访问 SaaS 应用程序。

STEP 2 | 移动用户端点上的浏览器检查 PAC 文件。

此 PAC 文件规定 URL 或 SaaS 请求应转到 Prisma Access 显式代理。

STEP 3 | HTTPS 客户端（移动用户端点上的浏览器）将 URL 请求转发到代理 URL。

STEP 4 | 流量重定向到显式代理，随后代理解密流量。

STEP 5 | 代理检查流量，并检查由 Prisma Access 显式代理设置的身份验证 Cookie。

该 Cookie 包含了可以识别移动用户的信息，并且使用 Cookie 来对用户进行身份验证。

STEP 6 | 如果在检查 Cookie 后，Prisma Access 判定用户未通过身份验证，则会将用户重定向至身份验证页面。

STEP 7 | IdP 对用户进行身份验证后，Prisma Access 会将用户的身份验证状态存储在身份验证缓存服务 (ACS) 中。身份验证的有效期取决于在显式代理配置期间您为 **Cookie Lifetime**（**Cookie** 生命周期）指定的值。

STEP 8 | 显式代理检查 Cookie 是否存在以及是否有效。如果 Cookie 不存在或无效，则用户将被重定向到 ACS。在 ACS 确认用户的身份验证后，用户将被重定向回采用令牌的显式代理。然后，代理验证该令牌，并为该用户设置该域的 Cookie。

STEP 9 | Prisma Access 根据管理员配置的安全策略规则来应用安全实施。

STEP 10 | 如果该 URL 未被安全策略规则阻止，则 Prisma Access 会将 URL 请求发送到互联网。

STEP 11 | （可选）配置 GlobalProtect 中的显式代理连接以实现始终开启的互联网安全防护。启用此功能可实现互联网流量的始终安全，同时通过 GlobalProtect 或第三方 VPN 提供对私人应用程序的按需访问。

为显式代理配置 SAML

按照以下步骤为显式代理配置 SAML 身份验证。

- Strata Cloud Manager
- Panorama

©2025 Palo Alto Networks, Inc.

使用 SAML 配置显式代理 (Strata Cloud Manager)

STEP 1 | 设置显式代理。

STEP 2 | （可选）配置 Cloud Identity Engine 显式代理身份验证。

STEP 3 | 配置安全策略规则。

1. 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Configuration Scope:Explicit Proxy**（配置范围：显式代理） > **Security Services**（安全服务） > **Security Policy**（安全策略）。
2. 根据您的需求和互联网网关安全策略最佳实践自定义默认策略规则。

   使用 *Prisma Access 5.1* 和 *PAN-OS 10.2.10* 或更高版本的数据平面，您只需要 ***Allow Web Access to Known Users***（允许已知用户进行 ***Web*** 访问）安全策略规则。

STEP 4 | 推送配置更改。

使用 SAML 配置显式代理 (Panorama)

STEP 1 | 设置显式代理。

STEP 2 | （可选）配置 Cloud Identity Engine 显式代理身份验证。

STEP 3 | 根据您的 Prisma Access 版本和数据平面版本，配置一个或多个策略规则。

版本要求	配置

Prisma Access 5.1 或更高版本以及 PAN-OS 10.2.10 或更高版本的数据平面。	为预先身份验证用户流量配置安全策略规则。
	1. 选择 **Explicit_Proxy_Device_Group**。
	2. 使用 **Web App**（**Web** 应用程序）标签创建应用程序筛选器
	3. 选择 **Policies**（策略） > **Pre Rules**（预规则） > **Add**（添加）。
	4. 创建规则。
	   1. **Add**（添加）规则。
	   2. 提供描述性名称。
	      例如，**`allow-pre-auth`**
	   3. 在 **Application**（应用程序）选项卡下，**Add**（添加）**Web App**（**Web** 应用程序）应用程序筛选器。
	   4. 在 **Source**（源）选项卡下，**Add**（添加）**known-user**（已知用户）。

©2025 Palo Alto Networks, Inc.

版本要求	配置
所有其他 Prisma Access 和数据平面版本。	根据您的需求和互联网网关安全策略最佳实践配置安全策略规则。

STEP 4 | **Commit**（提交）配置。

设置 Explicit Proxy

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) 如果您想在 Explicit Proxy 上启用基于私有源 IP 的可见性和实施 Prisma Access 环境中，请与您的客户团队联系以了解更多信息。	• Prisma Access 许可证

使用 Explicit Proxy 通过将浏览器流量重定向到 Prisma Access.

载入指南- 在许可和载入 Explicit Proxy 部署时，请遵循以下准则：

- 显式代理支持 的子集 Prisma Access 地点。
- 您不能添加用两个星号表示的位置;这些是 Local Zones，不受 Prisma Access.
- 如果您拥有 Local 或 Evaluating 许可证 Prisma Access 对于用户，并且您有一个移动用户 - GlobalProtect 部署以及一个移动用户 - 显式代理部署，则最多可以为每个部署五个位置（移动用户最多五个位置 - GlobalProtect，移动用户最多五个位置 - 显式代理）。如果您拥有 Worldwide 许可证，则最大位置数没有限制。
- Explicit Proxy 在以下情况下支持多租户：如果您有现有的 Prisma Access 非多租户部署和 将其转换为多租户部署，则只有第一个租户（您迁移的租户）支持显式代理。在第一个租户部署之后为多租户部署创建的任何后续租户都不支持显式代理。
- 在载入 Explicit Proxy 部署时，Palo Alto Networks 建议在单个浏览器中执行所有配置。但是，您可以从多个浏览器或浏览器会话添加安全策略。
- 的 URL 过滤操作 继续 或 覆盖 不受支持，并且不能与 Explicit Proxy 一起使用。

了解如何设置 Explicit Proxy。

- Strata Cloud Manager
- Panorama

Cloud Management

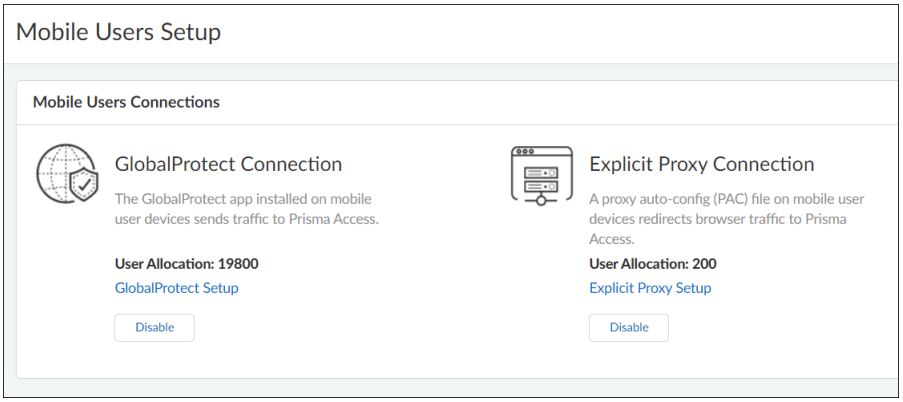
为移动用户设置显式代理连接；使用显式代理，移动用户设备上的代理自动配置 (PAC) 文件会将浏览器流量重定向到 Prisma Access。

在开始之前，请务必查看明确的代理 指南。

©2025 Palo Alto Networks, Inc.

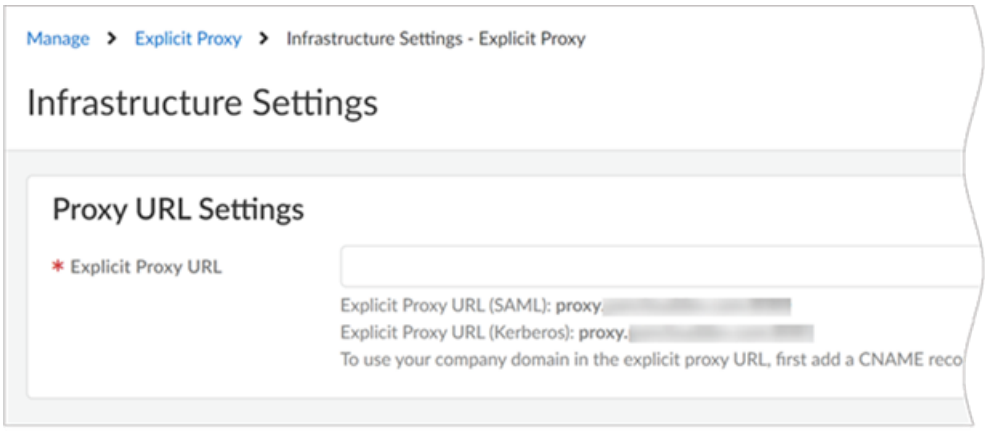
STEP 1 | 启用显式代理并分配用户

转至 工作流程 > **Prisma Access** 设置 > 移动用户 开始设置显式代理。当您启用显式代理时，系统将提示您指定将使用此连接类型的移动用户数量。



STEP 2 | 添加移动用户将用来连接的代理设置 **Prisma Access**

转到 **Infrastructure Settings**（基础架构设置）：



1. 指定显式代理 URL。

   默认情况下，名称为 *proxyname*.proxy.prismaaccess.com，其中 *proxyname* 是您指定的子域，并使用端口 8080。要在显式代理 URL 中使用您的公司域名，请先向您的组织域名添加 CNAME 记录。

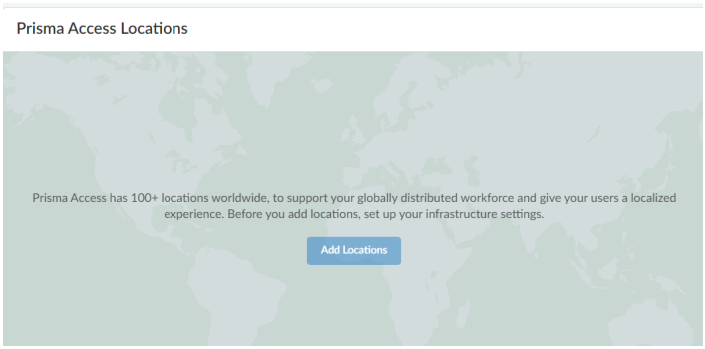
   您可以使用 SAML 或 Kerberos 身份验证类型来验证移动用户。
2. （可选）选择 启用代理 以启用基于代理的代理功能。

   启用此功能可在 代理模式 或 隧道和代理模式下设置显式代理。
3. 使用转发规则 来创作符合您要求的 PAC 文件或 将您自己的 PAC 文件上传到转发配置文件。

 ©2025 Palo Alto Networks, Inc.

STEP 3 | 选择 **Prisma Access** 您的移动用户将连接的位置

添加 Prisma Access 您想要支持移动用户的位置。



地图显示 Prisma Access位置。

如果要限制位置数量，请选择离用户最近或与用户位于同一国家/地区的位置，以提供最佳用户体验。如果某个位置在您的移动用户居住的国家/地区不可用，请选择离用户最近的位置以提供最佳性能。

您应该至少在两个区域启用显式代理位置以确保区域冗余。

STEP 4 | 对移动用户进行身份验证。

设置 **User Authentication**（用户身份验证），以便只有合法用户才能访问您的服务和应用程序。

SAML 和 Kerberos 是受支持的身份验证协议。 Prisma Access 支持 PingOne、Azure AD 和 Okta 作为 SAML 身份验证提供程序，但您应该能够使用任何支持 SAML 2.0 作为 SAML 身份提供程序 (IdP) 的供应商。了解有关如何 让移动用户验证 Prisma Access 的更多信息。

STEP 5 | 查看默认启用的最佳实践安全规则

Prisma Access 默认执行最佳实践的安全策略规则。这些规则允许您的用户安全地浏览一般互联网网站。用户是：

- 根据 URL 阻止访问已知恶意网站
- 禁止上传或下载已知恶意的文件
- 防范未知、前所未见的威胁
- 防范病毒、间谍软件（命令和控制攻击）和漏洞

完成初始设置后，您可以查看并更新这些默认规则以满足您的企业需求。

STEP 6 | 验证移动用户位置是否有效

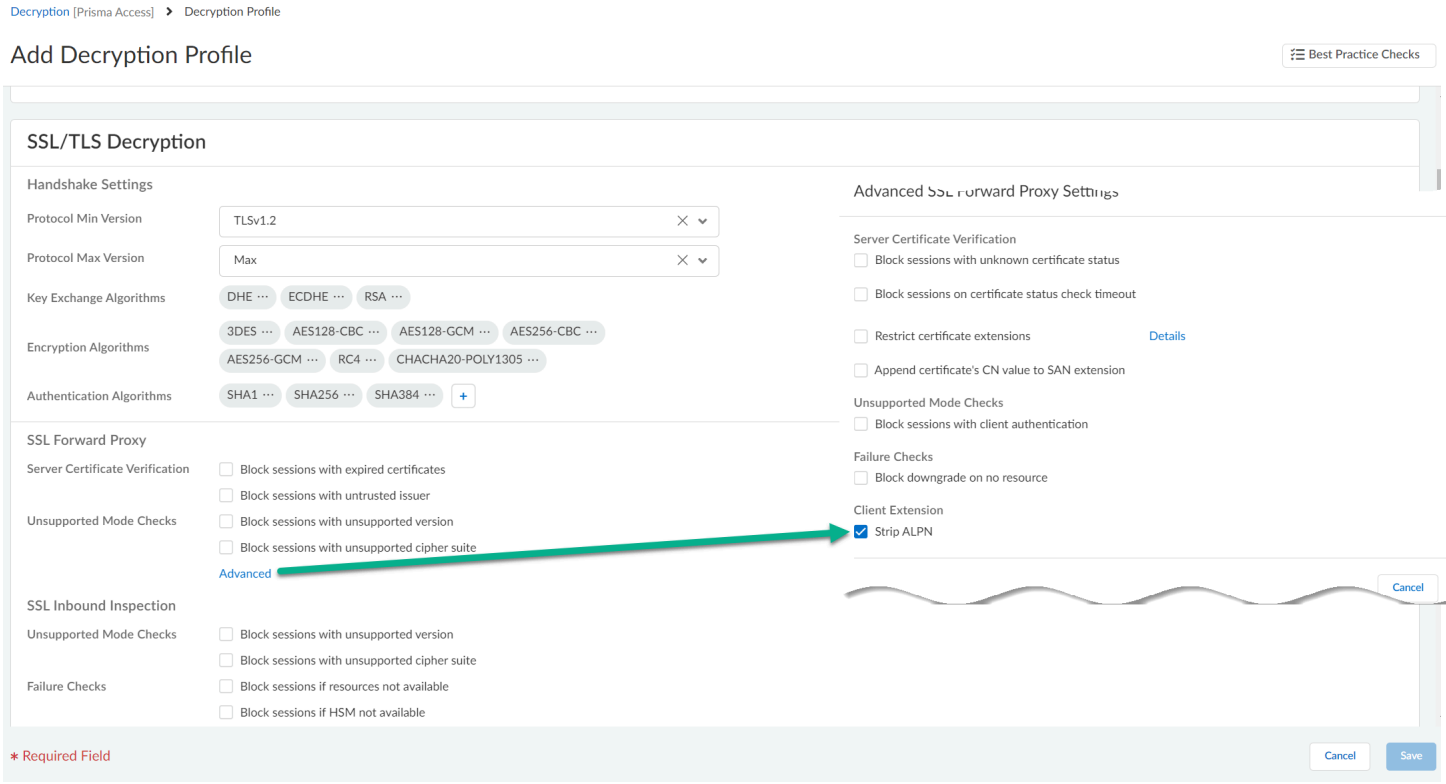
将初始配置推送到 Prisma Access，Prisma Access 开始配置您的移动用户环境。这可能需要最多 15 分钟。当您的移动用户位置启动并运行时，您将能够在“移动用户”设置页面、“概述”以及“见解”中验证。

您还可以通过选择“管理 > 服务设置 > 移动用户” 并“编辑基础设施设置”来验证您的设置，以确认在您配置的每个位置都设置了网关。

©2025 Palo Alto Networks, Inc.

STEP 7 | 启用显式代理流量解密

- 将支持的最高 TLS 版本设置为 1.2。
- 设置 **Strip ALPN**（高级 SSL 正向代理设置），因为显式代理不支持本机 HTTP/2，并且您必须删除 ALPN 标头。



STEP 8 | 下载 根 CA 并将其安装到您的端点上以进行 SSL 解密。

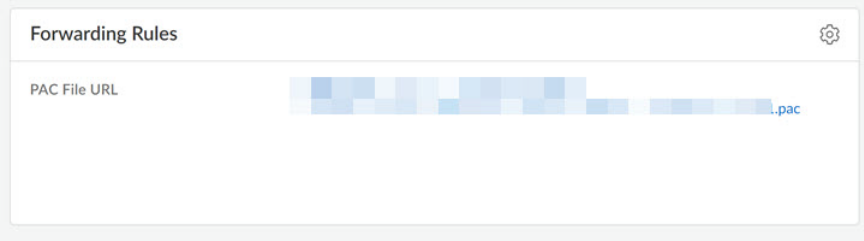
©2025 Palo Alto Networks, Inc.

STEP 9 | 编辑**PAC**文件内容。

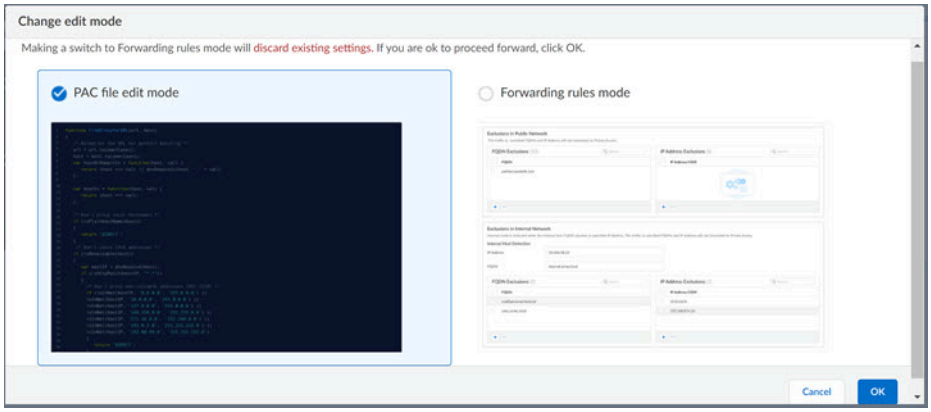
使用 转发配置文件 管理 *PAC* 文件。

编辑代理自动配置 (PAC) 文件，以获得符合您要求的显式代理。GlobalProtect 应用程序代理流量到 Prisma Access 基于 PAC 文件中的转发规则和逻辑。

转到 转发规则：



1. 下载 PAC 文件并对其 进行自定义，以便满足您的需求。然后，再次将其导入到此处，我们将向您提供 Prisma Access 托管的 PAC 文件所在地点的 URL。
2. 使用 **PAC** 文件编辑器 模式或 转发规则模式编辑 PAC 文件。
3. 默认选择 **PAC** 文件编辑器 模式。单击“确定”即可在PAC文件编辑模式下进行编辑。
4. 选择 转发规则模式，点击 确定，即可在转发规则模式下进行编辑。切换到转发规则模式会丢弃现有设置。



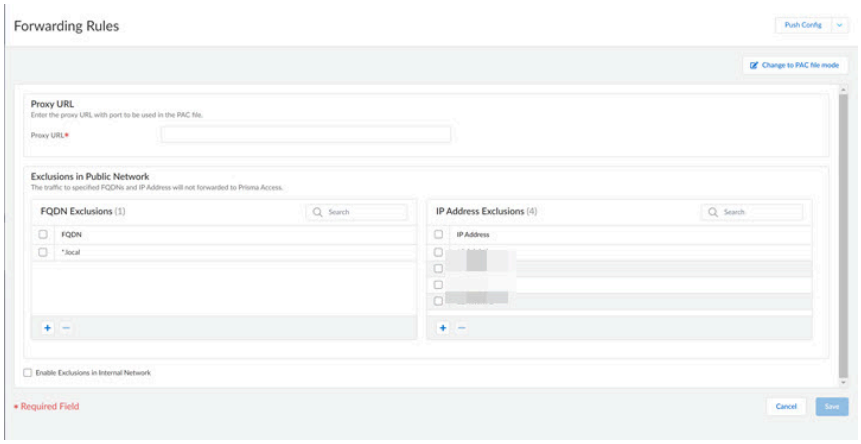
- 输入一个显式 **Proxy URL**（代理 **URL**）以及要在 PAC 文件中使用的端口。

  默认情况下，名称为 proxyname.proxy.prismaaccess.com，其中 proxyname 是您指定的子域，并使用端口 8080。
- 当您的显式代理移动用户从公共网络连接到 Prisma Access 时，在公共 网络中配置排除项 。
  - 配置 **FQDN** 排除 和 **IP** 地址排除。排除的 FQDN 和 IP 地址不会从 Prisma Access。
- 启用内部网络中的排除项，以在显式代理移动设备用户连接到时配置特定 IP 地址或 FQDN 的排除项 Prisma Access 在内部网络上。
  - 指定以下排除项，以便在用户在内部网络上时排除不同的流量。
    - 输入仅可从内部网络解析的主机的 **IP Address**（**IP** 地址）。

©2025 Palo Alto Networks, Inc.

- 输入解析为您输入的 IP 地址的 **FQDN**。
- 为特定的 FQDN 和 IP 地址配置排除项。到指定 FQDN 和 IP 地址的流量将不会从 Prisma Access。

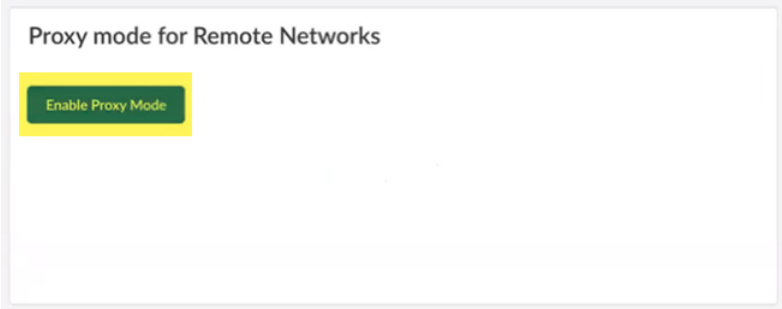
- **Save**（保存）更改。



 ©2025 Palo Alto Networks, Inc.

STEP 10 | 配置 **Advanced Security Settings**（高级安全设置）。

- 如果您想通过安全的 IPSec 隧道将流量从分支机构转发到显式代理， 请启用代理模式 并检索任播 IP 地址（如果您想将 显式代理与 Prisma Access 远程网络结合使用）。

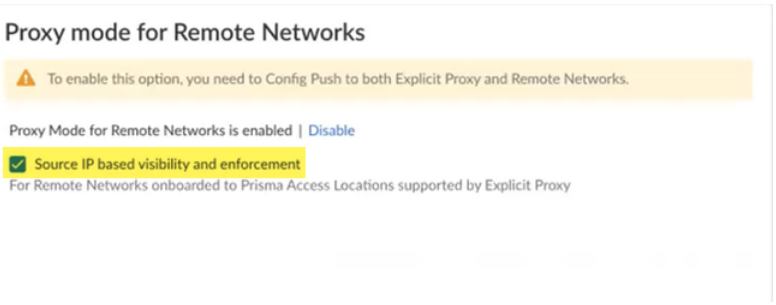


  该解决方案使用带有远程网络 IPSec 隧道的任播地址，以允许远程网络站点或分支位置的用户和设备使用显式代理。

- 仅代理模式部署 如果 您的远程网络上启用了代理模式，则添加策略以允许绑定到远程网络上的任播和单播 IP 的流量。如果您已启用 源 **IP** 可见性和强制执行，请使用显式代理中的安全策略中 的源 **IP** 字段来保护流量。您需要在远程网络中制定额外的策略。
- （可选）如果启用代理模式，则要利用分支机构中将流量转发到显式代理的系统的私有 IP 地址，请选择 基于源 **IP** 的可见性和实施。

  此功能具有以下要求：

  - Prisma Access 数据平面的最低版本 10.2.4
  - 一个 Prisma Access (Managed by Panorama) 部署时云服务插件版本至少为 4.1
  - 源 IP 地址仅显示 支持显式代理的远程网络位置。



- 指定 块源。

  将任何应阻止的源 IP 地址流量添加到 阻止源地址 列表中。

  指定地址、地址组或 EDL。

  要从强制执行中排除 IP 地址列表条目， 请添加例外 并选择要排除在阻止之外的 IP 地址。
- 指定 阻止的域。

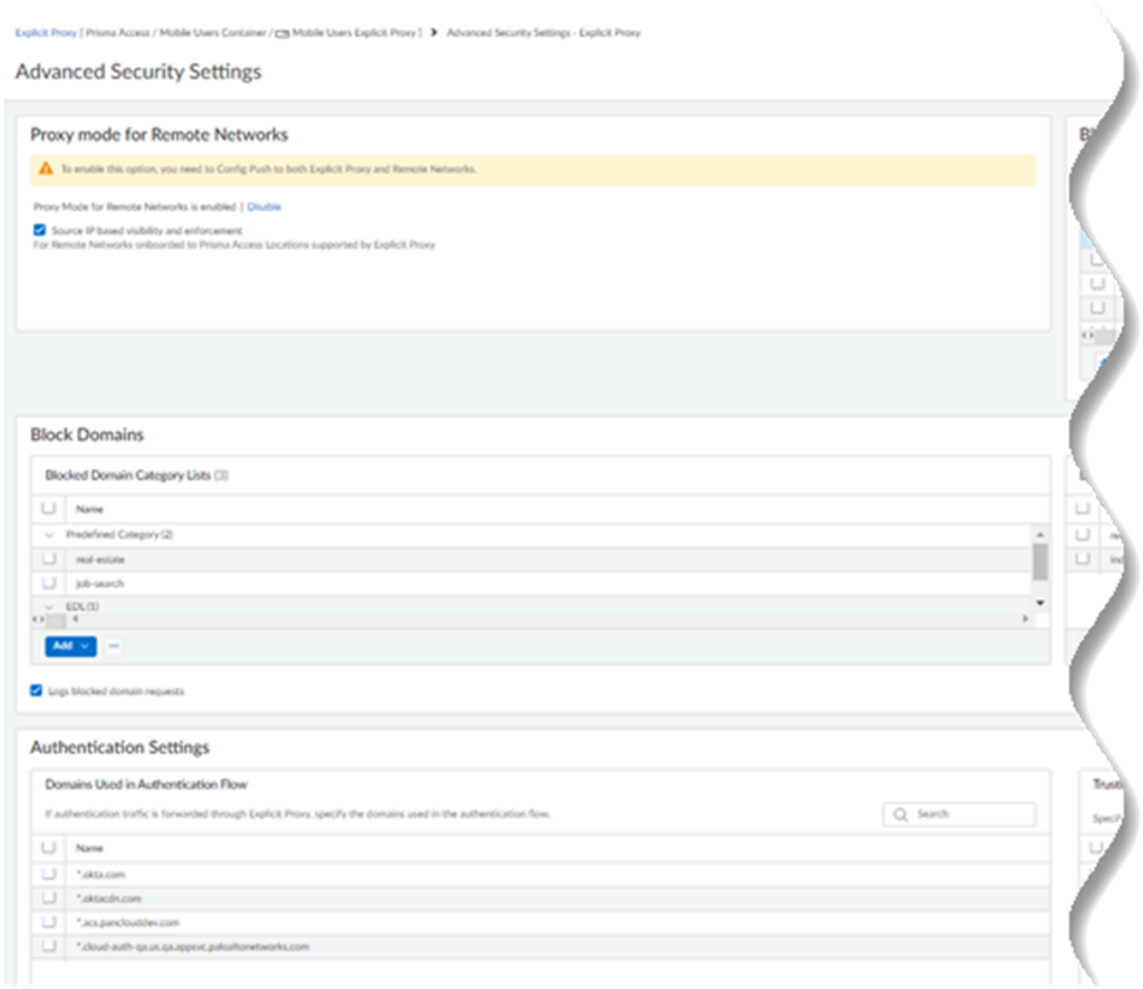
  指定恶意网站或您不希望用户访问的任何网站的域或域类别。 Prisma Access 当用户发起 HTTP GET（对于未加密的请求）或 HTTP CONNECT（对于加密的请求）时，阻止用户访

 ©2025 Palo Alto Networks, Inc.

问您在此区域指定的 URL 和 IP 地址。当用户尝试访问被阻止的网站时，他们会收到一个阻止页面。

- 如果您想要豁免任何包含在阻止域类别列表中的域，请在 例外列表中指定它们。

  任何输入的域名都不会被阻止，即使它们出现在您已阻止的域名类别中。
- 显式代理需要解密来验证用户身份。输入 身份验证流程中使用的域。
-



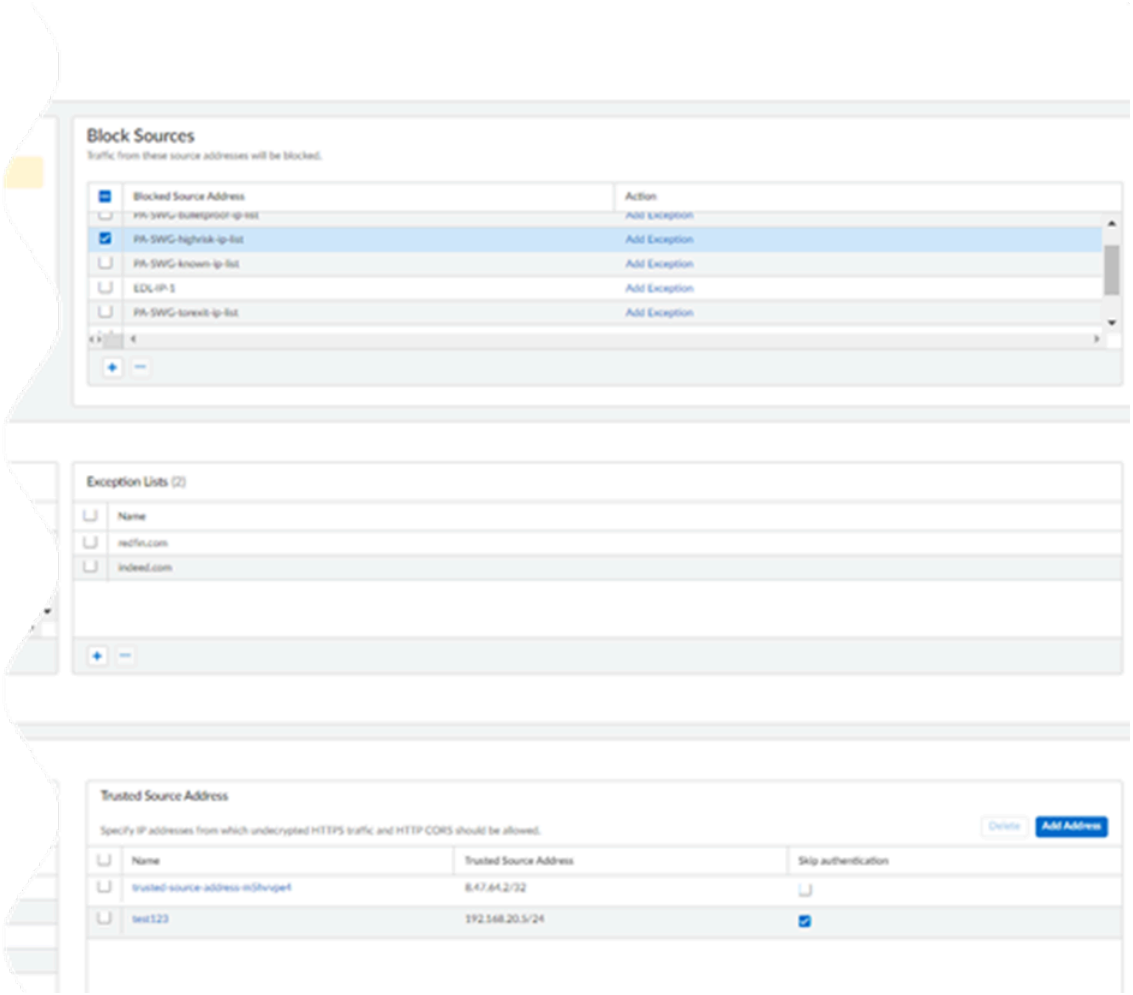
- 输入可允许未解密的 HTTPS 或 HTTP 跨源资源共享 (CORS) 流量到达 可信源地址的任何 IP 地址。
- 要绕过您输入的任何可信源地址的身份验证，请选择“跳过身份验证”。

  您可以使用 基于源 **IP** 的可视性和强制措施跳过身份验证，以跳过无法进行身份验证的无头系统的身份验证，设置安全策略，并获得流量的可视性 Prisma Access 显式代理。

  您可以添加 *IP* 地址或子网。扩展子网后最多支持 *100,000* 个 *IP* 地址。

  如果您选中 **Skip authentication**（跳过身份验证），以便跳过地址对象的身份验证，但随后又想通过取消选中该地址对象的 **Skip authentication**（跳过身份验证）来启用身份验证，则在您做出更改并提交和推送更改后，该更改最多可能需要 24 小时才会生效。

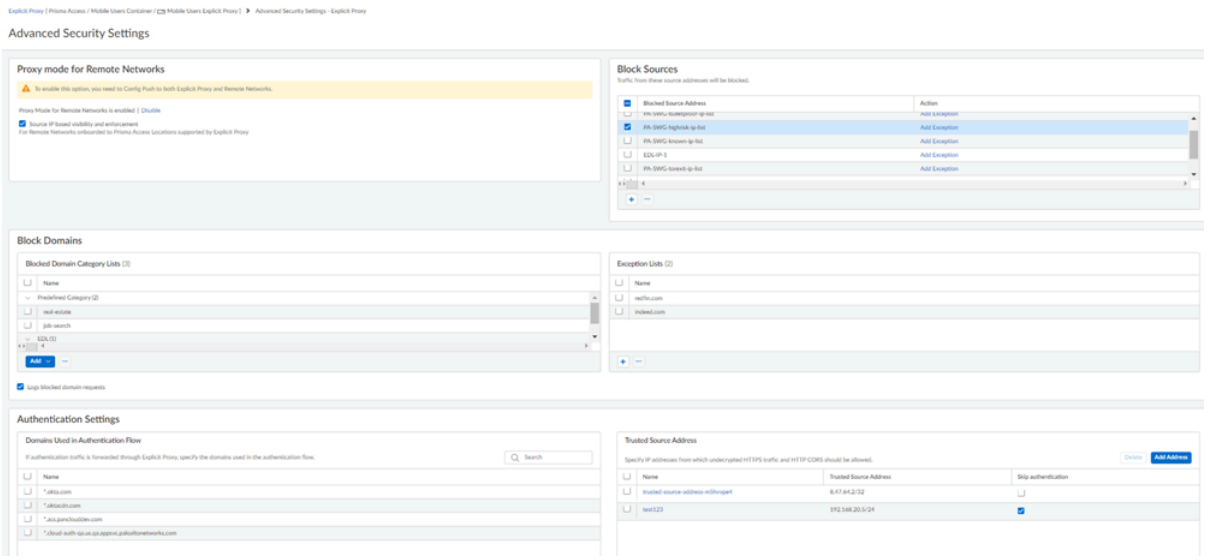
©2025 Palo Alto Networks, Inc.

- 

- 如果您有显式代理部署并添加了受信任的源 IP 地址列表，则可以 在传入的 **HTTP/HTTPS** 请求中使用 **X-Authenticated-User (XAU)** 标头进行身份识别。使用此功能允许从另一个使用 XAU 标头进行身份验证的代理登录的用户。

  您必须单击“保存”才能使 *XAU* 设置生效。

©2025 Palo Alto Networks, Inc.



设置显式代理（Panorama）

要使用显式代理保护移动用户的安全，请完成以下步骤。

在配置显式代理之前，请先查看 规划清单 并了解如何 设置显式代理 PAC 文件。

STEP 1 | 为显式代理设置身份验证。

SAML 和 Kerberos 是受支持的身份验证类型。

为 IdP 和 Panorama 配置 SAML 身份验证时请遵循以下准则：

- 全景指南：
  - 为 Prisma Access 配置 **SAML** 身份提供商 和 身份验证配置文件。您可以在后面的步骤中指定创建的身份验证配置文件。
  - 确保您在 **Explicit_Proxy_Template**下配置身份验证配置文件。
  - 在 IdP 服务器配置文件和 Panorama 上的 身份验证配置文件 中使用 邮件 作为用户属性。
  - 显式代理不支持在 SAML 身份提供者服务器配置文件中 向 **IdP** 签署 **SAML** 消息 。
  - 当您配置 Cloud Identity Engine 以检索用户和组映射信息时，请在组映射中使用 **mail** 或 **userPrincipalName** 作为 **SamAccountName**。
  - 在显式代理设置期间配置 组映射设置 时，对主用户名和电子邮件使用相同的目录属性，或者 Prisma Access 不能准确反映用户数量。例如，给定以下用户配置文件：

    ```
    sAMAccountName：muser Netbios：示例
     userPrincipalName：muser@example.com 邮
    件：mobile.user@example.com
    ```

    如果在 Cloud Identity Engine 配置中，您使用 `userPrincipalName` 作为 主用户名，使用 `mail`作为 电子邮件，则 Strata Logging Service 流量日志中返回的用户信息和ACS在认证日志中返回的用户信息将会有所不同。在此示例中，ACS 将 邮件 属性 (mobile.user@example.com) 发送到身份验证日志，并且 Strata Logging Service 将

 ©2025 Palo Alto Networks, Inc.

userPrincipalName 属性 (muser@example.com) 发送到流量日志。由于这种不匹配，在检查“状态”（全景 > 云服务 > 状态 > ） 页面中的显式代理状态时， 当前用户 和 用户（最近 **90** 天） 字段中的用户数将不准确。因此，在指定 组映射设置时，对 主用户名 和 电子邮件 使用相同的目录属性（例如， 邮件）。

- 使用 Panorama 管理 Prisma Access， Cloud Identity Engine 不会在安全策略规则中自动填充用户和组信息。

- **IdP** 准则：
  - 配置 SAML 时使用以下 URL：

    SAML 断言消费者服务 URL：**`https://global.acs.prismaaccess.com/saml/acs`**

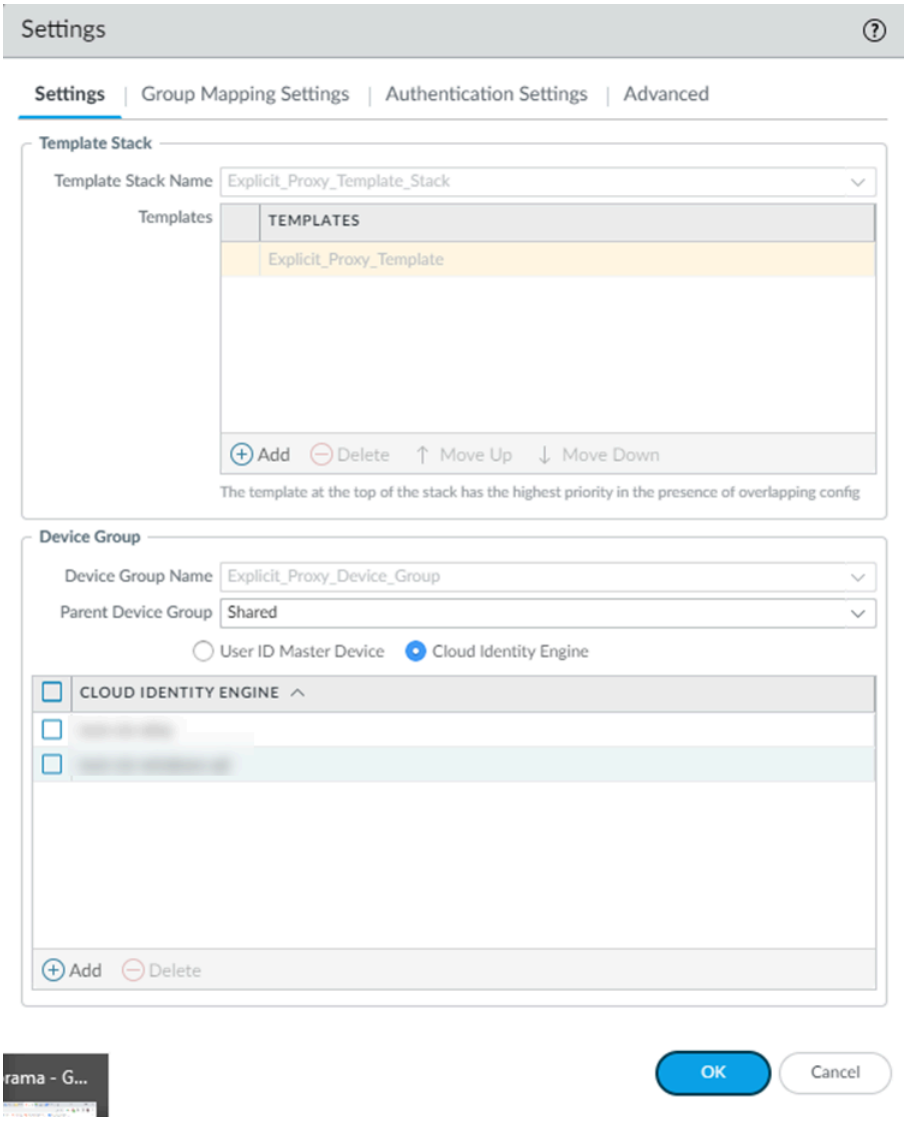
    实体 **ID**URL：**`https`** ://global.acs.prismaaccess.com/saml/metadata
  - 如果您使用 Okta 作为 IdP， 请使用 **EmailAddress** 作为 名称 **ID** 格式 设置。
  - 输入单点登录 URL`https://global.acs.prismaaccess.com/saml/acs`。
  - 不支持单点注销 (SLO)。
  - 要解决 IdP 身份验证问题，请使用 IdP 的监控和故障排除功能。ACS 不会记录 IdP 身份验证失败。
  - 为 SAML IdP 创建 身份验证配置 文件时，在“高级” 选项卡中， 选择“允许列表”中的所有内容， 否则“显式代理”将无法检索组映射。

 ©2025 Palo Alto Networks, Inc.

STEP 2 | 配置显式代理设置。

1. 选择 全景 > 云服务 > 配置 > 移动用户—显式代理， 然后单击齿轮图标来编辑显式代理设置。
2. 在 **Settings**（设置）选项卡中，编辑以下设置：
   - （可选）验证模板和模板堆栈名称。

     默认情况下， Prisma Access 创建一个新的模板堆栈 **Explicit_Proxy_Template_Stack** 和一个新的模板 **Explicit_Proxy_Template**。确保在 Panorama 中创建和编辑 设备 设置时使用此模板。
   - 在设备组部分中，选择包含要为显式代理推送的配置设置 的父设备组， 或将父设备组保留为 共享 以使用 Prisma Access 设备组共享层次结构。设备组名称 不能更改。
   - （可选）如果您已将下一代防火墙配置为主设备或添加了 云身份引擎 配置文件以在安全策略规则中填充用户和组信息，请选择用户 ID 主设备或云身份引擎；然后，选择您创建的主设备或云身份引擎配置文件。
   - 在许可证分配部分，指定为显式代理分配的移动用户数量。

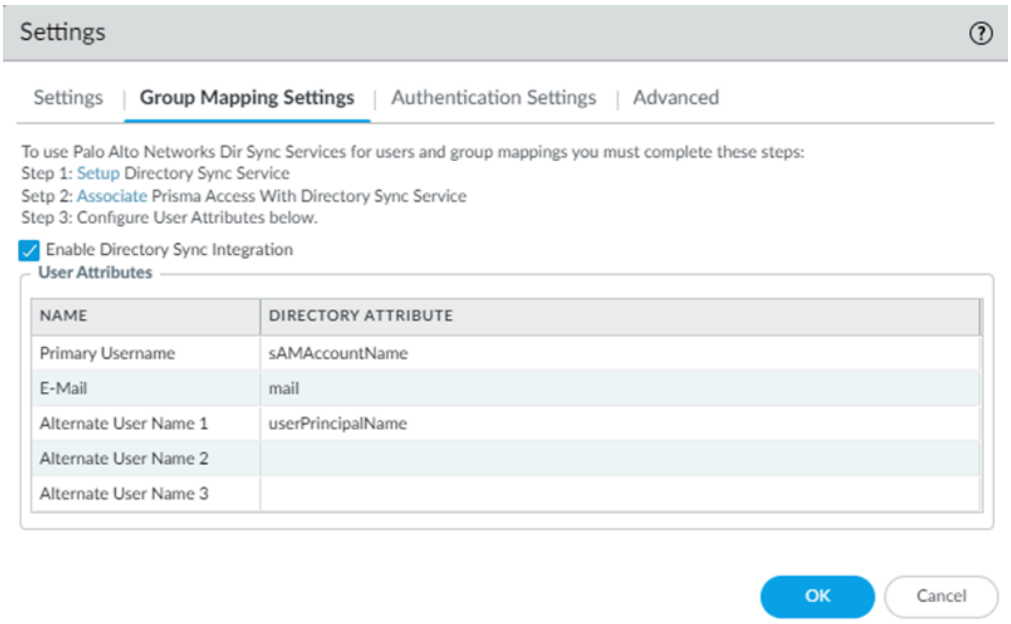


 ©2025 Palo Alto Networks, Inc.

3. 在 “组映射设置”选项卡中， 启用目录同步集成 （现称为 Cloud Identity Engine）以配置 Prisma Access 使用 Cloud Identity Engine 检索用户和组信息。

   您可以使用 Cloud Identity Engine 来填充显式代理部署的用户和组映射信息。

   在 主用户 名字段中输入目录属性的 邮件， 并在 电子邮件 字段中 输入邮件 。



4. 完成后单击 **OK**（确定）。

STEP 3 | ）配置 Block Settings（块设置）。

使用阻止设置在 DNS 解析阶段阻止对互联网目标的访问。

要将对显式代理的访问限制于特定的源 *IP* 地址，您还可以使用 特殊对象。这些使用特定名称的地址对象、地址组和外部动态列表 *(EDL)* 允许您为互联网流量指定的 *IP* 地址并阻止任何其他 *IP* 地址。

©2025 Palo Alto Networks, Inc.

STEP 4 | 在 身份验证设置 选项卡中，配置解密、X-Authenticated-User (XAU) 和身份验证设置。

1. 配置解密流量的设置。
   - 选择“解密与现有解密规则匹配的流量”；对于未解密的流量，仅允许来自经过身份验证的用户注册的已知 **IP** 的流量，以配置以下解密规则：
     - 与您配置的“解密”或“解密并转发”操作 的解密策略规则匹配的流量将被解密。

       如果用户访问未解密的 HTTPS 站点，且用户尚未从该 IP 地址向显式代理进行身份验证，则该用户将被阻止。但是，用户可以访问解密的站点，完成身份验证，然后访问未解密的站点。
     - 允许来自移动用户已通过身份验证的 IP 地址的未解密流量。

     显式代理需要解密来验证用户身份。在自定义 URL 类别中输入可以解密的域；然后，在“如果身份验证流量通过显式代理转发，则指定身份验证流程中使用的域”中指定这些类别。

     仅将身份验证所需的域添加到您指定的自定义 *URL* 类别，包括所有 *ACS* 和 *IdP FQDN*。您必须将身份验证 *URL* 添加到自定义 *URL* 类别，即使您已将它们添加到解密策略。
   - 要允许解密所有流量，请选择 解密所有流量（覆盖现有解密规则）。

     如果选择此单选按钮，请确保：
     - 您的解密策略中没有例外。
     - 您正在安全策略中应用基于源 IP 地址的限制。

     如果不遵循这些建议，则显式代理可能会被滥用为开放代理，而开放代理可能会被广泛滥用为进行拒绝服务攻击的转发服务。
     - 您至少有一个 SSL 正向代理证书指定为 正向信任证书。

       如果您没有前向信任证书，请在 Panorama 上创建一个；然后， 提交并推送 您的更改至 Prisma Access。如果没有前向信任证书，则提交显式代理更改时会导致提交错误。
2. （可选）输入应允许未解密的 HTTP 或 HTTP 跨源资源共享 (CORS) 流量到达 可信源地址身份验证绕过的任何 IP 地址。

   将 IP 地址添加到基于 IP 地址的地址对象并在字段中 添加 地址对象。

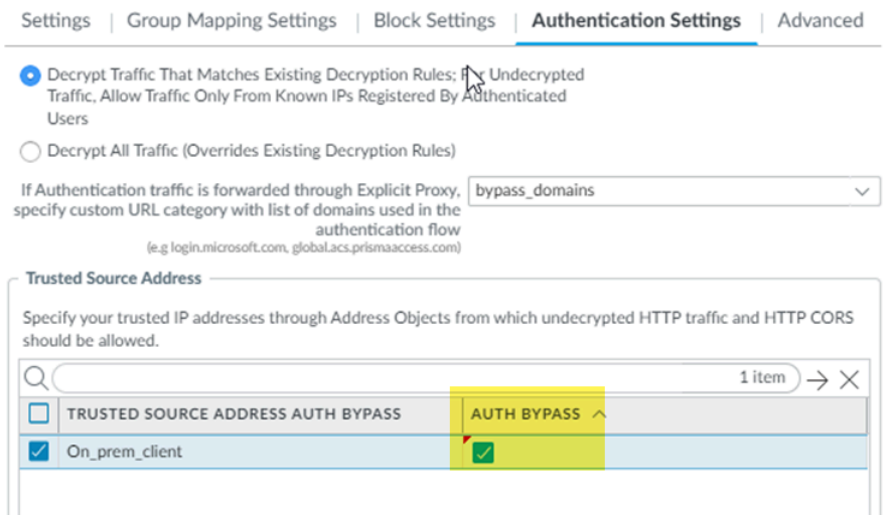
   最多输入 100,000 个地址。确保地址对象仅使用 IP 地址。
3. （可选）要绕过您输入的任何可信源地址的身份验证，请选择“**Auth Bypass**”。

   您可以将 **Auth Bypass** 与 基于源 **IP** 的可见性和强制措施 结合使用，以跳过无法进行身份验证的无头系统的身份验证、设置安全策略并获得 Prisma Access Explicit Proxy 上的流量的可见性。

   您可以添加 *IP* 地址或子网。扩展子网后最多可支持*10*万个*IP*地址。

 ©2025 Palo Alto Networks, Inc.

如果选中 **Auth Bypass**（绕过身份验证），以便跳过地址对象的身份验证，但随后又想通过取消选中该地址对象的 **Auth Bypass**（绕过身份验证）来启用身份验证，则在您做出更改并提交和推送更改后，该更改最多可能需要 24 小时才会生效。



4. （可选）要允许受信任的源地址 IP 地址使用 XAU 进行身份识别，请选择 在传入的 **HTTP/HTTPS** 请求中使用 **X-Authenticated-User (XAU)** 标头进行身份识别。

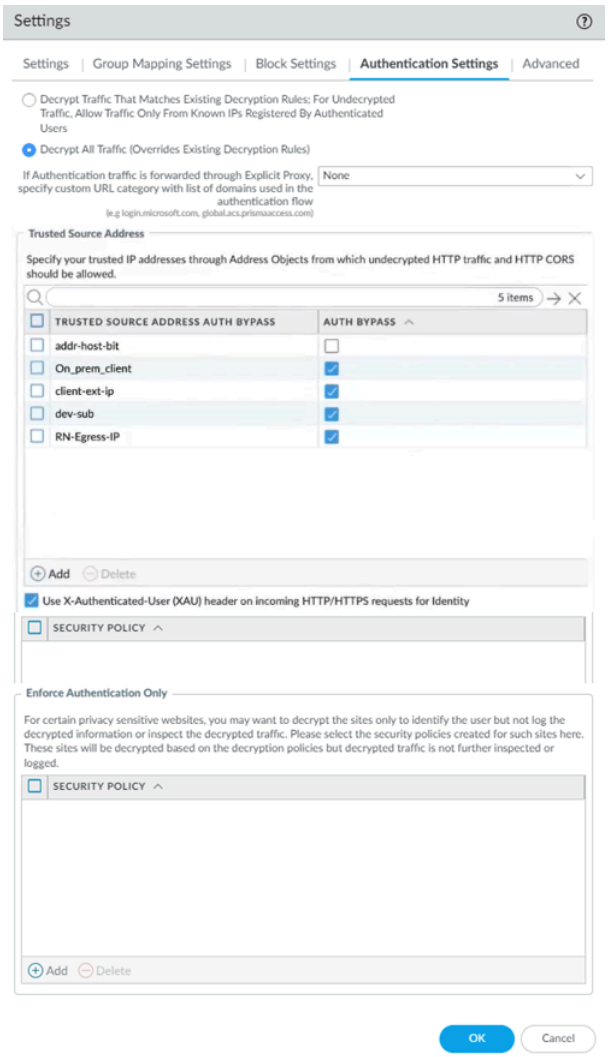
   如果您使用从第三方代理到显式代理的代理链，用户已在该代理中通过身份验证，并且该代理使用 XAU 标头，请选择此选项。

   XAU 标头是唯一支持显式代理标头提取的 HTTP 标头。不支持 X-Forwarded-For (XFF) 标头。

5. （可选）通过为这些站点创建安全策略规则，然后在 “仅强制身份验证” 区域中为这些站点指定 安全策略 或策略，指定隐私敏感网站的设置。

   对于您在 安全策略 或您添加的策略中指定的任何网站，显式代理会根据解密策略解密网站，但不会检查或记录解密的流量。

©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.

STEP 5 | （可选）配置 **Advanced**（高级）设置。

1. 如果您想通过安全的 IPSec 隧道将流量从分支机构转发到显式代理， 请启用代理模式 并检索任播 IP 地址（如果您想将 显式代理与 Prisma Access 远程网络结合使用）。

   该解决方案使用带有远程网络 IPSec 隧道的任播地址，以允许远程网络站点或分支位置的用户和设备使用显式代理。

2. （可选）要利用分支机构中将流量转发到显式代理的系统的私有 IP 地址，请选择 基于源 **IP** 的可见性和实施。

   此功能具有以下要求：

   - 最低 10.2.4 版本版本的 Prisma Access 数据平面
   - 具有最低 4.1 版本的云服务插件的 Prisma Access (Managed by Panorama) 部署
   - 在配置远程网络显式代理部署后，只有来自远程网络的 IP 地址才会显示源 IP 地址，并且只有显式代理支持的远程网络位置的源地址才会显示。

3. 仅代理模式部署 如果 您的远程网络上启用了代理模式，则添加策略以允许绑定到远程网络上的任播和单播 IP 的流量。如果您已启用 源 **IP** 可见性和强制执行，请使用显式代理中的安全策略中 的源 **IP** 字段来保护流量。您需要在远程网络中制定额外的策略。

4. 单击 **OK**（确定）。

 ©2025 Palo Alto Networks, Inc.

STEP 6 | 单击“配置”以配置显式代理设置。

1. 指定 显式代理 **FQDN**。

   默认情况下，名称为 *proxyname*.proxy.prismaaccess.com，其中 *proxyname* 是您指定的子域，并使用端口 8080。如果您想在显式代理 URL 中使用您组织的域名（例如，thisproxy.proxy.mycompany.com），请输入您组织的域的 CNAME 记录。

   例如，要将名为 thisproxy.prismaaccess.com 的代理 URL 映射到名为 thisproxy.proxy.mycompany.com 的代理，您需要将 thisproxy.proxy.prismaaccess.com 的 CNAME 添加到组织域中的 CNAME 记录。

2. （可选）选择 使用 **GlobalProtect** 代理进行身份验证 以启用基于代理的代理功能。

   启用此功能可在 代理模式 或 隧道和代理模式下设置显式代理。您还必须选中此复选框来启用 基于源 **IP** 的可见性和实施。

3. 指定 身份验证配置文件 和 **Cookie** 生存期。

   - 指定您在步骤 1中使用的 SAML 身份验证配置文件，或添加要使用的 新 身份验证配置文件 Prisma Access。

     您必须 配置 SAML 身份验证，包括配置 **SAML** 身份提供商 (IdP) 和 身份验证配置文件，才能使用显式代理。

   - （可选）为存储用户身份验证凭据的 Cookie 指定 **Cookie** 有效期 。

     Prisma Access 缓存用户的凭据并将其以 cookie 的形式存储。要更改该值，请指定要使用的时间长度（以秒、分钟、小时或天为单位）。

     为了防止用户在 *cookie* 有效期到期之前无法下载大文件，或者用户长时间访问单个网站时 *cookie* 过期的问题，*Palo Alto Networks* 建议您将 *Cookie* 有效期配置为至少一天。如果显式代理用户遇到 *cookie* 生存期过期问题，他们可以浏览到其他网站重新向 *ACS* 进行身份验证并刷新 *ACS cookie*。

     如果您正在下载文件，并且文件下载所用的时间超过了 **Cookie** 生存期，则文件下载将在生存期值到期时终止。因此，如果您下载需要很长时间才能下载的大文件，请考虑使用更长的 **Cookie** 有效期 。

 ©2025 Palo Alto Networks, Inc.

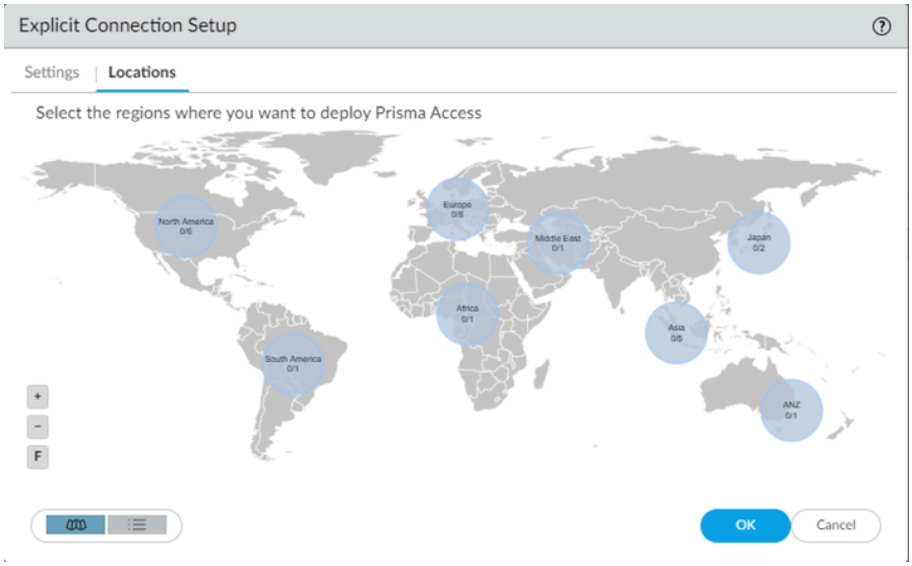
STEP 7 | 选择您想要为移动用户部署显式代理的 位置 以及与这些位置相关的区域。 Prisma Access 在您选择的每个位置添加一个代理节点。

显式代理支持所有 Prisma Access 位置。看 显式代理配置准则 查看位置列表。

“位置”选项卡显示地图。地图突出显示了全球区域（美洲、欧洲和亚太地区）以及每个区域内的可用位置。选择一个区域，然后选择每个区域想要部署的位置。

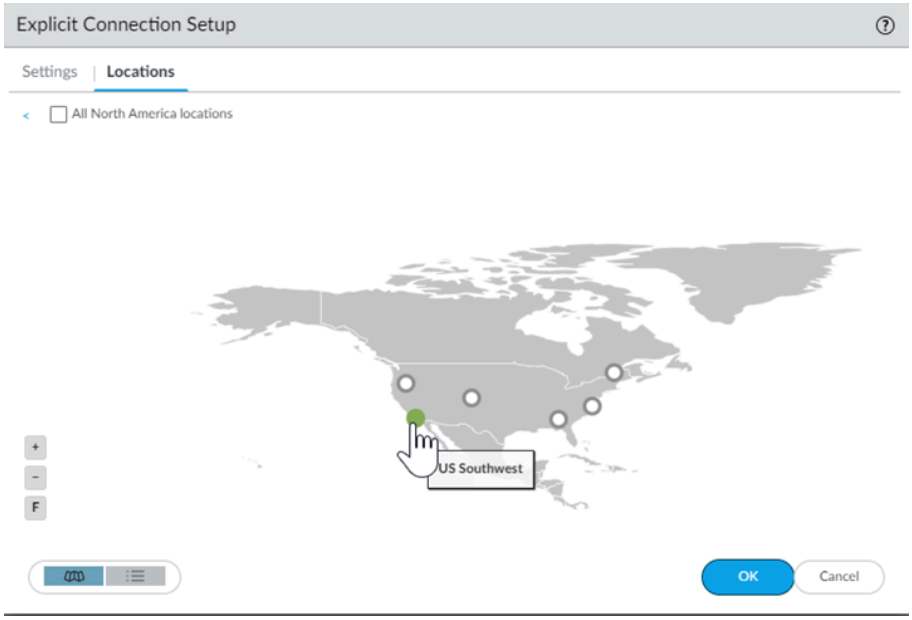
您应该至少在两个区域启用显式代理位置以确保区域冗余。

1. 单击 位置 选项卡并选择一个区域。



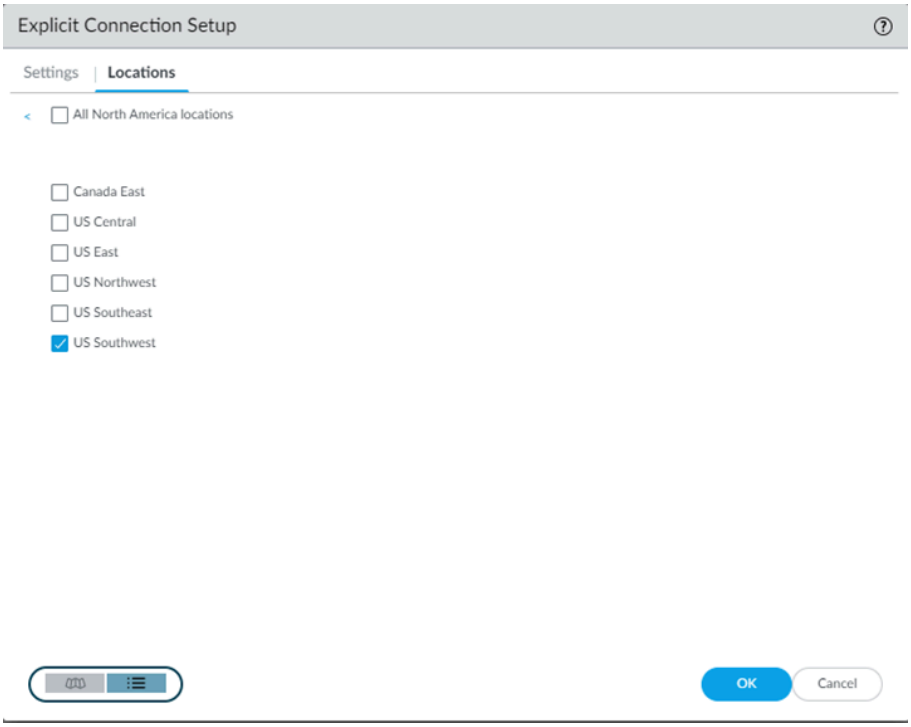
2. 使用地图在您选择的区域内选择一个或多个显式代理位置。

   将光标悬停在某个位置上即可突出显示该位置。白色圆圈表示可用位置；绿色圆圈表示您已选择该位置。



 ©2025 Palo Alto Networks, Inc.

除了地图视图，您还可以查看地区和位置的列表。从左下角选择地图视图和列表视图。在列表视图中，列表显示按列排序的区域，所有位置均按区域排序。您可以选择某个区域内的 所有 站点（对话框顶部）。



3. 单击“确定”添加位置。

STEP 8 | 配置安全策略规则来执行您组织的安全策略。

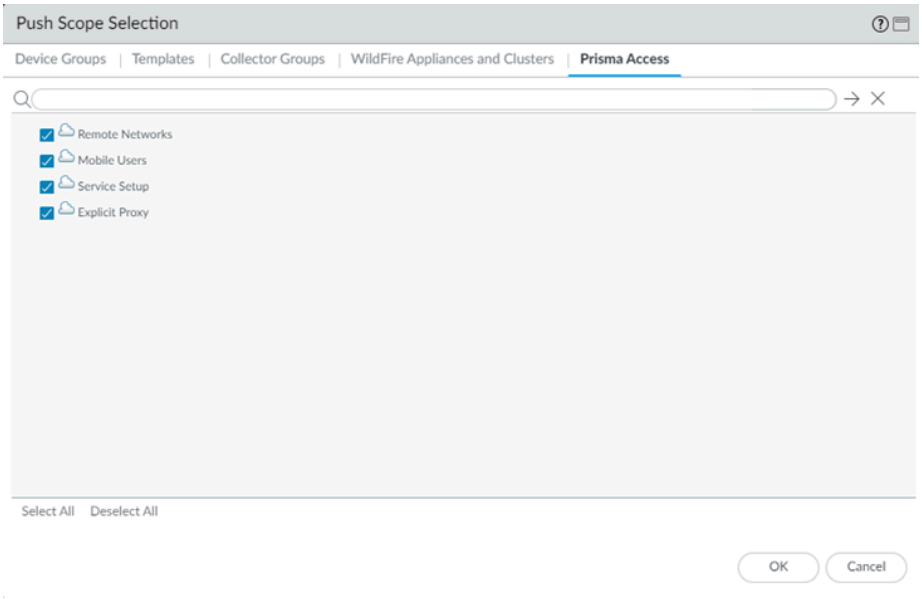
要进行所需的配置更改并控制移动用户可以从显式代理访问的 URL，请使用安全策略。配置安全策略时请遵循以下准则和要求：

- 根据您的业务目标，使用 App-ID 和需要访问这些应用程序的用户组为受批准的互联网和 SaaS 应用程序创建安全策略。
- 将安全配置文件附加到所有安全策略规则，以便您可以按照 安全配置文件最佳实践来防止已知和未知的威胁。

 ©2025 Palo Alto Networks, Inc.

STEP 9 | 将更改提交到 Panorama 并将配置更改推送到 Prisma Access。

1. 单击 **Commit**（提交） > **Commit and Push**（提交并推送）。
2. 编辑选择，然后在 **Prisma Access** 选项卡中，确保在 推送范围中选择了 显式代理，然后单击 确定。



3. 单击 **Commit and Push**（提交并推送）。

STEP 10 | 选择要与显式代理一起使用的 PAC 文件。

1. 选择 全景 > 云服务 > 配置 > 移动用户 > 显式代理。

   确保在 PAC 文件中输入端口 8080。
2. 选择您刚刚配置的显式代理设置的 连接名称 。
3. 输入用于显式代理的 **PAC**（代理自动配置）文件 。

   在将 *PAC* 文件上传到 *Prisma Access*。



   浏览 并上传文件。

   Prisma Access 为您提供了示例 PAC 文件；您可以 下载示例 **PAC** 文件，更改值，然后上传该文件。请参阅 设置您的显式代理 PAC 文件 以了解 PAC 文件要求和指南，我们将其中作为示例 PAC 文件内容的描述。

 ©2025 Palo Alto Networks, Inc.

用于显式代理部署的 Kerberos 身份验证

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证

“Prisma Access Mobile—显式代理”部署支持 Kerberos 身份验证。如果您的服务器、物联网设备或无头计算机无法使用 SAML 进行身份验证，则可以改用 Kerberos 身份验证。

如果您的部署同时使用 SAML 和 Kerberos 进行身份验证，则可以在单个显式代理部署中配置这两种身份验证类型。通过这种方式，您可以使用 SAML 对移动用户进行身份验证，同时使用 Kerberos 对服务器、物联网设备或无头计算机进行身份验证。Prisma Access 显式代理根据用于身份验证流量的端口来处理身份验证：

- 如果身份验证流量使用端口 8080，则显式代理使用 SAML 身份验证。
- 如果身份验证流量使用端口 8081，则显式代理使用 Kerberos 身份验证。

如果只配置了一个端口，则未配置的端口将使用与已配置端口相同的身份验证配置文件。

Kerberos SSO 仅适用于可以访问 *Kerberos* 基础设施的端点和系统。无法访问 *Kerberos* 基础设施的端点和系统必须使用 *SAML SSO*。

- 在显式代理部署中部署 Kerberos 的要求和建议
- 创建 Kerberos 密钥表
- 为显式代理部署配置 Kerberos 身份验证

在显式代理部署中部署 Kerberos 的要求和建议

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 许可证 ❑ 所需的数据平面最低版本：PAN-OS 10.1.3 或更高版本

在您创建 Kerberos 密钥表以在显式代理部署中实现 Kerberos 之前，请确保您的 Kerberos 部署满足以下要求和先决条件：

- 将您的数据平面更新到 PAN-OS 10.1.3 或更高版本。
- 确保您拥有可以用于 Prisma Access 身份验证服务器或设备的 Kerberos 帐户。

  需要一个帐户才能创建 Kerberos Keytab，即包含主体名称和加密的 Kerberos 密码的一个文件。
- 确保服务器和端点已加入域，这使得用户和机器能够使用其工作网络凭据安全地连接到其工作域。

©2025 Palo Alto Networks, Inc.

- 确保在移动用户的 PAC 文件中或在端点或服务器的代理设置中将 Kerberos 身份验证流量转发到 8081 端口。

  显式代理使用 8081 端口进行 Kerberos 身份验证，使用 8080 端口进行 SAML 身份验证。
- 确保您的 Kerberos 管理员有能力创建和导出 keytabs。
- 确保您拥有服务器、物联网设备或无头机器所在的分支或校园位置的传出IP地址。

  您将这些 IP 地址添加到被显式代理信任的地址列表中。

 ©2025 Palo Alto Networks, Inc.

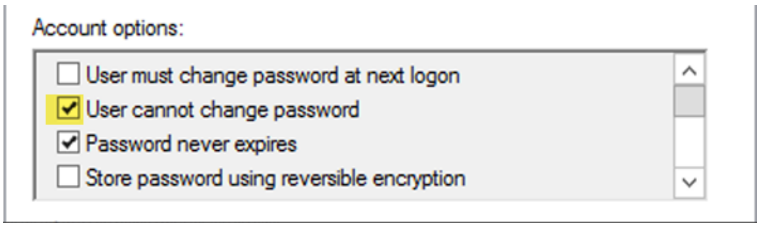
- 遵循 Kerberos 用户身份验证和创建的最佳实践。

  作为 Kerberos 帐户管理员，遵循最佳实践以保护其 Kerberos 环境并防止密码被泄露是他们的责任。在创建用户帐户、密码和服务主体名称 (SPN) 时，请遵循以下最佳实践。

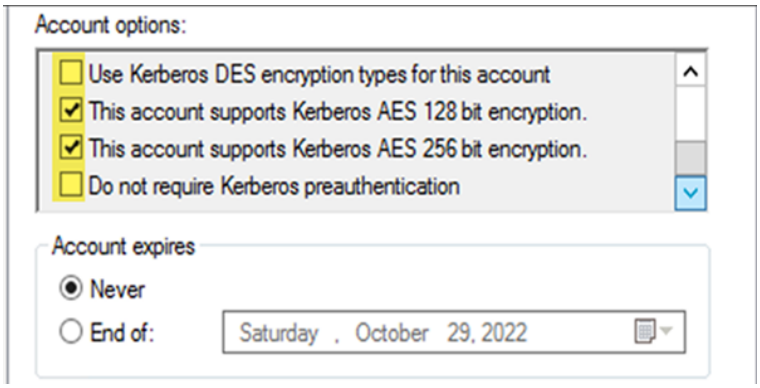
  Kerberos 用户帐户创建最佳实践：

  - 请勿重复使用管理员用户帐户。

    为将与 Prisma Access 显式代理一起使用的 Kerberos 帐户创建一个唯一的帐户名称。
  - 请不要与任何其他服务共享此帐户；请为 Prisma Access 显式代理使用专用用户帐户。
  - 确保用户无法更改 Kerberos 帐户的密码。

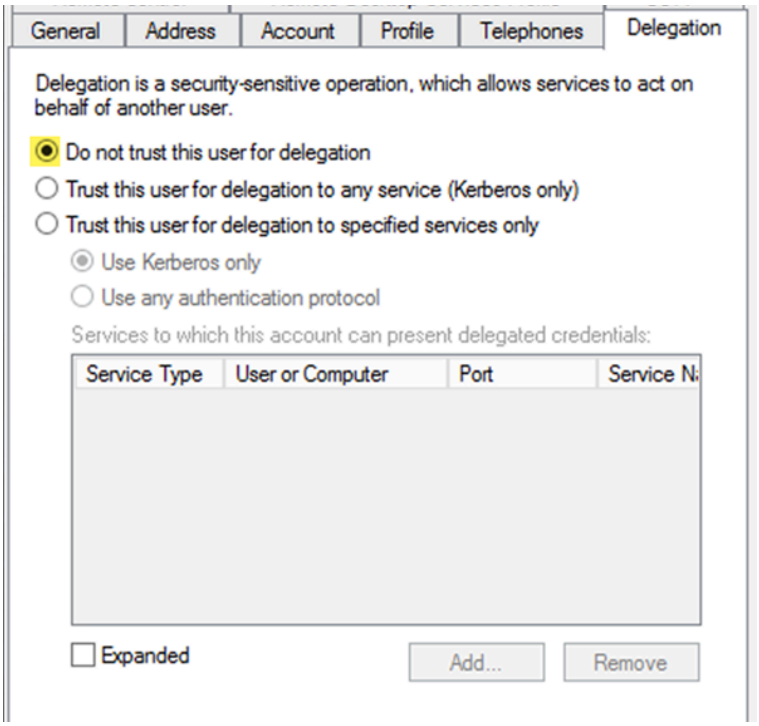


  - 在选择 Kerberos 帐户选项时，取消选择 **Use Kerberos DES encryption types for this account**（此帐户使用 **Kerberos DES** 加密类型）和 **Do not require Kerberos preauthentication**（不要求 **Kerberos** 预身份验证）。
  - 启用 AES-128 和 AES-256 位加密。

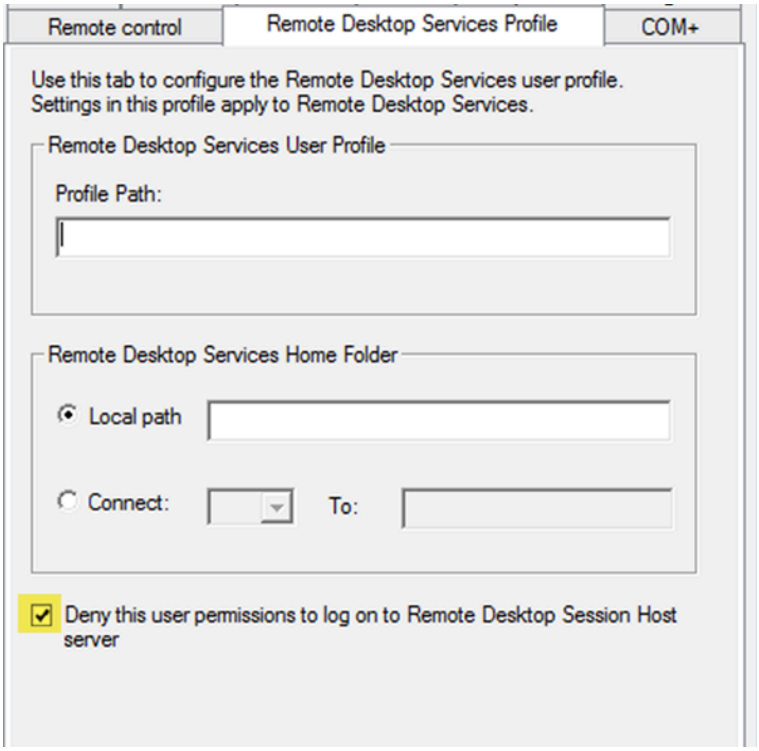


  - 禁用用户的委派。

 ©2025 Palo Alto Networks, Inc.

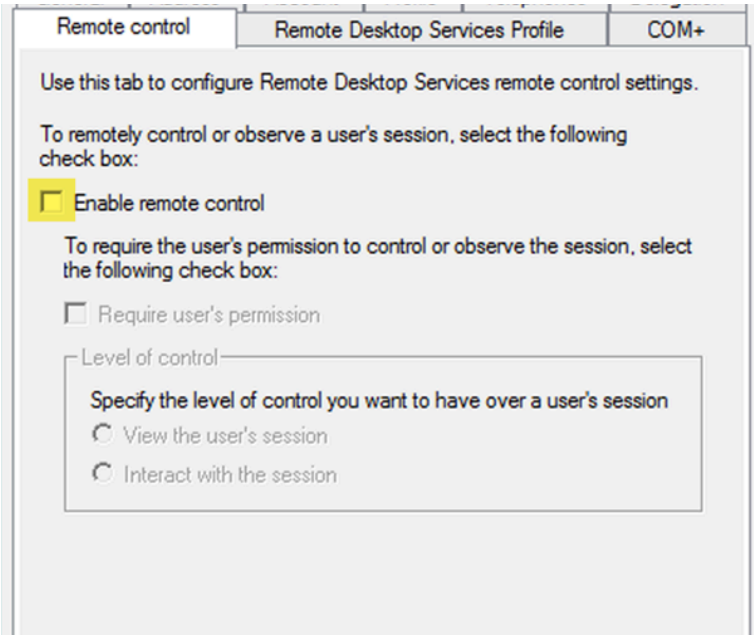


- 拒绝登录远程桌面会话的能力。

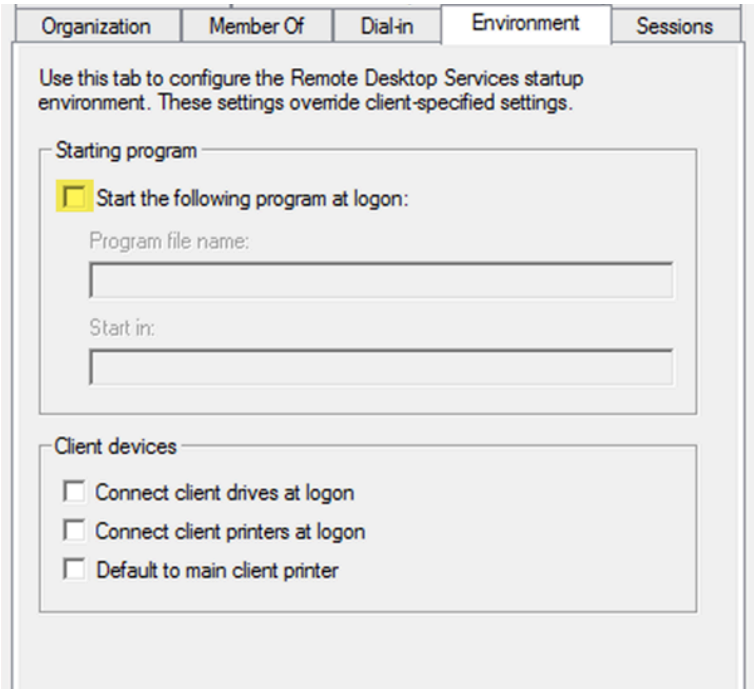


- 请勿启用远程控制。

 ©2025 Palo Alto Networks, Inc.



- 不允许用户在登录时启动程序。



- 您可以在您创建的身份验证配置文件的允许列表中指定用户或用户组，以限制身份验证仅限于具有合法业务需求的用户或机器。

SPN 和 **Keytab** 最佳实践：

- 确保 SPN 未与多个用户帐户关联，这可能导致重复的 SPN 故障。
- RC4-HMAC-NT 使用弱 NTML 哈希。遵循您组织的安全政策和指南，以包括或排除 RC5 密码。
- DES-CBC-CRC 和 DES-CBC-MD5 加密算法已被弃用，不再受 Prisma Access 支持。

©2025 Palo Alto Networks, Inc.

- 定期更改 SPN 的密码。遵循您组织的安全政策和密码轮换指南。
- 遵循您组织的密码复杂性实践（例如，以真正随机的方式创建SPN密码，使其不可读且不可猜测）。
- 如果您更改服务用户的密码或更改任何其他属性，请更新并重新生成新的 keytab 并将其上传到 Prisma Access。
- 如果您启用一个新的 PA 区域，您必须为该区域生成一个新的 keytab，如以下步骤所述。

以下示例输出显示了一个使用 Kerberos 最佳实践创建的帐户。

```
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
```

创建 Kerberos 密钥表

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 许可证 ❑ 所需的最低数据平面版本：PAN-OS 10.1.3 或更高版本

在查看为显式代理部署 Kerberos 的要求和建议后，您就可以创建 Kerberos 密钥表了。

为了获得最佳性能，密钥表文件的大小应小于 *60 KB*。

STEP 1 | 设置您的显式代理部署。

 ©2025 Palo Alto Networks, Inc.

STEP 2 | 获取设置 Kerberos 身份验证所需的 FQDN、代理 FQDN 和 DNS CNAME。

Kerberos 身份验证使用从 Prisma Access API 脚本检索到的信息来创建和配置 Kerberos 密钥表。该 API 脚本检索以下信息：

- **ep_geo_lb_fqdn** — 显式代理网络负载均衡器配置中使用的显式代理 DNS FQDN。此 FQDN 与 **Workflows**（工作流） > **Prisma Access** 设置 > **Explicit Proxy**（显式代理） > **Infrastructure Settings**（基础架构设置） > **Explicit Proxy URL**（显式代理 **URL**）下的 Prisma Access UI 中的显式代理 **Explicit Proxy URL**（显式代理 **URL**）相同。
- **ep_geo_lb_cname** — 显式代理租户的 DNS CNAME。
- **ep_regional_fqdn** — 用于已加入的显式代理位置的 FQDN。

  显式代理为每个位置提供网络负载均衡器的公共 IP 地址；ep_regional_fqdn 是与该 IP 地址关联的 FQDN。如果多个位置共享同一个公共 IP 地址，则这些位置使用同一个区域 FQDN。

1. 生成 API 密钥以用作 curl 命令的一部分。
   - 在 Prisma Access (Managed by Strata Cloud Manager) 上，选择 **Workflows**（工作流） > **Prisma Access** 设置 > **Prisma Access** > **Infrastructure Settings**（基础架构设置） > **Generate New API Key**（生成新的 **API** 密钥）。
   - 在 Panorama Managed Prisma Access 上，选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Service Setup**（服务设置） > **Generate API Key**（生成 **API** 密钥）
2. 创建一个 .txt 文件并在文件中输入以下命令选项：

   ```
   { "serviceType": "swg_proxy", "location": "deployed",
    "addrType": "network_load_balancer" }
   ```

3. 输入以下命令来检索使用 Kerberos 身份验证所需的 FQDN：

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

   其中 `option.txt` 是您在上一步中创建的 .txt 文件，`Current-API-Key` 是 Prisma Access API 密钥。
4. 记下 FQDN。

   每个已加入位置至少有一个 **ep_geo_lb_fqdn**、一个 **ep_geo_lb_cname** 和一个 **ep_regional_fqdn**。

STEP 3 | 通过输入以下命令，在组织的 Active Directory (AD) 中为 Prisma Access 显式代理服务创建新用户：

```
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
```

其中：

- *USER_NAME* 是用户对象的名称。
- *USER_GIVEN_NAME* 是用户的指定名称。
- *USER_SAMACCOUNTNAME* 是用户的安全帐户管理器 (SAM) 名称。
- *USER_NAME@DNS_DOMAIN_NAME* 用户的用户主体名称 (UPN)。
- *X_500_PATH* 是创建新对象的 OU 或容器的 X.500 路径（例如，`DC=EXAMPLE,DC=COM`。）
- *PASSWORD* 用于该帐户的密码。

以下 CLI 示例的用户名为 `example`，SAM 名称为 `example`，指定名称为 `PrismaAccess EP Service User`，UPN 为 `example@exmp.com`，路径为 `DC=EXMP,DC=COM`，密码为 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
```

上一个命令指定加密类型为 *RC4*，该加密类型使用弱 *NTLM* 哈希。请遵循组织的安全策略和指南，以决定在此命令中包含还是排除 *RC4*。

STEP 4 | 输入以下命令以防止密码过期并防止密码被更改：

```
Get-ADUser USER_NAME|Set-ADUser -PasswordNeverExpires:$True -
CannotChangePassword:$true
```

请遵循组织的安全策略和指南，了解密码过期和轮换策略。

STEP 5 | 输入以下命令以显示新创建的用户帐户：

```
Get-ADUser USER_NAME -property msDS-KeyVersionNumber
```

 ©2025 Palo Alto Networks, Inc.

STEP 6 | 将 SPN 与密钥表文件相关联，以便在 Windows AD 中使用 Kerberos 身份验证。

密钥表文件允许显式代理验证来自用户、服务器、IoT 设备或其他无头计算机的流量流动期间提供的 Kerberos 身份验证令牌。创建密钥表文件期间，显式代理要求将您在之前的步骤中使用 API 检索的值作为服务主体名称 (SPN)，与您在该步骤之后的步骤中创建的用户帐户相关联。

使用 **ep_geo_lb_fqdn**、**ep_geo_lb_cname** 和 **ep_regional_fqdn** 值。这些值允许显式代理对流向其中任一代理域的流量进行身份验证。

1. 通过输入以下命令，使用 **ep_geo_lb_fqdn** 值作为服务主体名称 (SPN) 生成并导出密钥表：

   ```
   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
   ```

   其中：

   - *ep_geo_lb_fqdn* 是从显式代理 API 脚本返回的 **ep_geo_lb_fqdn** 值。
   - *REALM* 是领域（例如 `EXMP.COM`）。

     在大多数情况下，使用大写字母输入领域。
   - *DOMAIN\USER_NAME* 是域级登录名（例如，`EXMP\example`）。
   - *PASSWORD* 是用于密钥表的密码。此密码不必与用户密码匹配，但必须与您在后续步骤中为 **ep_geo_lb_cname** 和 **ep_regional_fqdn** SPN 创建的值相匹配。
   - *KEYTAB_NAME_1* 是密钥表的名称。密钥表名称对于此 SPN 必须是唯一的。

   请务必遵循创建 *SPN* 和密码的最佳实践。

   以下 CLI 示例的 *ep_geo_lb_fqdn* 为 `example.proxy.prismaaccess.com`，*REALM* 为 `EXMP.COM`，*DOMAIN\USER_NAME* 为 `EXMP\example`，*PASSWORD* 为 `Ex@mple123`，导出的密钥表名称为 `exmp1.keytab`：

   ```
   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. 通过输入以下命令，使用 **ep_geo_lb_cname** 值作为 SPN 生成并导出密钥表：

   ```
   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
   ```

   其中：

   - *ep_geo_lb_cname* 是从显式代理 API 脚本返回的 **ep_geo_lb_cname** 值。
   - *REALM* 是领域（例如 `EXMP.COM`）。
   - *DOMAIN\USER_NAME* 是域级登录名（例如，`EXMP\example`）。

 ©2025 Palo Alto Networks, Inc.

- *PASSWORD* 是用于密钥表的密码。此密码必须与 **ep_geo_lb_fqdn** 和 **ep_regional_fqdn** SPN 密码相匹配。
- *KEYTAB_NAME_2* 是您想要导出的密钥表的名称。此名称应与您创建的其他 SPN 密钥表名称不同。

以下 CLI 示例的 *ep_geo_lb_cname* 为 `prisma-abcde12345.proxy.prismaaccess.com`，*REALM* 为 `EXMP.COM`，*DOMAIN\USER_NAME* 为 `EXMP\example`，*PASSWORD* 为 `Ex@mple123`，导出的密钥表名称为 `exmp2.keytab`：

```
ktpass -princ HTTP/prisma-
abcde12345.proxy.prismaaccess.com@EXMP.COM -mapuser EXMP
\example -ptype KRB5_NT_PRINCIPAL -crypto all -pass Ex@mple123
 -out exmp2.keytab
```

3. 通过输入以下命令，使用 **ep_regional_fqdn** 值作为 SPN 生成并导出密钥表：

```
ktpass -princ HTTP/ep_regional_fqdn@REALM -
mapuser DOMAIN\USER_NAME -ptype KRB5_NT_PRINCIPAL -crypto all
 -pass PASSWORD -out KEYTAB_NAME_3.keytab
```

其中：

- *ep_regional_fqdn* 是从显式代理 API 脚本返回的 **ep_regional_fqdn** 值。
- *REALM* 是领域（例如 `EXMP.COM`）。
- *DOMAIN\USER_NAME* 是域级登录名（例如，`EXMP\example`）。
- *PASSWORD* 是用于密钥表的密码。此密码必须与 **ep_geo_lb_fqdn** 和 **ep_geo_lb_cname** SPN 密码相匹配。
- *KEYTAB_NAME_3* 是您想要导出的密钥表的名称。此名称应与您创建的其他 SPN 密钥表名称不同。

以下 CLI 示例的 *ep_regional_fqdn* 为 `us-west-2.prisma-abcde12345.proxy.prismaaccess.com`，*REALM* 为 `EXMP.COM`，*DOMAIN\USER_NAME* 为 `EXMP\example`，*PASSWORD* 为 `Ex@mple123`，导出的密钥表名称为 `exmp3.keytab`：

```
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. （可选）如果您有其他位置使用不同的 **ep_regional_fqdn** 值，并且您想要为这些位置创建密钥表，请重复步骤 6.c，使用这些位置的 **ep_regional_fqdn** 值生成并导出一个或多个额外的密钥表。

为每个唯一的 **ep_regional_fqdn** 创建唯一的密钥表名称。例如，如果另一个位置的 **ep_regional_fqdn** 为 `us-east-2.prisma-`

 ©2025 Palo Alto Networks, Inc.

abcde12345.proxy.prismaaccess.com，请输入包含已导出密钥表文件的唯一名称的以下示例 CLI：

```
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
```

STEP 7 | 在 Ubuntu 中输入以下 `ktutil` 命令，删除创建的密钥表中不受支持的密码。

以下系统输出提供了清理各种密码的示例：

```
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)
```

```
# display all keytabs, get the key entry numbers to remove DES-
CBC-MD5 and DES-CBC-CRC. # Also, enable or disable RC4-HMAC based
 on your organization's policy. 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
```

其中 *KEYTAB_NAME_1*.keytab、*KEYTAB_NAME_2*.keytab 和 *KEYTAB_NAME_3*.keytab 是您在上一步中创建的密钥表。

STEP 8 | （可选）如果您为其他区域创建了更多密钥表，请输入上一个 `ktutil` 命令，将 *KEYTAB_NAME_1*.keytab 替换为您用于该区域或多个区域的密钥表名称，并指定不同的输出文件（例如，`new4.keytab`、`new5.keytab` 等），以删除这些密钥表中不受支持的密码。

©2025 Palo Alto Networks, Inc.

STEP 9 | 通过输入以下 `ktutil` 命令合并您创建的密钥表，其中 new1.keytab、new2.keytab 和 new3.keytab 是您在上一步中创建的密钥表，请务必在此命令中包含所有特定于区域的密钥表：

```
ktutil rkt new1.keytab rkt new2.keytab rkt new3.keytab # if you
 created any additional region-specific keytab files, add them
 here. wkt papxv1.keytab quit
```

完成后，您可以使用所创建的密钥表（在此示例中为 `papxv1.keytab`）作为用于显式代理的密钥表。

为显式代理部署配置 Kerberos 身份验证

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证

- Strata Cloud Manager
- Panorama

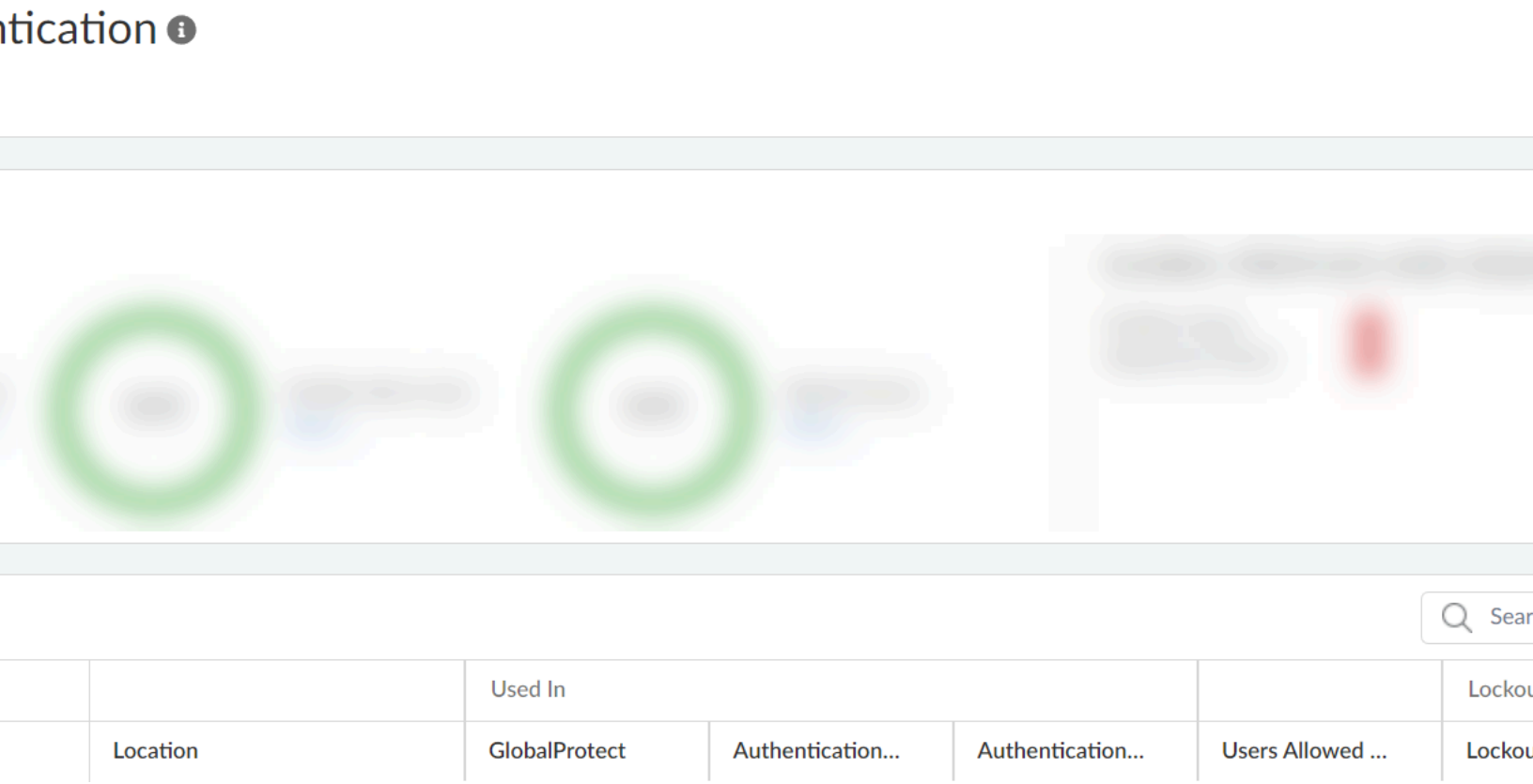
 ©2025 Palo Alto Networks, Inc.

为显式代理部署配置 **Kerberos** 身份验证 **(Strata Cloud Manager**）

STEP 1 | 设置 Kerberos 身份验证配置文件。

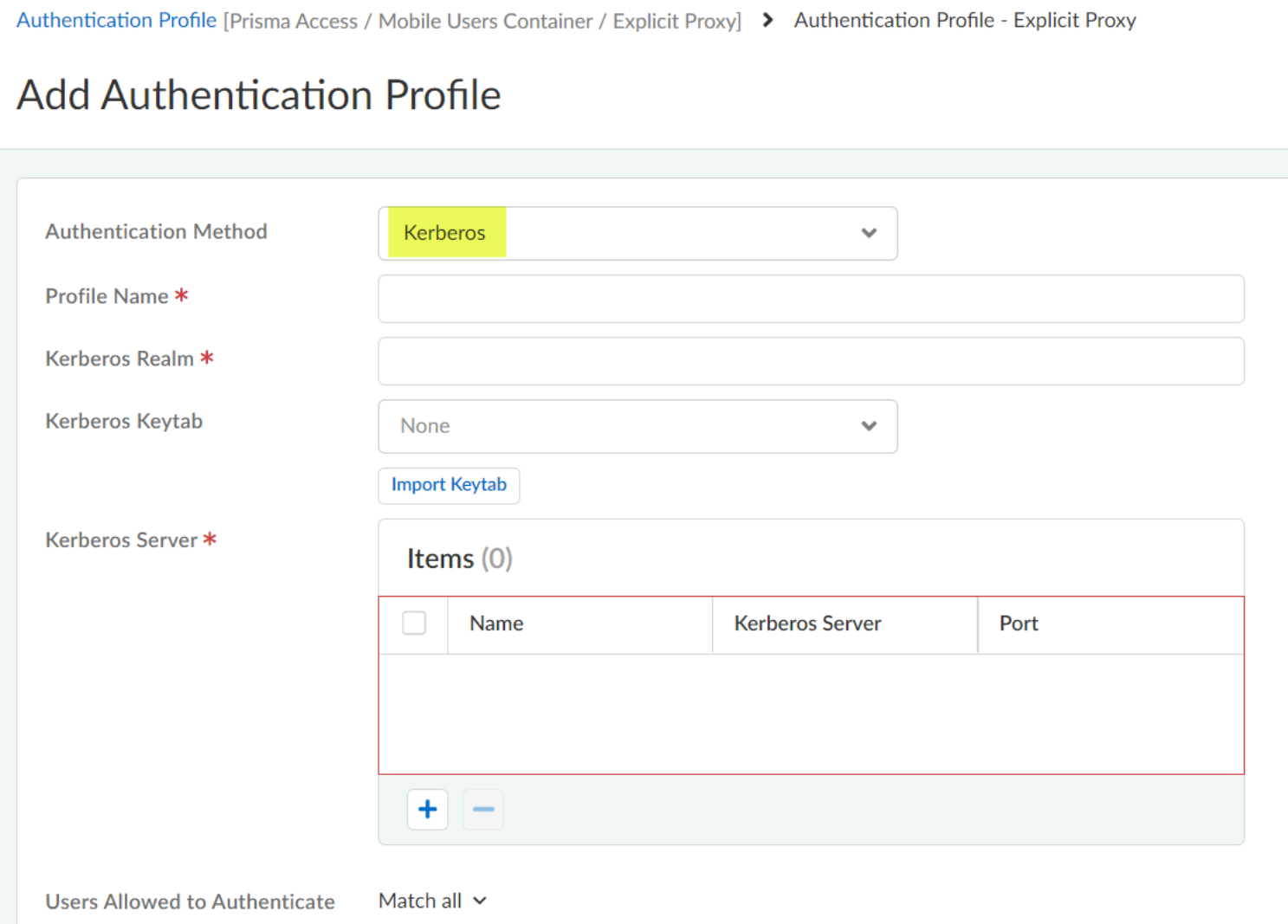
该配置文件定义了显式代理如何连接到 Kerberos 服务器以进行移动用户身份验证。

1. 转到 **Manage**（管理） > **Configuration**（配置） > **NGFW** 和 **Prisma Access** > **Identity Services**（身份服务） > **Authentication**（身份验证） > **Authentication Profiles**（身份验证配置文件），单击 **Add Profile**（添加配置文件）。



2. 选择 **Authentication Method**（身份验证方法）：**Kerberos**。

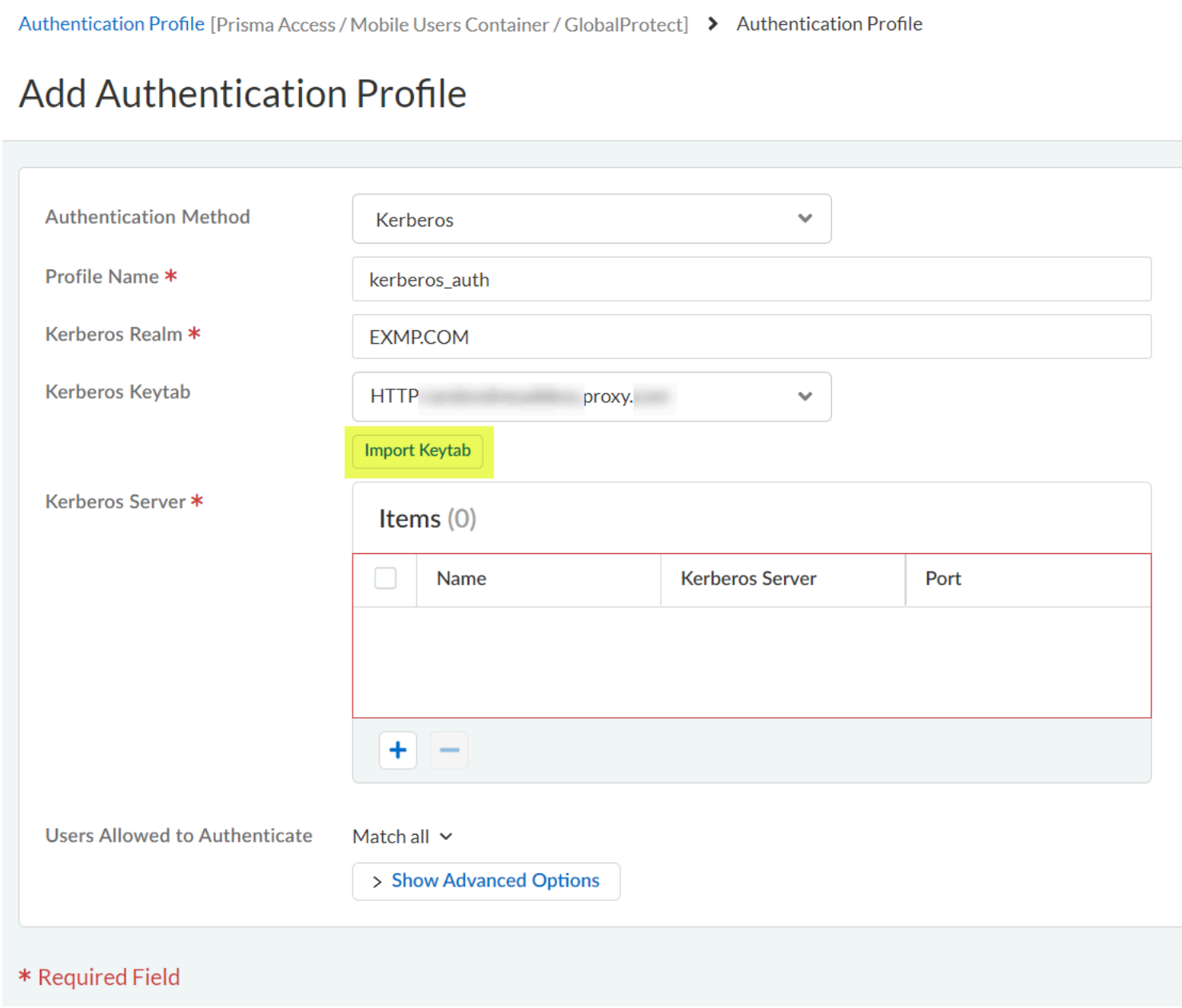
 ©2025 Palo Alto Networks, Inc.



3. 输入 **Profile Name**（配置文件名称）以标识服务器配置文件。

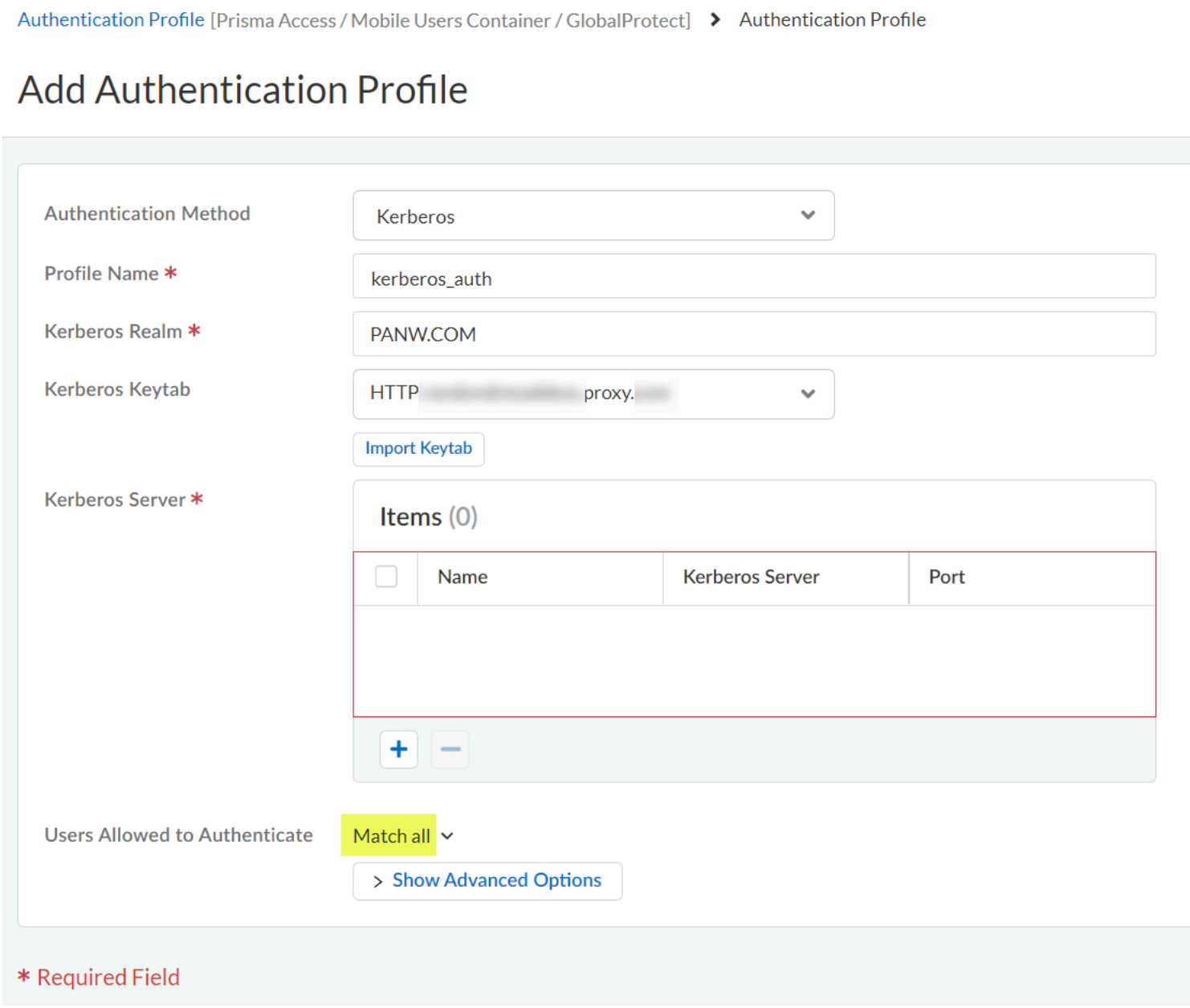
   身份验证配置文件指定了门户或网关验证用户身份时使用的服务器配置文件。
4. 输入 **Kerberos Realm**（**Kerberos** 域）（最多 127 个字符）以指定用户登录名的主机名部分。例如，用户帐户名 user@EXMP.COM 的领域为 EXMP.COM。
5. 导入您之前创建的 **Kerberos Keytab**（**Kerberos** 密钥表）（**Import Keytab**（导入密钥表））。

©2025 Palo Alto Networks, Inc.



6. 使用此配置文件添加 **Users Allowed to Authenticate**（允许进行身份验证的用户）。
   - 要选择所有用户，请选择 **Match all**（匹配全部）。
   - 如果您使用 Cloud Identity Engine 填充用户列表，请从列表中选择用户，或选择 **all**（全部）以允许所有用户进行身份验证。
   - 要添加可以使用 Kerberos 登录的本地用户，请单击 **Add Local User**（添加本地用户），添加 **Name**（名称）并创建 **Password**（密码）。
     - 配置用户身份验证和用户映射时，请使用 userPrincipalName (UPN) 格式；不支持其他格式（例如 samAccountName）。
     - 不支持 Unicode 字符的用户名。

©2025 Palo Alto Networks, Inc.

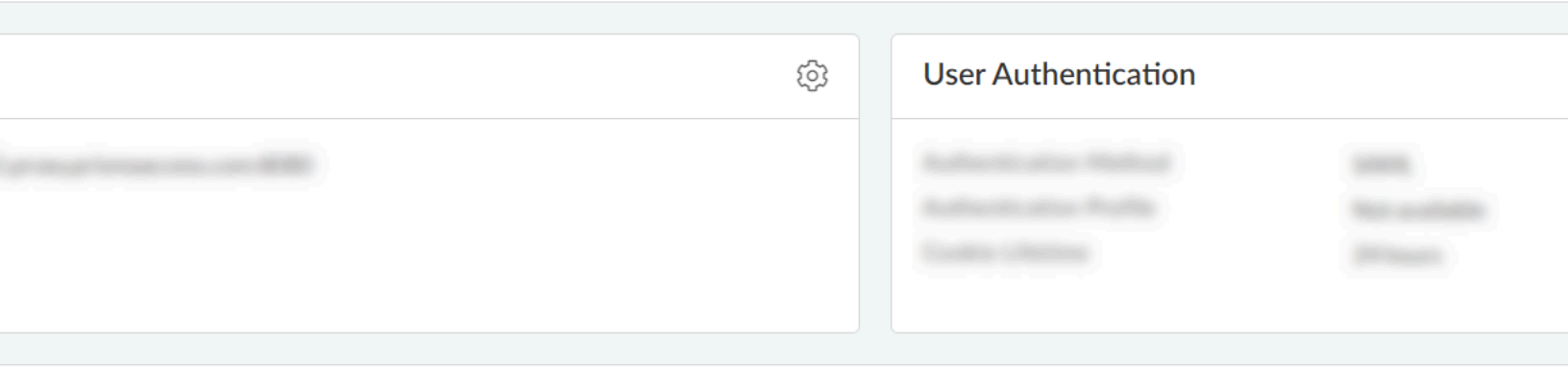


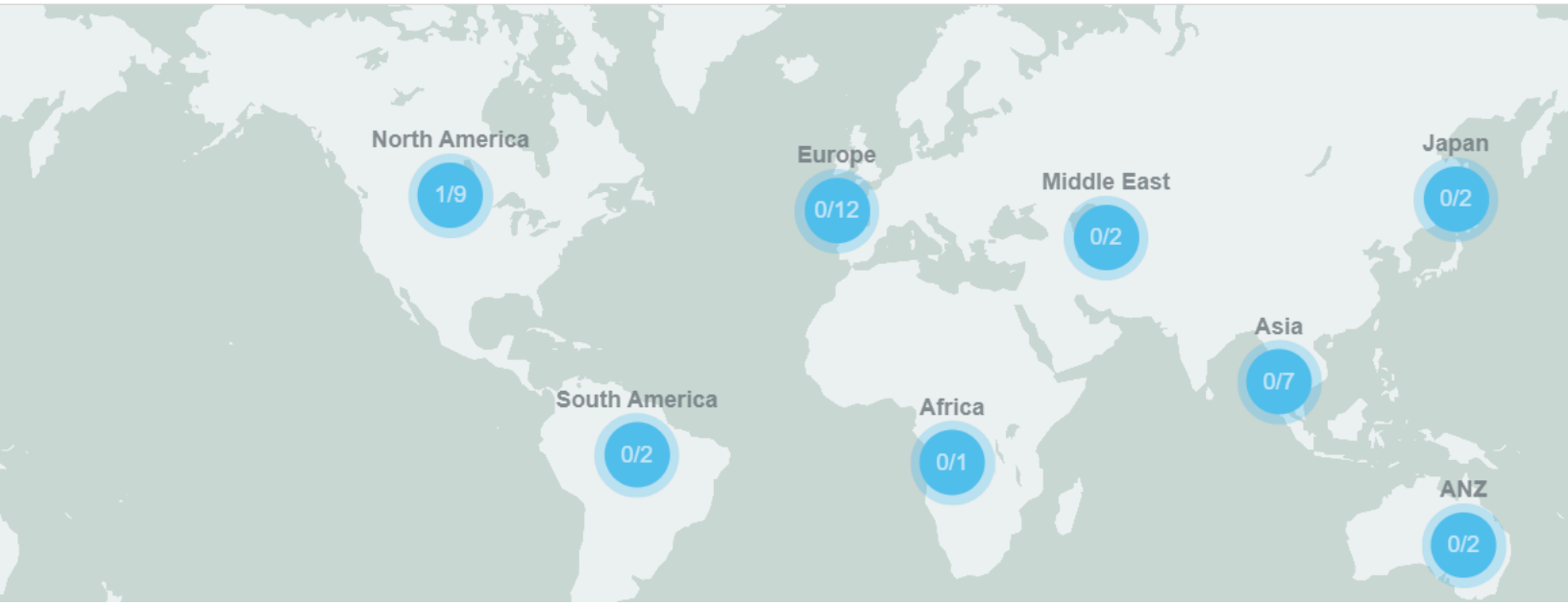
7. **Save**（保存）更改。

©2025 Palo Alto Networks, Inc.

STEP 2 | 将身份验证配置文件与身份验证方法关联。

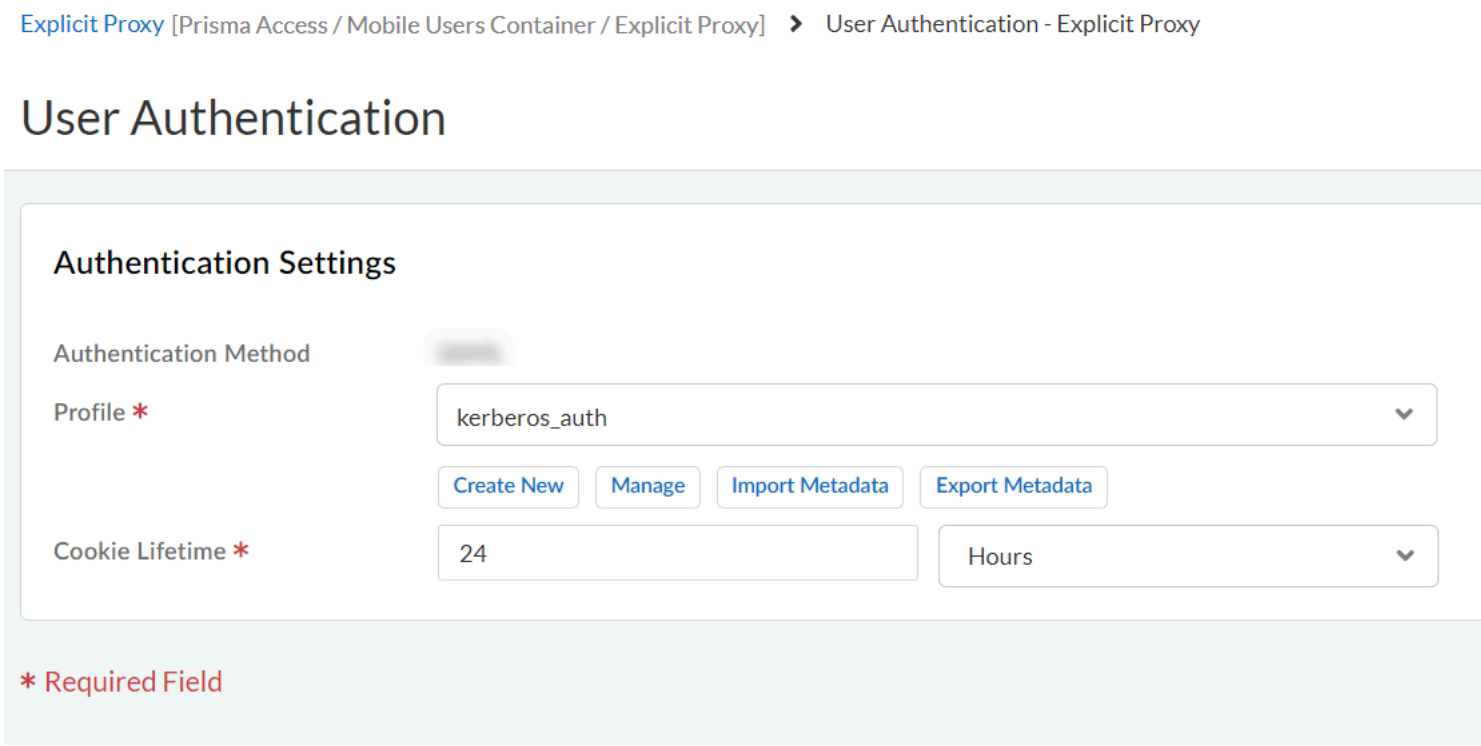
1. 转到 **Workflows**（工作流） > **Prisma Access** 设置 > **Explicit Proxy**（显式代理） > **User Authentication**（用户身份验证）。





2. 选择 **Connection Name**（连接名称）。
3. 在 **Authentication Method**（身份验证方法）中选择 **Kerberos**，然后选择您创建的 Kerberos **Profile**（配置文件）。

©2025 Palo Alto Networks, Inc.



4. **Save**（保存）更改。

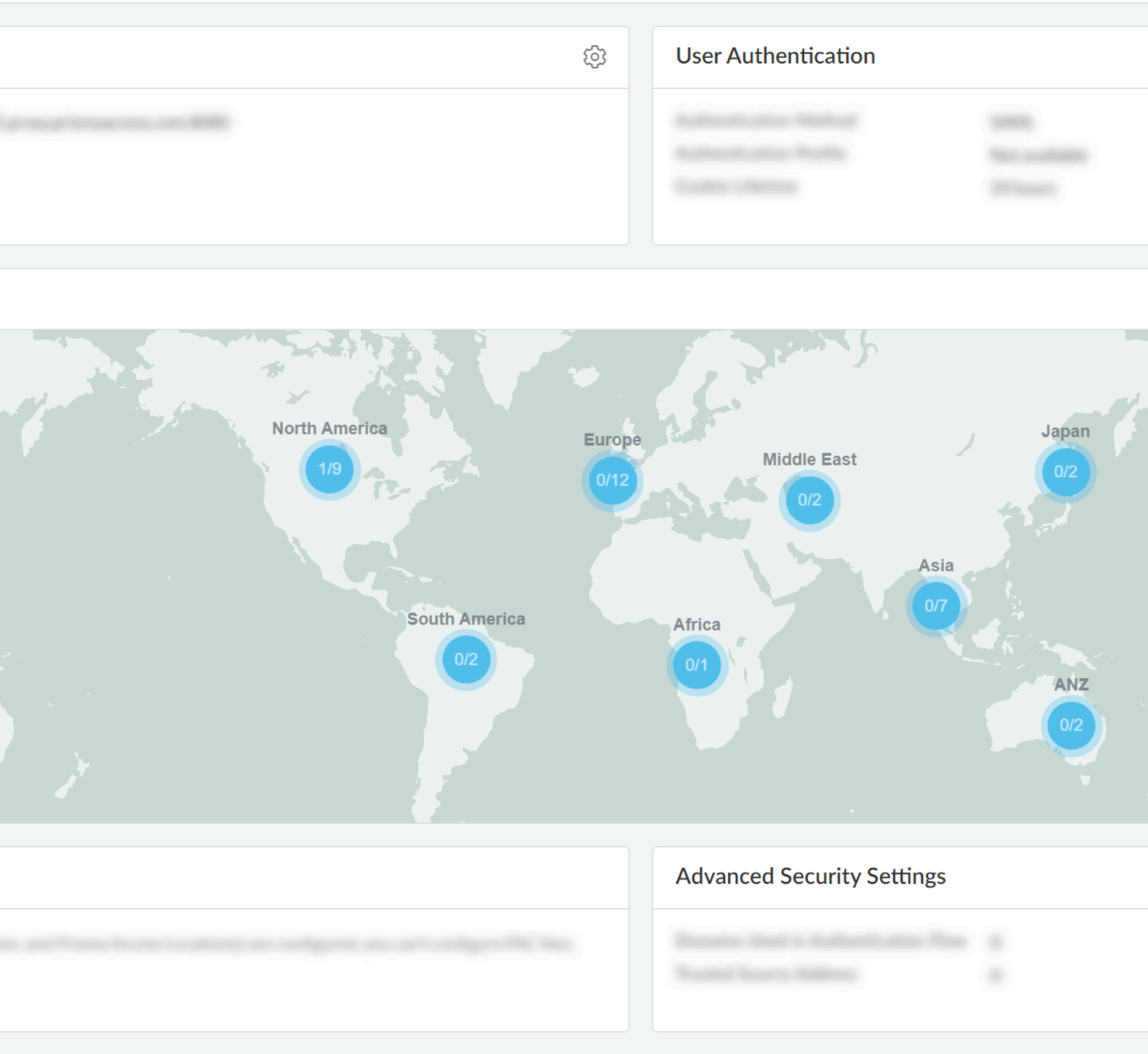
©2025 Palo Alto Networks, Inc.

STEP 3 | （可选）将用户、服务器、物联网设备或无头计算机所在的分支机构或园区位置的出口 IP 地址添加到受信任的显式代理地址列表中。

仅当您想为特定 IP 地址 **Skip Authentication**（跳过身份验证）或 **Use X-Authenticated User (XAU) header on incoming HTTP/HTTPS requests for identity**（在传入的 **HTTP/HTTPS** 身份请求上使用 **X-Authenticated-User (XAU)** 标头）时才需要执行此操作。

1. 转到 **Workflows**（工作流） > **Prisma Access** 设置 > **Explicit Proxy**（显式代理） > **Advanced Security Settings**（高级安全设置）。

 ©2025 Palo Alto Networks, Inc.

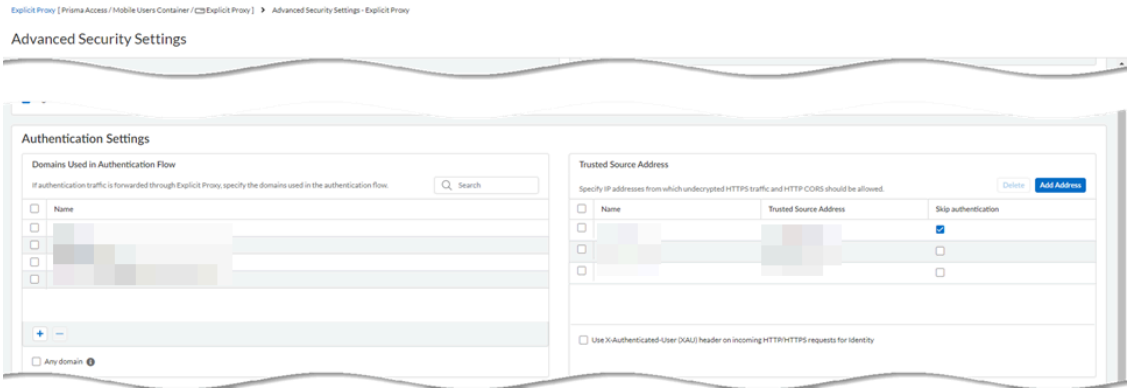


2. **Add Address**（添加地址）（一个或多个）到 **Trusted Source Address**（可信源地址）字段。

 ©2025 Palo Alto Networks, Inc.

如果未将出口端点 IP 地址添加到受信任的列表中，则显式代理会强制用户和计算机使用 SAML 和 Kerberos 进行身份验证。

最多输入 100,000 个 IP 地址。



3. **Save**（保存）更改。

STEP 4 | 为用户身份验证创建 allow-all 策略规则。

1. 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW** 和 **Prisma Access** > **Security Services**（安全服务） > **Security Policy**（安全策略） > **Add Rule**（添加规则） > **Pre Rules**（预规则） > **.**。
2. 命名该规则。
3. 将所有必需的匹配条件设置为 **Any**（任意）。
4. 将用户设置为 **Known**（已知）
5. 将操作设置为 **Allow**（允许）。
6. **Save**（保存）规则。

STEP 5 | 推送您的配置更改。

 ©2025 Palo Alto Networks, Inc.

STEP 6 | 通过查看流量和身份验证日志，确认 Kerberos 身份验证是否可与 Prisma Access 一起使用。

1. （仅限已解密流量）转到 **Activity**（活动） > **Log Viewer**（日志查看器） > **Firewall/Traffic**（防火墙/流量），检查 Kerberos 身份验证是否正常工作。

   如果您使用的是 *Strata Cloud Manager*，请转到 ***Incidents & Alerts***（事件和警报） > ***Log Viewer***（日志查看器） > ***Firewall/Traffic***防火墙/流量）。

   已解密流量在流量日志中显示用户名。

2. （仅限未解密流量）转到 **Activity**（活动） > **Log Viewer**（日志查看器） > **Firewall/Authentication**（防火墙/身份验证），检查 Kerberos 身份验证是否正常工作。

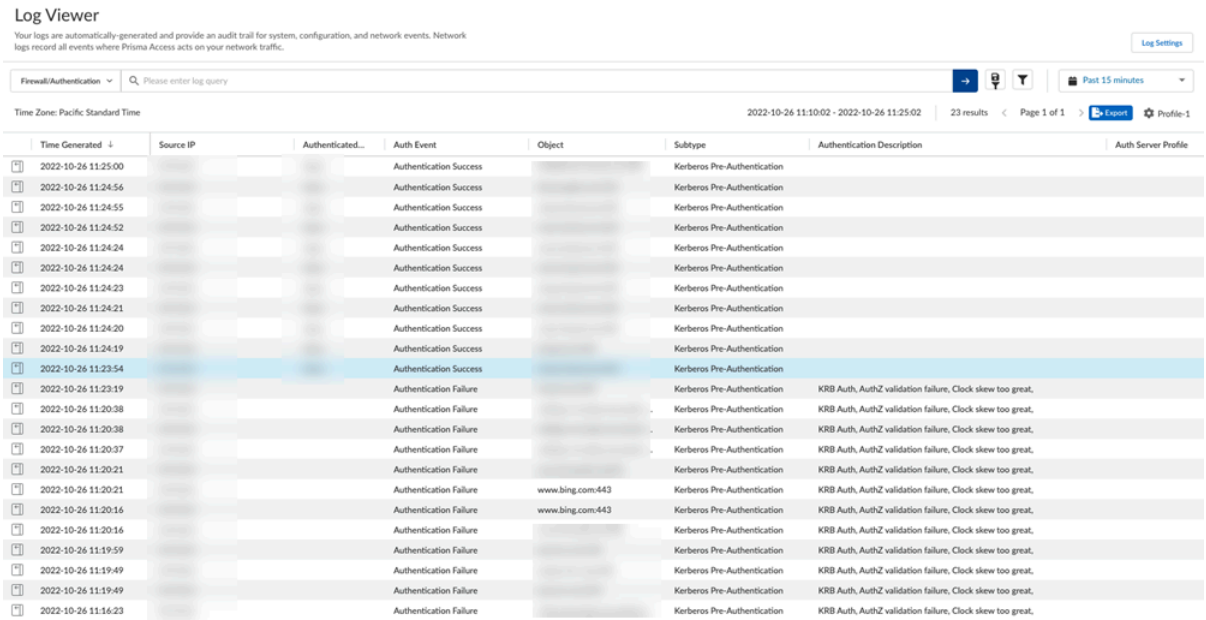
   如果您使用的是 *Strata Cloud Manager*，请转到 ***Incidents & Alerts***（事件和警报） > ***Log Viewer***（日志查看器） > ***Firewall/Authentication***（防火墙/身份验证）。

   以下字段提供身份验证事件的更多信息：

   - **Object**（对象）— 用户在重定向到 Kerberos 进行身份验证之前尝试访问的网站。
   - **Auth Event**（身份验证事件）— 身份验证尝试的状态。

     Authentication Success（身份验证成功）表示身份验证事件成功；**Authentication Failure**（身份验证失败）表示尝试失败并生成日志。
   - **Authentication Description**（身份验证说明）— 如果身份验证尝试失败，则提供有关失败类型的其他信息。

     例如，**user not allowed**（不允许用户使用）表示不允许该用户或组使用 Kerberos 进行身份验证，可能是因为未将其添加到身份验证配置文件的 **Allow List**（允许列表）中。



 ©2025 Palo Alto Networks, Inc.

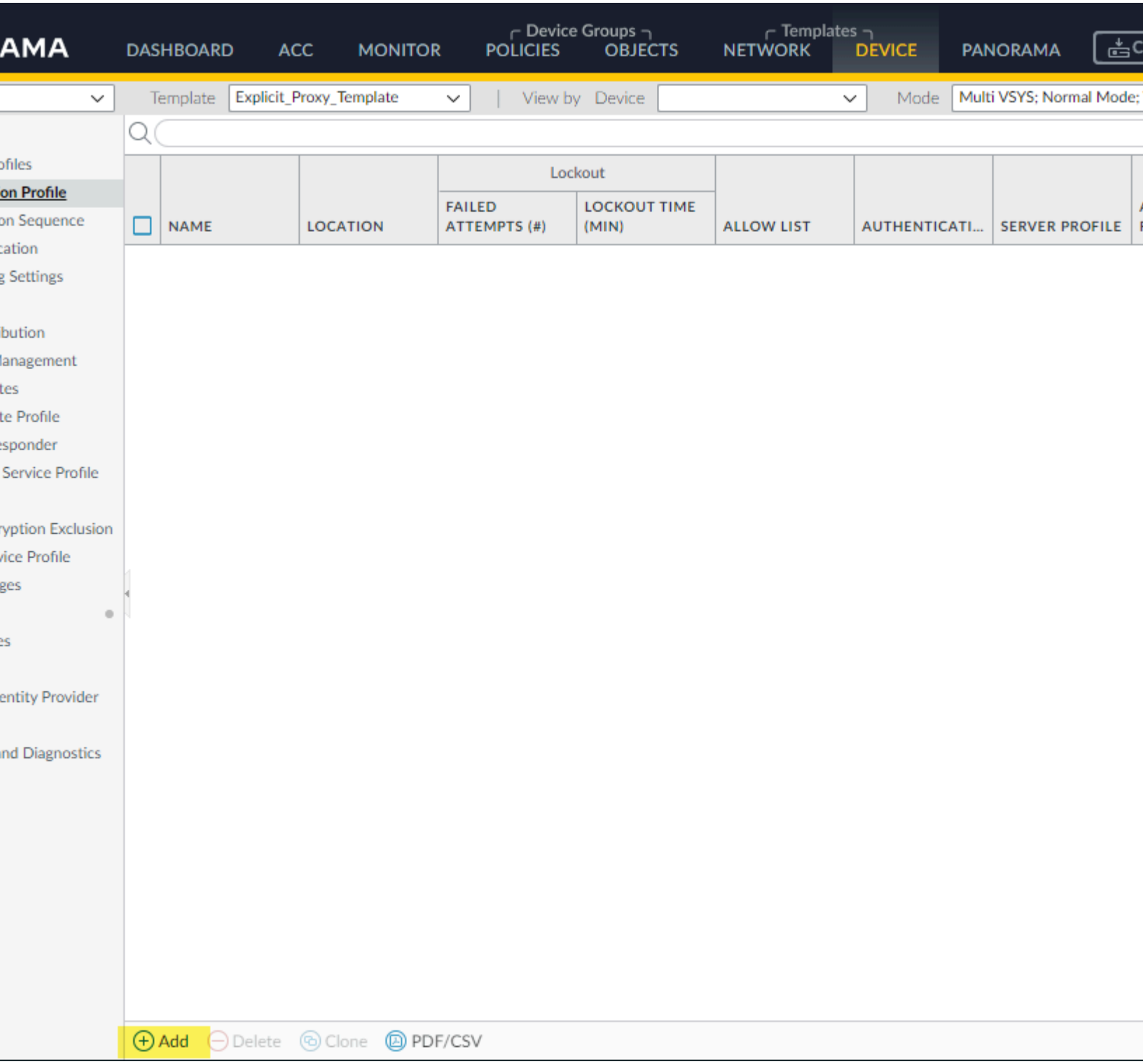
为显式代理部署配置 **Kerberos** 身份验证 **(Panorama**）

 ©2025 Palo Alto Networks, Inc.

STEP 1 | 设置 Kerberos 身份验证配置文件。

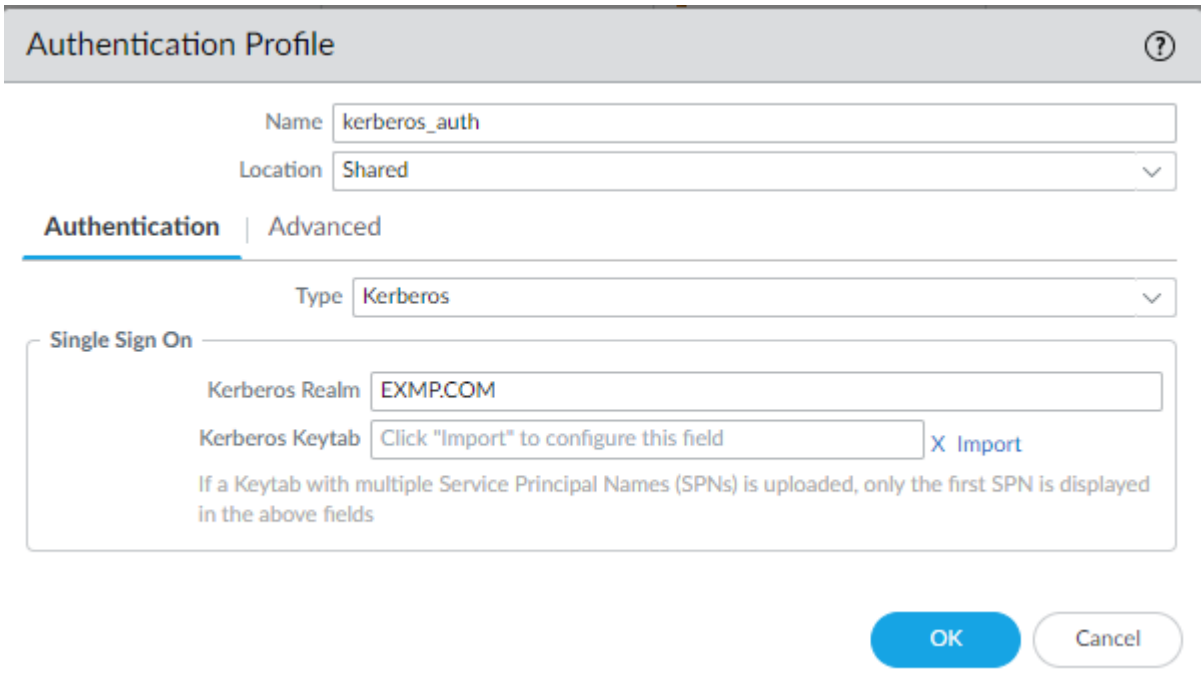
该配置文件定义了显式代理如何连接到 Kerberos 服务器以进行移动用户身份验证。

1. 转到 **Device**（设备） > **Authentication Profile**（身份验证配置文件） > **+ Add**（添加）。

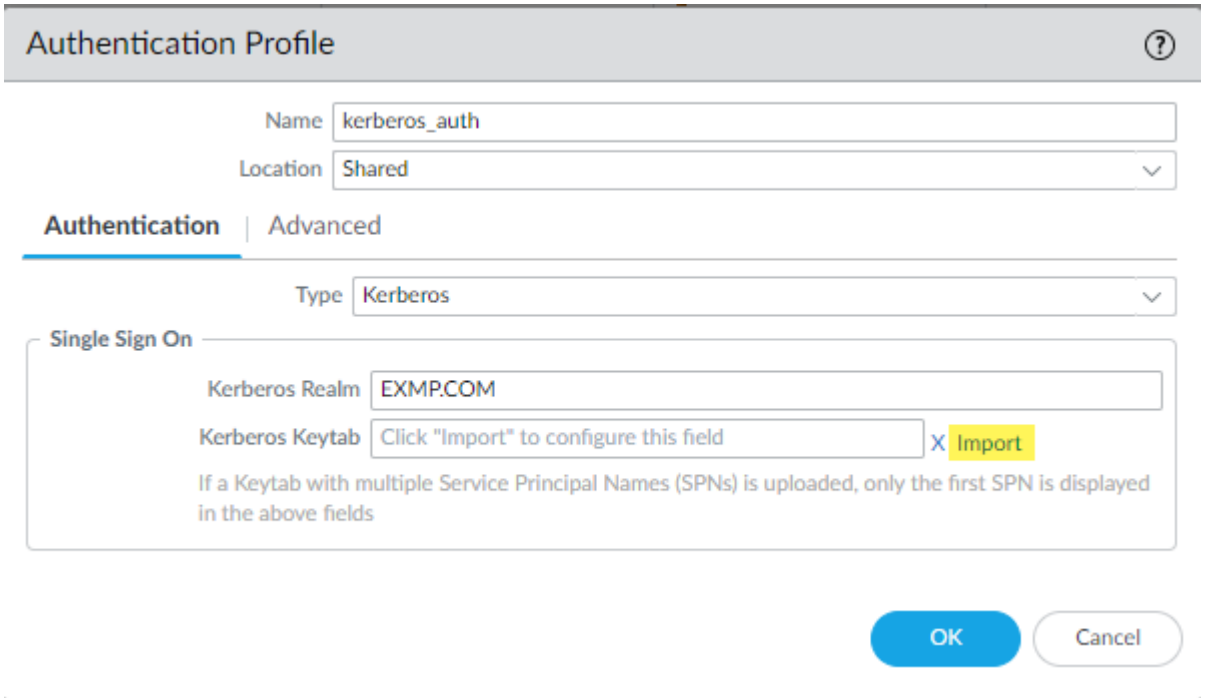


2. 选择 **Type**（类型）：**Kerberos**。

 ©2025 Palo Alto Networks, Inc.



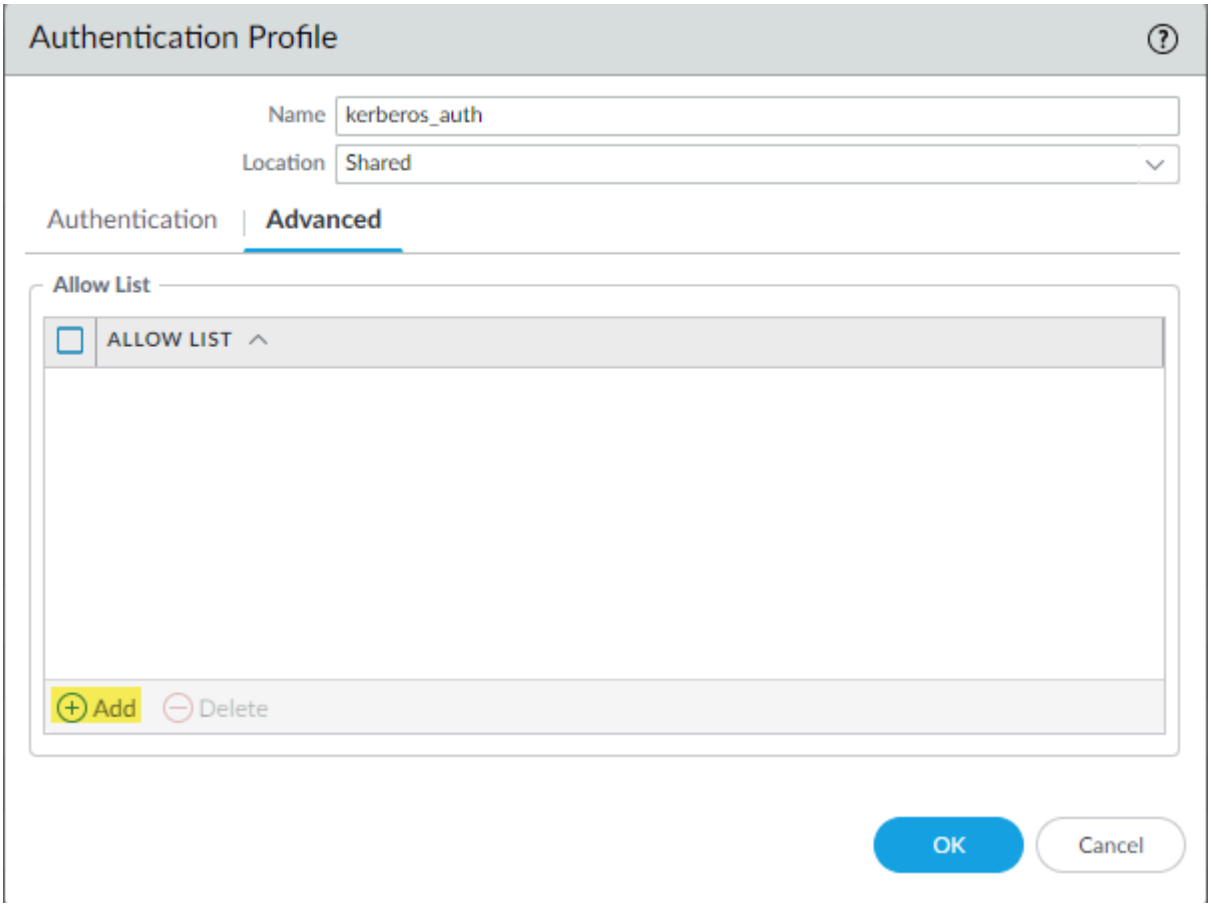
3. 输入 **Name**（名称）以标识身份验证配置文件。
4. 输入 **Kerberos Realm**（**Kerberos** 域）（最多 127 个字符）以指定用户登录名的主机名部分。例如，用户帐户名 user@EXMP.COM 的领域为 EXMP.COM。
5. **Import**（导入）您之前创建的 Kerberos 密钥表。



6. 使用此配置文件添加允许进行身份验证的用户。
   - 选择 **Advanced**（高级） > **+ Add**（添加）
   - 要选择所有用户，请选择 **all**（全部）。

 ©2025 Palo Alto Networks, Inc.

- 如果您使用 Cloud Identity Engine 填充用户列表，请从列表中选择用户，或选择 **all**（全部）以允许所有用户进行身份验证。
- 要添加可以使用 Kerberos 登录的本地用户，请输入其用户名。
  - 配置用户身份验证和用户映射时，请使用 userPrincipalName (UPN) 格式；不支持其他格式（例如 samAccountName）。
  - 不支持 Unicode 字符的用户名。



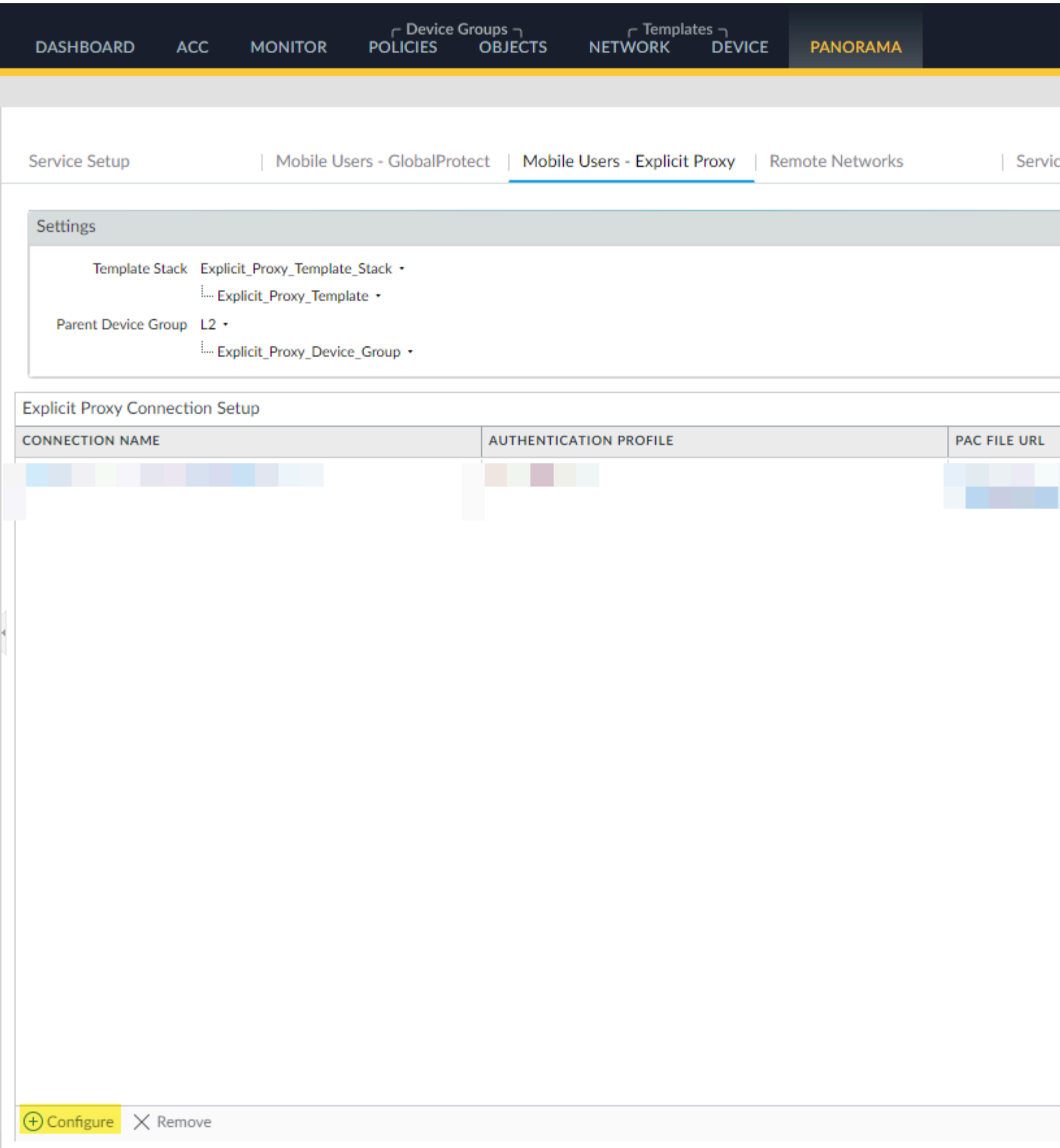
7. **Save**（保存）更改。

 ©2025 Palo Alto Networks, Inc.

STEP 2 | 将身份验证配置文件与身份验证方法关联。

1. 转到 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **+ Configure**（配置）。

 ©2025 Palo Alto Networks, Inc.



©2025 Palo Alto Networks, Inc.

2. 设置 **Explicity Proxy FQDN**（显式代理 **FQDN**）。
3. 选择您创建的 Kerberos **Profile**（配置文件）。
4. 选择 **OK**（确定）以保存更改。

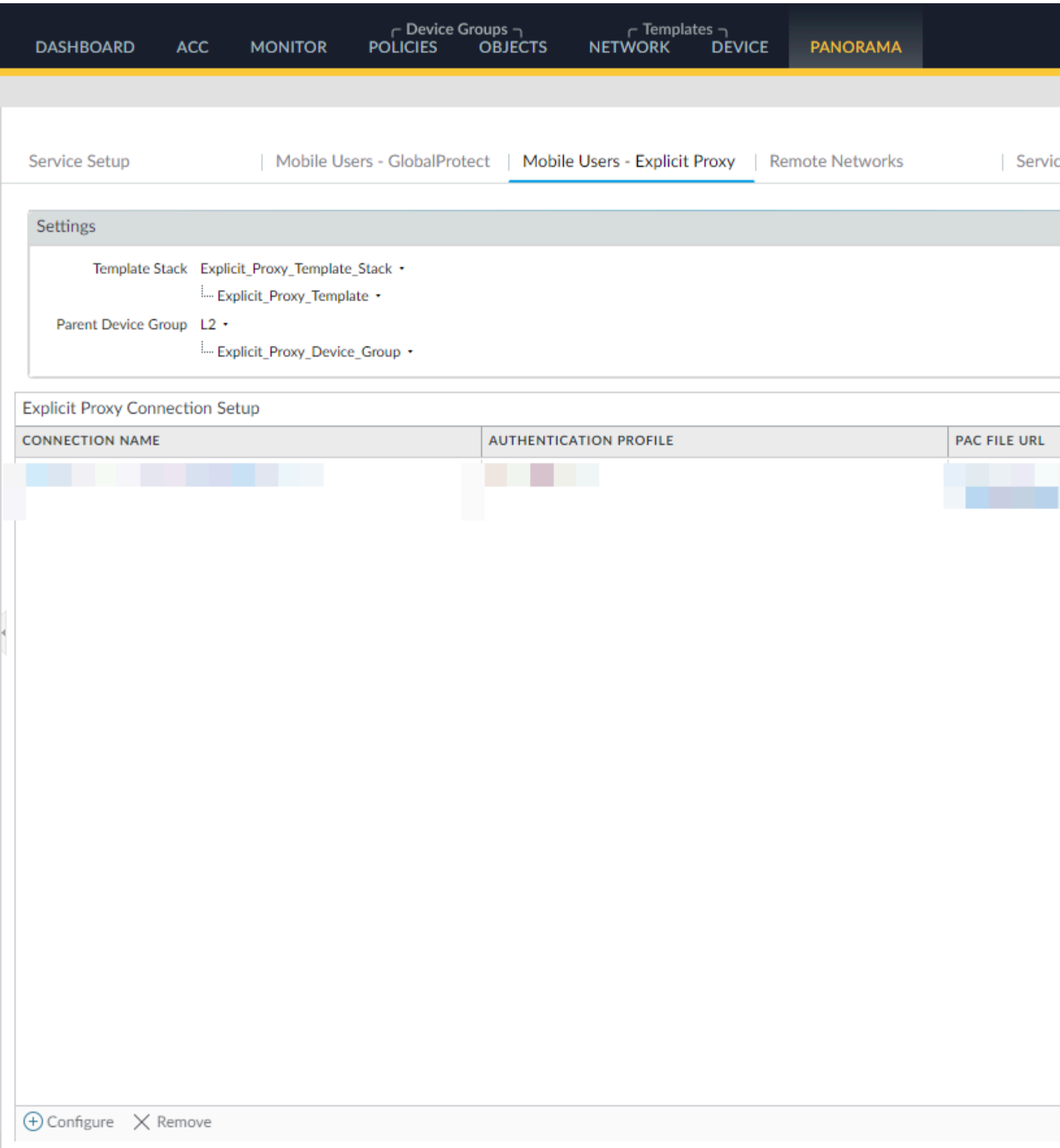
 ©2025 Palo Alto Networks, Inc.

STEP 3 | （可选）将用户、服务器、物联网设备或无头计算机所在的分支机构或园区位置的出口 IP 地址添加到受信任的显式代理地址列表中。

仅当您想为特定 IP 地址 **Skip Authentication**（跳过身份验证）或 **Use X-Authenticated User (XAU) header on incoming HTTP/HTTPS requests for identity**（在传入的 **HTTP/HTTPS** 身份请求上使用 **X-Authenticated-User (XAU)** 标头）时才需要执行此操作。

1. 转到 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Settings gear**（设置齿轮） > **Authentication Settings**（身份验证设置）。

 ©2025 Palo Alto Networks, Inc.



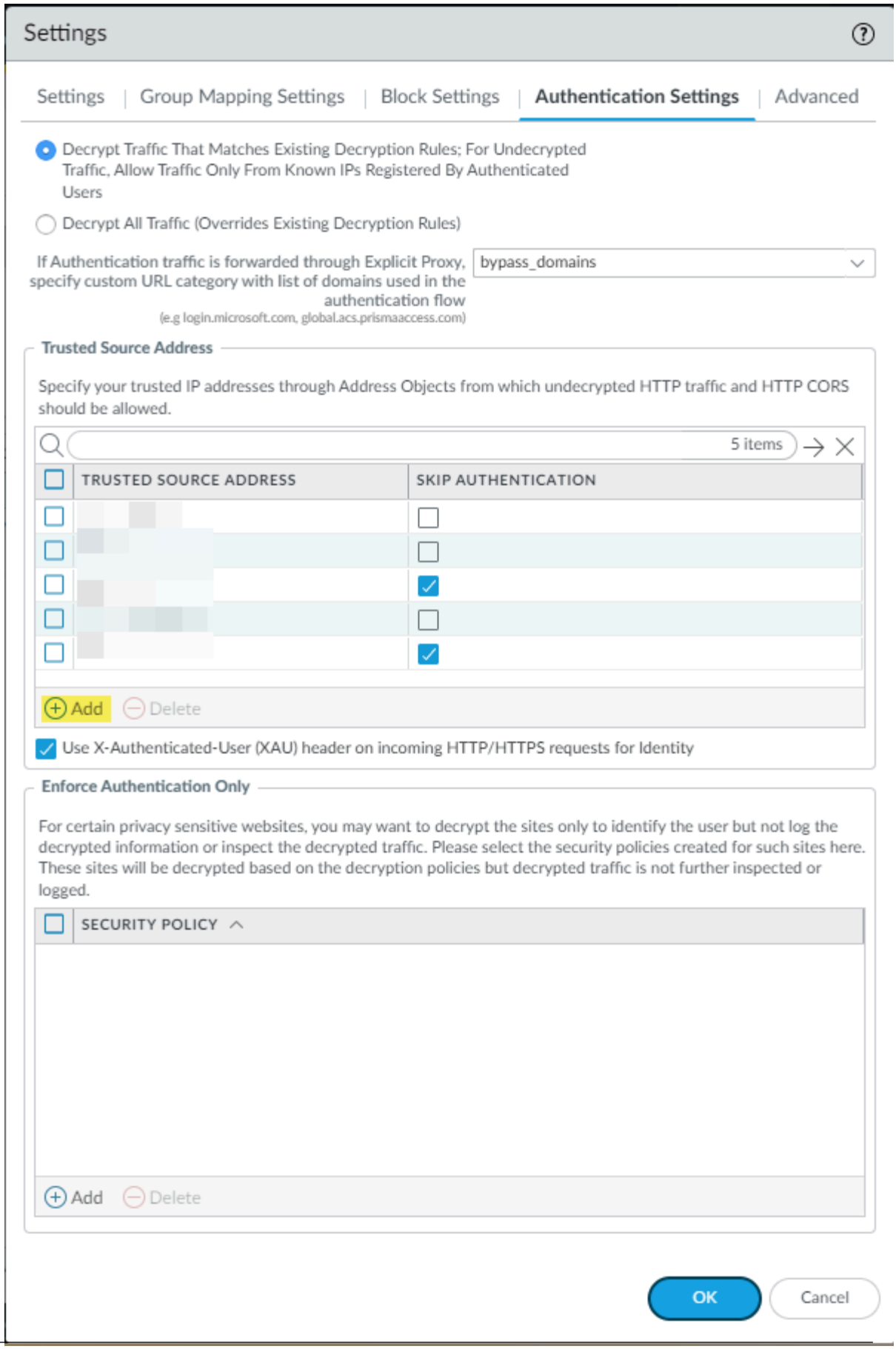
 ©2025 Palo Alto Networks, Inc.

2. **Add**（添加）地址到 **Trusted Source Address**（可信源地址）字段。

   如果未将出口端点 IP 地址添加到受信任的列表中，则显式代理会强制用户和计算机使用 SAML 和 Kerberos 进行身份验证。

   最多输入 100,000 个 IP 地址。

©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.

3. 选择 **OK**（确定）以保存更改。

STEP 4 | 为用户身份验证创建 allow-all 策略规则。

1. 选择 **Policies**（策略） > **Pre Rules**（预规则） > **+ Add**（添加）。
2. 命名该规则。
3. 选择 **Source**（源）
4. 将源用户设置为 **known-user**（已知用户）
5. 将所有其他必需值设置为 **Any**（任意）。
6. 选择 **OK**（确定）以保存规则。

STEP 5 | 提交并推送您的配置更改。

STEP 6 | 通过查看流量和身份验证日志，确认 Kerberos 身份验证是否可与 Prisma Access 一起使用。

1. （仅限已解密流量）转到 **Monitor**（监控） > **Log**（日志） > **Traffic**（流量），检查 Kerberos 身份验证是否正常工作。

   已解密流量在流量日志中显示用户名。

2. （仅限未解密流量）转到 **Monitor**（监控） > **Log**（日志） > **Authentication**（身份验证），检查 Kerberos 身份验证是否正常工作。

   以下字段提供身份验证事件的更多信息：

   - **Object**（对象）— 用户在重定向到 Kerberos 进行身份验证之前尝试访问的网站。
   - **Auth Event**（身份验证事件）— 身份验证尝试的状态。

     Authentication Success（身份验证成功）表示身份验证事件成功；**Authentication Failure**（身份验证失败）表示尝试失败并生成日志。
   - **Authentication Description**（身份验证说明）— 如果身份验证尝试失败，则提供有关失败类型的其他信息。

     例如，**user not allowed**（不允许用户使用）表示不允许该用户或组使用 Kerberos 进行身份验证，可能是因为未将其添加到身份验证配置文件的 **Allow List**（允许列表）中。

用于显式代理部署的 Cloud Identity Engine 身份验证

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证

使用 Cloud Identity Engine 为 Prisma Access—显式代理部署中的移动用户提供用户标识和用户身份验证。

©2025 Palo Alto Networks, Inc.

Cloud Identity Engine 为本地、基于云或混合网络环境中基于云的集中式解决方案提供用户标识和用户身份验证。Cloud Identity Engine 允许您根据用户和组编写安全策略，并通过实施基于行为的安全操作来帮助保护您的网络。

通过持续同步目录中的信息（无论是本地目录、基于云的目录还是混合目录），确保您的用户信息是准确且最新的，并且即使云身份提供程序暂时不可用，也能根据映射继续实施策略。

- 用于显式代理部署的 Cloud Identity Engine 身份验证 (Strata Cloud Manager)
- 用于显式代理部署的 Cloud Identity Engine 身份验证 (Panorama)

用于显式代理部署的 Cloud Identity Engine 身份验证 (Strata Cloud Manager)

Cloud Identity Engine 为 Prisma Access—显式代理部署中的移动用户提供用户识别和用户身份验证。Cloud Identity Engine 与显式代理身份验证缓存服务 (ACS) 集成，并使用 SAML 身份提供程序 (IdP) 为显式代理移动用户提供身份验证。

要使用 Cloud Identity Engine 为移动用户—显式代理部署配置身份验证，请完成以下步骤。

STEP 1 | 在 Prisma Access (Managed by Strata Cloud Manager) 中，为您的租户设置显式代理。

在配置显式代理之前，请了解显式代理的工作方式以及配置显式代理时应使用的准则。

如果您有多个租户，请为每个需要的租户配置显式代理。

STEP 2 | 登录到中心，并在 Cloud Identity Engine 应用程序中设置身份验证类型和身份验证提供商。

您可以按租户或支持帐户查看中心内的应用程序。

1. 在 Cloud Identity Engine 中配置 SAML 身份验证类型。

   Cloud Identity Engine 入门指南包含在 Cloud Identity Engine 中配置 SAML IdP 所需的步骤：

   - 在 Cloud Identity Engine 中将 Azure 配置为 IdP
   - 在 Cloud Identity Engine 中将 Okta 配置为 IdP
   - 在 Cloud Identity Engine 中将 PingOne 配置为 IdP
   - 在 Cloud Identity Engine 中将 PingFederate 配置为 IdP
   - 在 Cloud Identity Engine 中将 Google 配置为 IdP

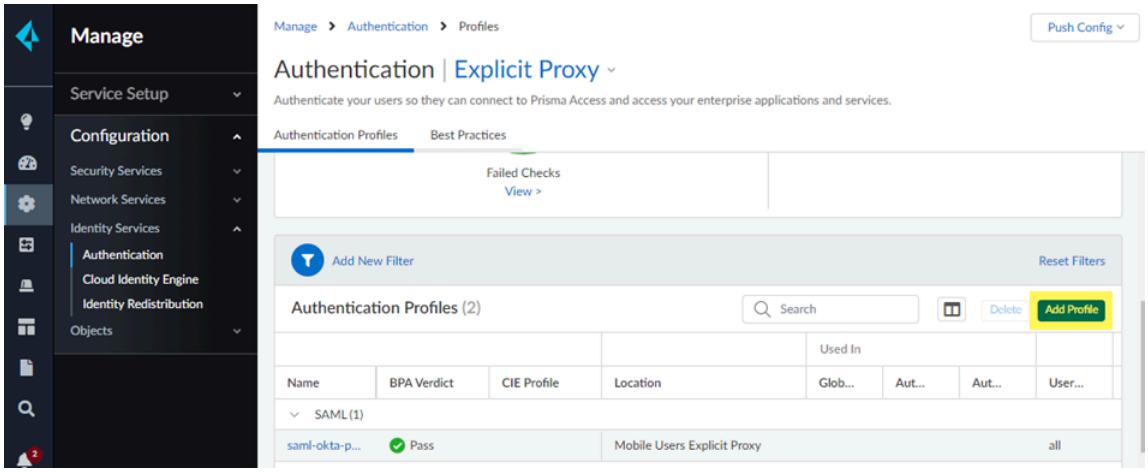
   请勿配置单点注销，这种方式不受支持。
2. 在 Cloud Identity Engine 中设置身份验证配置文件，并选择可以使用此身份验证方法的用户和组。

   当您在后续步骤中在 Prisma Access (Managed by Strata Cloud Manager) 中创建身份验证配置文件时指定此配置文件。

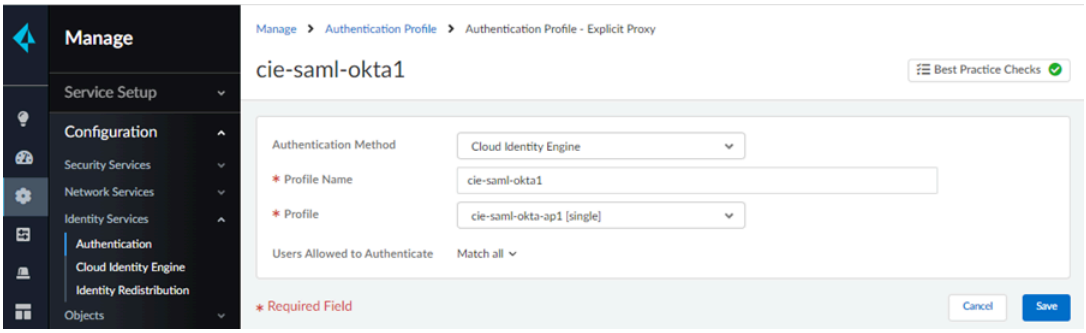
©2025 Palo Alto Networks, Inc.

STEP 3 | 返回 Prisma Access (Managed by Strata Cloud Manager) 并创建用于 Cloud Authentication Engine 的身份验证配置文件。

1. 转到 **Manage**（管理） > **Configuration**（配置） > **NGFW** 和 **Prisma Access** > **Identity Services**（身份服务） > **Authentication**（身份验证），将范围设置为 **Explicit Proxy**（显式代理），然后添加身份验证配置文件（**Add Profile**（添加配置文件））。



2. 选择 **Cloud Identity Engine** 的 **Authentication Method**（身份验证方法）。
3. 为该配置文件指定 **Profile Name**（配置文件名称）。
4. 选择您在上一步中创建的 Cloud Identity Engine 身份验证配置文件。

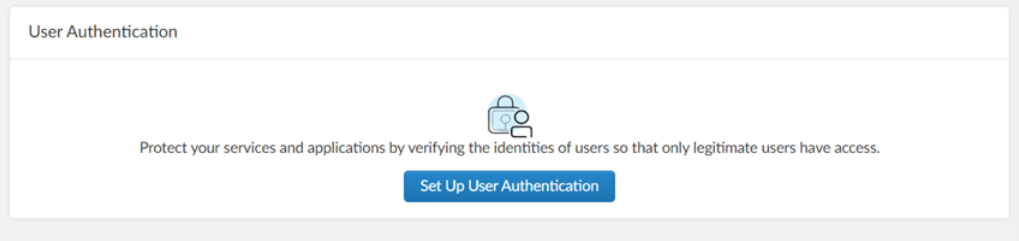


5. **Save**（保存）更改。

©2025 Palo Alto Networks, Inc.

STEP 4 | 在显式代理中设置用户身份验证。

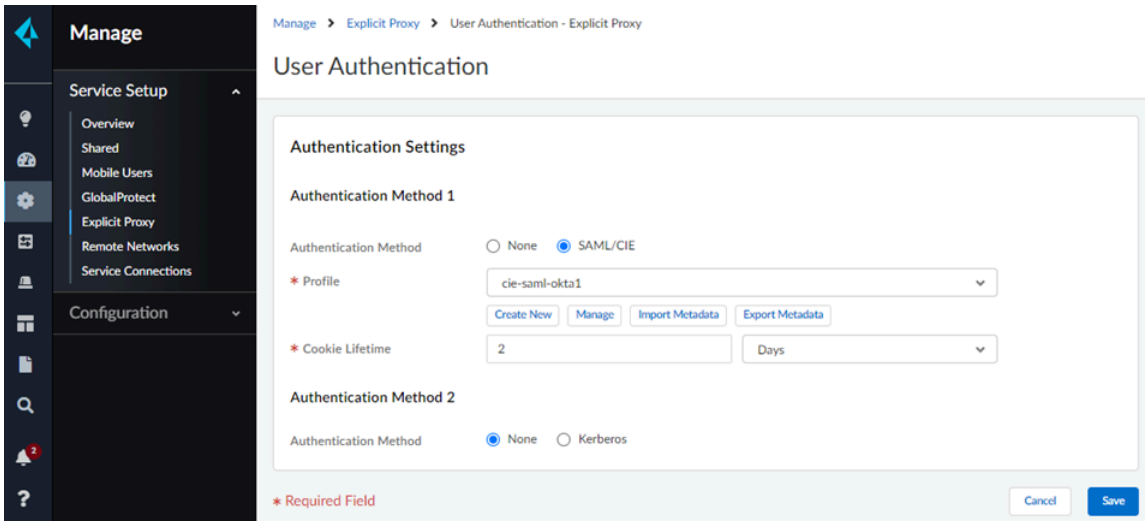
1. 转到 **Workflows**（工作流） > **Prisma Access** 设置 > **Explicit Proxy**（显式代理），单击 **Set Up User Authentication**（设置用户身份验证）。



2. 选择 **SAML/CIE** 作为 **Authentication Method**（身份验证方法）。
3. 选择您在云托管的 Prisma Access 中创建的身份验证配置文件。
4. 为存储用户身份验证凭据的 Cookie 指定 **Cookie Lifetime**（**Cookie** 生命周期）。

   IdP 对用户进行身份验证后，Prisma Access 会将用户的身份验证状态存储在身份验证缓存服务 (ACS) 中。身份验证的有效期取决于您在此处指定的 Cookie 生命周期值。

   为避免出现用户在 Cookie 生命周期到期前无法下载大文件，或者用户长时间访问单个网站时 Cookie 过期的问题，Palo Alto Networks 建议将 **Cookie Lifetime**（**Cookie** 生命周期）配置为至少一天。如果显式代理用户遇到 Cookie 生命周期过期问题，他们可以浏览到其他网站以重新向 ACS 进行身份验证并刷新 ACS Cookie。

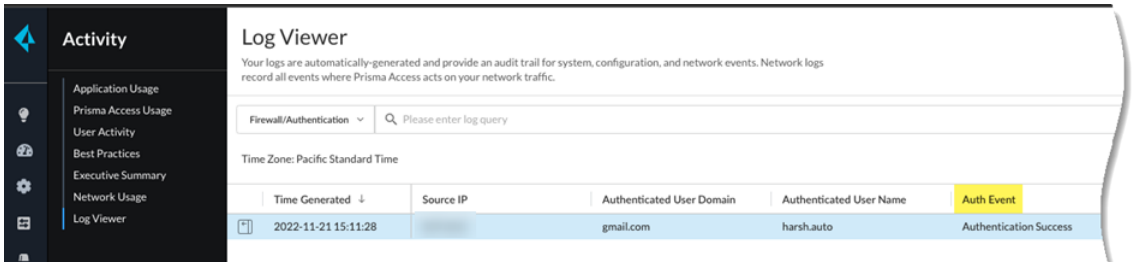


5. **Save**（保存）更改。

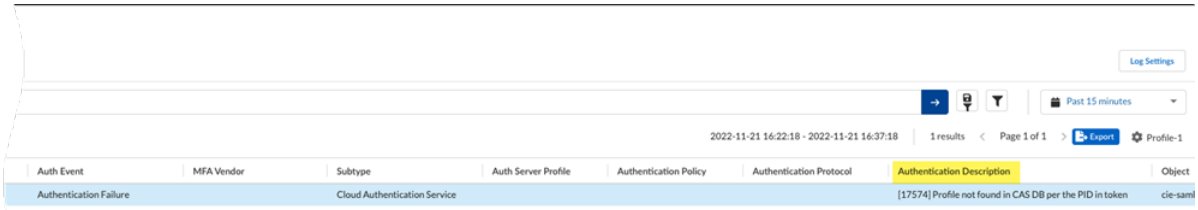
©2025 Palo Alto Networks, Inc.

STEP 5 | 验证 Cloud Identity Engine 是否成功验证显式代理移动用户的身份。

1. 在 Prisma Access (Managed by Strata Cloud Manager) 中，选择 **Incidents & Alerts**（事件和警报） > **Log Viewer**（日志查看器） > **Firewall/Authentication**（防火墙/身份验证）。
2. 查看 **Auth Event**（身份验证事件）状态。

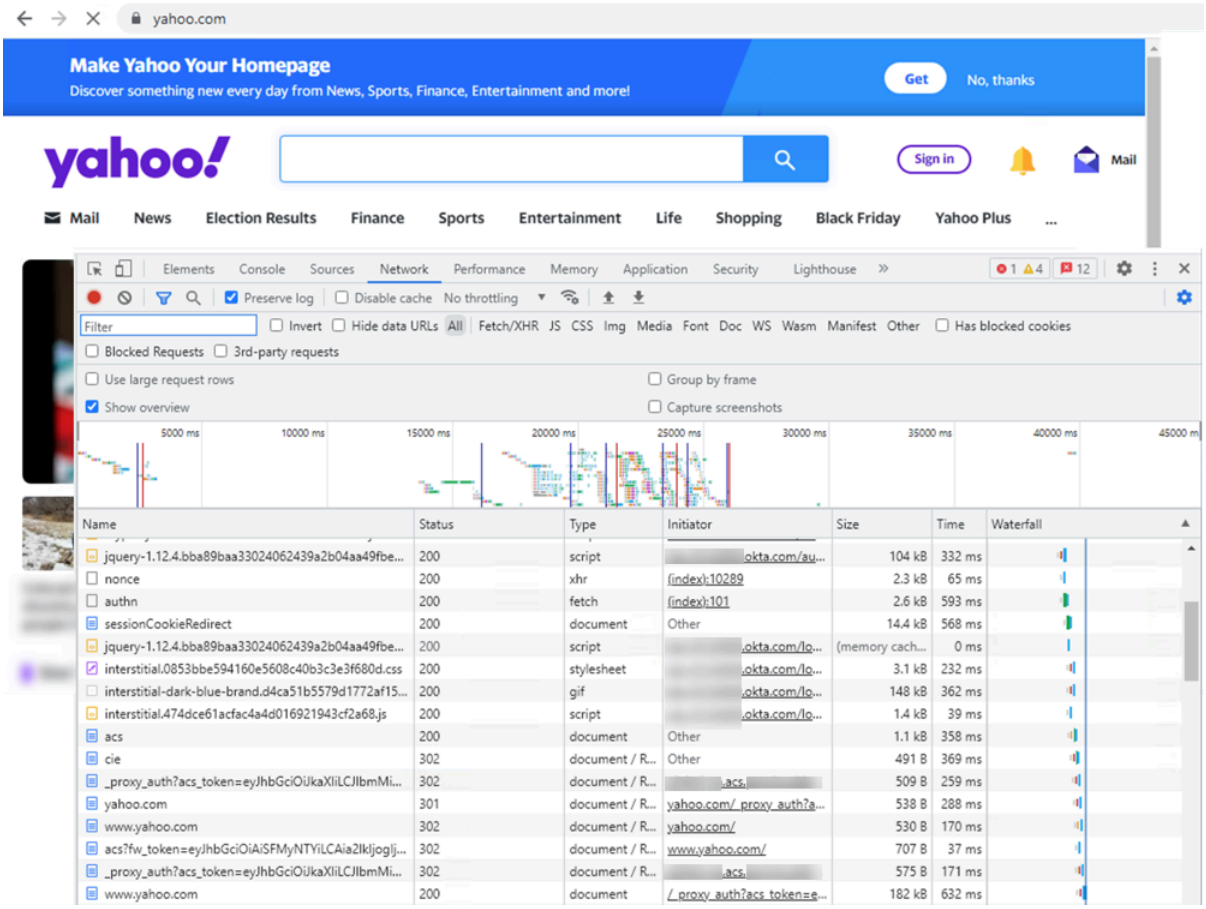


如果身份验证失败，请查看 **Authentication Description**（身份验证描述）以获取有关身份验证失败的更多详细信息。



3. 在移动用户的端点中，使用开发工具查看 Cloud Identity Engine 身份验证流程。

 ©2025 Palo Alto Networks, Inc.



用于显式代理部署的 Cloud Identity Engine 身份验证 (Panorama)

使用 Cloud Identity Engine 对 Prisma Access (Managed by Panorama) 显式代理移动用户进行身份验证

远程网络的代理模式

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) 如果您想在 Prisma Access 环境中启用基于私有源 IP 的显式代理可见性和实施，请联系客户团队以了解更多信息。	Prisma Access 许可证 远程网络的代理模式需要一个 Prisma Access 移动用户许可证和一个 Prisma Access 远程网络许可证。

远程网络上的代理模式有助于保护分支机构的用户和服务器的出站互联网流量，由于网络或合规性原因，这些分支机构需要基于 PAC 的连接方法。

您可以使用远程网络的代理模式：

- 保护来自使用非默认路由的分支站点的 Internet 流量。

©2025 Palo Alto Networks, Inc.

- 保护来自分支机构的互联网流量，无需将其回传到数据中心或总部站点。
- 通过私有 IP 地址连接到 Prisma Access 显式代理。

  Prisma Access 在全球为您提供四个任播 IP 地址，以及每个远程网络一个单播 IP 地址，您可以使用它们将流量转发到显式代理。
- 实施安全控制并根据分支机构系统的源 IP 获取可见性。
- 跳过基于源 IP 地址的服务器身份验证。
- 通过 IPSec 隧道从您的分支机构连接到 Prisma Access。
- 如果您需要超过 1000 Mbps 的带宽，可以使用多个远程网络连接创建高带宽远程网络连接，并在每个连接中指定显式代理任播和单播地址。

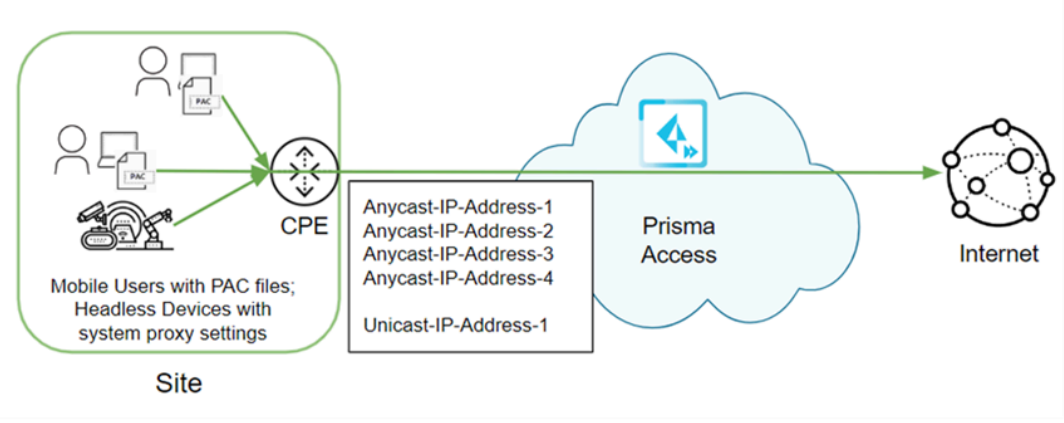
下图显示了为未配置默认路由的站点配置的远程网络。为了使用显式代理保护站点上的用户和无界面设备，管理员进行了以下配置更改：

- 已载入远程网络和显式代理位置，并已检索到 Prisma Access 从其基础设施子网中获取的任播和单播 IP 地址。

  您还可以为显式代理定向流量创建主机名，并将显式代理单播和任播 *IP* 地址添加到该主机名。
- 配置 CPE 以将显式代理流量转发到这些任播和单播地址。

  使用 PAC 文件中的任播 IP 地址，以便让 Prisma Access 从任何已载入的远程网络隧道中选择将流量转发到显式代理。使用单播地址，以便让 Prisma Access 通过特定远程网络隧道转发流量。在此示例中，您可以使用任播或单播地址，因为流量只通过一个远程网络 IPSec 隧道。
- 在用户端点的 PAC 文件中以及无界面设备的系统代理设置中指定这些 IP 地址。

配置完成后，Prisma Access 会将流量从远程网络隧道转发到显式代理。



- Strata Cloud Manager
- Panorama

远程网络的代理模式 (Strata Cloud Manager)

要使用 Cloud Managed Prisma Access 中的显式代理保护远程网络的用户，请完成以下步骤。

STEP 1 | 配置显式代理设置并载入要添加的显式代理地点。

 ©2025 Palo Alto Networks, Inc.

STEP 2 | 如果您还没有这样做，请载入您的远程网络。



您必须在显式代理支持的地点启用 *Prisma Access* 远程网络。

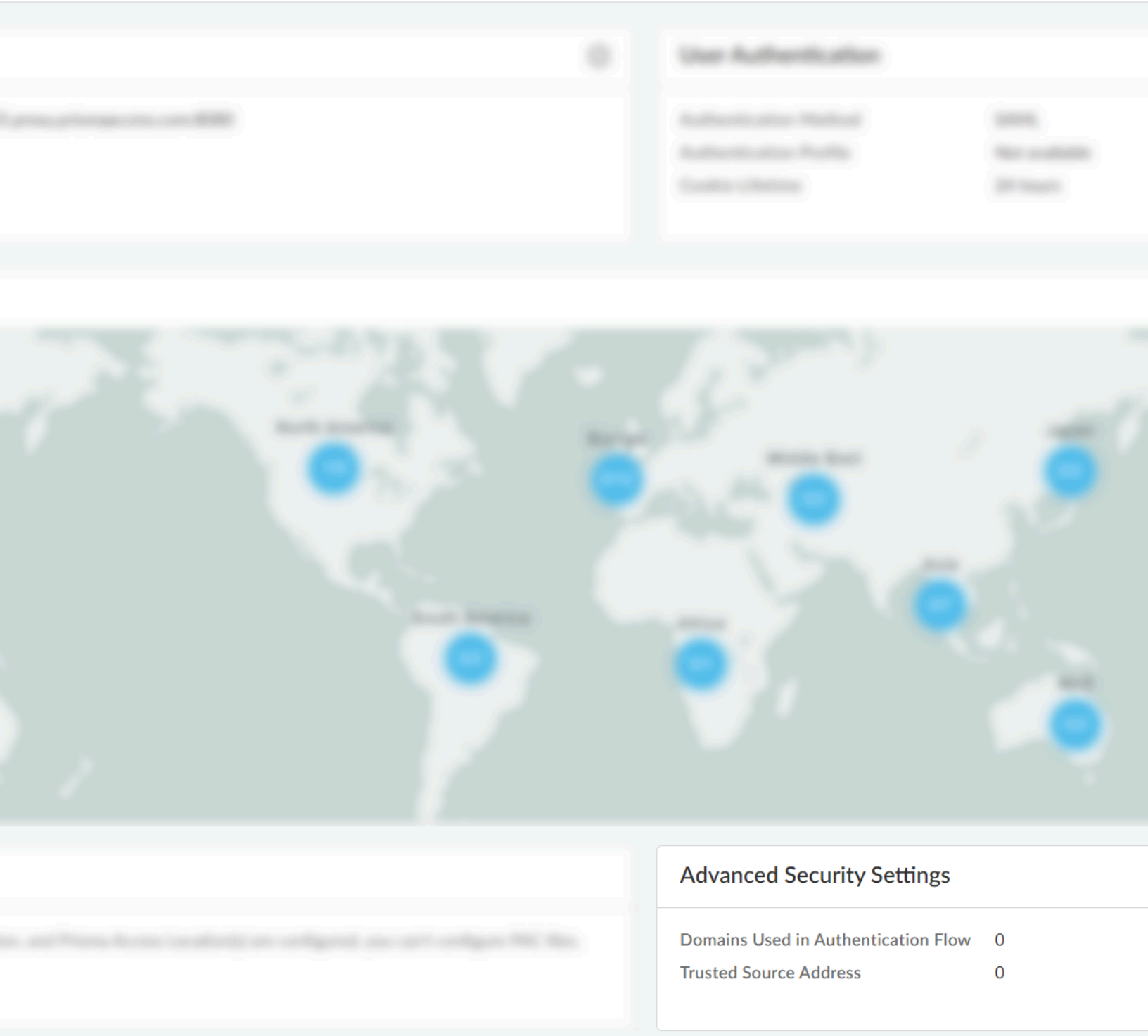
STEP 3 | **Push Config**（推送配置），确保在 **Push**（推送）范围中选定 **Mobile Users**—**Remote Workforce**（移动用户—远程工作）和 **Remote Networks**（远程网络）。

推送操作会检索需要将显式代理与远程网络集成的任播地址。

©2025 Palo Alto Networks, Inc.

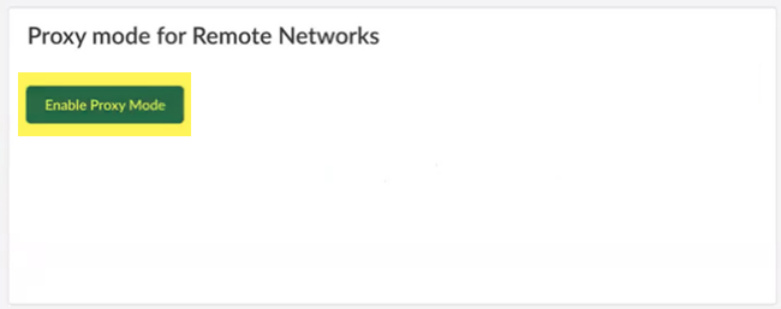
STEP 4 | 获取用于显式代理/远程网络部署的任播 IP 地址。

1. 转至 **Workflows**（工作流） > **Prisma Access** 设置 > **Explicit Proxy**（显式代理） > **Advanced Security Settings**（高级安全设置）。

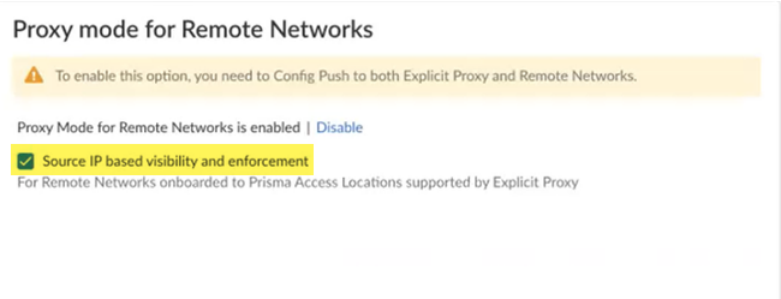


©2025 Palo Alto Networks, Inc.

2. **Enable Proxy Mode**（启用代理模式）。



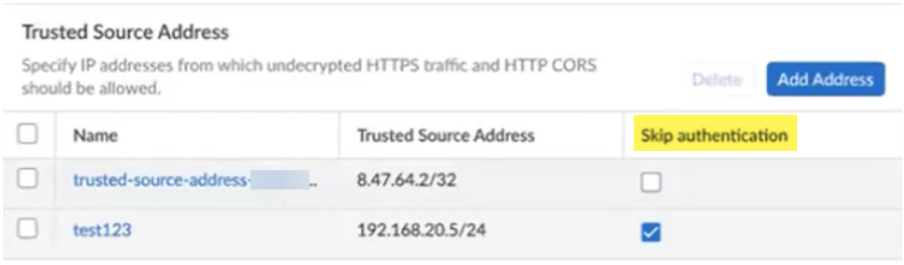
3. 要利用分支机构中将流量转发到显式代理的系统的源 IP 地址，请选择 **Source IP based visibility and enforcement**（基于源 **IP** 的可见性和强制性）。
   此功能有以下要求：
   - Prisma Access 数据平面的最低版本为 10.2.4
   - 必须使用显式代理支持的远程网络地点。



4. 添加策略，允许流量绑定到远程网络上的任意广播和单播 IP。如果您已启用 **Source IP visibility and enforcement**（源 **IP** 可见性和强制执行），请使用显式代理安全策略中的 **Source IP**（源 **IP**）字段来保护流量。在远程网络中，您需要使用其他策略。
5. （可选）要绕过您输入的任何可信源地址的身份验证，请在 可信源地址区域中指定应跳过身份验证的 IP 地址，然后选择 **Skip authentication**（跳过身份验证）。

   您可以将 **Skip authentication**（跳过身份验证）与 **Source IP based visibility and enforcement**（基于源 **IP** 的可见性和强制性）结合使用，以便让无法验证身份，设置安全策略和在 Prisma Access 显式代理上查看流量的无界面系统跳过身份验证。

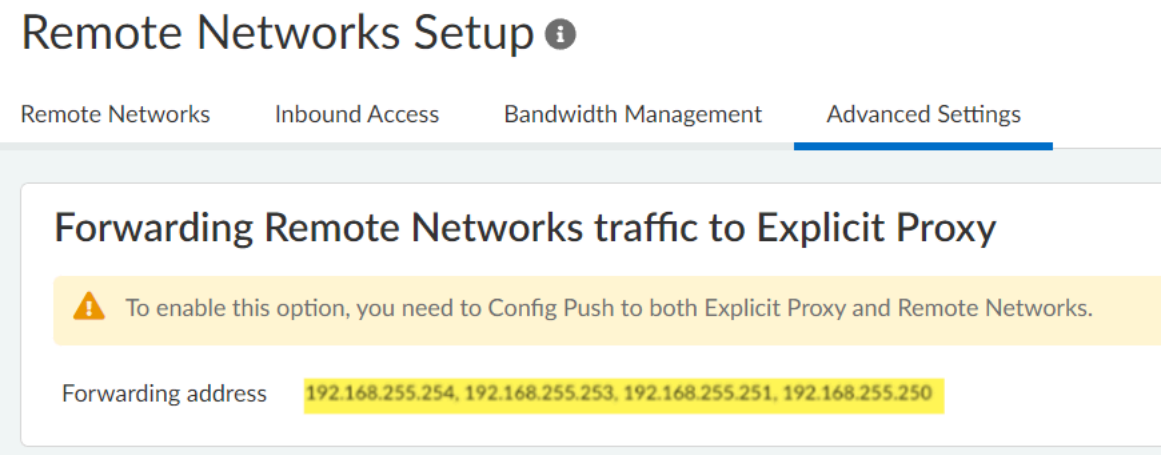
   您可以添加 *IP* 地址或子网。扩展子网后最多可支持 *100,000* 个 *IP* 地址。



6. 转至 **Workflows**（工作流） > **Prisma Access** 设置 > **Remote Networks**（远程网络）。

©2025 Palo Alto Networks, Inc.

7. **Push Config**（推送配置），确保在 **Push**（推送）范围中选定 **Mobile Users**—**Remote Workforce**（移动用户—远程工作）和 **Remote Networks**（远程网络）。
8. 转到远程网络设置中的 **Advanced Settings**（高级设置），并找到用于将流量转发到显式代理的任播 IP 地址。

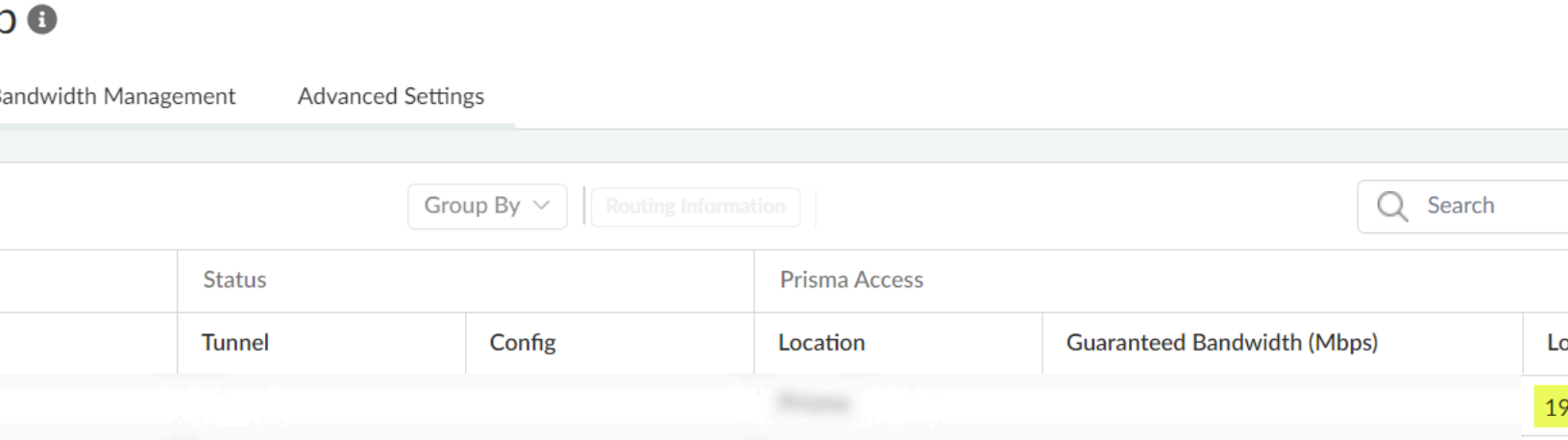


STEP 5 | （可选）查找用于显式代理/远程网络部署的单播地址。

仅当您要将特定远程网络作为目标，以便将流量转发到显式代理时，才需要使用 PAC 文件中的单播 IP 地址。如果您想使用所有已部署的远程网络，以便将流量转发到显式代理，请使用任播地址。

1. 转至 **Workflows**（工作流） > **Prisma Access** 设置 > **Remote Networks**（远程网络）。
2. 记录 **Loopback IP**（环回 **IP**）地址。

   如果有 IPv4 和 IPv6 地址，请记录 IPv4 地址。



远程网络的代理模式 (Panorama)

要使用 Prisma Access (Managed by Panorama) Access 中的显式代理保护远程网络用户的安全，请完成以下步骤。

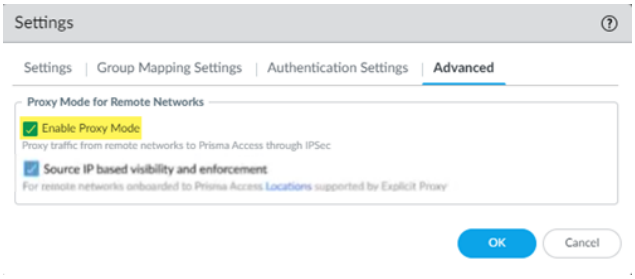
©2025 Palo Alto Networks, Inc.

STEP 1 | 配置显式代理部署并载入要添加的显式代理地点。

©2025 Palo Alto Networks, Inc.

STEP 2 | 检索用于显式代理/远程网络部署的任播 IP 地址。

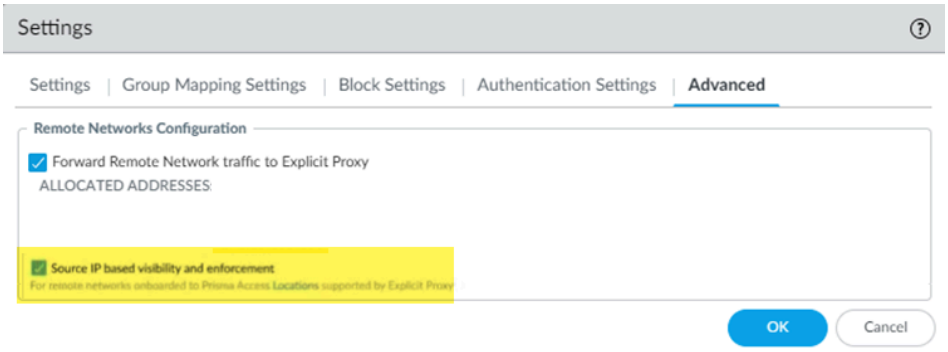
1. 选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Mobile Users—Explicit Proxy**（移动用户—显式代理）。
2. 选择齿轮图标来编辑 **Settings**（设置）。
3. 选择 **Enable Proxy Mode**（启用代理模式）。



4. 要利用分支机构中将流量转发到显式代理的系统的私有 IP 地址，请选择 **Source IP based visibility and enforcement**（基于源 **IP** 的可见性和强制性）。

   此功能有以下要求：

   - Prisma Access数据平面的最低版本为 10.2.4
   - 云服务插件最低版本为 4.1 的 Prisma Access (Managed by Panorama) 部署
   - 必须使用显式代理支持的远程网络地点。



5. 添加策略，允许流量绑定到远程网络上的任意广播和单播 IP。如果您已启用 **Source IP visibility and enforcement**（源 **IP** 可见性和强制执行），请使用显式代理安全策略中的 **Source IP**（源 **IP**）字段来保护流量。在远程网络中，您需要使用其他策略。
6. （可选）在 **Authentication Settings**（身份验证设置）下，输入任何 IP 地址。通过该地址，**Trusted Source Address Auth Bypass**（可信源地址身份验证绕过）应允许未解密的 HTTP 或 HTTP 跨源资源共享 (CORS) 流量。

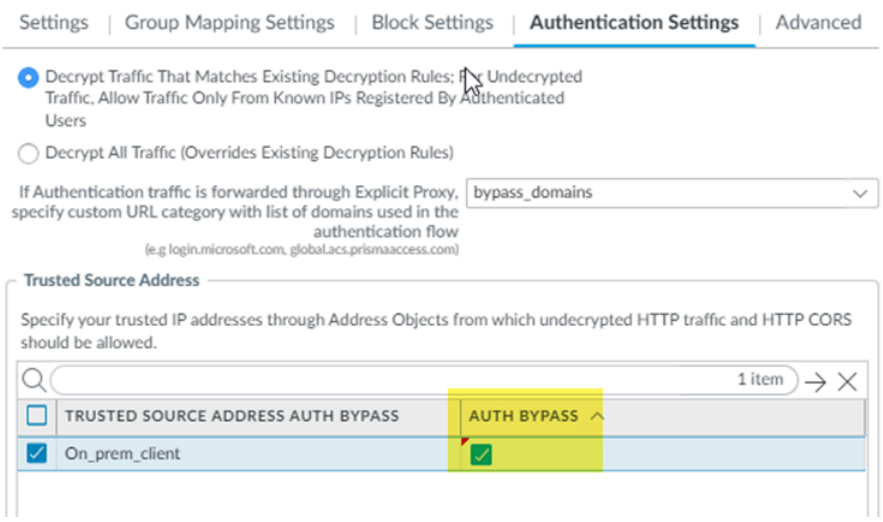
   将该 IP 地址添加到基于 IP 地址的地址对象，然后在字段中 **Add**（添加）地址对象。

   最多输入 100,000 个地址。确保地址对象仅使用 IP 地址。
7. （可选）要绕过输入的任何可信源地址的身份验证，请选择 **Auth Bypass**（绕过身份验证）。

   您可以将 **Auth Bypass**（绕过身份验证）与 **Source IP based visibility and enforcement**（基于源 **IP** 的可见性和强制性）结合使用，以便让无法验证身份，设置安全策略和在 Prisma Access 显式代理上查看流量的无界面系统跳过身份验证。

©2025 Palo Alto Networks, Inc.

您可以添加 *IP* 地址或子网。扩展子网后，最多支持 *100,000* 个 *IP* 地址。

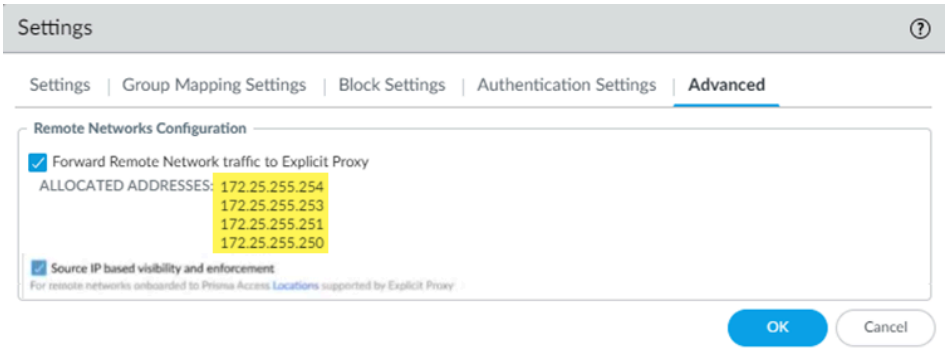


8. 选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Remote Networks**（远程网络）。
9. 如果您尚未载入远程网络地点，请载入。

   您必须在显式代理支持的地点启用 *Prisma Access* 远程网络。

10. 单击 **Commit**（提交） > **Commit and Push**（提交并推送）。
11. **Edit Selections**（编辑选择），在 **Prisma Access** 选项卡中，确保在 **Push Scope**（推送范围）中选择适用于网络的 **Prisma Access**，然后单击 **OK**（确定）。
12. **Commit and Push**（提交并推送）更改。

    要检索在显式代理/远程网络部署中使用的 IP 地址，必须对 Prisma Access 的远程网络执行提交和推送。
13. 返回显式代理 **Settings**（设置）（**Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Mobile Users—Explicit Proxy**（移动用户—显式代理） > **Settings**（设置） > **Advanced**（高级）），并记录显示在 **Remote Networks Configuration**（远程网络配置）下的 **ALLOCATED ADDRESSES**（已分配地址）。



 ©2025 Palo Alto Networks, Inc.

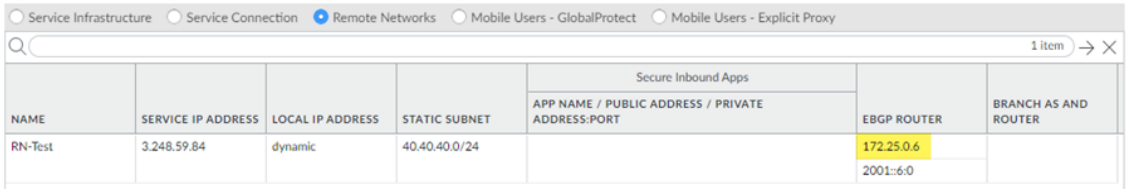
STEP 3 | （可选）查找用于显式代理/远程网络部署的单播地址。

仅当您要将特定远程网络作为目标，以便将流量转发到显式代理时，才需要使用 PAC 文件中的单播 IP 地址。如果您想使用所有已部署的远程网络，以便将流量转发到显式代理，请使用任播地址。

1. 选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息） > **Remote Networks**（远程网络）。
2. 记录 **EBGP Router**（**EBGP** 路由器）地址。

   如果有 IPv4 和 IPv6 地址，请记录 IPv4 地址。

   该地址也称为环回地址。如果您更改了配置，导致更改了 *EBGP* 路由器地址，则可以使用*Prisma Access*旧版 *API* 检索环回 *IP* 地址。



STEP 4 | 确保网络中的 CPE 设置正确，以便终端节点通过任播和单播 IP 地址将流量转发到显式代理。

显式代理如何识别用户

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证

显式代理会根据用户向代理进行身份验证的方式，在流量日志中识别用户，如下表所示。

身份验证类型	流量日志中的用户识别
使用 SAML 身份验证和解密进行登录的用户	用户名。
从另一个使用 X-Authenticated-User (XAU) 标头的代理登录的用户	XAU 标头信息 显式代理仅允许来自特定 IP 地址的流量使用 XAU 进行身份验证。您创建一个地址对象，并指定允许使用 XAU 进行身份验证的 IP 地址；然后，在设置显式代理期间，将该地址对象添加到 **Trusted Source Address**（可信源地址）字段中。
经过身份验证的跨源资源共享 (CORS) 请求	`swg-authenticated-ip-user` 用户。

©2025 Palo Alto Networks, Inc.

身份验证类型	流量日志中的用户识别
	一些流量来自经过身份验证的用户，这些用户的浏览器无法发送 Cookie，也无法执行身份验证重定向，例如 CORS 请求。在这种情况下，显式代理会将 `swg-authenticated-ip-user` 添加到流量日志中。
未解密的流量（前提是您已允许显式代理允许来自用户先前已进行过身份验证的 IP 地址的未解密流量）	`swg-authenticated-ip-user` 用户。 您可以指定显式代理，以允许来自用户已进行身份验证的 IP 地址的未解密流量；为此，在配置显式代理时，请指定 **Decrypt traffic that matches existing decryption rules; for undecrypted traffic, allow traffic only from known IPs registered by authenticated users**（对匹配现有解密规则的流量进行解密；对于未解密的流量，仅允许来自已通过身份验证的用户所注册的已知 **IP** 地址的流量）选项。在这些配置中，显式代理会将 `swg-authenticated-ip-user` 添加到流量日志中。
您选择绕过身份验证的域的流量	*swg-known-auth-bypass* 用户。 设置显式代理时，可以选择对来自特定域的流量绕过身份验证。来自这些域的流量的用户名在日志中显示为 *swg-known-auth-bypass*。

显式代理转发配置文件

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	☐ Prisma Access 移动用户许可证

通过显式代理转发配置文件，您可以使用多个 PAC 文件来定义要转发到 Prisma Access 的流量。使用转发配置文件，您可以轻松创建简单易用的转发规则，而不必去应对编写和维护 PAC 文件的复杂情况。

- 使用转发配置文件定义多个 PAC 文件
- 使用转发规则定义要转发到显式代理的流量
- 将转发配置文件附加到 GlobalProtect 应用程序配置

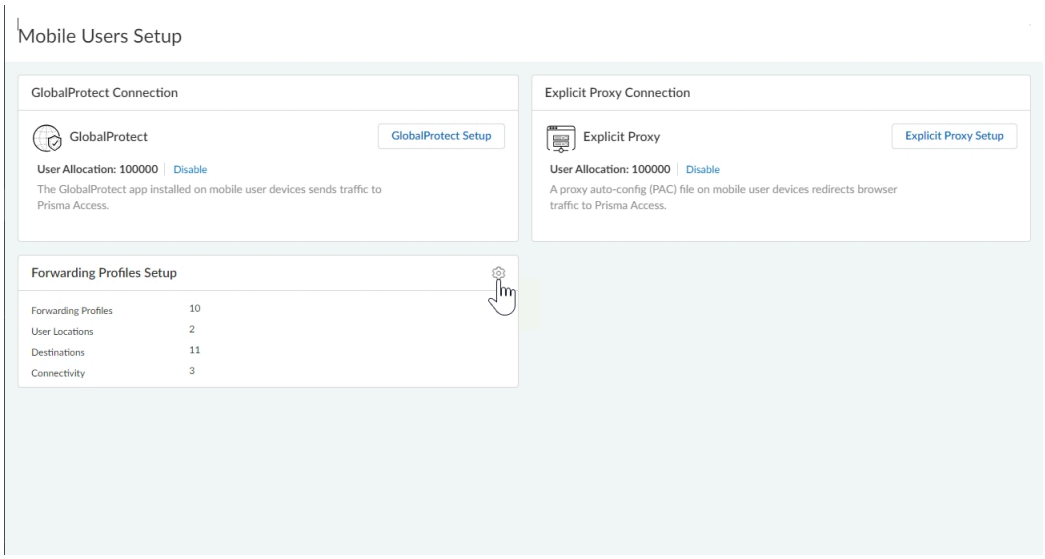
使用转发配置文件定义多个 PAC 文件

转发配置文件使您能够在部署中同时使用多个 PAC 文件，这样您就可以定义将哪些流量转发到 Prisma Access。

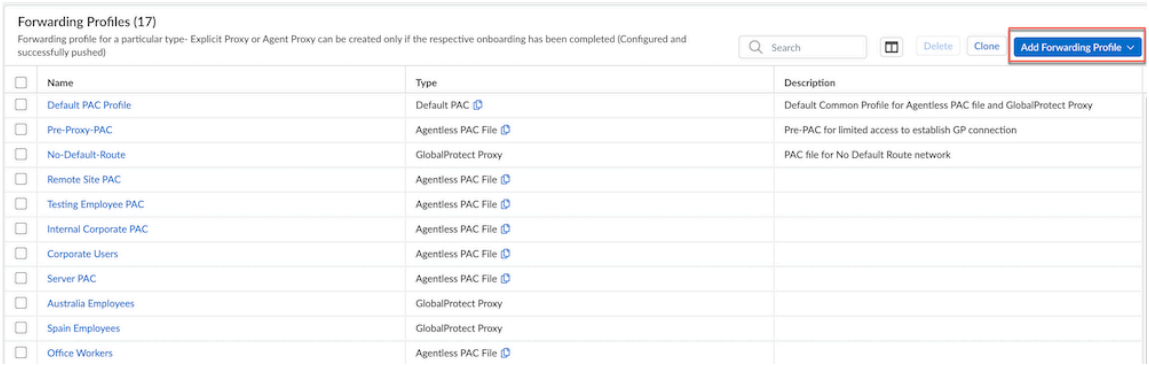
 ©2025 Palo Alto Networks, Inc.

STEP 1 | 创建转发配置文件。

1. 从 Strata Cloud Manager 中，选择 **Workflows**（工作流） > **Prisma Access** 设置 > **Mobile Users**（移动用户） > **Forwarding Profiles Setup**（转发配置文件设置）。



2. **Add Forwarding Profile**（添加转发配置文件）。



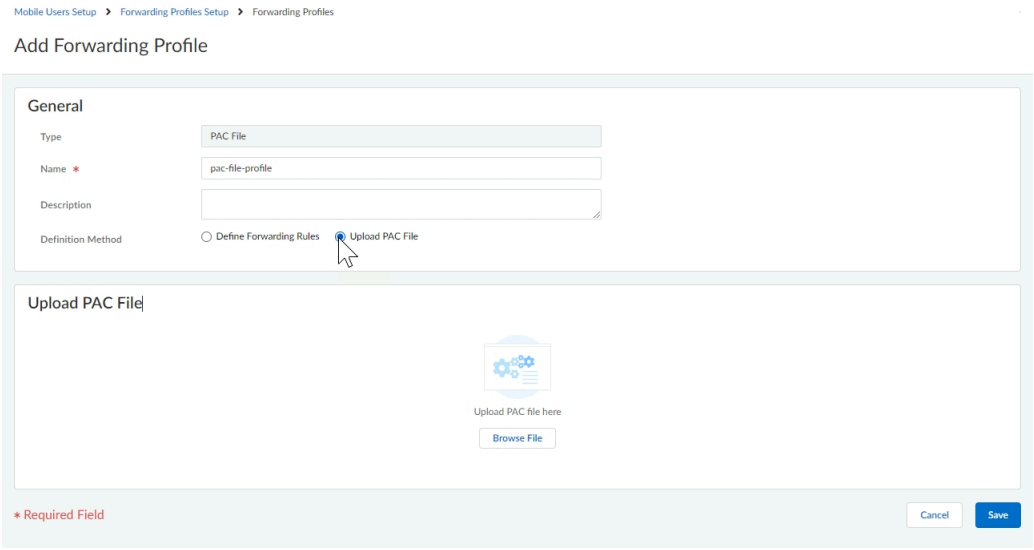
STEP 2 | 选择 **PAC File**（**PAC** 文件）。

PAC 文件 适用于 Prisma Access 显式代理。**GlobalProtect** 代理适用于代理模式下的 GlobalProtect。

 ©2025 Palo Alto Networks, Inc.

STEP 3 | 上传 PAC 文件。

1. 选择 **Upload PAC File**（上传 **PAC** 文件）以上传现有 PAC 文件，或使用 PAC 文件指南创建 PAC 文件。



2. 选择 **Browse file**（浏览文件）以浏览文件系统中的 PAC 文件。
3. **Save**（保存）配置文件。

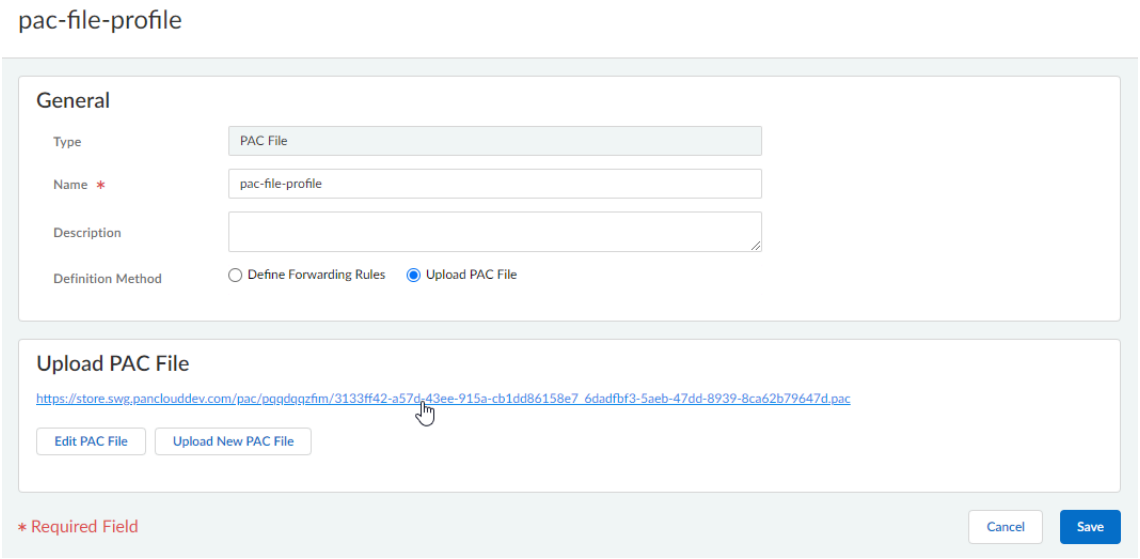
STEP 4 | 重复前两个步骤，使用不同的 PAC 文件创建另一个转发配置文件。

现在，这两个 PAC 文件已在您的部署中同时运行。

STEP 5 | 检索 PAC 文件 URL。

1. 回到您上传了 PAC 文件的配置文件。

   您应该会看到托管 PAC 文件的 URL。



©2025 Palo Alto Networks, Inc.

STEP 6 | （可选）编辑 PAC 文件。

要快速更改 PAC 文件，可以直接在 Web 界面中编辑

1. 在转发配置文件中，选择 **Edit PAC File**（编辑 **PAC** 文件）。
2. 进行更改并选择 **Save**（保存）。



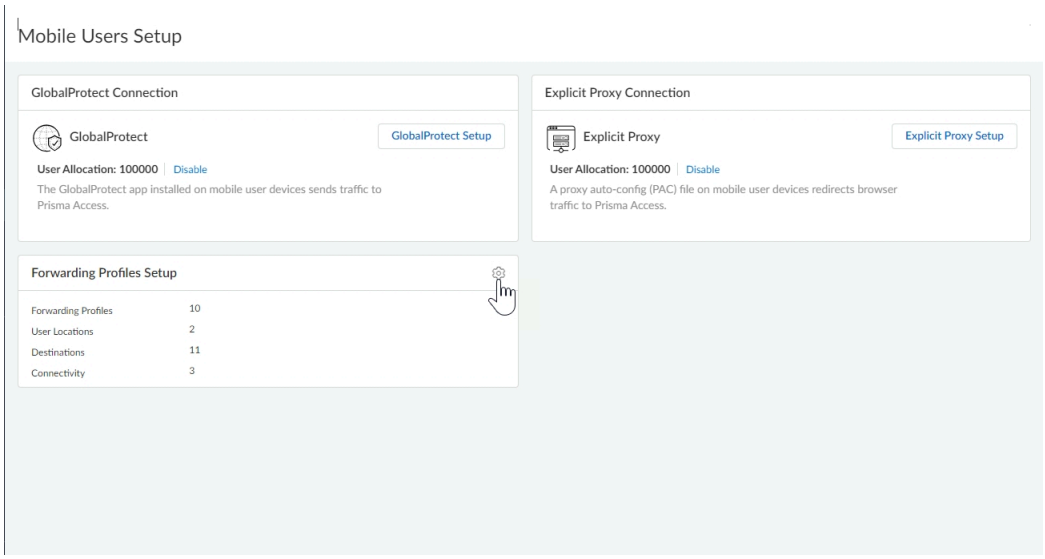
使用转发规则定义要转发到显式代理的流量

无需从头开始编写自己的 PAC 文件，可以创建简单的转发规则来生成 PAC 文件。

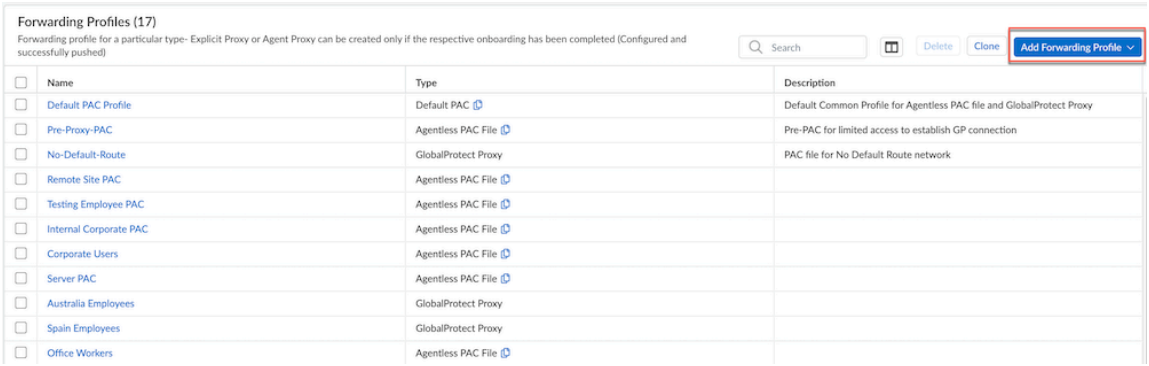
 ©2025 Palo Alto Networks, Inc.

STEP 1 | 创建转发配置文件。

1. 从 Strata Cloud Manager 中，选择 **Workflows**（工作流） > **Prisma Access** 设置 > **Mobile Users**（移动用户） > **Forwarding Profiles Setup**（转发配置文件设置）。



2. **Add Forwarding Profile**（添加转发配置文件）。



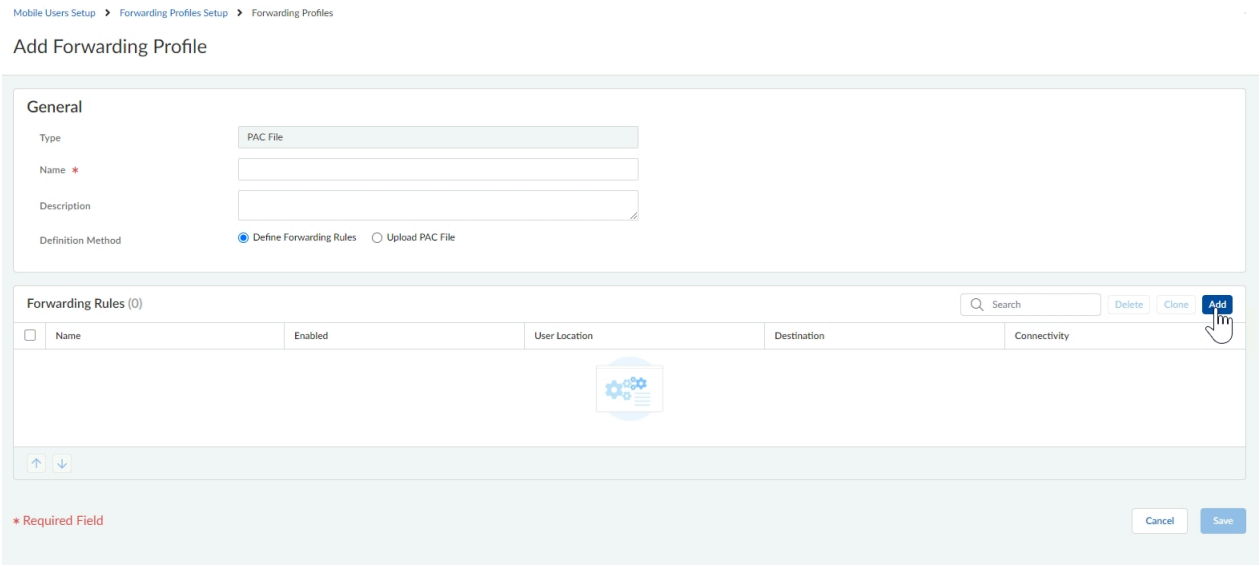
STEP 2 | 选择 **PAC File**（**PAC** 文件）。

PAC 文件 适用于 Prisma Access 显式代理。**GlobalProtect** 代理适用于代理模式下的 GlobalProtect。

 ©2025 Palo Alto Networks, Inc.

STEP 3 | 添加转发规则。

1. 选择添加。



2. 填写必填字段：

名称	配置文件的名称。
用户地点	您要为其创建转发规则的用户的位置。 要创建自定义位置，可以依次选择 **Workflows**（工作流） > **Prisma Access** 设置 > **Mobile Users**（移动用户） > **Forwarding Profiles Setup**（转发配置文件设置） > **User Locations**（用户位置）。 根据 *IP* 地址配置自定义用户位置时不能使用通配符。
目标	Web 流量的目的地。可以从预定义目标中进行选择，也可以通过 **Workflows**（工作流） > **Prisma Access** 设置 > **Mobile Users**（移动用户） > **Forwarding Profiles Setup**（转发配置文件设置） > **Destinations**（目标）创建自定义目标。
连性	选择 **Direct**（直接）将使流量绕过代理。 选择 **Global Proxy**（全局代理）将使流量通过代理。

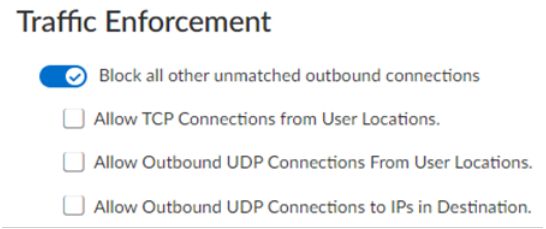
3. 完成后选择 **Add**（添加）。

©2025 Palo Alto Networks, Inc.

4. 如果想阻止所有不符合转发规则的出站流量（例如 UDP），请启用 **Traffic Enforcement**（流量实施）。此选项需要 GlobalProtect 代理版本 6.3.1 并且默认情况下处于禁用状态。如果您的某些应用程序要求您允许 UDP 连接，则可以使用用户位置或目标对象添加这些例外。

   可以按如下方式自定义阻止操作：

   - 阻止来自端点的所有 UDP 出站连接。
   - 允许来自特定位置的 TCP。例如，您可以允许来自办公室的所有 TCP 流量。
   - 允许来自特定位置的 UDP。例如，您可以允许来自办公室的所有 TCP 流量。
   - 如果某些应用程序需要 UDP 连接，您可以允许到特定目标的出站 UDP 连接。

5. 选择 **Save**（保存）以保存包含您已创建的规则的配置文件。

   该配置文件将显示在您的转发配置文件列表中。打开此列表后，您将看到根据规则生成的 PAC 文件的 URL。选择 **View PAC file**（查看 **PAC** 文件）以查看其内容。

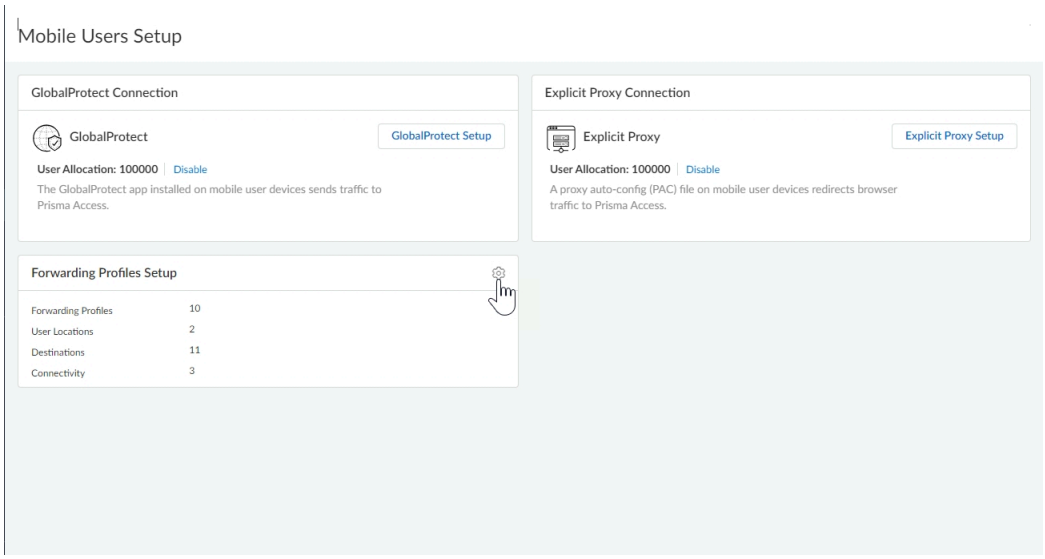
将转发配置文件附加到 GlobalProtect 应用程序配置

可以使用转发配置文件来简化 GlobalProtect 应用程序代理的配置。

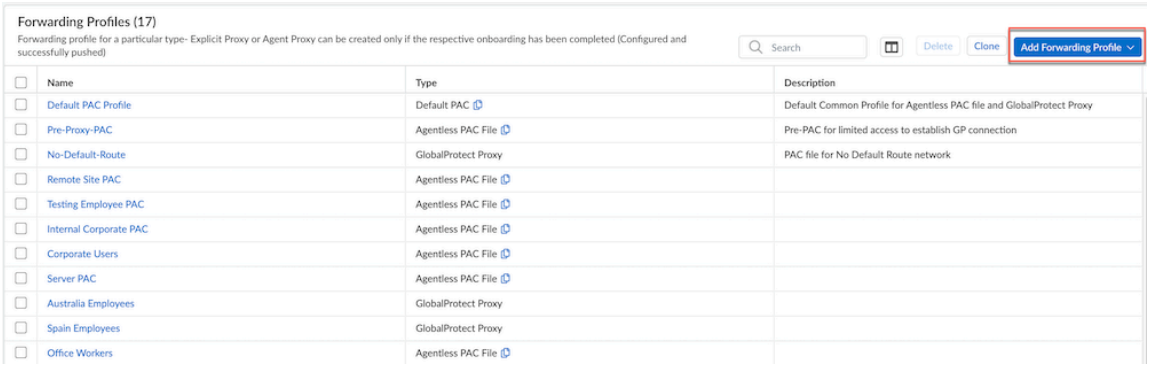
©2025 Palo Alto Networks, Inc.

STEP 1 | 创建转发配置文件。

1. 从 Strata Cloud Manager 中，选择 **Workflows**（工作流） > **Prisma Access** 设置 > **Mobile Users**（移动用户） > **Forwarding Profiles Setup**（转发配置文件设置）。



2. **Add Forwarding Profile**（添加转发配置文件）。



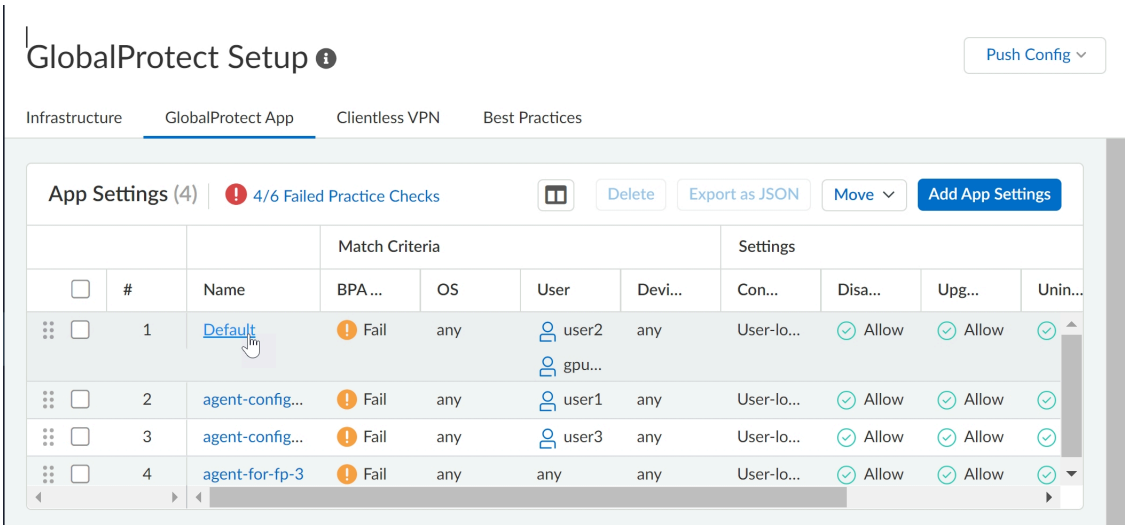
STEP 2 | 选择 **GlobalProtect Proxy**（**GlobalProtect** 代理）。

STEP 3 | 通过上传 PAC 文件或创建转发规则来配置转发配置文件。

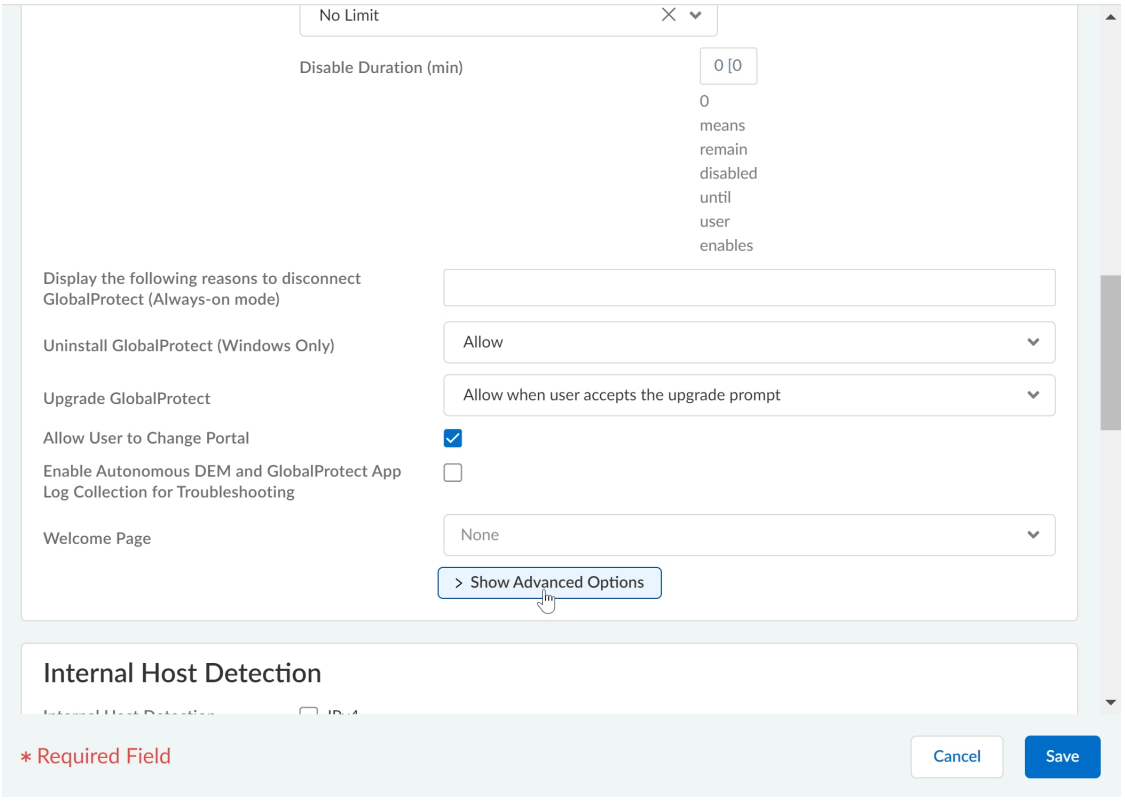
 ©2025 Palo Alto Networks, Inc.

STEP 4 | 将转发配置文件添加到您的 GlobalProtect app 代理配置。

1. 选择 **Workflows**（工作流） > **Prisma Access** 设置 > **GlobalProtect** > **GlobalProtect App**（**GlobalProtect** 应用程序）。
2. 选择一个配置文件。



3. 在应用程序配置下，选择 **Show Advanced Options**（显示高级选项）。

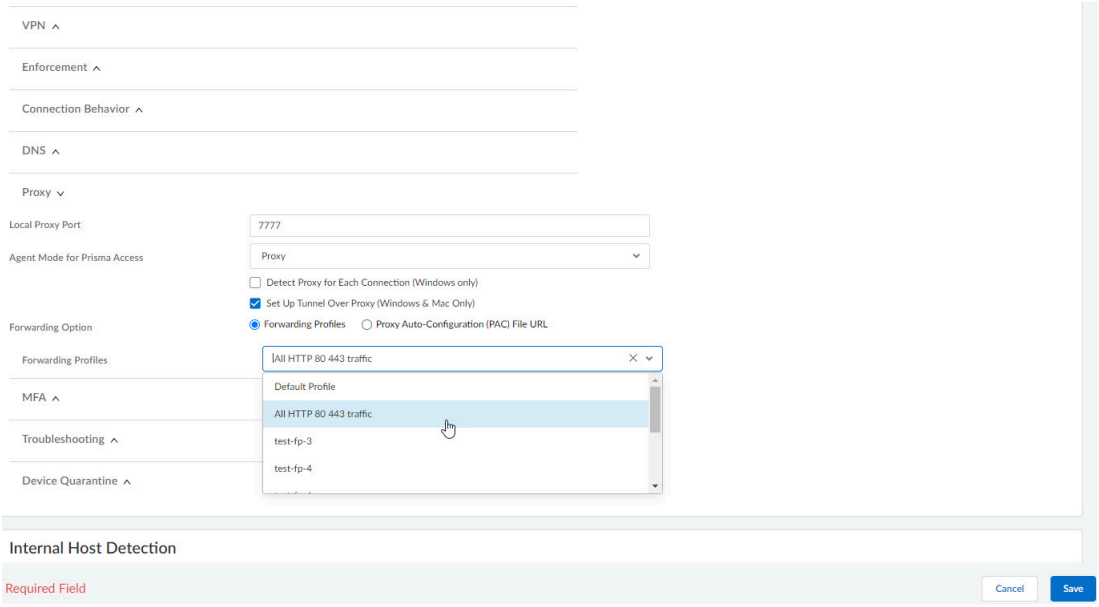


4. 展开 **Proxy**（代理）设置。
5. 根据您的 GlobalProtect 代理模式，选择 **Proxy**（代理）或 **Tunnel and Proxy**（隧道和代理）

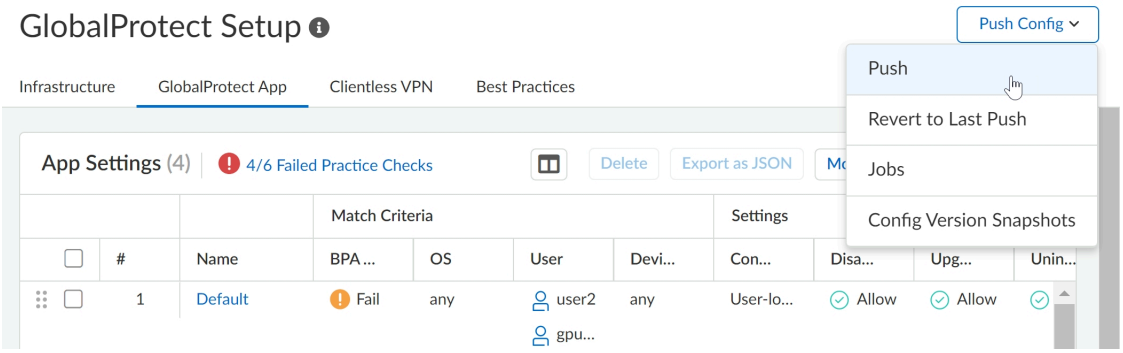
©2025 Palo Alto Networks, Inc.

如果选择 ***Tunnel***（隧道）模式，则无法添加转发配置文件。

6. 选择 **Forwarding Profiles**（转发配置文件），然后选择您想要使用的转发配置文件。



7. **Save**（保存）更改。
8. 选择 **Push Config**（推送配置） > **Push**（推送）。



PAC 文件指南

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证

- Strata Cloud Manager
- Panorama

©2025 Palo Alto Networks, Inc.

PAC 文件指南 (Strata Cloud Manager)

配置 PAC 文件以与显式代理一起使用时，请遵循以下指南和要求：

- 请注意，如果您在代理模式下使用 GlobalProtect 代理，代理将把 PAC 文件分发到您的主机。代理通过 HTTPS 访问 PAC 文件。PAC 文件是公开的。
- PAC 文件将用户流量引导至显式代理。
- 您只能承载一个要用于 Prisma Access 的 PAC 文件，并且显式代理 PAC 文件位于美国。如果您需要在美国境外访问备用的 PAC 文件，您可以在企业内部托管该 PAC 文件。
- 要访问 PAC 文件，请确保您的端点可以访问以下 IP 地址：
  - 34.111.7.85
  - 34.160.172.204
  - 34.110.206.116
  - 34.95.107.244
  - 34.149.8.36

  如果您采用无默认路由网络，则必须为这些 *IP* 地址添加路由才能访问 *PAC* 文件。
- PAC 文件仅支持 ASCII 文本格式。Palo Alto Networks 建议您在 VI 或 Vim 等文本编辑器中创建和保存 PAC 文件。
- 创建显式代理配置并提交和推送更改后，请上传您的 PAC 文件或在 PAC 文件编辑器中指定您的 PAC 配置。
- 在 `return"PROXY foo.proxy.prismaaccess.com:8080";` 语句中，必须至少有一个显式代理的 URL 是以流入 Prisma Access 的流量开头。要么使用推送更改时使用的配置域名，要么使用有效的 IPv4 地址或 DIRECT 关键字，例如 `PROXY paloaltonetworks-245139.proxy.prismaaccess.com: 8080` 或 `PROXY 1.2.3.4:8080` 等。
- 如果未绕过代理，则必须提供 PROXY 关键字。如果没有为代理绕过配置任何 `DIRECT` 关键字，则需要有效的代理语句。
- 如果在无效的 PROXY 语句之前找到了有效的 PROXY 语句，则显式代理会在第一个语句之后跳过所有代理语句的有效性检查。例如，带有有效语句 `PROXY paloaltonetworks-245139.proxy.prismaaccess.com: 8080` 后跟无效语句 `PROXY foo.proxy.prismaacess.com: 8080` 的 PAC 文件将被视为有效，因为显式代理会跳过对 `foo.proxy.prismaacess.com: 8080` 的有效性检查。
- 如果使用 PROXY 语句让 ACS 流量绕过 Prisma Access 代理，则 PROXY 语句不应使用显式代理 URL。在此配置中，显式代理提供了错误消息，但允许您上传 PAC 文件。您可以使用有效的 FQDN 或 IPv4 地址将 ACS 流量引导至其他代理，或者使用 `DIRECT` 关键字将流量直接引导至互联网。
- 代理语句中仅支持 IPv4 地址。请勿在 PROXY 语句中使用 IPv6 地址。
- PAC 文件的最大文件大小为 750 KB。
- 如果 ACS/IdP 流量需要通过显式代理，则将这些域添加到身份验证绕过列表和无解密策略规则中。

 ©2025 Palo Alto Networks, Inc.

- 如果在默认路由环境中设置显式代理，则必须排除门户、网关和 SAML FQDN。您可以使用 PAC 文件绕过 FQDN。
- 上传 PAC 文件后无法删除。但可以上传新的 PAC 文件，或在 PAC 文件编辑器中编辑以覆盖现有文件。

显式代理为您提供了一个示例 PAC 文件，您可以修改该文件并将其用作显式代理部署的 PAC 文件。Prisma Access 提供的示例 PAC 文件包含以下数据：

```
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";
```

如果要使用 Prisma Access 提供的默认 PAC 文件，可以选择修改 PAC 文件中的字段，如下表所述。

文本	说明
`var resolved_ip = dnsResolve(host); ... return "DIRECT";`	如果不修改此文件中的数据，以下主机名和 IP 地址将绕过显式代理： • `if (isPlainHostName(host)`—绕过不包含句点的主机名的显式代理（例如，http://intranet）。 • `shExpMatch(host, "*.local") ||`—绕过内部网络（本地主机）中托管的任何主机名的代理。 • `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"))`—绕过专用或环回 IP 地址范围内的任何 IP 地址的显式代理。
`if (url.substring(0,4) == "ftp:") return "DIRECT";`	绕过 FTP 会话的显式代理。

©2025 Palo Alto Networks, Inc.

文本	说明
`if (shExpMatch(host, "*.okta.com") || shExpMatch(host, "*.oktacdn.com")) return "DIRECT";`	绕过 SAML IdP 的显式代理。确保添加 IdP 使用的所有 FQDN。 如果您使用 Okta 作为用于 SAML 身份验证的 IdP，请输入 **`*.okta.com`** 和 **`*.oktacdn.com`**。
`if (shExpMatch(host, "*.acs.prismaaccess.com")) return "DIRECT";`	绕过 Prisma Access 身份验证缓存服务 (ACS) 的显式代理。 您可以为部署添加特定的 **ACS FQDN**，而不使用通配符。在 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息） > **Mobile Users—Explicit Proxy**（移动用户—显式代理） > **ACS FQDN** 中查找此 FQDN。
`return "PROXY foo.proxy.prismaaccess.com:8080"`	绕过显式代理 URL 的显式代理。 在 `return"PROXY foo.proxy.prismaaccess.com:8080";` 语句中，必须至少有一个显式代理的 URL 是流向 Prisma Access 的流量。要么使用推送更改时使用的配置域名，要么使用有效的 IPv4 地址或 DIRECT 关键字，例如 `PROXY paloaltonetworks-245139.proxy.prismaaccess.c 8080` 或 `PROXY 1.2.3. 4:8080`。

PAC 文件指南 (Panorama)

配置 PAC 文件以与显式代理一起使用时，请遵循以下指南和要求：

- 请注意，如果您在代理模式下使用 GlobalProtect 代理，代理将把 PAC 文件分发到您的主机。代理通过 HTTPS 访问 PAC 文件。PAC 文件是公开的。
- PAC 文件将用户流量引导至显式代理。
- 您只能承载一个要用于 Prisma Access 的 PAC 文件，并且显式代理 PAC 文件位于美国。如果您需要在美国境外访问备用的 PAC 文件，您可以在企业内部托管该 PAC 文件。
- 要访问 PAC 文件，请确保您的端点可以访问以下 IP 地址：
  - 34.111.7.85
  - 34.160.172.204
  - 34.110.206.116
  - 34.95.107.244
  - 34.149.8.36

©2025 Palo Alto Networks, Inc.

- PAC 文件仅支持 ASCII 文本格式。Palo Alto Networks 建议您在 VI 或 Vim 等文本编辑器中创建和保存 PAC 文件。
- 创建显式代理配置并提交和推送更改后，上传 PAC 文件。上传 PAC 文件后，不需要进行提交和推送操作。
- 在 `return"PROXY foo.proxy.prismaaccess.com:8080";` 语句中，必须至少有一个显式代理的 URL 是以流入 Prisma Access 的流量开头。要么使用推送更改时使用的配置域名，要么使用有效的 IPv4 地址或 DIRECT 关键字，例如 `PROXY paloaltonetworks-245139.proxy.prismaaccess.com: 8080` 或 `PROXY 1.2.3.4:8080` 等。
- 如果未绕过代理，则必须提供 PROXY 关键字。如果没有为代理绕过配置任何 `DIRECT` 关键字，则需要有效的代理语句。
- 如果在无效的 PROXY 语句之前找到了有效的 PROXY 语句，则显式代理会在第一个语句之后跳过所有代理语句的有效性检查。例如，带有有效语句 `PROXY paloaltonetworks-245139.proxy.prismaaccess.com: 8080` 后跟无效语句 `PROXY foo.proxy.prismaacess.com: 8080` 的 PAC 文件将被视为有效，因为显式代理会跳过对 `foo.proxy.prismaacess.com: 8080` 的有效性检查。
- 如果使用 PROXY 语句让 ACS 流量绕过 Prisma Access 代理，则 PROXY 语句不应使用显式代理 URL。在此配置中，显式代理提供了错误消息，但允许您上传 PAC 文件。您可以使用有效的 FQDN 或 IPv4 地址将 ACS 流量引导至其他代理，或者使用 `DIRECT` 关键字将流量直接引导至互联网。
- 代理语句中仅支持 IPv4 地址。请勿在 PROXY 语句中使用 IPv6 地址。
- PAC 文件的最大文件大小为 256 KB。
- 如果 ACS/IdP 流量需要通过显式代理，则将这些域添加到身份验证绕过列表和无解密策略规则中。
- 如果在默认路由环境中设置显式代理，则必须排除门户、网关和 SAML FQDN。您可以使用 PAC 文件绕过 FQDN。
- 上传 PAC 文件后无法删除。然而，您可以上传一个新的 PAC 文件以覆盖现有文件。
- 如果您在 Prisma Access 中更改了显式代理 URL，但没有更改 PAC 文件以反映此更改，则不会应用此更改。您必须上传一个新的 PAC 文件，指定新的显式代理 URL。

显式代理为您提供了一个示例 PAC 文件，您可以修改该文件并将其用作显式代理部署的 PAC 文件。Prisma Access 提供的示例 PAC 文件包含以下数据：

```
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";
```

 ©2025 Palo Alto Networks, Inc.

如果要使用 Prisma Access 提供的默认 PAC 文件，可以选择修改 PAC 文件中的字段，如下表所述。

文本	说明
`var resolved_ip = dnsResolve(host); ... return "DIRECT";`	如果不修改此文件中的数据，以下主机名和 IP 地址将绕过显式代理： • `if (isPlainHostName(host)`—绕过不包含句点的主机名的显式代理（例如，http://intranet）。 • `shExpMatch(host, "*.local") ||`—绕过内部网络（本地主机）中托管的任何主机名的代理。 • `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"))`—绕过专用或环回 IP 地址范围内的任何 IP 地址的显式代理。
`if (url.substring(0,4) == "ftp:") return "DIRECT";`	绕过 FTP 会话的显式代理。
`if (shExpMatch(host, "*.okta.com") || shExpMatch(host, "*.oktacdn.com")) return "DIRECT";`	绕过 SAML IdP 的显式代理。确保添加 IdP 使用的所有 FQDN。 如果您使用 Okta 作为用于 SAML 身份验证的 IdP，请输入 **`*.okta.com`** 和 **`*.oktacdn.com`**。
`if (shExpMatch(host, "*.acs.prismaaccess.com")) return "DIRECT";`	绕过 Prisma Access 身份验证缓存服务 (ACS) 的显式代理。 您可以为部署添加特定的 **ACS FQDN**，而不使用通配符。在 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息） > **Mobile Users—Explicit Proxy**（移动用户—显式代理） > **ACS FQDN** 中查找此 FQDN。

©2025 Palo Alto Networks, Inc.

文本	说明
`return "PROXY foo.proxy.prismaaccess.com:8080"`	绕过显式代理 URL 的显式代理。 在 `return"PROXY foo.proxy.prismaaccess.com:8080";` 语句中，必须至少有一个显式代理的 URL 是流向 Prisma Access 的流量。要么使用推送更改时使用的配置域名，要么使用有效的 IPv4 地址或 DIRECT 关键字，例如 `PROXY paloaltonetworks-245139.proxy.prismaaccess.c 8080` 或 `PROXY 1.2.3. 4:8080`。

显式代理最佳实践

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证

在实施显式代理部署时，请遵循推荐的最佳实践，以实现最佳性能和理想的用户体验：

- 一般显式代理部署最佳实践：
  - 在至少两个区域中部署显式代理以实现冗余。
  - 如果所有用户都位于 NAT 设备之后，并且显式代理将 NAT 设备的 IP 地址视为源 IP 地址，则应为每 500 个移动用户分配一个 NAT IP 地址。
  - 使用转发配置文件来配置 PAC 文件。
- **PAC** 文件最佳实践 — 时，绕过所有 SAML、CIE 和身份验证缓存服务 (ACS) URL。
- **SAML** 身份验证最佳实践：
  - 将 SAML 身份验证的 **Cookie Lifetime**（**Cookie** 生命周期）选项设置为 24 小时可获得最佳的用户体验，也不会中断身份验证。
  - 如果你已配置代理模式下的 GlobalProtect 或隧道与代理模式下的 GlobalProtect，请在 GlobalProtect 门户上将 **Cookie Lifetime**（**Cookie** 生命周期）设置为 12 小时。
- **Kerberos** 身份验证最佳实践 — 密钥表文件的大小应小于 60 KB。
- 安全策略规则最佳做法 — 采用安全策略规则最佳实践时，请将策略中的 **Action**（操作） 设置为 **Deny**（拒绝），而非 **Drop**（丢弃） 或 **Reset**（重置）。此操作有助于快速释放显式代理安全处理节点 (EP-SPN) 内的资源，以获得最佳性能。
- 解密最佳实践 — 配置至少一个解密策略和一个解密证书。
- **IP** 源地址最佳实践 — 要将显式代理的访问限制为特定的源 IP 地址，请使用特殊对象，其中包括地址对象、地址组和外部动态列表 (EDL)。

©2025 Palo Alto Networks, Inc.

监控显式代理并排除故障

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证

了解如何监控 Prisma Access 显式代理部署并对其进行故障排除。

- Strata Cloud Manager
- Panorama

监控显式代理并排除故障 (Strata Cloud Manager)

监控 Prisma Access 显式代理部署详细信息，以帮助您解决任何问题。

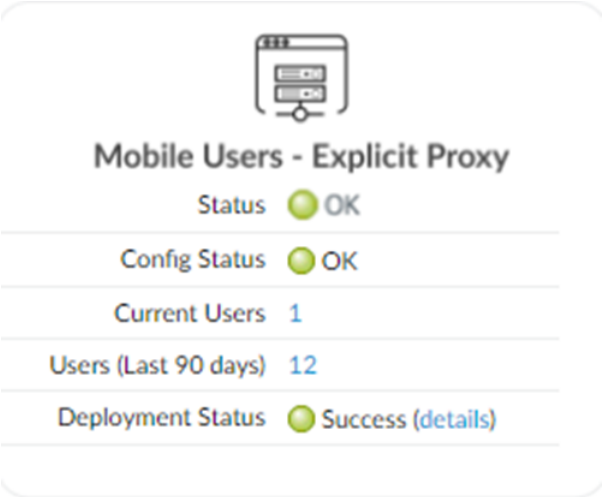
- 单击 **Monitor**（监控） > **Users**（用户），然后选择 **Explicit Proxy**（显式代理）连接方式。
- 选择 **Monitor**（监视） > **Users**（用户），并将连接方式选择为 **Explicit Proxy**（显式代理），以查看通过其设备浏览器上的显式代理连接到 Prisma Access 安全服务的移动用户。
- 选择 **Monitor**（监控）> **Prisma Access** 位置 > **Explicit Proxy Mobile Users**（显式代理移动用户），以查看适用于移动用户的所有 Prisma Access 位置的运行状况概览。
- 检查流量日志（**Incidents & Alerts**（事件与警报）> **Log Viewer**（日志查看器），然后选择日志类型 **Traffic**（流量））和身份验证日志（**Incidents & Alerts**（事件与警报）> **Log Viewer**（日志查看器），然后选择日志类型 **Authentication**（身份验证）），以排查与身份验证相关的问题。

监控显式代理并排除故障 (Panorama)

在为移动用户配置显式代理后，可通过检查 Prisma Access 显式代理部署的状态来监控状态并排除任何问题。

©2025 Palo Alto Networks, Inc.

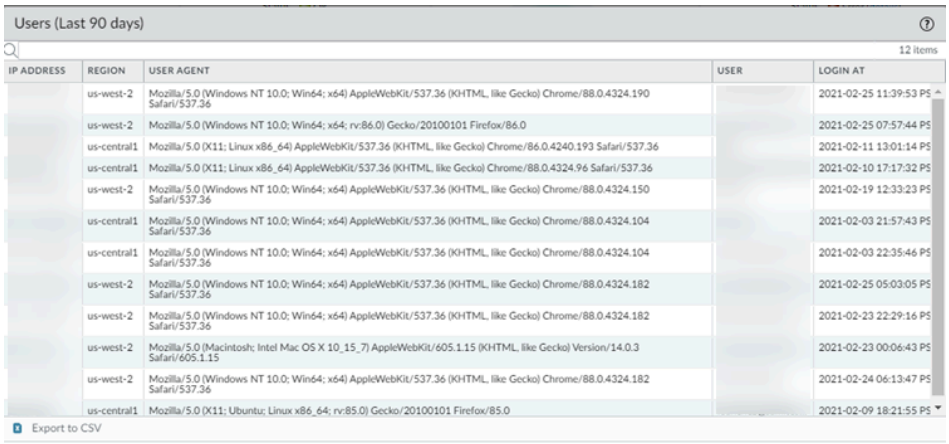
- 选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Status**（状态）以查看显式代理状态。



移动用户的 **Status**（状态）和 **Config Status**（配置状态）字段指示 Prisma Access 与移动用户之间的连接是 **OK**（正常）、无法获取隧道上的状态（**Warning**（警告）），还是移动用户无法连接到显式代理（**Error**（错误））。

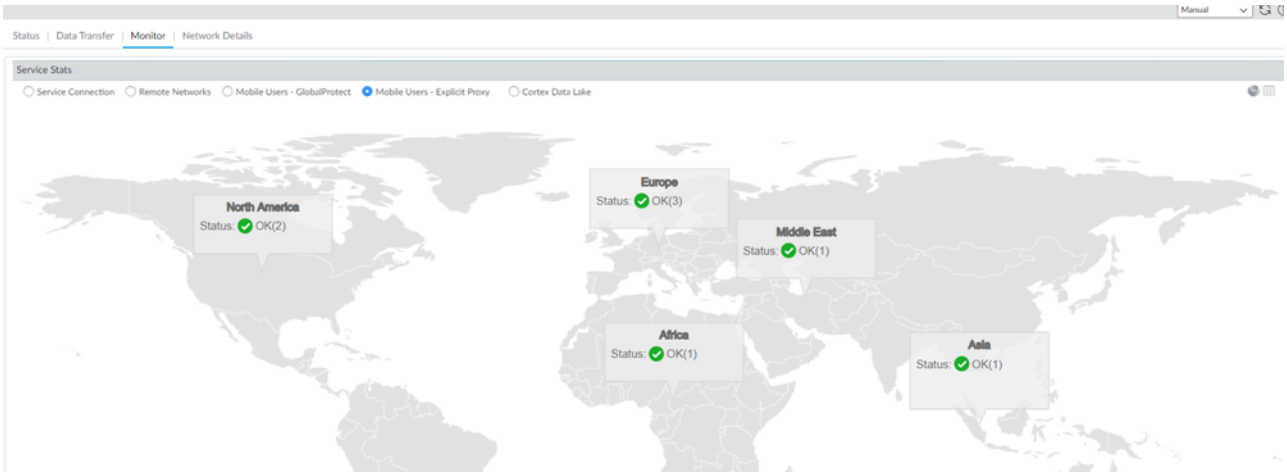
单击 **Current Users**（当前用户）和 **Users (Last 90 days)**（用户（过去**90**天））旁边的超链接，可获取有关移动用户的更多信息。

- **Current Users**（当前用户）—在过去五分钟内浏览过流量的已认证用户的当前数量。
- **Users (Last 90 days)**（用户（过去**90**天））—过去 90 天内经过认证的显式代理用户的数量。

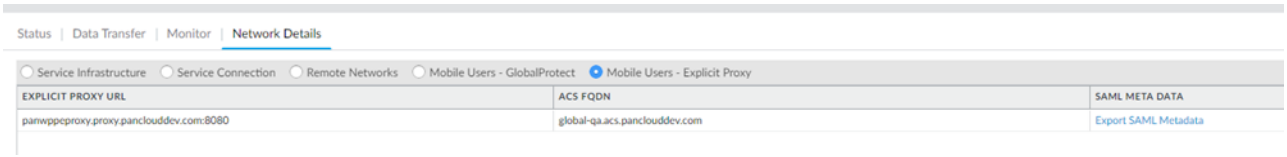


 ©2025 Palo Alto Networks, Inc.

- 选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Monitor**（监控） > **Mobile Users**—**Explicit Proxy**（移动用户—显式代理），可显示一张展示已部署的显式代理位置的地图。



- 选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息） > **Mobile Users**—**Explicit Proxy**（移动用户—显式代理）以查看以下详细信息：



  - **Explicit Proxy URL**（显式代理 **URL**）—用于显式代理的 URL。
  - **ACS FQDN**—ACS 的 FQDN。
  - **SAML Meta Data**（**SAML** 元数据）—SAML 使用的身份验证配置文件元数据。您可以选择 **Export SAML Metadata**（导出 **SAML** 元数据）以保存元数据文件。
- 要排查与身份验证相关的问题，请检查流量日志（**Monitor**（监控） > **Logs**（日志） > **Traffic**（流量））和身份验证日志（**Monitor**（监控） > **Logs**（日志） > **Authentication**（身份验证））。显式代理在日志中显示以下 IP 地址和位置：
  - **IP** 地址—如果移动用户在 PAC 文件中绕过了 ACS FQDN，则在流量日志中 **Source**（源）列以及在 **Explicit_Proxy_Device_Group** 下查看时身份验证日志中的 **IP Address**（**IP** 地址）列所显示的 IP 地址，将与移动用户的 IP 地址相同。如果用户不绕过 PAC 文件中的 ACS FQDN，则源 IP 地址是指向 ACS 的显式代理云防火墙的公共 IP 地址。
  - 位置—如果移动用户在 PAC 文件中绕过了 ACS FQDN，则在 **Authentication Logs**（身份验证日志）、**Current Users**（当前用户）以及 **Users (Last 90 days)**（用户（最近 **90** 天））中 **Region**（区域）列所显示的区域名称，将是部署 ACS 的五个区域（us-west-2、us-east-1、eu-west-2、eu-west-3、ap-south-1）之一，并显示显式代理从客户端浏览器执行重定向操作所在的区域。如果移动用户在 PAC 文件中绕过了 ACS FQDN，则在 **Authentication Logs**（身份验证日志）、**Current Users**（当前用户）以及 **Users (Last 90 days)**（用户（最近 **90** 天））中 **Region**（区域）列所显示的区域名称，将是部署 ACS 的五个区域（us-west-2、us-east-1、eu-west-2、eu-west-3、ap-south-1）之一，并显示显式代理从显式代理防火墙执行重定向操作所在的区域。

 ©2025 Palo Alto Networks, Inc.

显式代理的阻止设置

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Panorama Managed Prisma Access	• Prisma Access 许可证

要启用此功能，请联系您的 **Palo Alto Networks** 客户代表或合作伙伴，他们将联系站点可靠性工程 **(SRE)** 团队并提交请求。

当用户使用显式代理访问互联网目标时，互联网目标的 DNS 解析由显式代理执行。要在 DNS 解析阶段阻止对互联网目标的访问，您可以使用阻止设置。您可以根据 DNS 安全类别、URL 过滤类别或外部动态列表 (EDL) 进行阻止。

对于您阻止的域名，Prisma Access 会阻止这些域名，并且用户会在 HTTP GET 请求（针对未加密的网站）或 HTTP Connect 请求（针对加密的网站）期间收到阻止页面，这意味着在初始连接请求期间阻止这些域名。当您阻止访问该站点时，用户在通过身份验证流程后会看到阻止页面，并且系统会捕获用户名以执行进一步的取证和安全运营中心 (SOC) 工作流。

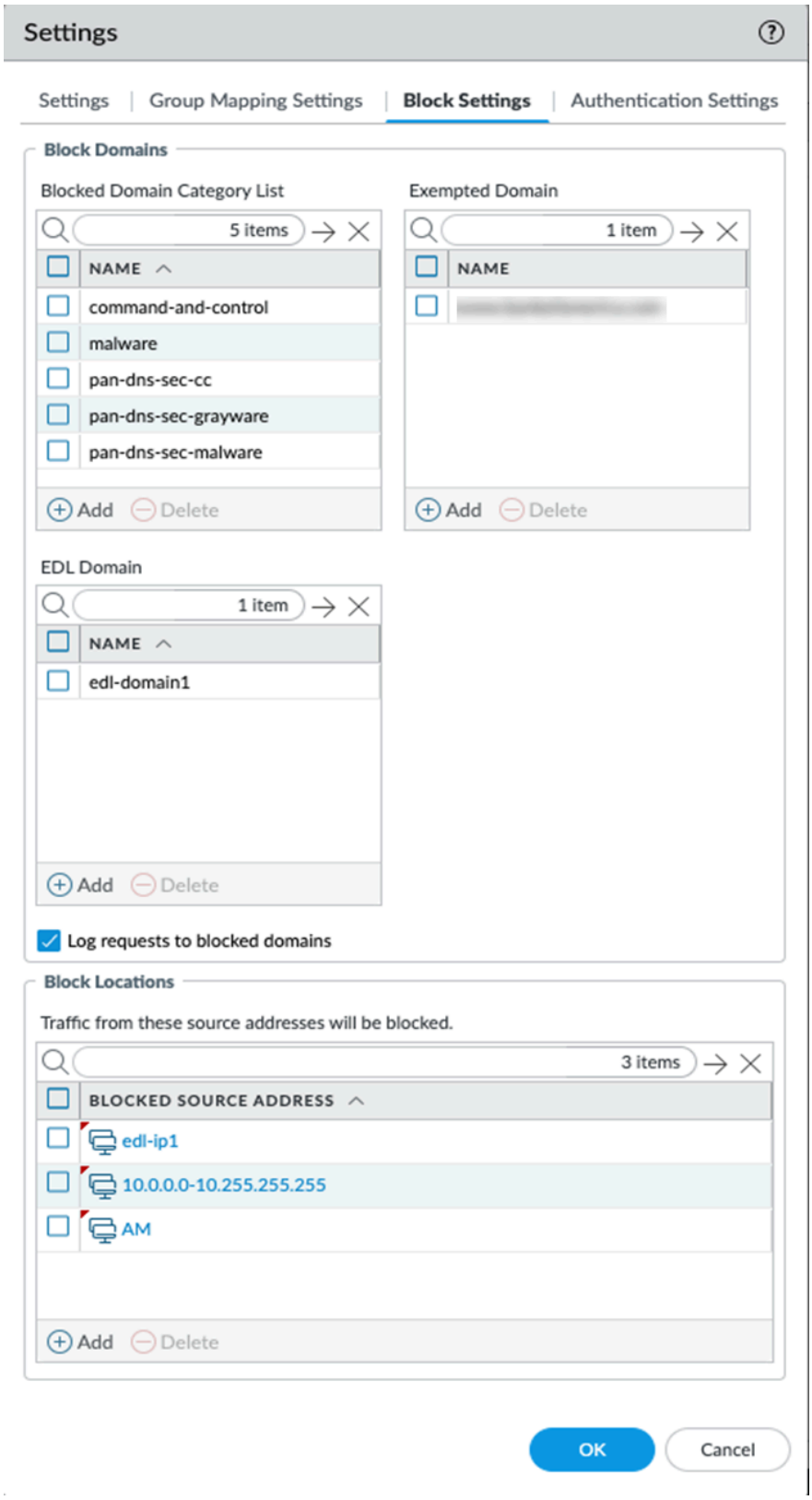
如果您使用的是 Prisma Access (Managed by Strata Cloud Manager)，请参阅设置显式代理中的步骤 8。要配置 Panorama 托管的 Prisma Access 的阻止设置，请完成以下步骤。

©2025 Palo Alto Networks, Inc.

STEP 1 | 配置 **Block Settings**（阻止设置）以阻止域名或域名类别。

指定恶意网站或您不希望用户访问的任何网站的域名或域名类别。当用户发起 HTTP GET（针对未加密请求）或 HTTP CONNECT（针对加密请求）时，Prisma Access 会阻止用户访问您在此区域指定的 URL 和 IP 地址。当用户尝试访问被阻止的网站时，会显示阻止页面。

©2025 Palo Alto Networks, Inc.



1. 在 **Blocked Domain Category List**（阻止域名类别列表）中，输入要阻止的预定义类别。不支持自定义 URL 类别。

 ©2025 Palo Alto Networks, Inc.

2. 在 **EDL Domain**（**EDL** 域名）中，输入要阻止的基于域名的外部动态列表 (EDL)。

   您只能选择 EDL 类型为**Dynamic Domain Lists**（动态域名列表）的 EDL；不允许使用动态 IP 列表和动态 URL 列表。

3. 如果您想要豁免 **Blocked Domain Category List**（阻止域名类别列表）中包含的任何域名，请将它们指定为 **Exempted Domain**（豁免域名）。

   在此处输入的任何域名将不会被阻止，即使它们出现在您已阻止的域名类别中。

   - 最多可输入 100 个域名。
   - 域名记录的最大长度为 256 个字符。

STEP 2 | 在 **Blocked Source Address**（阻止的源地址）区域中选择要阻止的 IP 地址。

您可以 **Add**（添加）地址、地址组、基于 IP 地址的 EDL，或基于地区和国家的 IP 地址。

使用以下 IP 地址准则：

- 仅使用 **Type**（类型）为 **IP List**（**IP** 列表）或 **Predefined IP List**（预定义 **IP** 列表）的 EDL。
- 仅使用类型为 **IP Range**（**IP** 范围）或 **IP Netmask**（**IP** 网络掩码）的地址对象。
- 不支持具有动态对象成员资格的地址组。
- 请勿在 IP 地址对象中使用自定义区域；而是使用预定义区域。

STEP 3 | 选择 **Log requests to blocked domains**（记录已被阻止的域名请求），以便 Prisma Access 记录已被阻止的域名请求。

由于阻止域名日志可能会从僵尸网络生成大量流量，因此在启用日志记录时请务必小心，或仅将其用于故障排除目的。即使您限制代理的使用（例如，如果您限制使用特定的 IP 地址），也能够不受限制地启用日志记录。

使用特殊对象将显式代理互联网流量限制到特定 IP 地址

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证

显式代理为您提供特殊的地址对象、地址组和外部动态列表 (EDL)，以将对显式代理的访问限制到特定的源 IP 地址。使用以下确切名称创建这些特殊对象中的一个或多个时，显式代理会允许您指定的源 IP 地址并阻止任何其他 IP 地址：

- 对象 — 在 Explicit_Proxy_Device_Group 中选择 **Objects**（对象） > **Addresses**（地址），并创建一个名为 **Palo Alto Networks Explicit Proxy Allowed Source Address** 的对象。
- 地址组 — 在 Explicit_Proxy_Device_Group 中选择 **Objects**（对象） > **Address Groups**（地址组），并创建名为 **Palo Alto Networks Explicit Proxy Allowed Source Address Group** 的对象。

 ©2025 Palo Alto Networks, Inc.

- 外部动态列表 **(EDL)** — 在 Explicit_Proxy_Device_Group 中选择 **Objects**（对象） > **External Dynamic Lists**（外部动态列表），创建名为 **Palo Alto Networks Explicit Proxy Allowed Source List** 的 EDL，并创建类型为 **IP List** 的 EDL。

您可以指定 IP 地址，例如分支机构的传出 IP 地址。

不允许使用通配符（如 *.*）跳过大量域的显式代理身份验证，除非您使用这些特殊对象之一将源流量限制为特定的源 IP 地址。

单独或联合使用地址对象、地址组或 EDL；例如，可以只创建地址组，而不创建地址对象或 EDL。

使用显式代理访问数据中心

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ （对于 ZTNA 连接器和 Colo-Connect）Prisma Access 5.2.1版本 ❑ （对于服务连接）Prisma Access 5.0 版本 ❑ （对于私有及合作伙伴应用程序访问权限）适用于 Windows 或 macOS 的 GlobalProtect app 版本 6.2

您可以使用服务连接、ZTNA 连接器 或 Colo-Connect 访问数据中心内的资源，例如外部动态列表或私有及合作伙伴应用程序，同时仍然可以受益于显式代理连接。

以下 *RFC 6598 IP* 地址不支持通过服务连接、*Colo-Connect* 或 *ZTNA* 连接器的显式代理访问私有应用程序：

- *100.64.0.0/15*
- *100.88.0.0/15*
- *100.72.0.0/15*

在 *ZTNA* 连接器应用程序 *IP* 块或连接器 *IP* 块中使用上述 *IP* 地址的现有 *ZTNA* 连接器无法通过显式代理在代理模式下使用 *Prisma Access Browser* 或 *GlobalProtect* 代理。您必须联系 *Palo Alto Networks* 代表以将您的 *IP* 地址迁移到其他块。

- Strata Cloud Manager
- Panorama

使用显式代理访问数据中心 (Strata Cloud Manager)

STEP 1 | 根据您的要求在 Prisma Access 中配置服务连接、Colo-Connect 或 ZTNA 连接器。

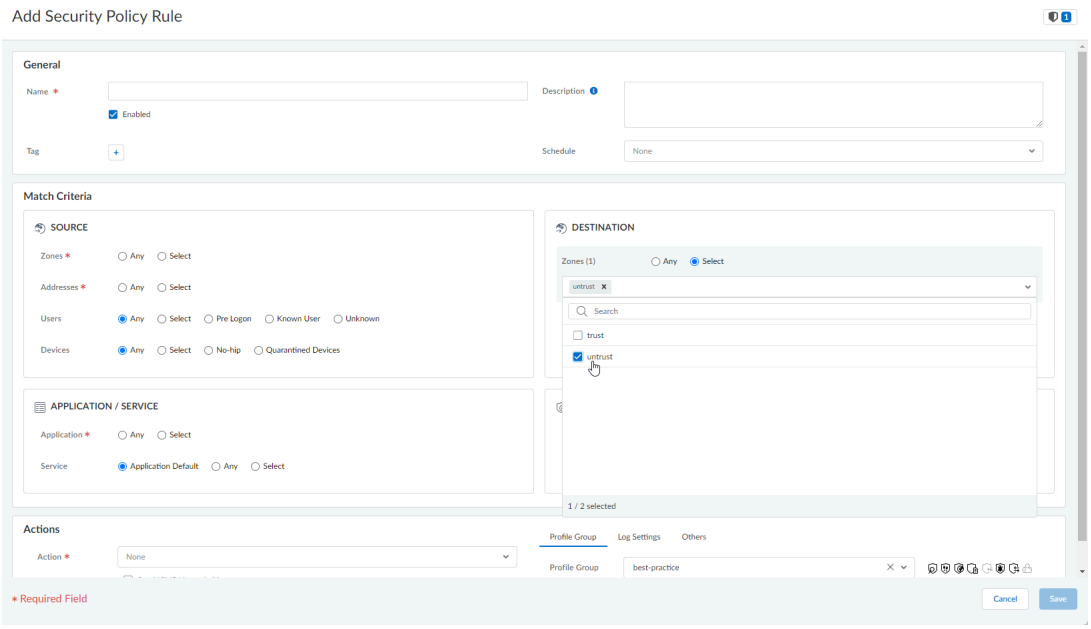
STEP 2 | 配置 DNS 设置。

 ©2025 Palo Alto Networks, Inc.

STEP 3 | 确保互联网绑定流量的策略规则中的 **DESTINATION**（目标） **Zones**（区域） 设置为 **untrust**（非信任）区域而不是 **any**（任何）区域。

若未能执行此步骤，可能会导致您的数据中心遭到意外访问。

1. 转至 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**），将 **Configuration Scope**（配置范围）设置为 **Prisma Access** > **Mobile Users Container**（移动用户容器） > **Explicit Proxy**（显示代理），然后选择 **Security Policy**（安全策略） > **Security Services**（安全服务）。
2. 打开互联网绑定流量的规则。
3. 确保将 **DESTINATION**（目标）下的 **Zones**（区域）设置为 **untrust**（不可信）。



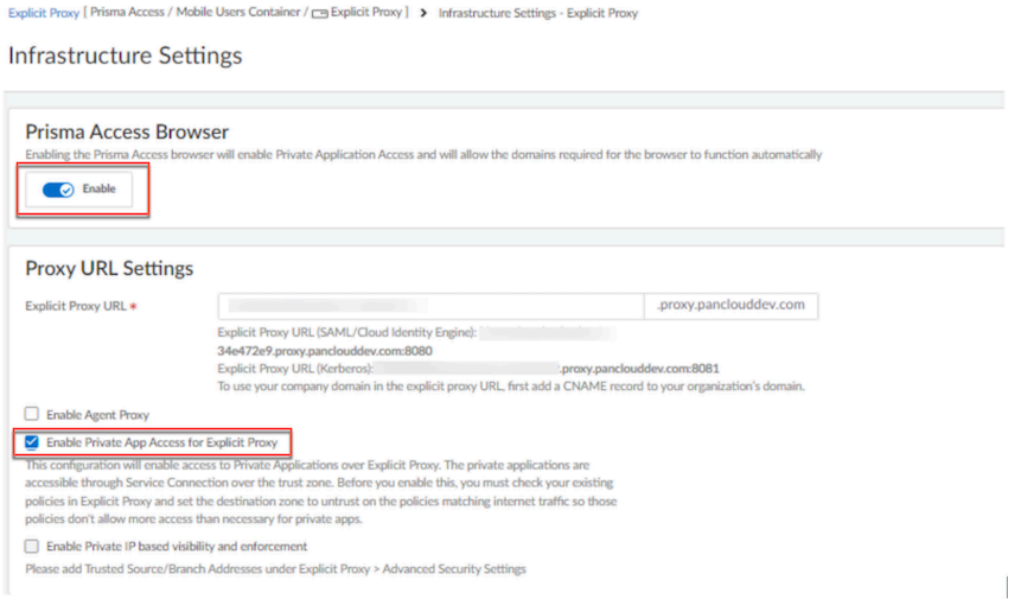
4. 对所有互联网绑定流量规则重复上述操作。

STEP 4 | 启用私有应用程序访问权限。

- 使用 Prisma Access Browser 启用私有应用程序访问权限。
  1. 选择 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Explicit Proxy**（显式代理） > **Infrastructure Settings**（基础架构设置），然后选择启用

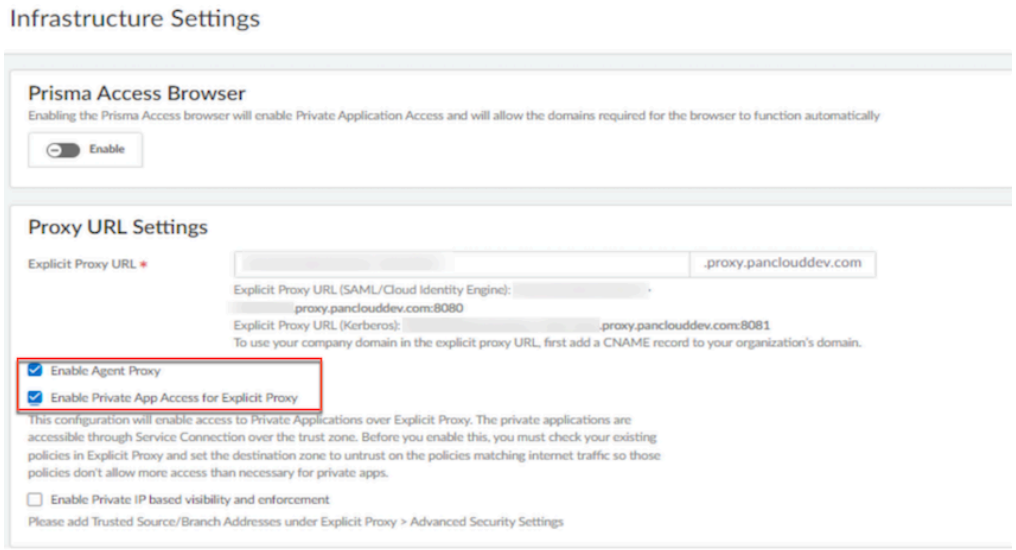
 ©2025 Palo Alto Networks, Inc.

Prisma Access Browser。在 **Proxy URL Settings**（代理 **URL** 设置）下，选择 **Enable Private App Access for Explicit Proxy**（为显式代理启用私有应用程序访问权限）。



- 使用常规浏览器启用私有应用程序访问权限。

  1. 选择 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Explicit Proxy**（显示代理） > **Infrastructure Settings**（基础架构设置） > **Enable Agent Proxy**（启用客户端代理） > **Enable Private App Access for Explicit Proxy**（为显式代理启用私有应用程序访问权限）。



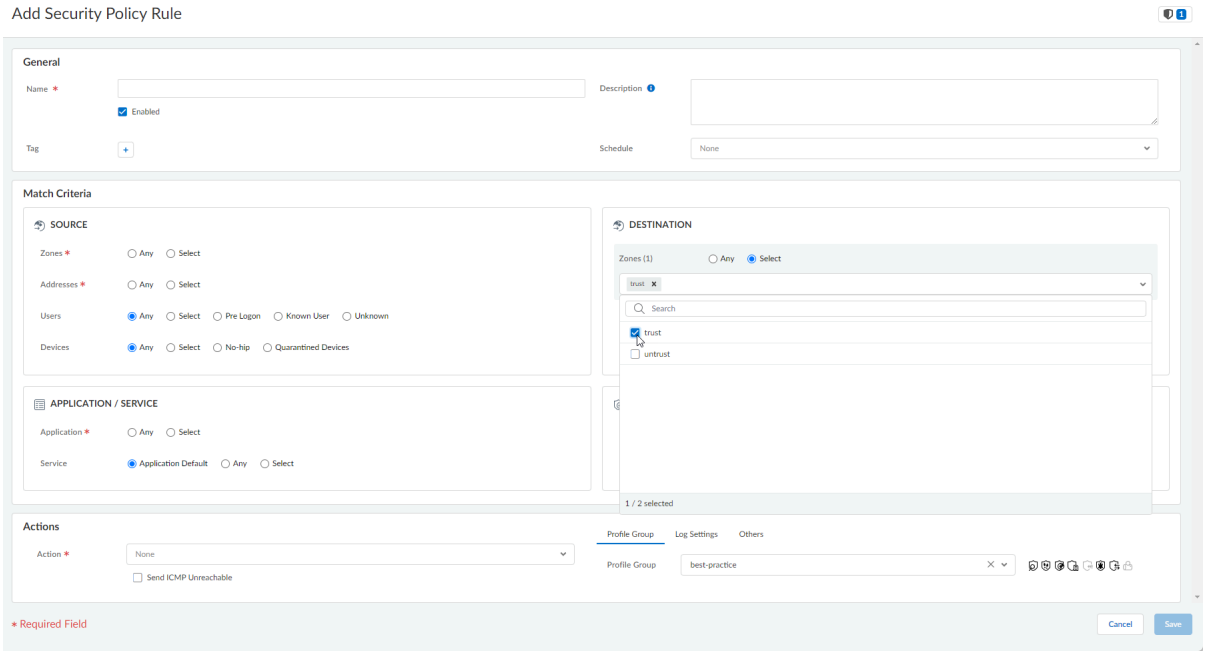
STEP 5 | 为您想要访问的数据中心资源创建安全策略规则。

1. 转至 **Manage**（管理） > **Configuration**（配置） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**），将 **Configuration Scope**（配置范围）设置为 **Prisma Access** > **Mobile Users Container**（移动用户容器） > **Explicit Proxy**（显示代理），然后选择 **Security Policy**（安全策略） > **Security Services**（安全服务）。

©2025 Palo Alto Networks, Inc.

2. 创建安全策略规则。

在数据中心访问的规则中，确保将 DESTINATION（目标）下的 **Zones**（区域）设置为 **trust**（信任）。



STEP 6 | 如果在“显式代理”下启用“私有应用程序访问权限”，请在载入 ZTNA 连接器后 **Push Config**（推送配置）以保存配置更改。

使用显式代理访问数据中心 (Panorama)

STEP 1 | 根据您的要求在 Prisma Access 中配置服务连接、Colo-Connect 或 ZTNA 连接器。

STEP 2 | 配置 DNS 设置。

STEP 3 | 配置区域映射。

1. 选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Mobile Users - Explicit Proxy**（移动用户-显式代理） > **Zone Mapping**（区域映射）
2. 将用于访问数据中心资源的区域添加到 **Trusted Zones**（信任区域）。

STEP 4 | 确保互联网绑定流量的策略规则中的目标区域设置为非信任区域而不是任何区域。

若未能执行此步骤，可能会导致您的数据中心遭到意外访问。

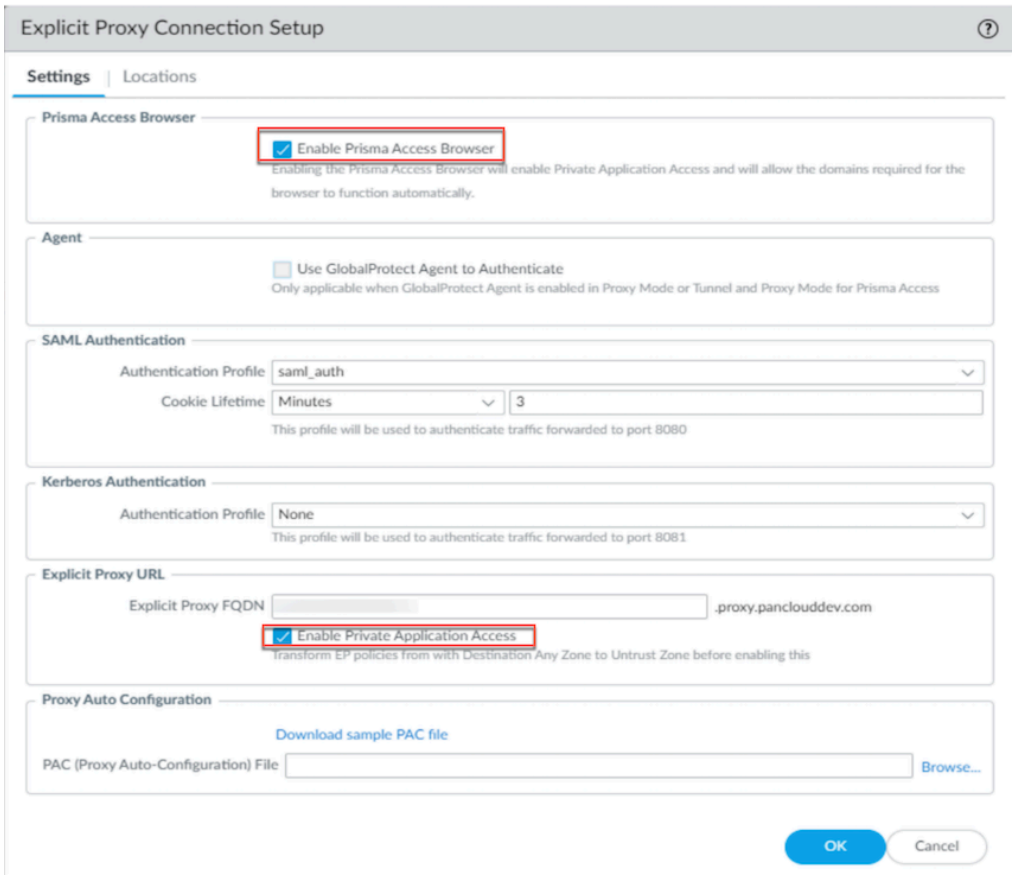
1. 选择 **Policies**（策略）。
2. 将设备组设置为 **Explicit_Proxy_Device_Group**。
3. 将目标区域从任何区域更改为您在之前的步骤中配置的非信任区域之一。

©2025 Palo Alto Networks, Inc.

STEP 5 | 启用私有应用程序访问权限。

- 使用 Prisma Access Browser 启用私有应用程序访问权限。

  1. 转至 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Mobile Users - Explicit Proxy**（移动用户-显式代理） > **Settings**（设置） > **Advanced**（高级） > **Enable Prisma Access Browser**（启用 **Prisma Access Browser**） > **Enable Private Application Access**（启用私有应用程序访问权限）

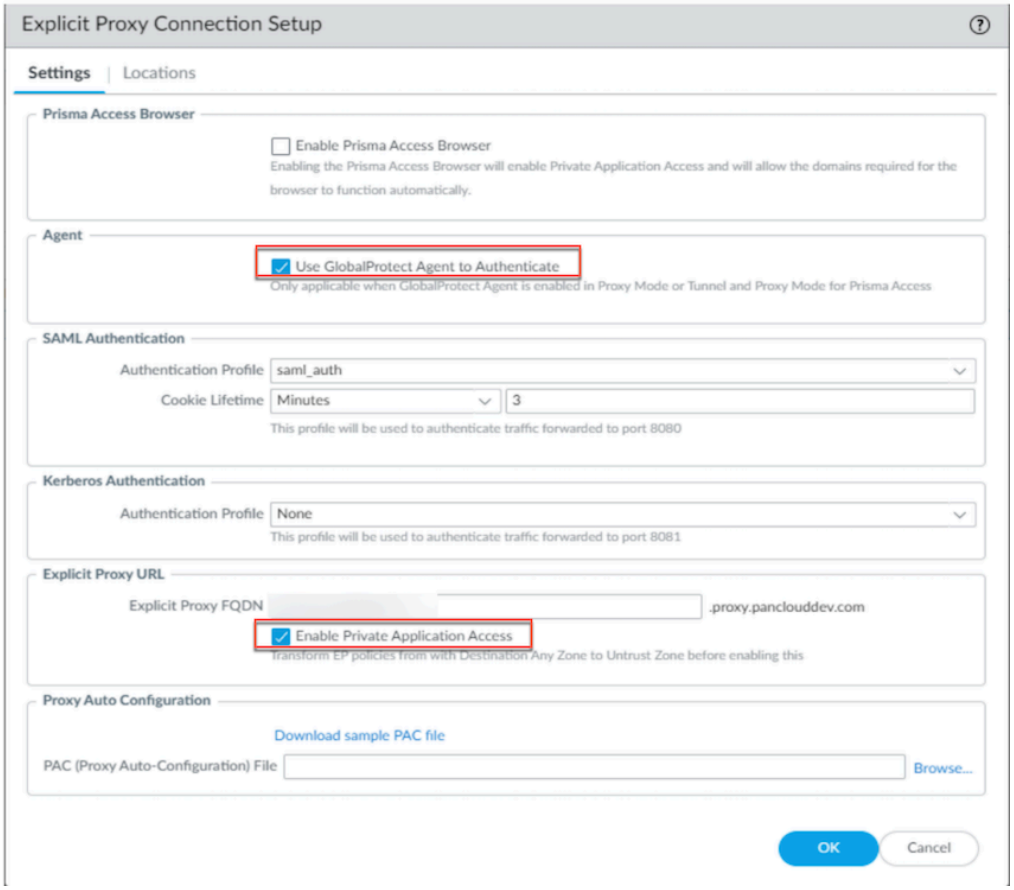


- 使用常规浏览器启用私有应用程序访问权限。

  1. 转至 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Mobile Users - Explicit Proxy**（移动用户-显式代理） > **Settings**（设置） > **Advanced**（高级） >

©2025 Palo Alto Networks, Inc.

Use GlobalProtect Agent to Authenticate（使用 **GlobalProtect** 代理进行身份验证）> **Enable Private Application Access**（启用私有应用程序访问权限）



STEP 6 | 为您想要访问的数据中心资源创建安全策略规则。

1. 选择 **Policies**（策略）。
2. 将设备组设置为 **Explicit_Proxy_Device_Group**。
3. 创建安全策略规则。

   在数据中心访问规则中，确保使用在之前的步骤中配置的 **Trusted**（信任）区域。

基于应用程序的 Office 365 与显式代理集成

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• 移动用户许可证

了解如何将基于浏览器的 Office 365 版本与显式代理集成。

- Strata Cloud Manager
- Panorama

©2025 Palo Alto Networks, Inc.

基于应用程序的 Office 365 与显式代理集成 (Panorama)

Prisma Access 显式代理支持基于浏览器的 Office 365 (M365) 版本，包括 Office Online (office.com)。按照以下步骤将基于浏览器的 Office 365 版本与显式代理集成。

虽然显式代理不支持基于应用程序的 Office 365 版本，但您可以按照这些准则将显示代理与基于 Office 365 应用程序的策略一起使用。

设置基于浏览器的 **Office 365** 与 **Prisma Access** 显式代理的集成

如果您使用基于浏览器的 Office 365 版本，请完成以下任务以将 Office 365 与显式代理集成。

STEP 1 | （可选）如果您想使用基于租户的限制（仅允许特定数量的租户对 Office 365 进行访问控制），可使用包含自定义 URL 类别的 HTTP 标头插入，以允许特定租户访问 Office 365。

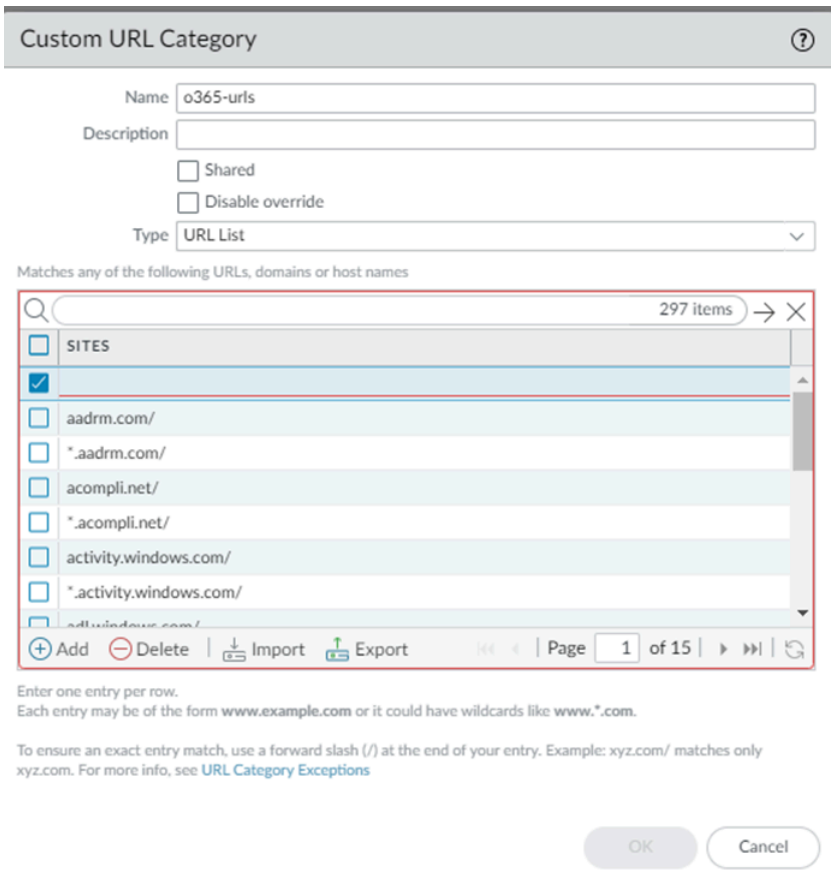
©2025 Palo Alto Networks, Inc.

STEP 2 | 为用于 Office 365 的 URL 添加解密策略。

1. 选择 **Objects**（对象） > **Custom Objects**（自定义对象） > **URL Category**（**URL** 类别），然后选择 **Add**（添加）以添加一个自定义 URL 类别。

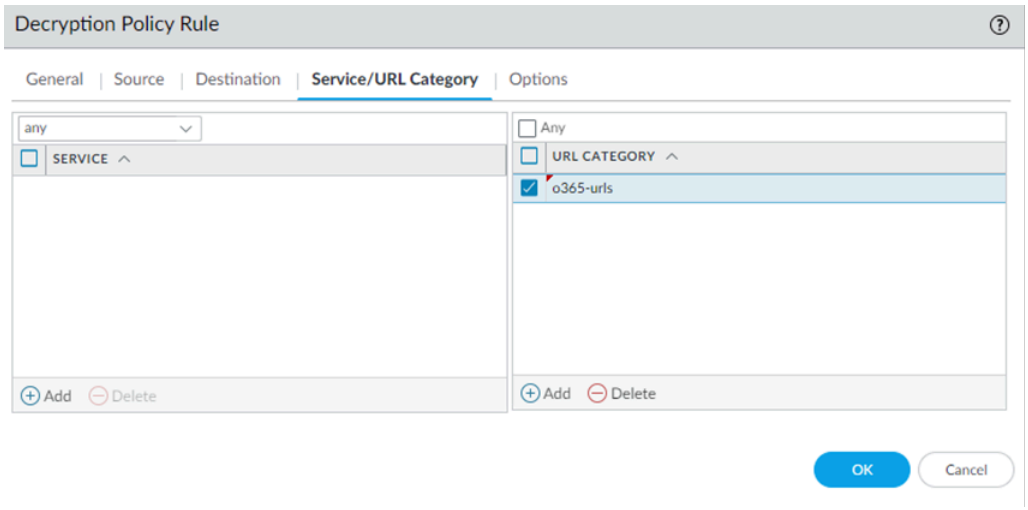
   确保您在 **Explicit_Proxy_Device_Group** 中。
2. 指定 **URL List**（**URL** 列表）的 **Type**（类型）。
3. 选择 **Add**（添加）以添加要启用 Office 365 集成的站点列表。

   为了简化网址的上传，可以在 https://saasedl.paloaltonetworks.com/feeds/m365/worldwide/any/all/url 复制 Office 365 网址列表，将这些 URL 保存到文件中，然后选择 **Import**（导入）以将文件导入到自定义网址类别。



4. 选择 **Policies**（策略） > **Decryption**（解密） > **Pre Rules**（预规则），然后选择 **Add**（添加）以添加解密策略规则。
5. 指定您创建的 **URL Category**（**URL** 类别）。

 ©2025 Palo Alto Networks, Inc.



6.

STEP 3 | 为数据和威胁防护功能添加解密策略，比如企业数据丢失防护（企业数据丢失防护）、WildFire、威胁防护 或 SaaS 安全。

STEP 4 | 使用 EDL 托管服务来创建外部动态列表。

STEP 5 |

使用显式代理设置基于应用程序的 **Office 365** 集成

显式代理不支持 Office 365 的基于客户端（应用程序）的完整版本，因为 Office 365 使用非 Web 端口和协议以及固定证书，这会阻止使用解密。如果您需要保护来自 Office 365 客户端应用程序的流量，则可以使用以下 Prisma Access 功能之一来实现：

- 部署采用显式代理的“移动用户—GlobalProtect”部署，并使用 GlobalProtect 拆分隧道选项将流量从 Office 365 应用程序路由到 GlobalProtect 隧道，同时根据您的 PAC 文件和 GlobalProtect 隧道的包含和排除选项，指定要发送到 GlobalProtect 隧道、直接发送到互联网或显式代理的其他互联网流量。
- 如果您的组织要求流向互联网的流量通过显式代理，或者如果您的网络没有默认路由，则可以部署采用显式代理的远程网络部署采用显式代理的远程网络部署在此部署中，显式代理为您提供了任播和单播地址的列表，您可以配置 CPE 以通过这些地址将流量路由到远程网络，然后从远程网络路由到显式代理和互联网。

  要将 Office 365 用于此部署类型，请指定 PAC 文件规则以绕过非 Web Office 365 直接连接到互联网。
- 如果您无法在环境中部署 GlobalProtect 或 Prisma Access 远程网络，则可以配置显式代理 PAC 文件以绕过 Office 365 流量。使用 URL 列表绕过。

要启用 *Office 365* 与 *Prisma Access* 显式代理集成的 *URL* 列表

要将非浏览器 Office 365 应用程序与显式代理集成，另一个可行方案是指定与 Office 365 相关的 URL，并在显式代理 PAC 文件中绕过这些 URL。使用以下方法之一获取要绕过的 URL 列表：

©2025 Palo Alto Networks, Inc.

- 将 Palo Alto Networks EDL 托管服务中提供的 EDL URL 用于 Microsoft 365 应用程序。

  通过使用 Feed URL 作为 EDL 源，利用该托管服务可减轻保障 SaaS 应用程序流量安全的运营负担。当 SaaS 提供商为 SaaS 应用程序添加新的端点时，相应的 Feed URL 也会更新。

  对于全球范围内的 Microsoft 365 URL，请使用 URL https://saasedl.paloaltonetworks.com/feeds/m365/worldwide/any/all/url。为 IPv4 和 IPv6 以及特定于国家和政府的应用程序提供了其他 URL。
- 在以下网址中检索 Microsoft 提供的 Office 365 IP 地址和 URL 列表：https://learn.microsoft.com/en-us/microsoft-365/enterprise/urls-and-ip-address-ranges。Microsoft 还提供 Office 365 IP 地址和 URL 网络服务，网址为：https://learn.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-ip-web-service。

使用 Blue Coat 代理配置代理链

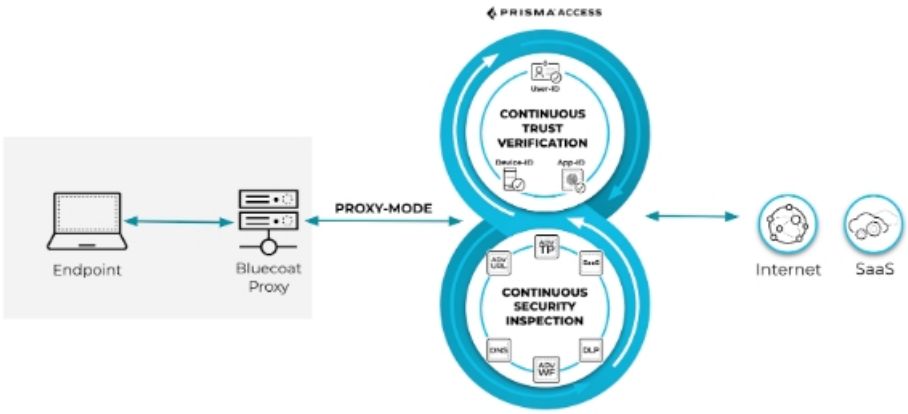
在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 许可证。

代理链通过级联多个代理服务器来创建多跳互联网路径，以提供额外的安全层或满足合规性要求。每个服务器都会将您的流量转发到下一个服务器，最终使流量到达互联网。此技术使用您现有的网络基础架构，并能够连接到上游代理以实现安全的 HTTP 和 HTTPS 通信。集成可保留用户浏览器设置，同时增强了安全性与控制性。

企业使用代理链功能的原因：

1. 通过提供多层保护和绕过地理限制来增强隐私性和匿名性。
2. 通过过滤恶意内容、垃圾邮件和网络钓鱼尝试来实现安全性和控制性，为用户的浏览体验添加额外的安全层。
3. 公司可以使用代理链实施内部策略规则，根据用户角色或位置限制对某些网站或服务的访问。
4. 您无需部署新系统，而是可以通过代理链连接到上游代理服务器来执行特定任务，从而利用现有的网络基础架构。这可能是一种经济高效的解决方案。

了解有关 Prisma Access 显式代理的工作原理的更多信息。



 ©2025 Palo Alto Networks, Inc.

在以下场景中，客户想要通过代理链将流量从本地 Blue Coat 代理传输到 Prisma Access 显式代理。本地 Blue Coat 代理使用在 Blue Coat 代理上插入的 X-Authenticated-User (XAU) 标头对用户进行身份验证，并将用户名传递给 Prisma Access 显式代理。

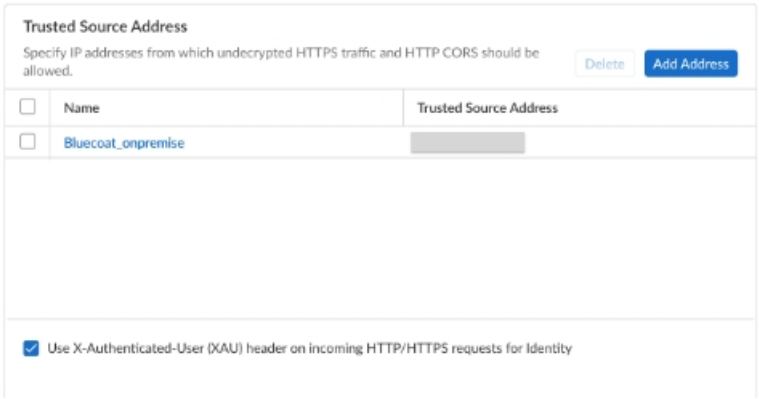
在非默认路由网络中，需要显式代理 *IP* 地址的静态路由和目标 *NAT*。

STEP 1 | 配置 Prisma Access。

1. 设置显式代理。
2. 将 Blue Coat 显式代理添加为可信源地址。
   1. 选择 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Explicit Proxy**（显式代理） > **Advanced Security Settings**（高级安全设置） > **Add Address**（添加地址）。
   2. 输入 Blue Coat 显式代理的 IP 地址。

      您可以添加 *IP* 地址或子网。

   3. 选择 **Use X-Authenticated-User (XAU) header on incoming HTTP/HTTPS requests for Identity**（在传入的 **HTTP/HTTPS** 身份请求上使用 **X-Authenticated-User (XAU)** 标头）。

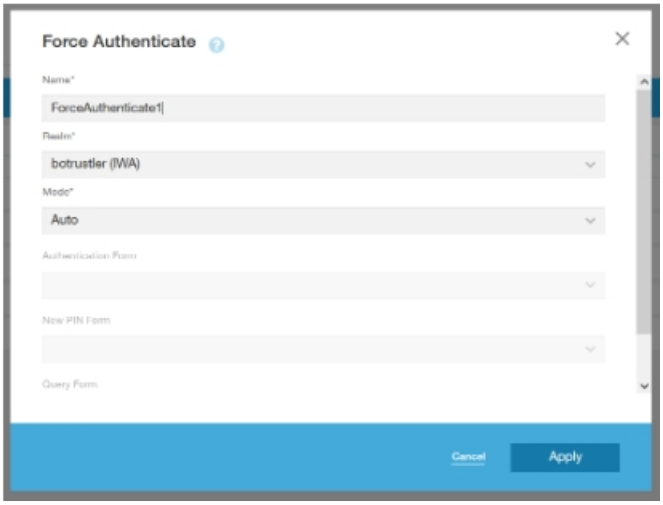


 ©2025 Palo Alto Networks, Inc.

STEP 2 | 在 Blue Coat 代理上执行配置。

1. 强制进行身份验证。



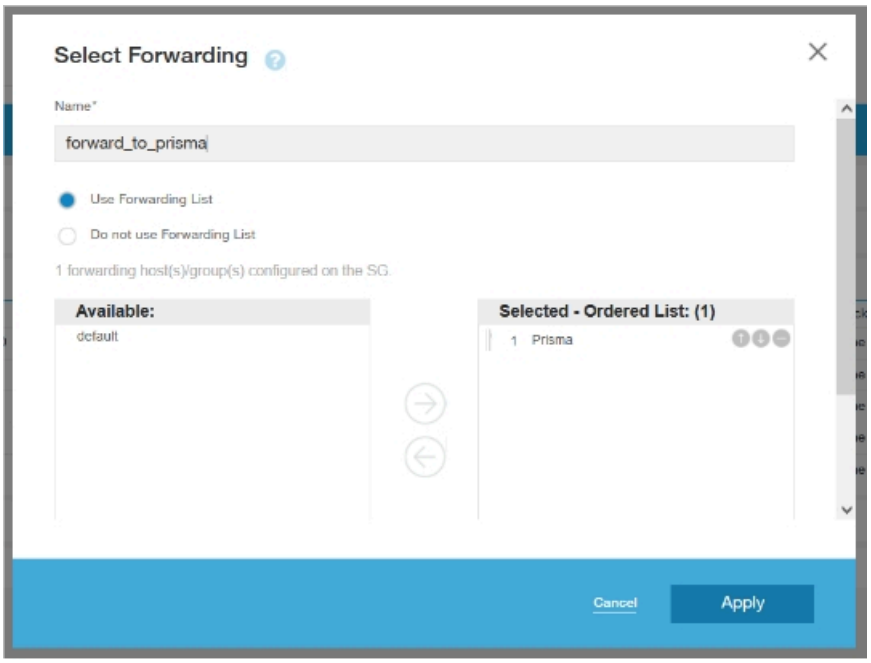


2. 配置转发层。



1. 获取 Prisma Access 显式代理的 IP 地址。
   1. 在 Strata Cloud Manager 中，选择 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Explicit Proxy**（显式代理） > **Infrastructure Settings**（基础架构设置）。
   2. 复制代理 FQDN。

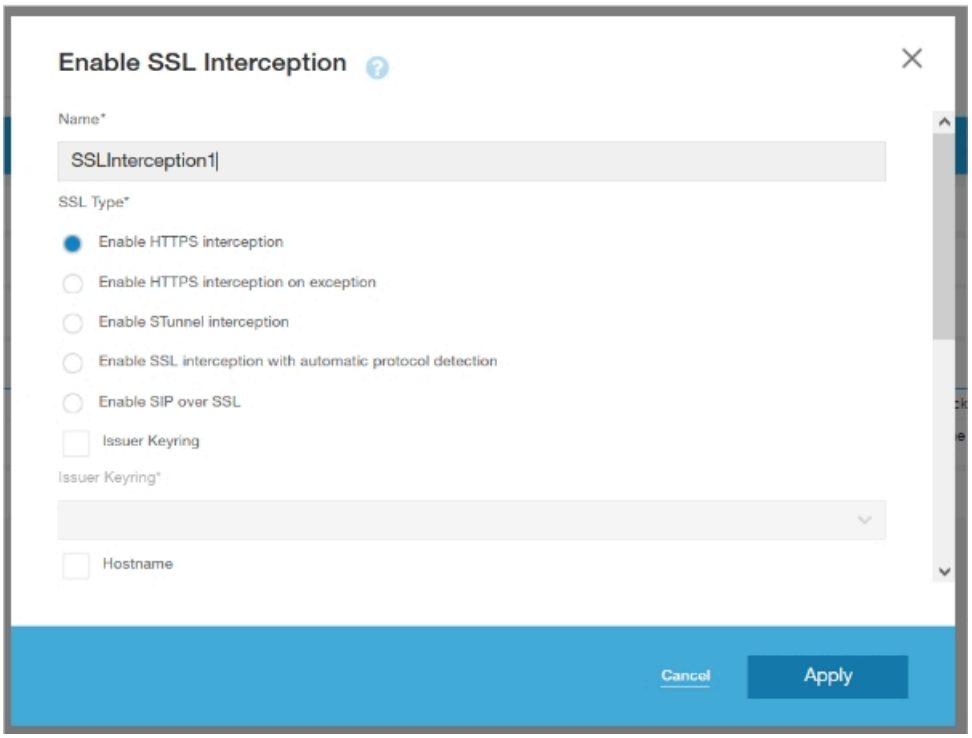
©2025 Palo Alto Networks, Inc.





2. 启用 HTTPS 解密以插入标头。

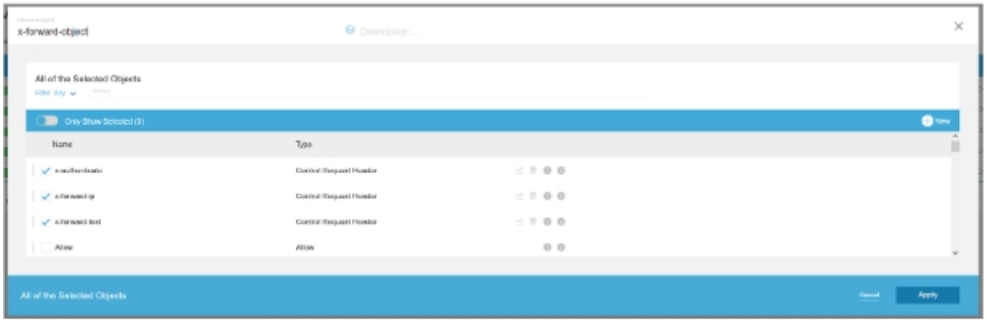
   要插入标头，必须启用解密。

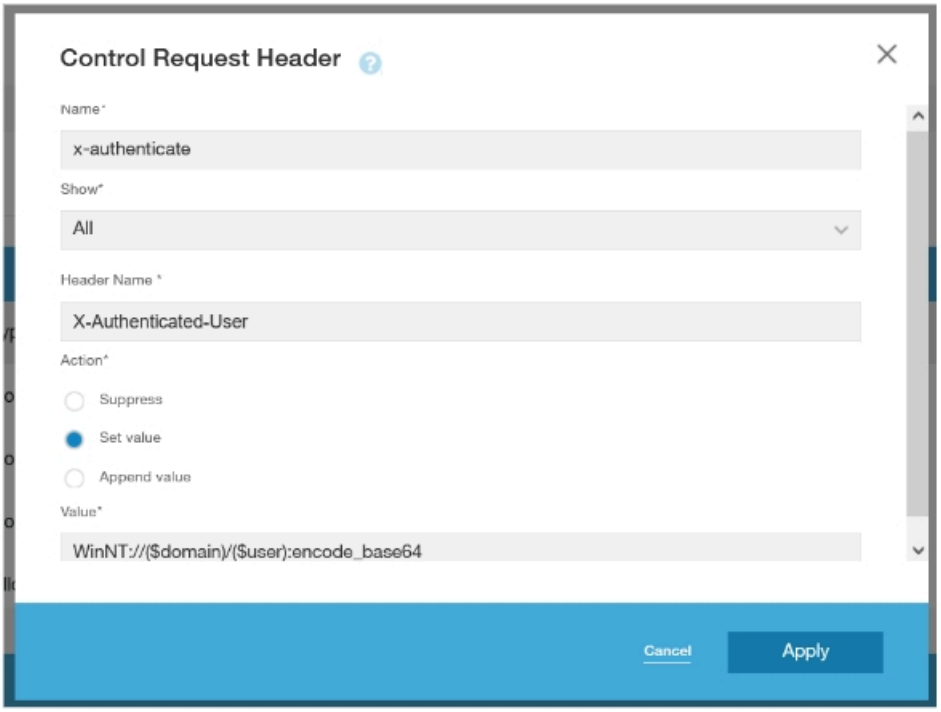


 ©2025 Palo Alto Networks, Inc.

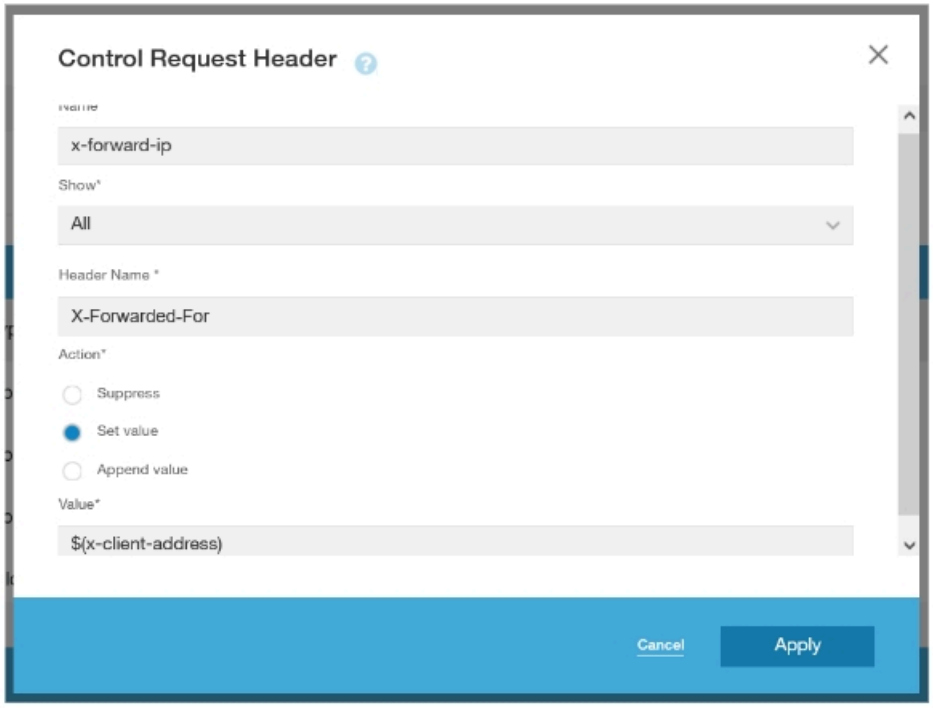


3. 配置标头转发。





©2025 Palo Alto Networks, Inc.



通过 *XFF* 标头收到的客户端 *IP* 地址仅可被记录，不能用于策略。

4. 将标头值编码设置为 base64：

```
define action Encode_All_XFF set( request.x_header.X-
Authenticated-User, "$(user:encode_base64)" ) end define action
 x-authenticate set( request.x_header.X-Authenticated-User,
 "WinNT://($$domain)/($$user):encode_base64" ) end
```

STEP 3 | 验证配置。

1. 在 Strata Cloud Manager 中，选择 **Incidents and Alerts**（事件和警报） > **Log Viewer**（日志查看器）
2. 检查 `X-Forwarded-For` 列和 `Users` 列，以验证用户和 IP 地址信息在 Prisma Access 上是否可见。

STEP 4 | 请考虑以下几点注意事项：

1. Blue Coat 代理需要身份验证和解密才能插入 XAU 标头信息。
2. X-Authenticated-User 身份验证标头值应采用 Base64 格式。
3. Prisma Access 显式代理可以看到解密流量的用户身份。

在 GlobalProtect（或第三方 VPN）中使用显式代理

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	• Prisma Access 许可证

©2025 Palo Alto Networks, Inc.

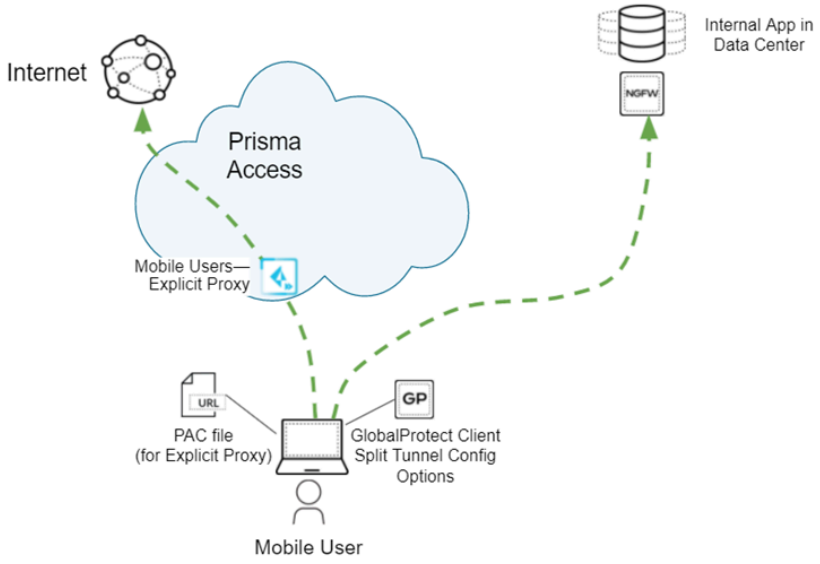
在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	

你可以将显式代理与 GlobalProtect 或第三方 VPN 结合使用：

- 显式代理和 **GlobalProtect**
  - 在分割隧道模式下使用 GlobalProtect 仅提供对私有应用程序的安全访问。
  - 使用显式代理来保护公共应用程序，包括互联网流量和外部 SaaS 应用程序。
- 显式代理和第三方 **VPN**

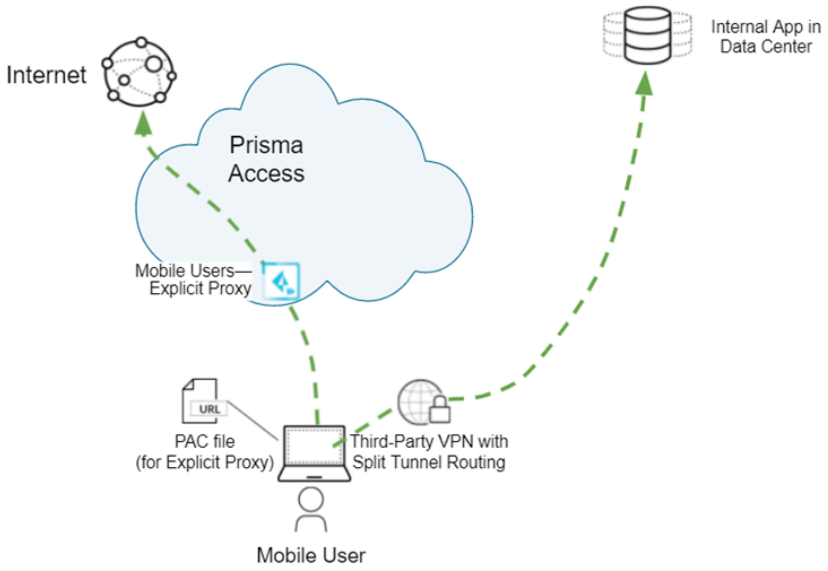
  如果您使用 VPN 客户端访问数据中心和私有应用程序，则可以继续使用该客户端来保护对私有应用程序的访问，同时使用显式代理和 PAC 文件来保护对公共应用程序的访问。您可以在靠近移动用户的位置部署显式代理，这样就无需为网络安全将流量回传到数据中心。

下图显示了使用 GlobalProtect 网关和显式代理的部署。GlobalProtect 使用 GlobalProtect 客户端将流量路由到帕洛阿尔托网络的新一代防火墙。要配置此部署，您需要在 GlobalProtect 中创建拆分隧道配置，允许使用 GlobalProtect 保护私有应用程序，使用显式代理保护公共应用程序。配置完成后，移动用户使用 GlobalProtect 连接到贵组织数据中心中的私有应用程序，并使用显式代理连接到基于互联网的私有应用程序。



如果您有第三方 VPN，则可以使用它来连接数据中心中的私有应用程序，同时使用 Explicit Proxy 保护公共应用程序，如下图所示。

©2025 Palo Alto Networks, Inc.



入门：

- 工作原理
- 显式代理 — 指南
- 显式代理和 GlobalProtect：设置步骤
- 显式代理与第三方 VPN

将显式代理与 GlobalProtect 或第三方 VPN 结合使用的要求

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证

在开始配置之前，请确保遵循使用 GlobalProtect 或第三方 VPN 部署显式代理所需的要求和建议：

- 要将显式代理与 GlobalProtect 一起使用，您必须部署 GlobalProtect（移动用户 - GlobalProtect 部署或使用 GlobalProtect 网关和门户的独立 GlobalProtect 部署）。

  您可以在 GlobalProtect 中配置拆分隧道配置。本节中的示例展示了基于域 (URL) 或应用程序拆分的流量；但是，您也可以基于访问路由拆分流量。

  您还可以在 GlobalProtect 中国年配置拆分 DNS选项，以便配置哪些域由 VPN 分配的 DNS 服务器进行解析，哪些域由本地 DNS 服务器解析。
- 要将显式代理与第三方 VPN 一起使用，您必须部署 VPN 解决方案。

©2025 Palo Alto Networks, Inc.

- 列出您想要使用移动用户（GlobalProtect 或第三方 VPN 部署）保护的应用程序。

  例如，如果您使用 GlobalProtect 配置显式代理，则应配置 GlobalProtect 以保护对私有应用程序或资源的所有访问，同时配置显式代理 PAC 文件以保护公共应用程序或 SaaS 应用程序。本节中的配置示例有 GlobalProtect 解析内部域和 Explicit Proxy 解析外部域。
- 为 Explicit Proxy 和 GlobalProtect 或第三方 VPN 配置身份验证。
  - 对于显式代理，您必须使用 SAML 身份验证。遵循在显式代理部署中的配置 SAML 的指南，包括用于 SAML 登录的 URL。
  - 对于移动用户 — GlobalProtect 部署，如果您使用 SAML 身份验证并以 Okta 作为身份提供者 (IdP)，请参阅 Prisma Access 集成指南（Panorama 管理）中用于使用 Okta 配置 SAML 身份验证的过程。
  - 对于独立的 GlobalProtect 部署，您可以在 PAN-OS 中配置 SAML 身份验证。
  - 对于第三方 VPN，请参阅该 VPN 的产品文档。

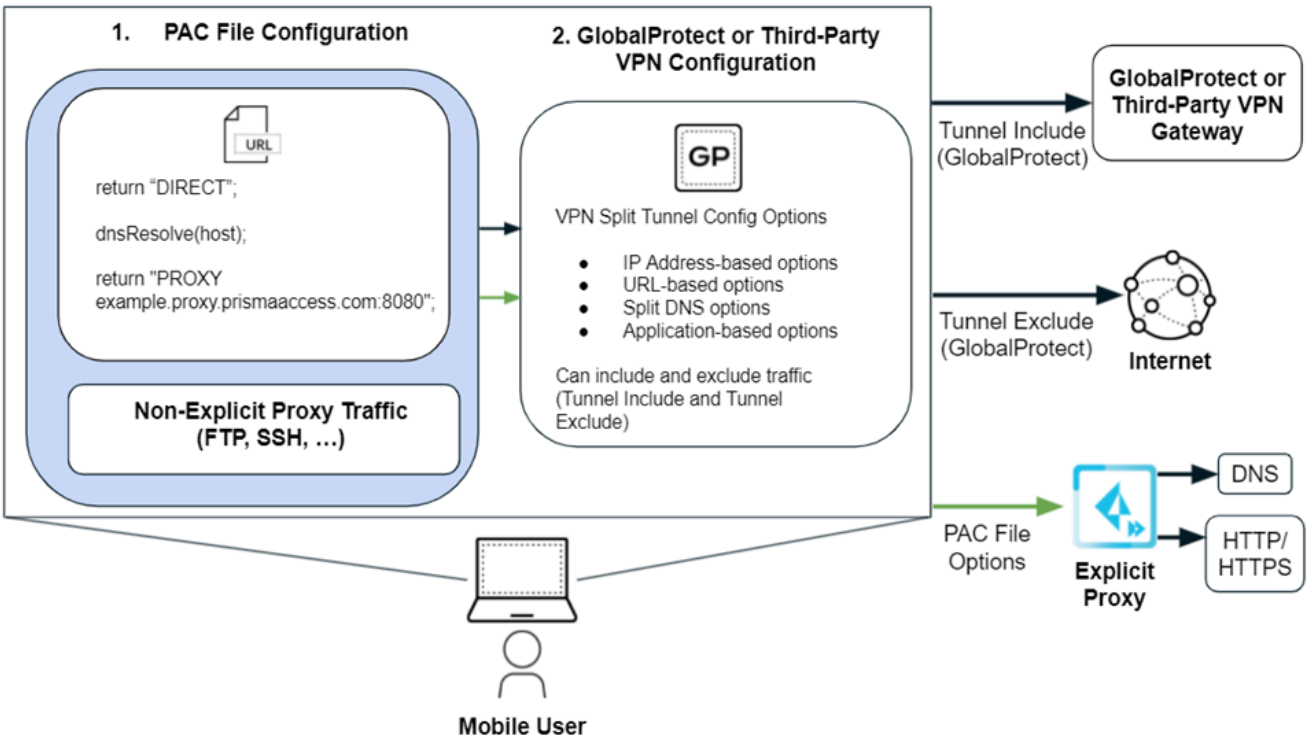
  Palo Alto Networks 建议您在每个移动用户的终端上使用默认浏览器进行 SAML 身份验证，这样您就可以通过编辑门户配置来利用单点登录 (SSO)，如设置 Explicit Proxy中所述。
- 您必须确保移动用户使用的浏览器遵守 PAC 文件中的配置。

显式代理和 GlobalProtect：工作原理

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证

在决定应使用显式代理保护哪些应用程序或流量以及应使用 GlobalProtect 或第三方 VPN 保护哪些应用程序之前，应首先了解 GlobalProtect 和 Prisma Access 如何根据显式代理和 VPN 配置做出转发决定。本节中的示例假定您已将显式代理和 GlobalProtect 部署到组织的网络中，并已配置 GlobalProtect 拆分隧道选项。下图显示了该过程。

©2025 Palo Alto Networks, Inc.



当移动用户请求私有或基于互联网的资源或应用程序时，该请求将由端点上的显式代理 PAC 文件进行评估。

- PAC 文件中的 `return "DIRECT";` 函数会使表达式中指定的流量绕过显式代理处理。

  显式代理为您提供了一个 PAC 文件示例，该文件将 `return "DIRECT";` 函数用于 IP 地址和 URL。请参阅 以查看 PAC 文件的内容及其使用说明。

- PAC 文件中的 `dnsresolve(host)` 函数会强制端点进行 DNS 查询，以将主机名解析为 IP 地址。然后，此查询遵循 VPN 策略（例如，分割隧道或拆分 DNS），以将 DNS 请求转发到目标 DNS 服务器。

  显式代理随附的 PAC 文件在表达式中同时使用 `dnsresolve(host)`、`return"DIRECT";` 和私有 IP 地址。如果在 DNS 查找后，返回的 IP 地址包含在表达式中的私有 IP 地址中，则与私有 IP 地址关联的流量将绕过显式代理处理。

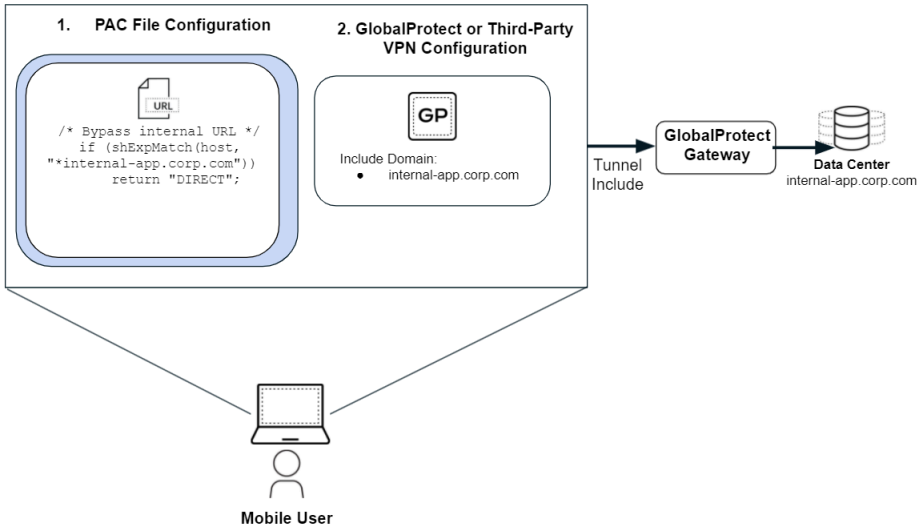
- 在 PAC 文件中指定为 `return"PROXY sitename:8080";` 的流量将被转发到显式代理。

在根据 PAC 文件中的条件对 Web 请求进行评估后，将其发送到端点上的 GlobalProtect 或第三方 VPN 配置进行处理，并在 GlobalProtect 应用程序中对拆分隧道配置选项的流量进行评估。可以根据域 (URL)、应用程序或子网来拆分流量。如果在 GlobalProtect 中配置了拆分 DNS 选项，则还会根据这些 DNS 选项评估流量。

处理流量后，会根据 PAC 文件和 VPN 处理，将流量发送到 GlobalProtect、直接发送到互联网或发送到显式代理。

下图显示移动用户尝试使用 URL **`internal-app.corp.com`** 访问私有资源。

©2025 Palo Alto Networks, Inc.

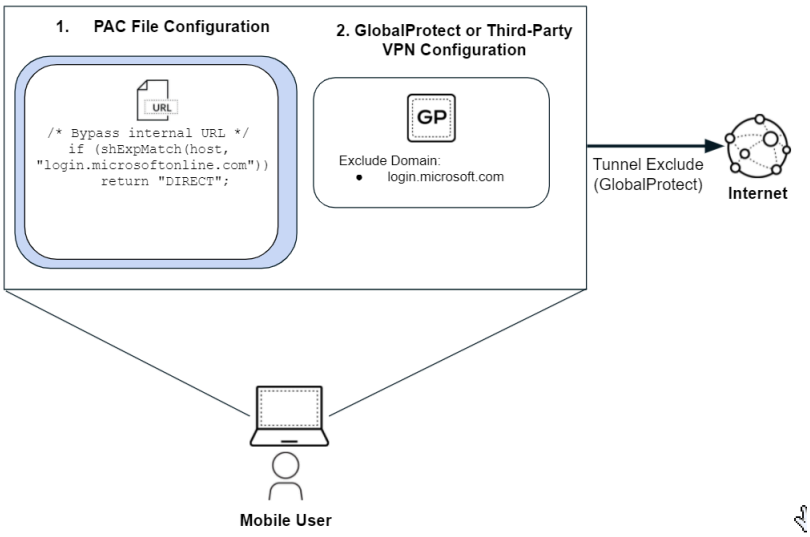


- PAC 文件具有以下配置，以允许 **internal-app.corp.com** 绕过显式代理。

```
    /* Bypass internal URL */ if (shExpMatch(host, "*internal-
app.corp.com")) return "DIRECT";
```

- 当移动用户从其浏览器请求 **internal-app.corp.com** 时，浏览器会评估 PAC 文件中的条件。根据该评估的结果，浏览器不会将请求转发给代理，而是将其直接发送给 GlobalProtect 应用程序。
- GlobalProtect 发现 **Include Domain**（包含域）中列出了 **internal-app.corp.com**，于是通过 VPN 隧道来发送请求。
- GlobalProtect 根据 GlobalProtect 中的配置选项将请求发送到 **internal-app.corp.com** 中的资源。

您可能希望配置一些资源（如登录资源），使其既不使用显式代理，也不使用 GlobalProtect 或第三方 VPN 进行处理。下图显示了用户通过在浏览器中输入 **login.microsoftonline.com** 登录到 Microsoft Online。



 ©2025 Palo Alto Networks, Inc.

- PAC 文件具有以下配置，以允许 **internal-app.corp.com** 绕过显式代理通信。

```
   /* Bypass internal URL */ if (shExpMatch(host,
"login.microsoftonline.com")) return "DIRECT";
```

- 当移动用户从其浏览器请求 **login.microsoftonline.com** 时，PAC 文件会评估来自移动用户端点中的 PAC 文件的请求，然后将其发送到 GlobalProtect VPN 配置（本例中为 GlobalProtect）进行处理。
- GlobalProtect 应用程序发现 **Exclude Domain**（排除域）中列出了 **login.microsoftonline.com**。
- 根据 GlobalProtect 中的配置选项，GlobalProtect 绕过 VPN 并将请求直接发送到互联网。

显式代理和 GlobalProtect：设置步骤

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证

为了让您的移动用户安全连接，可以将显式代理与 GlobalProtect 或第三方 VPN 结合使用。

- 显式代理和 GlobalProtect
  - 在拆分隧道模式下使用 GlobalProtect 可提供对私有应用程序的安全访问。
  - 使用显式代理来保护公共应用程序，包括互联网流量和外部 SaaS 应用程序。
- 显式代理和第三方 VPN
  - 使用 VPN 客户端访问数据中心和私有应用程序，并保护对私有应用程序的访问。
  - 使用显式代理和 PAC 文件来保护对公共应用程序的访问。

在决定应使用显式代理和 GlobalProtect 或第三方 VPN 保护哪些应用程序或通信之前，应首先了解 GlobalProtect 和 Prisma Access 如何根据显式代理和 VPN 配置做出转发决定。

移动用户请求私有或基于互联网的资源或应用程序时，该请求将被发送到安装在端点上的显式代理 PAC 文件。

- PAC 中指定为 return "DIRECT"; 的流量将绕过显式代理处理。与 return "DIRECT"; 配合使用的 DNS 解析（主机）允许指定 IP 通过显式代理处理。
- 在 PAC 文件中指定为 return "PROXY sitename:8080"; 的流量将被转发到显式代理。

处理流量后，会根据 PAC 文件和 VPN 处理，将流量发送到 GlobalProtect、直接发送到互联网或发送到显式代理。

PAC 文件的配置可允许“internal-app.corp.com”绕过显式代理。当移动用户从其浏览器请求“internal-app.corp.com”时，浏览器会评估 PAC 文件中的条件。GlobalProtect 发现“Include Domain（包含域）”中列出了“internal-app.corp.com”，于是通过 VPN 隧道来发送请

 ©2025 Palo Alto Networks, Inc.

求。GlobalProtect 根据 GlobalProtect 中的配置选项将请求发送到“internal-app.corp.com”中的资源。

- Strata Cloud Manager
- Panorama

显式代理和 **GlobalProtect**：设置步骤 **(Strata Cloud Manager)**

要使用显式代理实施“GlobalProtect — 移动用户”，请完成以下步骤。

这些配置步骤基于以下关于您网络环境的假设；如果您的网络环境不同，配置方式可能也会不同：

- 移动用户能够访问并解析 GlobalProtect Portal 主机名、网关 FQDN、显式代理 URL 和 PAC 文件 URL。

  在这里下面找到这些信息：

  - **GlobalProtect** 网关 **FQDN** 和门户主机名

    # 前往 **Workflows**（工作流） > **Prisma Access** 设置 > **GlobalProtect** > **Infrastructure**（基础设施），然后编辑 **Infrastructure Settings**（基础设施设置）设置。
  - 显式代理 **URL** 和 **PAC** 文件 **URL**

    # 转到 **Workflows**（工作流） > **Prisma Access** 设置 > **Explicit Proxy**（显式代理） > **Infrastructure**（基础设施），然后编辑 **Infrastructure Settings**（基础设施设置）设置。
- 移动用户能够从 GlobalProtect 解析内部域。

STEP 1 | 决定要将哪些应用程序发送到 GlobalProtect，以及要将哪些应用程序发送到显式代理。

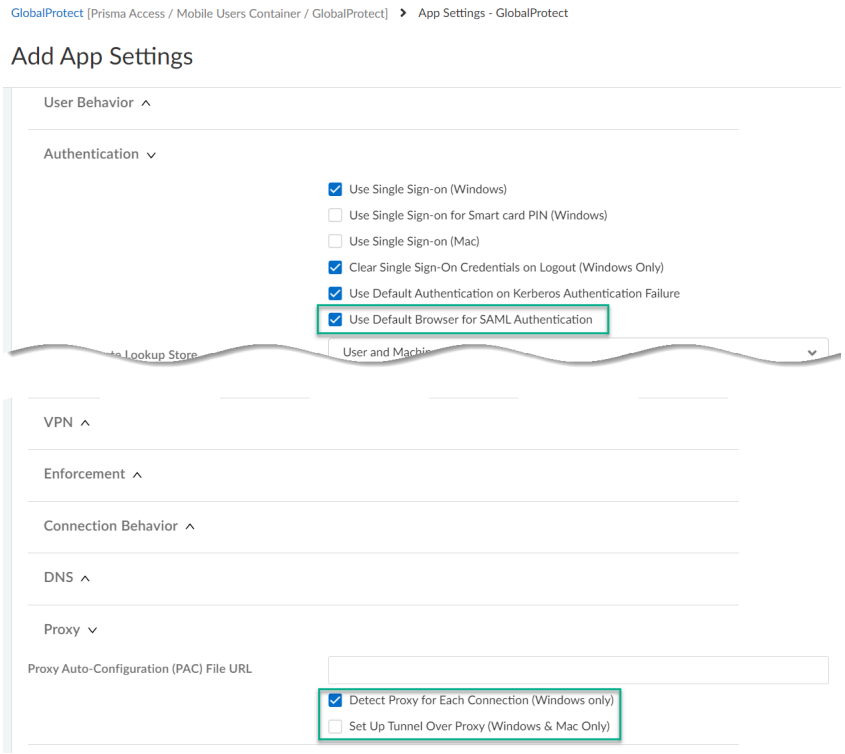
以下步骤将托管在您的数据中心的私有应用程序定向到 GlobalProtect，而对互联网和公共 SAAS 应用程序的请求则被定向到显式代理。

 ©2025 Palo Alto Networks, Inc.

STEP 2 | 编辑 GlobalProtect 门户设置。

转至 **GlobalProtect** > **App Settings**（应用程序设置） > **App Configuration**（应用程序配置） > **Advanced Settings**（高级设置）

1. 在 **Proxy**（代理）设置中：
   - 选中 **Detect Proxy for Each Connection**（检测每个连接的代理）
   - 清除 **Set Up Tunnel Over Proxy (Windows & Mac Only)**（设置代理上的隧道（仅限 **Windows** 和 **Mac**））
2. 在 **Authentication**（身份验证）设置中：
   - 选中 **Use Default Browser for SAML Authentication**（使用默认浏览器进行 **SAML** 身份验证）



STEP 3 | 在 GlobalProtect 中创建一个拆分隧道，以便能够将内部流量定向至 GlobalProtect。

转至 **GlobalProtect** > **Tunnel Settings**（隧道设置） > **Split Tunneling**（拆分隧道）。根据域 (FQDN)、访问路由或应用程序来配置拆分隧道。

©2025 Palo Alto Networks, Inc.

STEP 4 | 配置 PAC 文件以排除为 GlobalProtect 拆分通道指定的域。

要下载 PAC 文件以便编辑，请转到 **Workflows**（工作流程） > **Prisma Access** 设置 > **Explicit Proxy**（显式代理） > **Infrastructure**（基础设施） > **Infrastructure Settings***（基础设施设置） > **Proxy Auto Configuration**（代理自动配置）。

以下示例展示了一个 PAC 文件，其中托管私有应用程序 (internal-app.corp.com) 的 URL 绕过了内部代理。以下 PAC 文件中的参数均为示例值：

- 门户主机名为 `splittunnel.gpcloudservice.com`。
- 移动用户网关包含在爱通配符 FQDN `*examplegateways.gw.gpcloudservice.com` 中。
- PAC 文件 URL 为 `https://pacfileurl.pac`。
- `internal-app.corp.com` 正在托管由“移动用户 —GlobalProtect”保护的私有应用程序。
- Okta 用于 SAML 身份验证。
- The Explicit Proxy URL is `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"; }
```

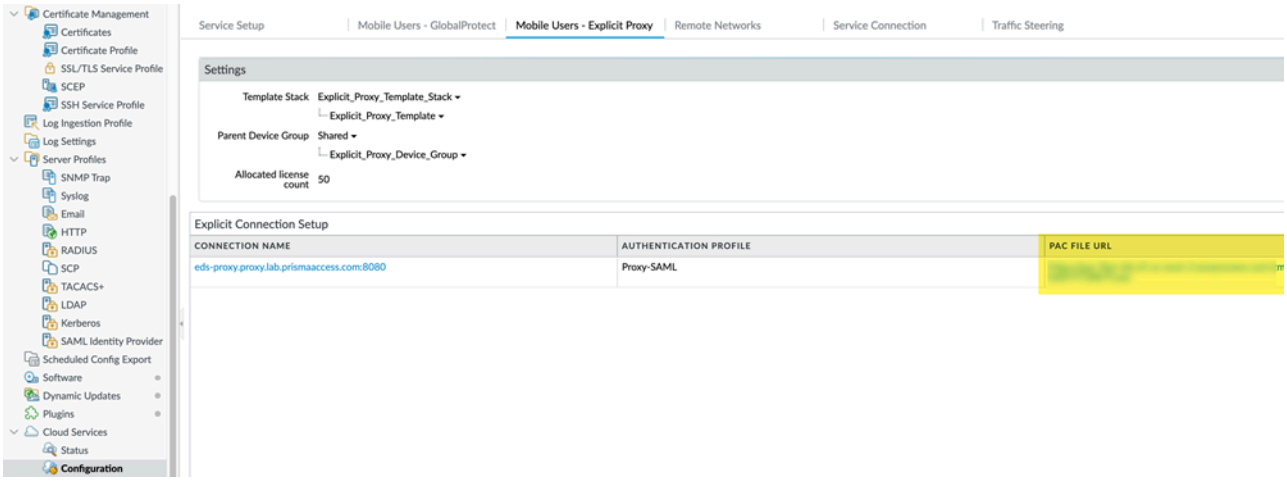
显式代理和 **GlobalProtect**：设置步骤 **(Panorama)**

要使用显式代理实施“GlobalProtect — 移动用户”，请完成以下步骤。

这些配置步骤基于以下关于您网络环境的假设；如果您的网络环境不同，配置方式可能也会不同：

 ©2025 Palo Alto Networks, Inc.

- 移动用户能够访问并解析 GlobalProtect 门户主机名、网关 FQDN、显式代理 URL 和 PAC 文件 URL。
  - 要查找网关 FQDN，请选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息） > **Mobile Users—GlobalProtect**（移动用户 — **GlobalProtect**） > **Gateways**（网关）。
  - 要查找 **PAC** 文件 **URL**，请选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Mobile Users—Explicit Proxy**（移动用户 — 显式代理） > **PAC File URL**（**PAC** 文件 **URL**）。



- 移动用户能够从 GlobalProtect 解析内部域。

STEP 1 | 规划您的 移动用户 — 显式代理部署和 GlobalProtect 部署（您的 移动用户 - GlobalProtect 或独立 GlobalProtect 部署）。

STEP 2 | 决定要将哪些应用程序发送到 GlobalProtect，以及要将哪些应用程序发送到显式代理。

以下步骤将托管在您的数据中心的私有应用程序定向到 GlobalProtect，而对互联网和公共 SAAS 应用程序的请求则被定向到显式代理。

STEP 3 | 在管理 Prisma Access 的 Panorama 中，配置 GlobalProtect 门户设置。

1. 选择 **Network**（网络） > **GlobalProtect** > **Portals**（门户）。

   确保在 **Template**（模板）下拉菜单中的 **Mobile_User_Template** 中。
2. 选择 **GlobalProtect_Portal** 以编辑 Prisma Access 门户配置。
3. 选择 **Agent**（代理）选项卡，然后选择 **DEFAULT**（默认）配置，或者选择 **Add**（添加）以添加一个新配置。
4. 选择 **App**（应用程序）选项卡。
5. 进行以下应用程序配置更改：
   - 在 **Detect Proxy for Each Connection**（检测每个连接的代理）中，选择 **Yes**（是）。
   - 在 **Set Up Tunnel Over Proxy (Windows & Mac Only)**（设置代理上的隧道（仅限 **Windows** 和 **Mac**））中，选择 **No**（否）。
   - 在 **Use Default Browser for SAML Authentication**（使用默认浏览器进行 **SAML** 身份验证）中，选择 **Yes**（是）。

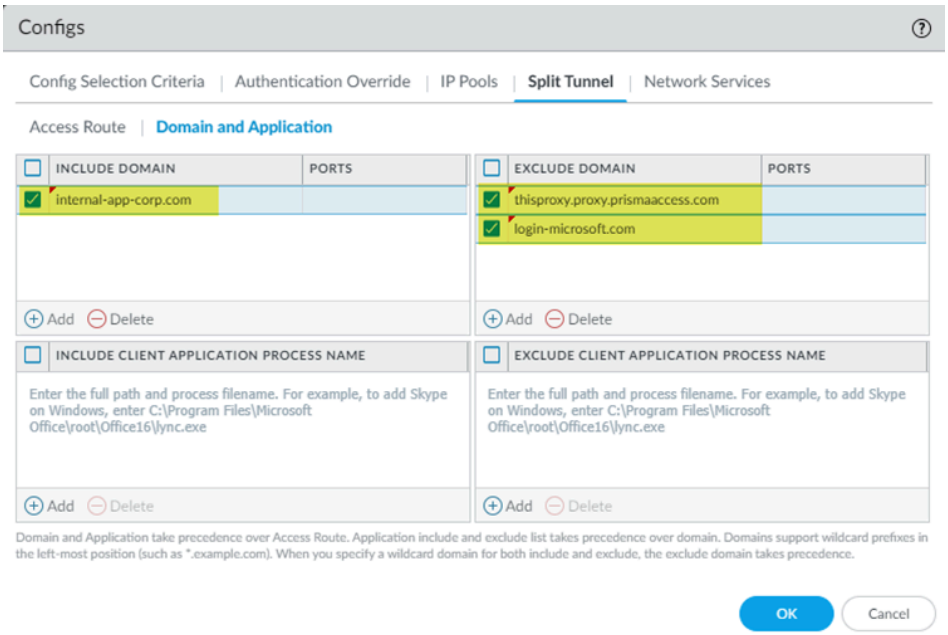
©2025 Palo Alto Networks, Inc.

STEP 4 | 在 GlobalProtect 中创建一个拆分隧道，以便能够将内部流量定向至 GlobalProtect。

以下示例使用拆分隧道来基于域 (FQDN) 定向流量。您还可以根据流量的访问路由来配置拆分隧道。

1. 仍在 GlobalProtect 代理配置中时（**Network**（网络） > **GlobalProtect** > **Gateways**（网关） > **GlobalProtect External Gateway**（**GlobalProtect** 外部网关））时，选择 **Agent**（代理） > **Client Settings**（客户端设置）。
2. 选择 **DEFAULT**（默认）配置，或选择 **Add**（添加）以添加新配置。
3. 选择 **Split Tunnel**（拆分隧道） > **Domain and Application**（域和应用程序）。
4. 依次选择 **Add**（添加）和 **Include Domain**（包含域）以添加包含域，可以选择 **Ports**（端口）以选择要与域搭配使用的端口。

   此示例使用 internal-app.corp.com 作为您在数据中心托管应用程序的 URL。将此 URL 和 SAML 身份验证 URL 添加到 **Exclude Domain**（排除域）中。



5. 单击 **OK**（确定）保存更改。
6. **Commit and Push**（提交并推送）更改。

STEP 5 | 配置 PAC 文件以排除您为拆分隧道输入的域。

以下示例展示了一个 PAC 文件，其中托管私有应用程序 (internal-app.corp.com) 的 URL 绕过了内部代理。以下 PAC 文件中的参数均为示例值：

- 门户主机名为 `splittunnel.gpcloudservice.com`。
- 移动用户网关（**Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息） > **Mobile Users—GlobalProtect**（移

©2025 Palo Alto Networks, Inc.

动用户 — **GlobalProtect**） > **Gateways**（网关））包含在通配符 FQDN `*examplegateways.gw.gpcloudservice.com` 中。

- **PAC** 文件 **URL**（**PAC File URL**）（**Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Mobile Users**—**Explicit Proxy**（移动用户 — 显式代理） > **PAC File URL**（**PAC** 文件 **URL**））为 `https://pacfileurl.pac`。
- `internal-app.corp.com` 正在托管由“移动用户 —GlobalProtect”保护的私有应用程序。
- Okta 用于 SAML 身份验证。
- 显式代理 URL 为 `example.proxy.prismaacess.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"; }
```

显式代理与第三方 VPN

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证

要将第三方 VPN 与显式代理配合使用，必须能够在网络中进行以下更改：

- 必须将第三方 VPN 配置为执行拆分隧道，将互联网流量定向到显式代理。

  如需有关配置第三方 VPN 的任何帮助，请联系您的第三方 VPN 供应商。
- 修改 PAC 文件，让显式代理绕过以下任何 VPN 组件：
  - 与第三方 VPN 关联的任何 IP 地址
  - 第三方 VPN 所需的任何登录 URL

在以下示例中，您配置了 PAC 文件，让显式代理使用私有 IP 地址绕过内部资源以及身份验证流量。

```
++++++++++++++++ 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 */
```

 ©2025 Palo Alto Networks, Inc.

```
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"; }
```

显式代理用户的 IP 地址优化 - 代理部署

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) 如果您想在 Prisma Access 环境中使用此功能，请与客户团队联系以了解更多信息。	• Prisma Access 5.2 • Prisma Access 数据平面 10.2.4 • Panorama 插件版本 5.2.0

IP 地址优化是一套体系结构增强功能，可减少部署中的 IP 地址总数，简化您的允许列表工作流，同时提高弹性并加快 Prisma Access 租户的载入速度。

IP 地址粘性

如果 SaaS 应用程序和网站要求用户会话在整个用户会话中保持相同的 Prisma Access 出口 IP 地址，则可以通过 IP 地址粘性来保护这些 SaaS 应用程序和网站。

简化 **SaaS** 应用程序载入

添加 Prisma Access 地点或在现有 Prisma Access 地点遇到扩展事件时，可能需要向显式代理部署分配新的 IP 地址。最佳实践是检索新的出口和网关 IP 地址，并将它们添加到 SaaS 应用程序的允许列表中。IP 地址优化减少了在大型部署中必须管理的 IP 地址数量。

故障排除

如果您想要针对特定应用程序进行 IP 地址优化，可以将它们添加到 URL 类别或外部动态列表 (EDL)。配置特殊对象后，只有这些对象中包含的域名才会进行 IP 地址优化。

Panorama — 将 URL 类别配置为 **PANW EP IP** 亲和性 **URL** 列表，或将 EDL 配置为 **PANW EP IP** 亲和性列表。避免使用通配符条目（例如 **.***）或顶级域名（例如 **.com**）。

Strata Cloud Manager — 支持 URL 列表 **PANW EP IP** 亲和性 **URL** 列表。

“移动用户 — 显式代理”部署的 DNS 解析

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • 如果您想在 Prisma Access 环境中使用此功能，请与客户团队联系以了解更多信息。	❑ Prisma Access 许可证 ❑ Prisma Access 版本 5.2.0

 ©2025 Palo Alto Networks, Inc.

Prisma Access 允许您指定 DNS 服务器来解析组织内部域和外部域。Prisma Access 根据 DNS 服务器的配置代理 DNS 请求。显式代理支持以下 DNS 功能：

- 使用第三方浏览器与显式代理配合使用
- 将按区域划分的 DNS 服务器与 Prisma Access Browser 配合使用

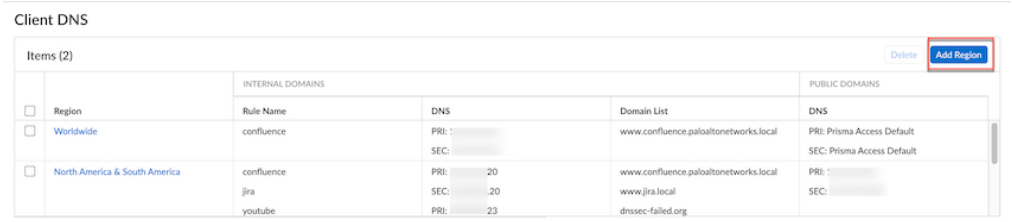
- 显式代理配置的 *DNS* 代理优先于在 ***Prisma Access Setup***（***Prisma Access*** 设置）下面定义的内部 *DNS* 服务器设置。
- 为显式代理启用 *DNS* 代理后，必须将现有 *DNS* 配置从 ***Prisma Access Setup***（***Prisma Access*** 设置）> ***Internal DNS Servers***（内部 ***DNS*** 服务器）迁移到 ***Workflows***（工作流）> ***Prisma Access Setup***（***Prisma Access*** 设置）> ***Explicit Proxy***（显式代理）> ***Infrastructure Settings***（基础设施设置）> ***DNS Proxy***（***DNS*** 代理）

配置 **DNS** 安全

要配置 DNS 代理设置，请完成以下步骤：

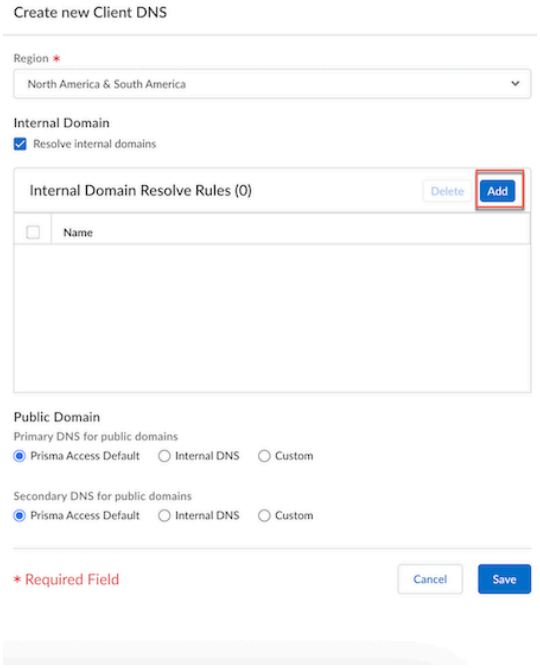
1. 添加显式代理 DNS 服务器规则。
    1. 转到 **Workflows**（工作流）> **Prisma Access Setup**（**Prisma Access** 设置）> **Explicit Proxy**（显式代理）> **Infrastructure Settings**（基础设施设置）。
    2. 单击设置图标，然后转到 **Client DNS**（客户端 **DNS**）。
    3. 单击 **Add Region**（添加区域）以添加一个区域，并为其指定一个唯一名称。
    4. 选择一个区域或位置，或者选择 **Worldwide**（全球）。

        如果指定多个代理服务器设置，其中混合了“*Worldwide*（全球）”设置和大区设置，则 *Prisma Access* 将依次使用位置组、大区和全球的设置。*Prisma Access* 按照列表中从上到下评估规则。
    5. 添加 DNS 服务器的 IP 地址。



 ©2025 Palo Alto Networks, Inc.

2. 选择是否需要 Prisma Access 来解析内部域；如果需要，请依次选择 **Add**（添加）、**Internal Domain Resolve Rules**（内部域解析规则）来添加一个或多个内部域解析规则。



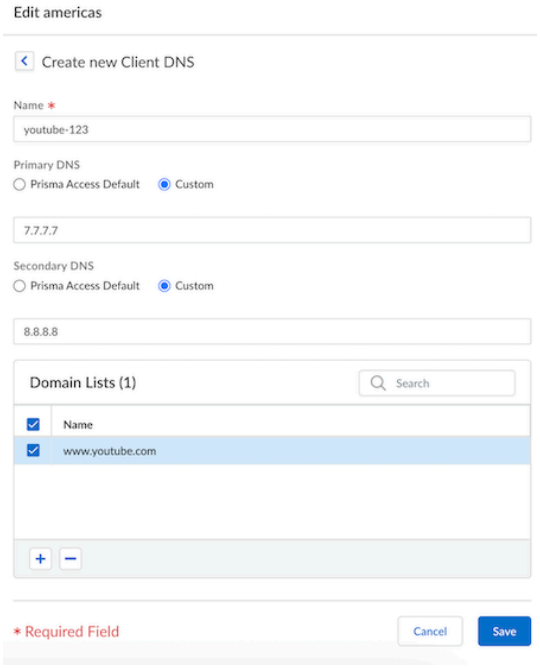
3. 依次选择 **Add**（添加）和 **Internal Domain Resolve Rules**（内部域解析规则）以添加和定义内部域规则。

   目前，仅 *Prisma Access Browser* 和客户端代理支持内部域解析规则。

4. 选择 **Name**（名称）以为规则添加唯一名称，然后在 **Primary DNS**（主 **DNS**）和 **Secondary DNS**（辅助 **DNS**）添加自定义 IP 地址。
5. 选择 **Prisma Access Default**（**Prisma Access** 默认值）可使用默认的 Prisma Access DNS 服务器来解析内部域。如果您希望内部 DNS 服务器仅解析您指定的域，请单击 + 并在 **Domain Lists**（域列表）中输入要解析的域。

©2025 Palo Alto Networks, Inc.

6. 如果您有可以访问内部域的自定义 DNS 服务器，请指定 **Primary DNS**（主 **DNS**）和 **Secondary DNS**（辅助 **DNS**）服务器的 IP 地址。



7. 如果您希望内部 DNS 服务器仅解析您指定的域，请单击 **+** 并在 **Domain Lists**（域列表）中输入要解析的域。在域前面指定一个星号；例如 *.acme.com。单击 **Save**（保存）
8. 单击 **Push Config**（推送配置）以保存并推送配置更改。

©2025 Palo Alto Networks, Inc.

查看用户到IP地址或用户组的映射

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Panorama Managed Prisma Access	• Prisma Access 许可证

Prisma Access Insights可让您实时查看移动用户的用户到IP地址或用户到组映射。对于远程网络和服务连接，您可以查看用户到用户组的映射。

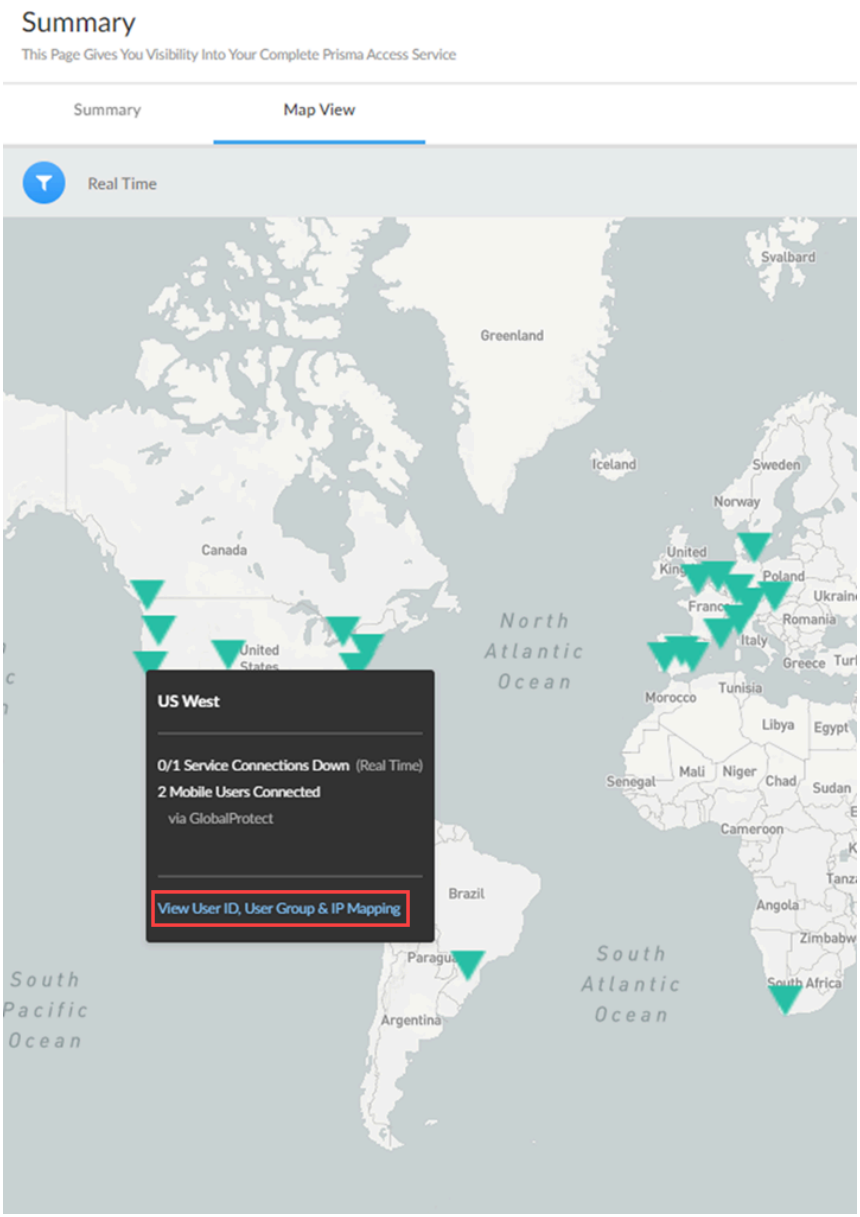
地图上的倒三角用颜色编码以指示 Prisma Access 位置状态：

- 绿色：所有实例都已启动。
- 红色：所有实例都已关闭。
- 黄色：“不确定性”是“向上”、“向下”和“未知”的组合，可能需要您的注意。
- 灰色：所有情况都是未知的。

STEP 1 | 从“摘要”操控板中，选择“地图视图”。

©2025 Palo Alto Networks, Inc.

STEP 2 | 将鼠标光标悬停在某个位置上，直到出现一个弹出对话框。



STEP 3 | 从对话框中选择查看用户ID、用户组和IP映射。**UserID and User Group Distribution Check**（**User-ID** 和用户组分布检查）对话框随即打开。

©2025 Palo Alto Networks, Inc.

STEP 4 | 选择 **Prisma Access** 位置和 **Node Type**（节点类型）。的呢过 **Node Type**（节点类型）为 **Mobile Users (GlobalProtect)**（移动用户 **(GlobalProtect)**）时，不考虑 **Prisma Access** 位置筛选器。

对于远程网络和服务连接，您只能看到用户ID到用户组的映射。

1. 选择 **Prisma Access Location**（**Prisma Access** 地点）。如果您选择的 Prisma Access 位置没有任何关联的远程网络或服务连接，您会在远程网络站点字段或服务连接站点字段中看到“无可用数据”消息（视情况而定），并且显示用户组和导出到CSV按钮被禁用。
2. 从节点类型中，选择远程网络或服务连接。
3. 从远程网络站点或服务连接站点字段中，选择要从中检索数据的站点。
4. 在视图中，选择是否要查看用户ID属于哪些用户组（用户）或哪些用户属于与站点关联的特定组（组）。
   - 如果选择用户，请输入用户的用户ID（例如saas\testuser3）以获取用户ID到用户组的映射，然后选择显示用户组。用户ID所属的所有组的列表显示在“用户ID-IP映射”下。

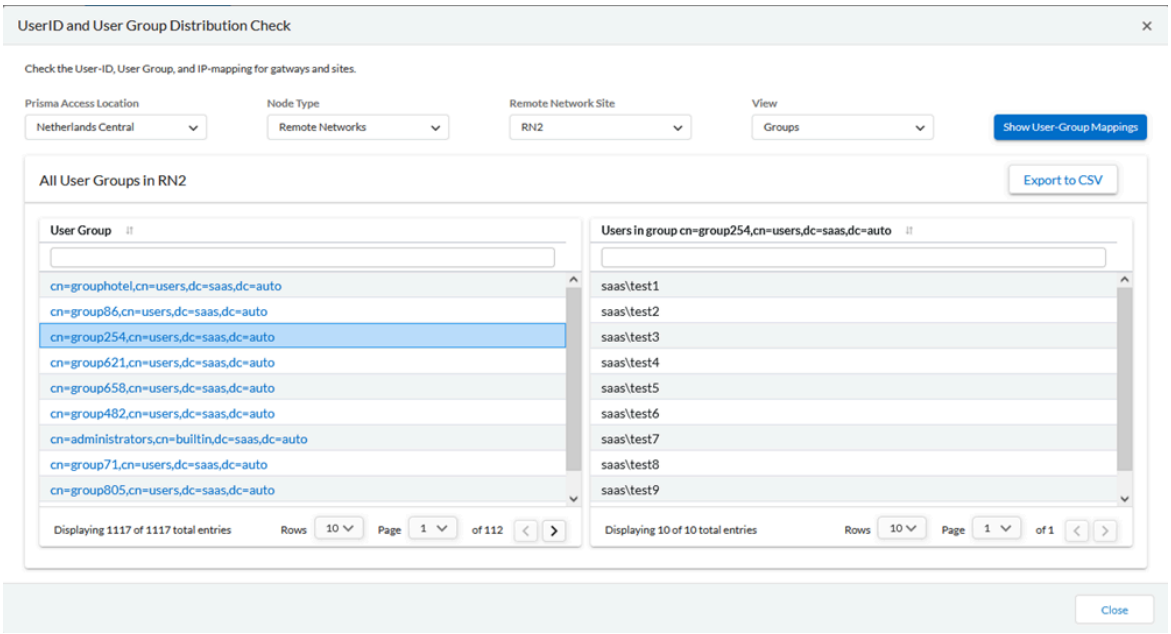
     您可以通过在“用户组”（User Group）文本框中输入组名或包含在要查找的组名中的字符串来搜索特定组。如果您搜索不存在的组，则会看到一条错误消息，提示“无可用数据”。您还可以通过切换"用户组“旁边的箭头图标对组列表进行排序。您可以选择要显示的条目数，也可以通过单击前进和后退箭头来滚动页面。

     如果选择“组”，则选择"显示用户-组映射将在 ***<selected_site>*** 中的所有用户组“下显示站点中可用的所有组。如果选择一个组，则属于该组的所有用户都将显示在右窗格中。导出到CSV按钮被激活，您可以将属于该组的所有用户导出到CSV文件中。导出的CSV文件包含组的所有条目，即使它们在导出时未显示在UI中。

     您可以通过在“用户组”（User Group）文本框中输入组名或包含在要查找的组名中的字符串来搜索特定组。如果您搜索不存在的组，则会看到一条错误消息，提示“无可用数

 ©2025 Palo Alto Networks, Inc.

据”。您还可以通过切换"用户组“旁边的箭头图标对组列表进行排序。您可以选择要显示的条目数，也可以通过选择前进和后退箭头来滚动页面。



Node Type（节点类型）：**Mobile Users (GlobalProtect)**（移动用户 **(GlobalProtect)**）

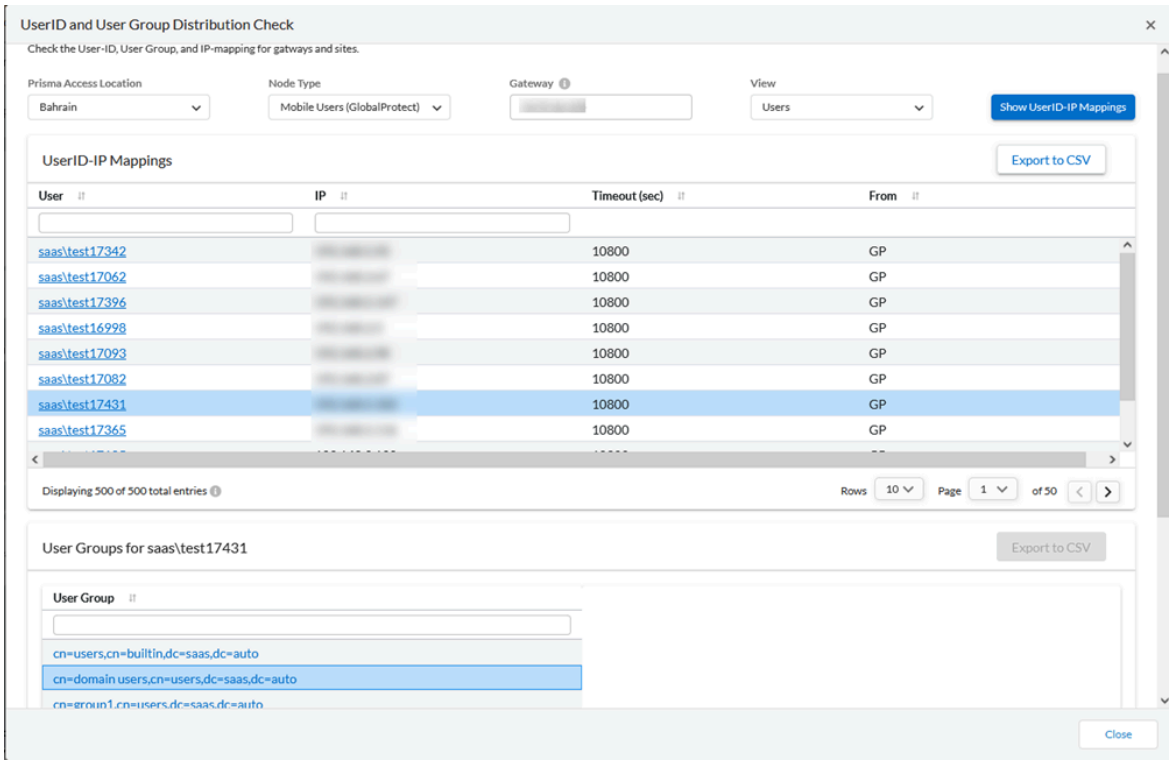
您可以看到用户ID到IP的映射以及用户ID到用户组的映射。当选定的节点类型为移动用户（GlobalProtect）时，不会考虑Prisma访问位置过滤器。相反，Prisma Access Insights 使用 GlobalProtect 网关 IP 地址来查找数据。

1. 在网关文本框中输入GlobalProtect IP网关地址。
2. 选择是否要查看连接到指定GlobalProtect网关的用户的用户ID到用户IP映射（Users）或用户ID到用户组映射（Groups）的数据。

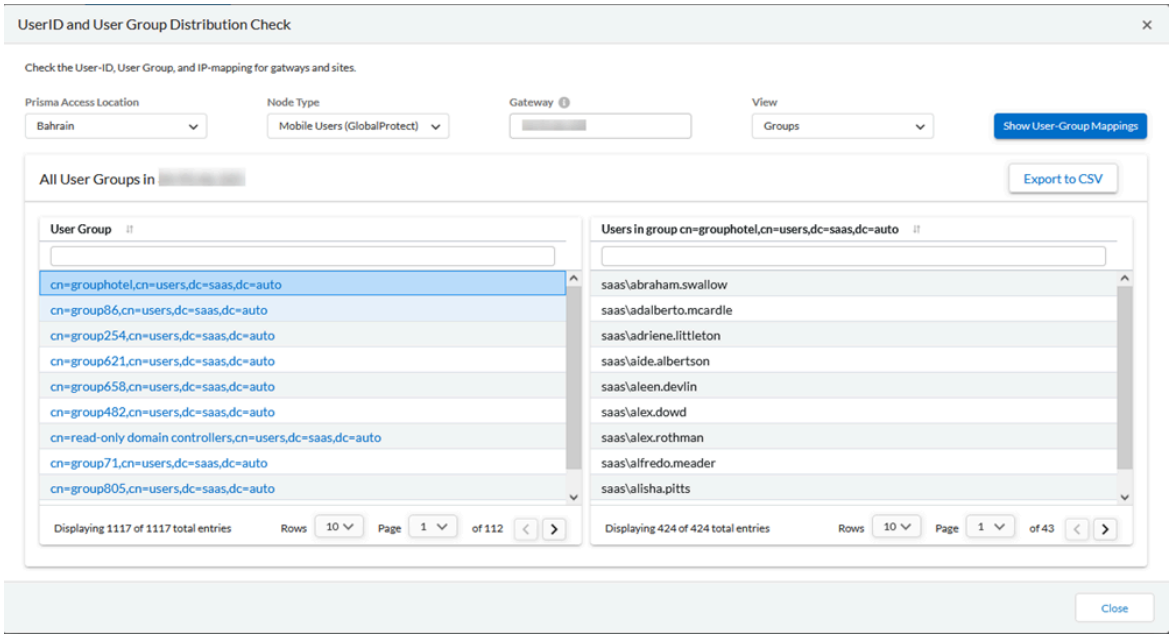
   如果选择了用户，请选择显示用户ID-IP映射。将显示一个用户ID到其用户IP映射的表，该表将显示用户ID到用户IP条目的有效期（以秒为单位）。选择特定用户将显示该用户所属的

©2025 Palo Alto Networks, Inc.

组。选择一个组会显示属于该组的每个用户。它还启用了Export to CSV按钮，该按钮允许您导出该组中的所有用户，而不管UI中显示的任何筛选视图。



如果选择了“组”，请选择“显示用户-组映射”。属于该GlobalProtect网关的所有用户组的列表将显示在“用户组”下。选择用户组将在右窗格中显示属于该组的所有用户。它还启用了Export to CSV按钮，该按钮允许您导出该组中的所有用户，而不管UI中显示的任何筛选视图。



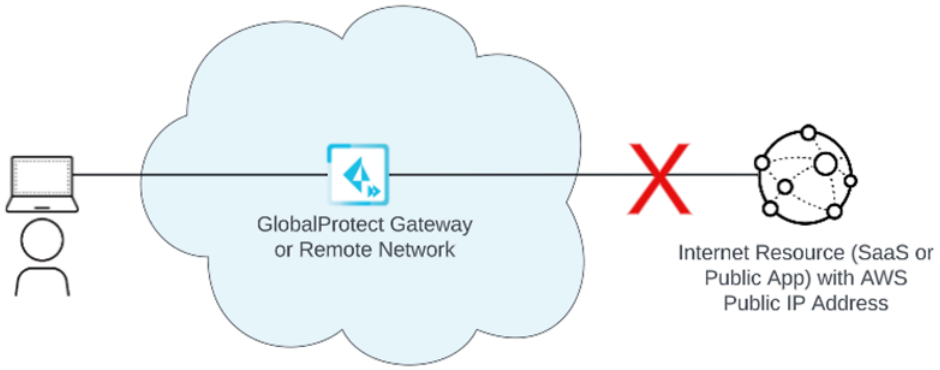
©2025 Palo Alto Networks, Inc.

报告移动用户站点访问问题

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证

一些网站（例如 stubhub.com、ticketmaster.com 或 dollartree.com）会阻止来自 AWS 云 IP 地址范围的流量。当通过 Prisma Access 保护的用户尝试访问这些网站时，可能会被拒绝访问，并在网络浏览器上显示以下消息：

```
访问被拒绝。您无权访问此服务器上的“http://www.dollartree.com/”。参考编号
 #18.7f955b8.1509600370.44eb7c8
```



要报告此问题，请在 Web 浏览器中输入 https://reportasite.gpcloudservice.com/ 并提供无法访问的网站的 URL。24-48 小时后，返回 https://reportasite.gpcloudservice.com/ 并输入相同的 URL 以查看其状态。

Palo Alto Networks 为您提供 URL 使用的 IP 地址；在某些情况下，您必须将此 IP 地址添加到组织的允许列表中，以免此流量被黑洞化。如果您有被重定向的 URL，请将这些 IP 地址添加到您的允许列表中：

- 65.154.226.160
- 154.59.126.110
- 66.232.36.110

Prisma Access URL 重定向过程

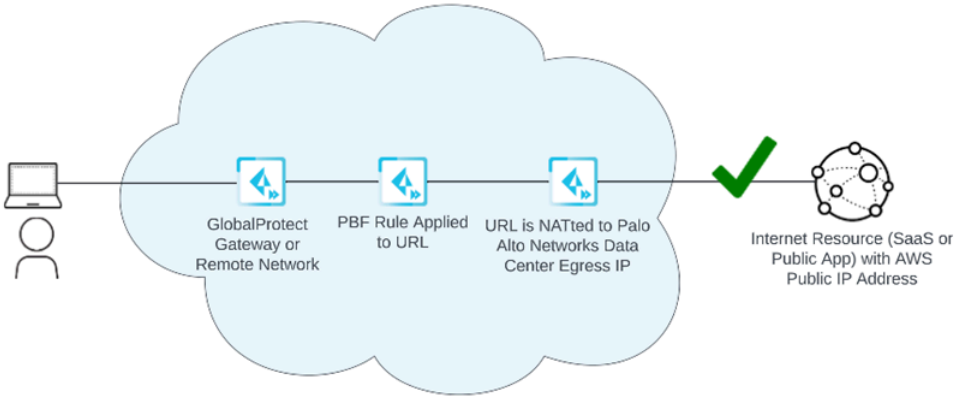
一些网站会阻止来自云 IP 地址范围的流量。当通过 Prisma Access 保护的用户尝试访问这些网站，可能会被拒绝访问。为了确保恢复对这些网站的访问，Palo Alto Networks 会审查所有此类报告的网站，如果发现访问问题，则对网站进行分类，并添加将 IP 地址 NAT 为可访问的 IP 地址的

©2025 Palo Alto Networks, Inc.

传出策略。Palo Alto Networks 会彻底审查这些网站，以确定它们的信誉，并且只有信誉良好的网站才会被添加到传出规则中，而其他网站则会被拒绝，使用以下流程：

1. 您使用 https://reportasite.gpcloudservice.com/ 通知我们存在访问问题的 URL。
2. 站点可靠性工程 (SRE) 自动化审查 URL。
3. 如果 SRE 确定该 URL 是安全的，则会将基于策略的转发 (PBF) 规则应用于该 URL 及其父域。
4. 流量通过 Prisma Access 从 GlobalProtect 网关或远程网络路由到 URL 处理中心，其中 PBF 规则应用于域，然后从中心到 Palo Alto Networks 数据中心。
5. 当流量从数据中心流出时，URL 会被源 NAT 为数据中心的 IP 地址。

由于这些操作，往返于 SaaS 应用程序的流量不会被丢弃，因为数据中心 IP 地址的信誉良好。



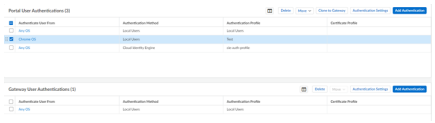
 ©2025 Palo Alto Networks, Inc.

允许移动用户向 Prisma Access 进行身份验证

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证

可以使用任何支持的身份验证类型向连接到 Prisma Access 的移动用户进行身份验证。按照以下步骤为 GlobalProtect 或显式代理移动用户设置身份验证。

STEP 1 | 转至 **Workflows**（工作流） > **Prisma Access** 设置，然后转至您的 移动用户：GlobalProtect，或者显式代理配置，然后选择 **Set Up User Authentication**（设置用户身份验证）。



STEP 2 | 从支持的身份验证类型中选择 **Authentication Method**（身份验证方法）。

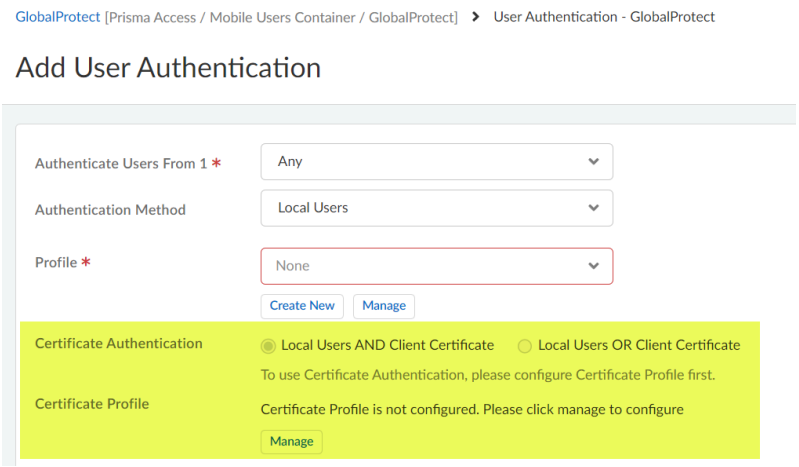
如果您尚未将 Prisma Access 与您的身份验证服务集成，这里介绍了操作方法。

STEP 3 | 选择您配置的身份验证配置文件，以使 Prisma Access 能够连接到要用于对用户进行身份验证的服务。

- 如果在步骤 2 中使用了 SAML，请指定 SAML 身份验证配置文件，或者创建新的 SAML 身份验证配置文件以与 Prisma Access 一起使用。
- 如果在步骤 2 中使用了 CIE，请指定 CIE 身份验证配置文件，或者创建新的 CIE 身份验证配置文件以与 Prisma Access 一起使用。
- 如果在步骤 2 中使用了 Kerberos，请指定 Kerberos 身份验证配置文件，或者创建新的 Kerberos 身份验证配置文件以与 Prisma Access 一起使用。

©2025 Palo Alto Networks, Inc.

STEP 4 | 指定证书身份验证设置：



- 证书身份验证

  为增强安全性，请使用证书（除身份验证服务外）获取用户名并向 Prisma Access 验证用户身份。要基于客户端证书对用户进行身份验证，其中一个证书字段（如“Subject Name（主题名称）”字段）必须标识用户名。通过客户端证书身份验证成功进行身份验证的移动用户无法选择注销 GlobalProtect 应用程序。

  使用 Prisma Access，您可以选择要求移动用户同时通过证书身份验证和基于身份验证类型的身份验证，也可以只要移动用户成功通过其中一项检查，就向其授予访问权限。

- 证书配置文件

  使用可选的证书配置文件验证移动用户通过连接请求向 Prisma Access 提交的证书。证书配置文件指定用户名和用户域字段内容；列明 CA 证书和阻止会话的标准；并提供确定 CA 证书吊销状态的方法。由于证书是移动用户认证的一部分，因此必须在用户首次登录之前，将证书配置文件中使用的证书预先部署给移动用户。证书配置文件会指定哪个证书字段包含用户名（“Subject（主题）”字段或“Subject Alt（备用主题）”字段）。如果证书配置文件指定了“用户名字段”中的“主题”，则端点提供的证书必须包含公用名方可进行连接。如果证书配置文件将“带电子邮件或主体名称的主题备用名称”指定为“用户名字段”，则证书必须包含相应字段，以便在 GlobalProtect 应用程序验证至 Prisma Access 时用作用户名。

STEP 5 | 为存储用户身份验证凭据的 Cookie 指定 **Cookie Lifetime**（**Cookie** 生命周期）。

IdP 对用户进行身份验证后，Prisma Access 会将用户的身份验证状态存储在身份验证缓存服务 (ACS) 中。身份验证的有效期取决于您在此处为 **Cookie Lifetime**（**Cookie** 生命周期）指定的值。

为避免出现用户在 Cookie 有效期到期前无法下载大文件，或者用户长时间访问单个网站时 Cookie 过期的问题，Palo Alto Networks 建议将 Cookie 有效期至少配置为一天。如果显式代理用户遇到 Cookie 生命周期过期问题，他们可以浏览到其他网站以重新向 ACS 进行身份验证并刷新 ACS Cookie。

身份验证支持和功能

以下是 Prisma Access 集成以提供身份验证的服务，以及在规划身份验证设置时需要考虑的功能：

身份验证支持：

 ©2025 Palo Alto Networks, Inc.

- 云身份引擎
- SAML
- TACACS+
- RADUIS
- LDAP
- Kerberos
- MFA
- 本地数据库身份验证

身份验证功能的优势：

- SSO
- 身份验证门户
- 身份验证序列

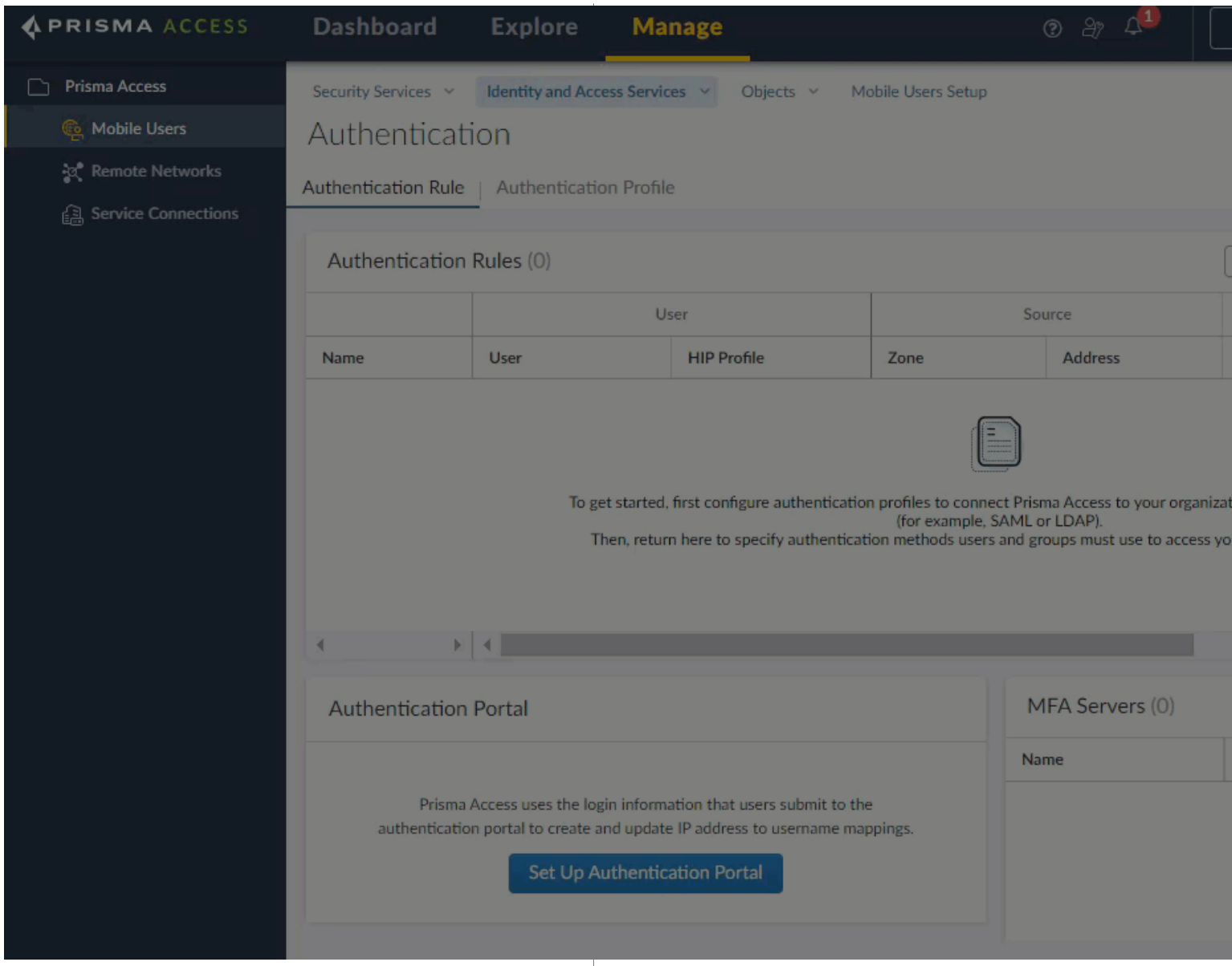
身份验证支持

云身份引擎	您可以通过配置基于 SAML 2.0 的身份提供程序 (IdP)、客户端证书和证书颁发机构 (CA) 链或两者来部署 Cloud Identity Engine，以便进行用户身份验证。指定如何对用户进行身份验证后，设置身份验证配置文件以定义身份验证安全策略，并可选择在防火墙或 Panorama 上配置身份验证策略。
SAML	如果您的用户访问网络外部的服务和应用程序，则可以使用 SAML 将 Prisma Access 与控制外部和内部服务及应用程序访问的身份提供程序 (IdP) 集成。SAML 单点登录 (SSO) 支持一次登录访问多个应用程序，当每个用户需要访问多个应用程序，并且要为每个应用程序进行身份验证时，用户的工作效率会受到影响，在这样的环境中，单点登录非常有用。在这种情况下，SAML 单点登录 (SSO) 允许一次登录访问多个应用程序。同样，SAML 单点退出 (SLO) 使用户能够通过退出一个会话来结束多个应用程序的会话。SSO 适用于通过 GlobalProtect 应用程序访问应用程序的移动用户或通过身份验证门户访问应用程序的远程网络用户。GlobalProtect 应用程序用户可以使用 SLO。 您不能在身份验证序列中使用 *SAML* 身份验证配置文件。

 ©2025 Palo Alto Networks, Inc.

TACACS+	增强型终端访问控制器访问控制系统 (TACACS+) 是一组通过集中式服务器进行身份验证和授权的协议。TACACS+ 加密用户名和密码，比仅加密密码的 RADIUS 更安全。因使用 TCP，TACACS+ 也更可靠，而 RADIUS 则使用 UDP。
RADIUS	远程身份验证拨入用户服务 (RADIUS) 是一种广受支持的网络协议，提供集中式身份验证和授权。您还可以向 Prisma Access 添加 RADIUS 服务器来实现多重因素身份验证。
LDAP	轻型目录访问协议 (LDAP) 是用于访问信息目录的标准协议。您可以使用 LDAP 对通过身份验证门户访问应用程序或服务的用户进行身份验证。
Kerberos	Kerberos 是一种身份验证协议，它使用唯一密钥（称为票证）来识别各方，从而实现各方之间的安全信息交换。使用 Kerberos，您可以通过身份验证门户对访问应用程序的用户进行身份验证。启用 Kerberos SSO 后，仅初次访问网络需要用户登录（例如登录到 Microsoft Windows）。首次登录后，用户可以访问网络中任何基于浏览器的服务，而无需在 SSO 会话到期之前再次登录。 要使用 Kerberos，首先需要一个用于对用户进行身份验证的 Prisma Access 的 Kerberos 帐户。该帐户需要创建 Kerberos Keytab，即包含防火墙或 Panorama 的主体名及哈希密码的文件。SSO 进程需要 keytab。 Kerberos SSO 仅适用于 Kerberos 环境内部的服务和应用程序。要使 SSO 用于外部服务和应用程序，请使用 SAML。
MFA	多因素身份验证 (MFA) 提供了一种实施不同类型的多种身份验证质询（称为因素）的方法，以保护您最敏感的服务和应用程序。例如，您可能需要对关键财务文档而不是搜索引擎进行严格的身份验证。 Prisma Access 具有内置的受支持的 MFA 供应商列表，该列表会随着新供应商的添加而自动更新：

©2025 Palo Alto Networks, Inc.



本地数据库身份验证	创建一个在 Prisma Access 上本地运行且包含用户帐户（用户名和密码或散列密码）及用户组的数据库。在您只知道哈希密码（而不是明文密码）的情况下，此类身份验证对于创建重用现有 Unix 帐户凭据的用户帐户非常有用。对于使用明文密码的帐户，您也可以定义密码复杂度和过期设置。此身份验证方法适用于通过身份验证门户或 GlobalProtect 应用程序访问服务和应用程序的用户。

©2025 Palo Alto Networks, Inc.

身份验证功能优势

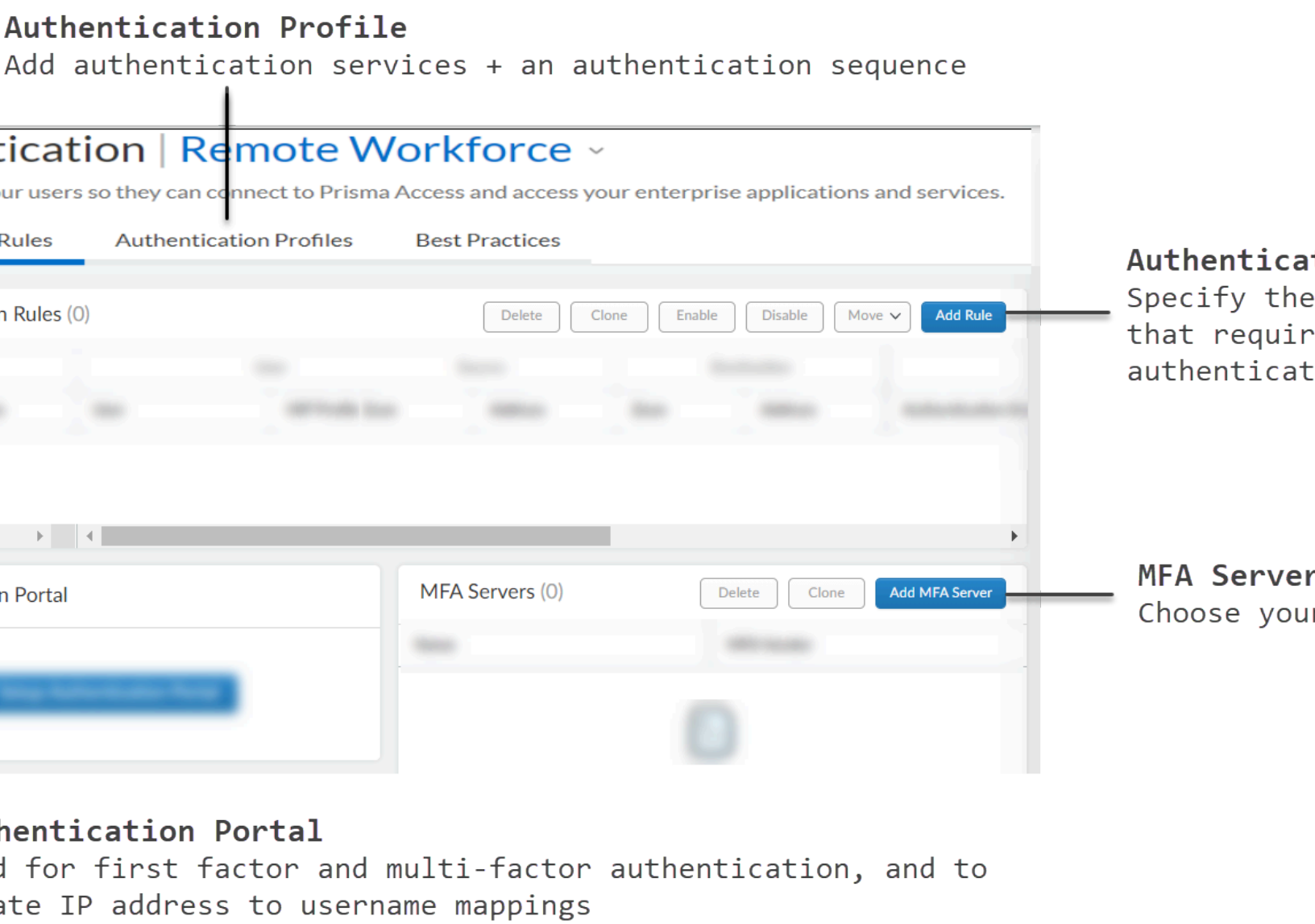
SSO	如果您使用 SAML 或 Kerberos，则可以实现单点登录 (SSO)，这使得用户只需进行一次身份验证即可访问多个服务和应用程序。SAML 和 Kerberos 支持 SSO。
身份验证门户	将符合身份验证规则的 Web 请求重定向到 Prisma Access 登录页面，并提示用户进行身份验证。Prisma Access 使用用户提交到此身份验证门户的信息来创建或更新 IP 地址到用户名的映射。 这对于远程网络特别有用，这样您就可以继续根据用户（或组）监控和强制执行流量。当用户发起符合身份验证规则的 Web 流量（HTTP 或 HTTPS）时，Prisma Access 会提示用户通过身份验证门户进行身份验证 Prisma Access 根据用户提交给门户的信息来创建或更新 IP 地址到用户名的映射。这可以确保您确切地知道远程网络站点上谁正在访问您最敏感的应用程序和数据。
身份验证序列	如果您出于不同的目的使用多种类型的身份验证，则可以设置身份验证序列来对您的配置文件进行排名。Prisma Access 根据您的排名检查每个配置文件，直到其中一个配置文件成功验证了用户的身份。

设置身份验证

要使用 Prisma Access 设置身份验证，请先将身份验证服务添加到 Prisma Access。然后指定需要身份验证的流量。基于这些设置添加更多身份验证功能，如 MFA、身份验证序列，或启用 Prisma Access 以创建和更新 IP 地址到用户名映射。

下面介绍如何开始 — 为 Prisma Access 启用身份验证所需的所有设置都在一个位置：管理 > 配置 > **NGFW** 和**Prisma Access** > 身份服务 > 身份验证。选择 **Prisma Access** 配置范围。

©2025 Palo Alto Networks, Inc.



身份验证规则 此处指定需要进行身份验证的流量

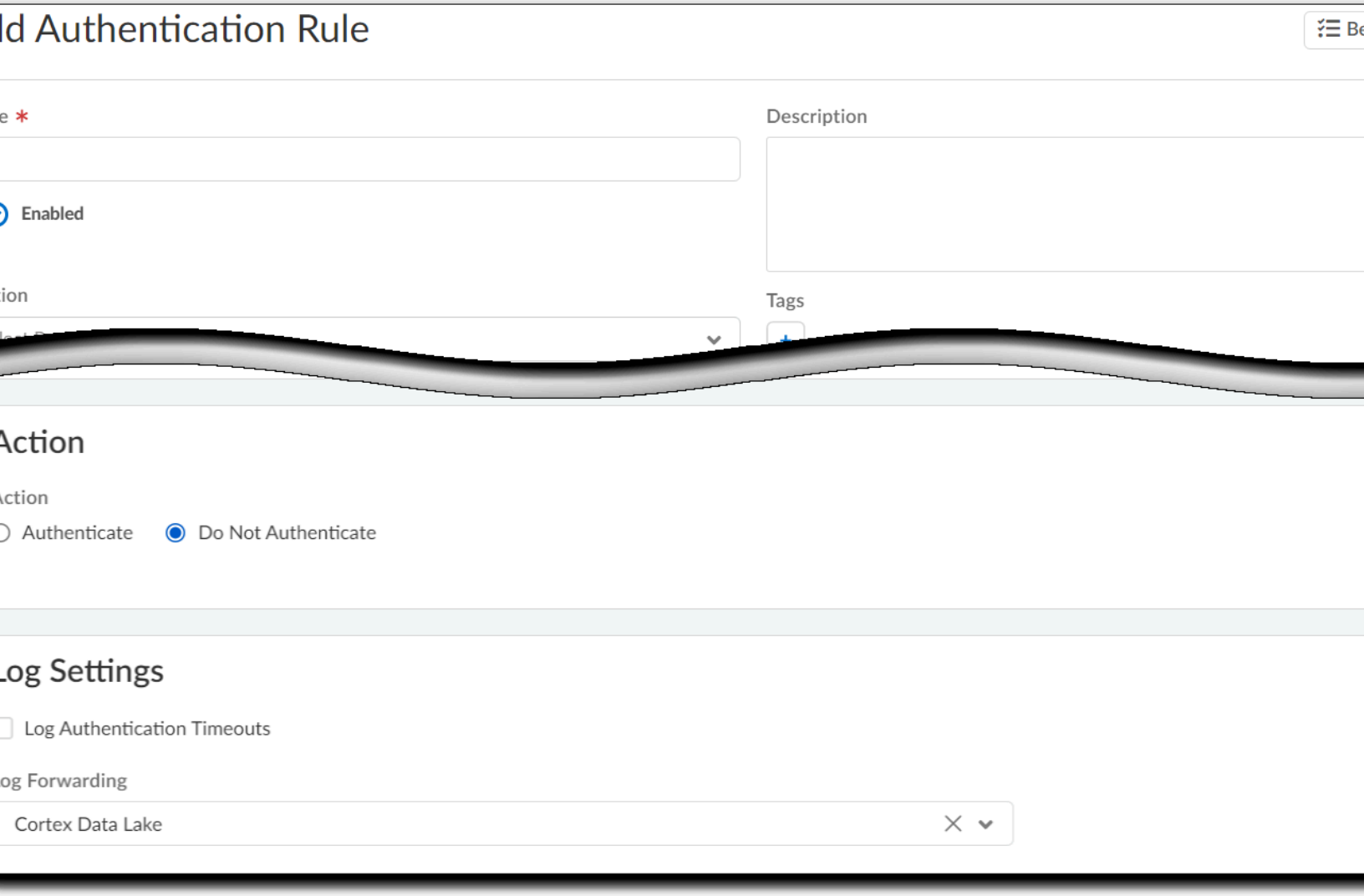
设置身份验证规则的一部分包括向规则中添加身份验证配置文件。当 Prisma Access 检测到与身份验证规则匹配的流量时，会将身份验证配置文件中定义的身份验证方法和设置应用到匹配的流量。配置文件是定义如何要求用户进行身份验证的内容。

1. 转到 **Manage**（管理） > **Configuration**（配置） > **NGFW** 和 **Prisma Access** > **Identity Services**（身份服务） > **Authentication**（身份验证） > **Authentication Rule**（身份验证

 ©2025 Palo Alto Networks, Inc.

规则），然后 **Add Authentication Rule**（添加身份验证规则）。选择 **Prisma Access** 配置范围。

2. 定义需要身份验证的用户、服务和 URL 类别。
3. 将规则操作设置为 **Authenticate**（身份验证），然后选择定义身份验证方法的 **Profile**（配置文件），该身份验证方法将用于与此规则匹配的通信。



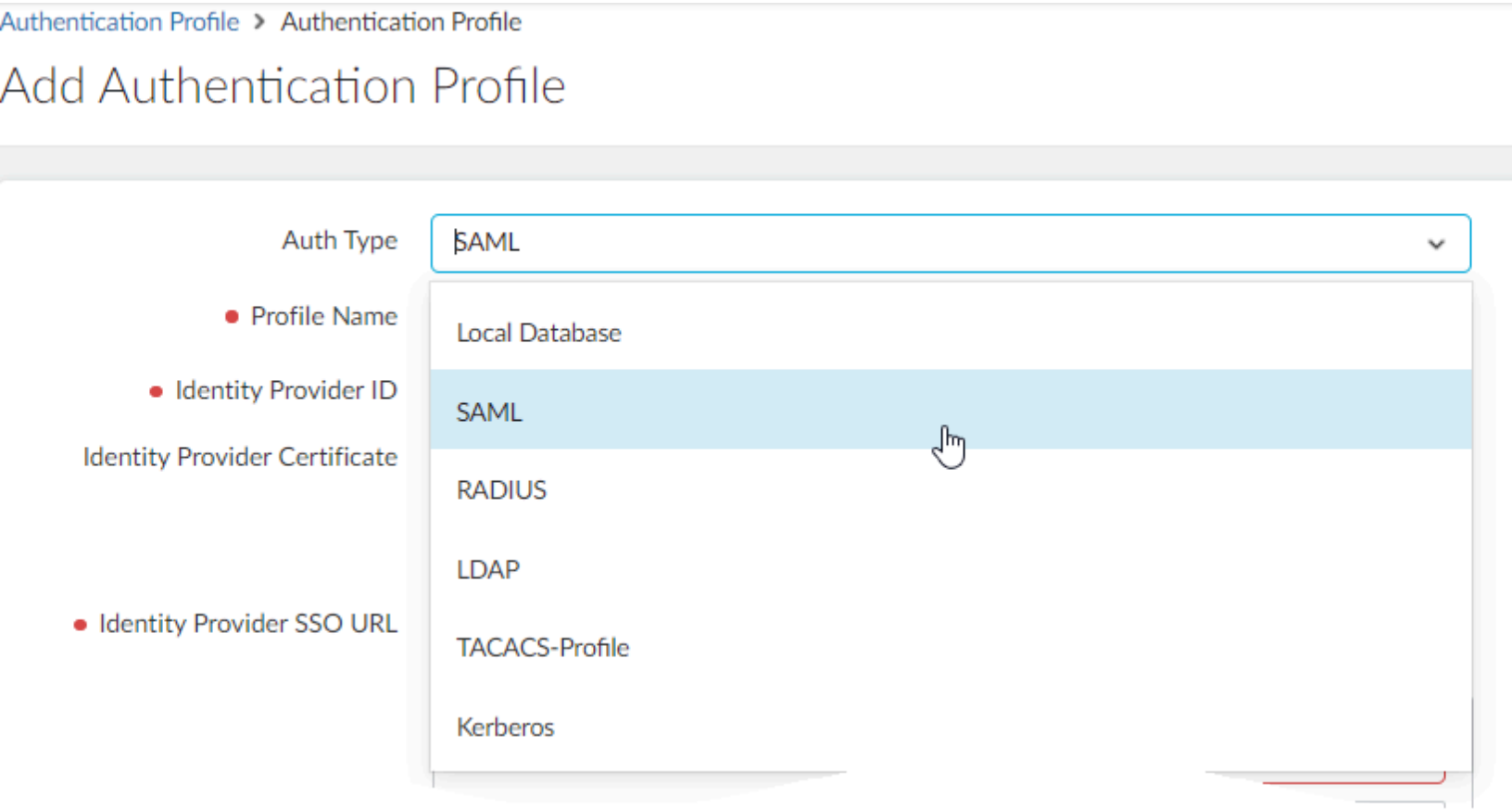
 ©2025 Palo Alto Networks, Inc.

身份验证配置文件 在此处添加您的身份验证服务，并定义身份验证设置

将 Prisma Access 连接到您要用于对用户进行身份验证的服务 — SAML、TACACS +、RADIUS、LDAP 或 Kerberos — 并定义身份验证设置（例如，为失败的登录尝试设置限制）。

如果您使用的是本地身份验证服务，则必须先创建服务连接，以便将本地身份验证服务连接到 *Prisma Access*。然后，返回此处设置您的身份验证配置文件。

转到 **Manage**（管理） > **Configuration**（配置） > **NGFW** 和 **Prisma Access** > **Identity Services**（身份服务） > **Authentication**（身份验证） > **Authentication Profile**（身份验证配置文件） > **Add Profile**（添加配置文件），然后从设置配置文件 **Auth Type**（身份验证类型）开始。选择 **Prisma Access** 配置范围。

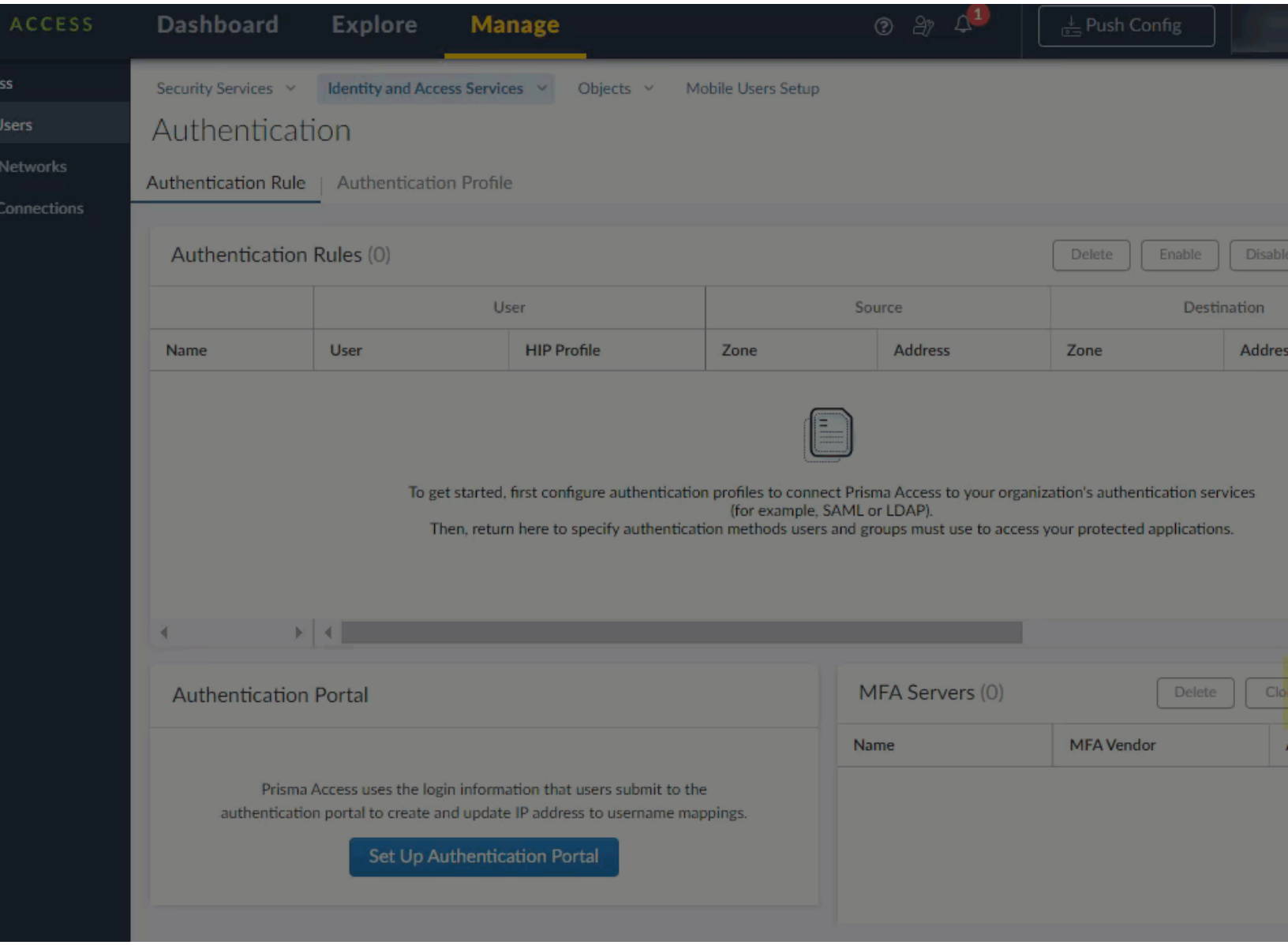


系统会提示您添加有关您选择的身份验证服务的详细信息，以便将 Prisma Access 连接到该服务，并读取用户凭据和角色权限。配置文件中提供了用于自定义身份验证的其他设置，这些设置可能因您设置的身份验证类型而异。

 ©2025 Palo Alto Networks, Inc.

MFA 服务器 指定您使用的 MFA 供应商

要使用多种方法对敏感应用程序的用户进行身份验证，请首先添加要使用的 MFA 供应商（**Add MFA Server**（添加 **MFA** 服务器））。Prisma Access 会提供一个 MFA 供应商列表来供您选择。



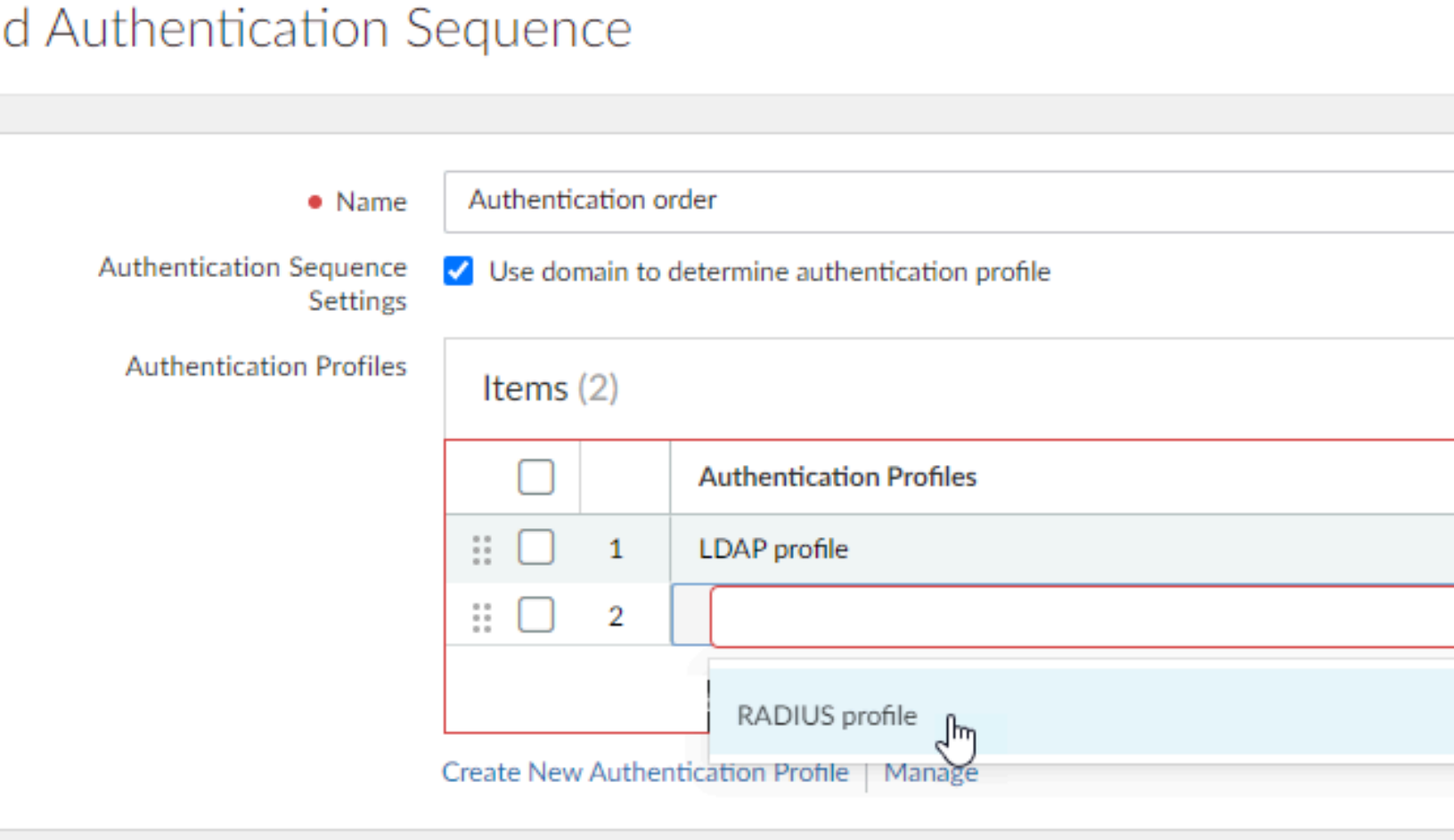
身份验证门户为远程网络站点上的用户设置身份验证门户（也称为强制网络门户），并让 Prisma Access 可以创建 IP 地址到用户名的映射

对于第一因素身份验证（登录和密码），远程网络站点的用户必须通过身份验证门户进行身份验证。如果身份验证成功，Prisma Access 会为每个所需的附加身份验证因素显示一个 MFA 登录页面。Prisma Access 使用用户提交的凭据创建和更新 IP 地址到用户名的映射。这意味着，您将始终知道远程网络站点上谁在访问 Web 内容和企业应用程序。

©2025 Palo Alto Networks, Inc.

身份验证序列按照您希望 Prisma Access 尝试的顺序对身份验证配置文件进行排名

选择 **Manage**（管理） > **Configuration**（配置） > **NGFW** 和 **Prisma Access** > **Identity Services**（身份服务） > **Authentication**（身份验证） > **Authentication Profile**（身份验证配置文件） > **Add Authentication Sequence**（添加身份验证序列）。选择 **Prisma Access** 配置范围。 Prisma Access 按顺序逐一检查，直到成功验证用户身份。



 ©2025 Palo Alto Networks, Inc.

让移动用户能够访问公司资源

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Panorama Managed Prisma Access	• Prisma Access 许可证

要启用 Prisma Access 以使用户只能能访问互联网的，则无需设置任何网络服务，因为 Prisma Access 会提供一个默认的 IP 地址池和一个云默认 DNS 服务器。

但是，如果您希望您的移动用户能够访问总部、数据中心或已接入 Prisma Access 的远程网络站点的内部资源，则需要执行以下操作：

- 定义 IP 地址池，Prisma Access 使用这些地址池为您的移动用户分配 IP 地址。
- 设置 Prisma Access 服务基础设施，
- 并允许访问您的总部或数据中心，接入服务连接。

如果希望您的移动用户能够连接到远程网络站点，那么即使不打算使用该连接来提供对数据中心或总部位置的访问权限，也必须至少配置一个服务连接。尽管所有分支机构之间都实现了完全的网状连接，但移动用户的连接却并非如此。创建一个服务连接会建立起所需的中心辐射型架构，该架构能够让移动用户的流量路由至您的分支机构网络。在这种情况下，您可以按如下方式最低限度配置服务连接：

- 当接入服务连接时，使用与您的移动用户距离最近的 Prisma Access 位置。
- 为服务连接设置主 IPSec 隧道时，请使用占位符值配置 IPSec 对身份验证和隧道设置。
- 为服务连接启用路由和 QoS 时，请添加占位符 IP 子网。

  由于 Prisma Access 不会通过此通道路由任何流量，因此只需确保您使用的 IP 子网不会与连接到 Prisma Access 的其他已配置子网冲突或重叠。

STEP 1 | 转到 **Manage**（管理） > **Mobile Users**（移动用户） > **Mobile Users Setup**（移动用户设置），然后编辑 **Infrastructure Settings**（基础设施设置）以调整移动用户的网络设置。

©2025 Palo Alto Networks, Inc.

STEP 2 | 选择 **Client IP Pool**（客户端 **IP** 池），以查看或调整 Prisma Access 用于向移动用户分配 IP 地址的客户端 IP 池。

- 默认情况下，所有移动用户都可以使用 **Worldwide**（全球）IP 池。
- 可以选择 **Customize per region**（按区域自定义）以按照区域进行自定义，从而使用专用于区域或位置的设置 IP 池。对于您未指定 IP 池的区域或位置，Prisma Access 将使用全球 IP 池。

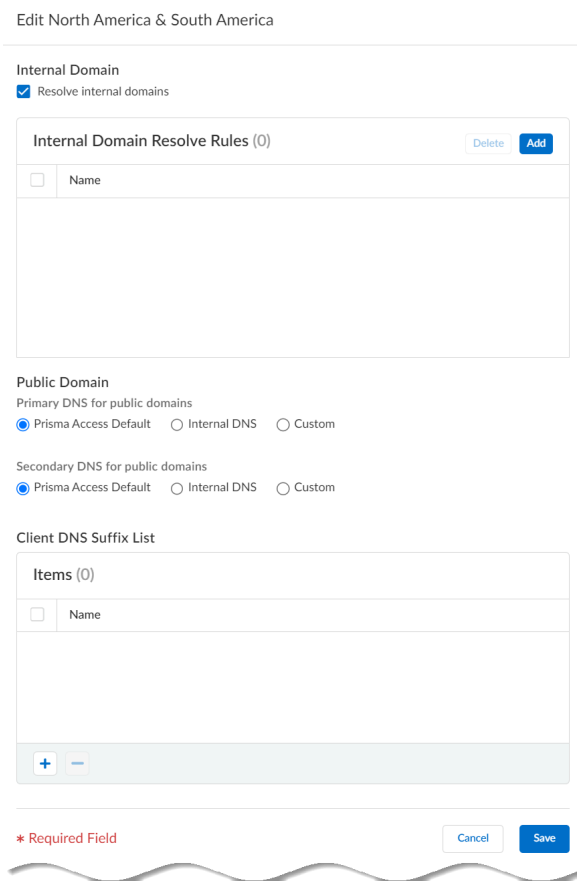
您定义的 IP 地址池必须满足以下要求：

- 作为最佳实践，定义符合 RFC 1918 的 IP 地址池以防止 IP 地址冲突。
- 确保您定义的 IP 地址池与您内部使用的其他 IP 地址没有重叠。
- 确保您定义的 IP 地址池与您用于 Prisma Access 的基础设施 IP 地址池不重叠。
- 请勿指定与 169.25 4.0.0/16 和 100.6 4.0.0/10 子网范围重叠的任何子网，因为 Prisma Access 保留这些 IP 地址和子网供其内部使用。
- 请确保指定的 IP 地址池能够充分覆盖组织中的所有移动用户，原则如下：
- 如果您计划使用部署在一个或两个地区的全球地址池，则所需的最小 IP 地址池为 /23（512 个 IP 地址）。
- 如果您计划使用部署在三个或更多区域的全球地址池，所需的最小 IP 地址池为 /19（8192 个 IP 地址），这些地址可以在单个IP地址池中，也可以分布在多个地址池中。
- 如果您计划按区域定义 IP 地址池，那么在任何一个区域中，最小的地址池大小是 /23（512 个IP地址）。
- 在您不打算进行部署 Prisma Access 的区域，则无需分配 IP 地址池。为用户接入 Prisma Access 时，如果选择了美国东部（北弗吉尼亚州）、美国东部（俄亥俄州）和美国西部（北加利福尼亚州）这样，则只需要为美洲地区指定一个 IP 地址池。但请注意，其他地区的用户将无法连接到 Prisma Access。
- 如果您计划定义全球和区域池的混合，请确保每个区域至少分配 512 个 IP 地址。例如，对于三区域部署，您可以在欧洲区域指定 1024 个地址，在全球指定 512 个地址。
- 最佳实践是指定 IP 地址池，让组织中的每个唯一移动用户至少有一个 IP 地址，以便这些用户可以同时登录。如果您指定的 IP 地址池的 IP 地址数量小于您的许可用户数量，Prisma Access 将显示一条警告信息。但是如果您的 IP 地址池有限，并且您不希望所有用户同时登录，则可以忽略该消息并使用较小的池。

 ©2025 Palo Alto Networks, Inc.

STEP 3 | 添加 **Client DNS**（客户端 **DNS**）设置 — 您可以使用默认值 **Worldwide**（全球），也可以根据地区自定义设置。

选择您要自定义 DNS 设置的区域：



选中 **use these DNS settings to resolve internal domains**（使用这些 **DNS** 设置来解析内部域）选项，也可以选择 **Use the internal DNS Server for resolving public domains too**（也使用内部 **DNS** 服务器解析公共域）。如果不选择此选项，Prisma Access 将使用其云默认 DNS 服务器来解析公共域的请求。

Prisma Access 中的 *DNS* 代理会将请求发送到您指定的 *DNS* 服务器。*DNS* 请求中的源地址是您分配给区域的 *IP* 池中的第一个 *IP* 地址。为确保您的 *DNS* 请求能够到达服务器，需要确保允许移动用户 *IP* 地址池中的所有地址向您的 *DNS* 服务器发送流量。

STEP 4 | 如果希望移动用户能够访问总部或数据中心网络或其他分支机构位置的资源，则必须配置 Prisma Access 基础设施设置以启用网络主干。

转至 **Manage**（管理） > **Prisma Access** > **Prisma AccessSetup**（设置）。

STEP 5 | 若要使移动用户能够访问总部或数据中心上的资源，请创建服务连接以将这些站点连接到 Prisma Access。

转至 **Manage**（管理） > **Service Connections**（服务连接） > **Service Connections Setup**（服务连接设置）。

©2025 Palo Alto Networks, Inc.

STEP 6 | 准备就绪以后，选择 **Push Config**（推送配置）以将配置推送到 Prisma Access，从而保存您的移动用户设置。

©2025 Palo Alto Networks, Inc.

Prisma Access 远程网络

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证

随着您的业务规模扩大，办公地点在地理上分散开来，适用于网络的 Prisma Access 能让您快速将远程网络站点接入，并为您的用户提供一流的安全防护。它提供了一个方便的选项，消除了在每个远程位置配置和管理设备的复杂性。该服务提供了一种高效的方式，可轻松添加新的远程网络站点，最大程度减少运营方面的挑战，确保这些站点的用户始终保持连接并受到安全保护。此外，它还允许您通过 Panorama 进行集中策略管理，从而为远程网络站点提供一致且简化的安全防护。

要将远程网络位置连接到 Prisma Access，您可以使用 Palo Alto Networks 新一代防火墙，也可以使用能够建立到服务的 IPSec 隧道的第三方 IPSec 兼容设备（包括 SD-WAN）。

除了 IPSec 隧道连接之外，Prisma SD-WAN 还允许您使用作为远程网络接入的 CloudBlade，以将 Prisma SD-WAN 控制器和 ION 设备与 Prisma Access 集成。

远程网络规划清单

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证

在开始接入远程网络之前，请确保您已准备好以下配置项，这样才能确保您能够成功启用服务并为远程网络位置的用户实施策略：

- 是否需要访问公司资源？

  如果您的远程网络需要访问总部或数据中心的基础设施或资源，请创建一个至公司网站的 Prisma Access 服务连接。如果远程网络位置是自主的并且不需要访问其他位置的基础设施，则无需执行此操作。

- **Prisma Access** 个地点

  当您的分支机构的用户连接到 Prisma Access，则您选择的 Prisma Access 位置决定了提供互联网内容的语言。为了获得最佳用户体验，请选择与您的分支机构位于同一国家的地区和位置，以确保为您的用户提供最佳体验。如果某个地点不在您的分支机构所在的国家/地区，请选择使用与该站点大多数用户相同语言的地点。

  很少有地点被标记为本地区域。这些位置提供了靠近大型人口和工业中心的 Prisma Access 计算位置。

- **IP** 子网

  要使 Prisma Access 将流量路由到您的远程网络，需要为 Prisma Access 要保护的子网提供路由信息。可以通过多种方式来实现这一点。既可以在远程网络位置为每个子网定义静态路由，也可以在服务连接位置与 Prisma Access 之间配置 BGP，或者同时使用这两种方法。如果配置两条静态路由并启用 BGP，则静态路由优先。如果您的远程网络位置只有几个子网，使用静态路由可能会很方便，但在大型部署中，远程网络的子网彼此重叠，在这种情况下，使用 BGP 将使您能够更轻松地扩展。

- 聚合带宽模型—远程网络位置的带宽按每个计算位置，在聚合级别分配。您的每个接入位置都有一个为其分配带宽的相应计算位置。您按计算位置分配带宽，而不是按位置分配带宽。该方法称为聚合带宽模型。

  聚合带宽模型适用于所有新部署。如果您现有的部署是按位置分配带宽，则可以从按位置分配带宽迁移到按计算位置分配带宽。

  在迁移到聚合带宽模型之前，请务必查看规划向新模式的迁移。

  您接入的所有位置都共享为该计算位置分配的带宽。例如，您需要使用位于新加坡、泰国和越南的远程网络加入四个分支机构。所有这些地点都映射到亚洲东南部的计算地点。如果您为亚洲东南部的计算地点分配 200 Mbps 带宽，则 Prisma Access 会将 200 Mbps 带宽分配给您在

©2025 Palo Alto Networks, Inc.

该地点加入的四个分支机构。如果您还添加了香港的地点，您会注意到香港映射到香港计算地点，并且需要向该计算地点增加带宽。将每个计算地点的最小带宽指定为 50 Mbps。

Prisma Access 根据每个地点的负载或需求动态分配带宽。使用前面的示例，其中四个站点总共使用高达 200 Mbps 的带宽，如果一个或多个站点使用的带宽不如其他站点那么多，Prisma Access 会为需求量较大的地点提供更多带宽，以便您更有效地利用分配的带宽。此外，如果其中一个站点出现故障，则 Prisma Access 会在该计算地点仍处于正常运行状态的其他站点之间重新分配带宽。

标记为 **Local Zones**（本地区域）的位置支持远程网络的最大带宽为 500 Mbps。要支持 1 Gbps 的带宽，请联系 Palo Alto Networks 支持部门。这些位置提供了靠近大型人口和工业中心的 Prisma Access 计算位置；但是它们也存在一些限制。要添加本地服务区，请联系您的 Palo Alto Networks 代表。

- 如果您在访问 URL 时遇到问题，请向 Palo Alto Networks 支持部门报告网站问题。
- 规模调整指南和带宽分配注意事项

  计算某一站点所需的带宽时请注意，带宽使用量包括远程网络连接的出站和入站流量（即，分配的带宽是入站和出站的总和），而且您接入的所有位置都共享该计算位置的分配带宽。为了帮助您确定特定站点所需的带宽量，请考虑每个地点的 ISP 提供的带宽。
- 重叠子网

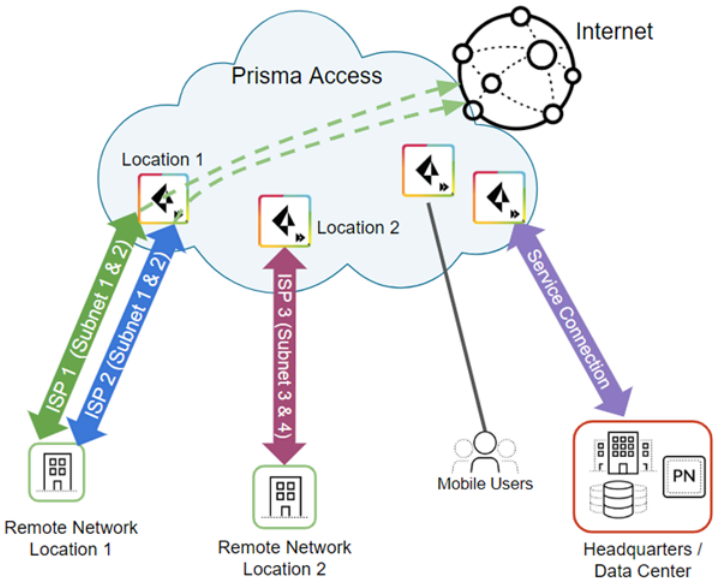
  通常，Prisma Access 实例中不能有任何重叠的子网。也就是说，所有远程网络位置、服务连接和移动用户 IP 地址池的 Prisma Access 的子网不能重叠。但是，在某些情况下，您无法避免子网重叠，例如，如果您收购了一家使用与您现有子网重叠的子网的公司。在某些情况下，您可

 ©2025 Palo Alto Networks, Inc.

能希望通过设计配置两个具有重叠子网的区域；例如，如果您想在零售店位置创建具有不同策略规则的单独的客户网络。

Prisma Access 允许您接入具有重叠子网的远程网络位置，但仅支持来自具有重叠子网的分支机构的互联网绑定流量。同一租户中没有重叠子网的分支机构可以从 Prisma Access 获得全部功能。请参阅下图中的表格以了解更多详细信息。

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



但请记住，子网重叠的站点有以下限制：

- 没有远程网络到远程网络的入站流量。其他远程网络位置不知道将流量路由到何处，因为多个远程网络位置路由到相同子网。但是，任何远程网络位置的用户和服务都可以访问其他远程网络位置的资源，前提是该站点没有重叠的子网，并且任何站点都可以通过 Prisma Access 基础设施访问互联网。
- 来自服务连接的流量无法访问任何具有重叠子网的远程网络位置的资源，因为它不知道将流量路由到哪个远程网络位置。但子网重叠的远程网络位置可以从服务连接访问资源。
- 由于入站路由限制，移动用户无法访问子网重叠的远程网络位置中的资源。

如果你正在使用 *Strata Cloud Manager* 来管理 *Prisma Access*，转到 ***Workflows***（工作流）> ***Prisma Access Setup***（***Prisma Access*** 设置）> ***Remote Networks***（远程网络）> ***Advanced Settings***（高级设置）。编辑 ***Overlapped Subnets***（重叠子网）设置以启用重叠子网。如果您使用 *Panorama* 来管理 *Prisma Access*，则转至 ***Panorama*** > ***Cloud Services***（云服务）> ***Configuration***（配置）> ***Remote Networks***（远程网络），然后选中 ***Overlapped Subnets***（重叠子网）。

- **IPSec** 终止节点—您在接入期间将 *IPSec* 终止节点分配给远程网络。每个 IPSec 终止节点最多可以指定 500 个远程网络站点（对于 Prisma Access 5.0 及更高版本）或 400 个远程网络站点

©2025 Palo Alto Networks, Inc.

（对于 Prisma Access 5.0 之前的版本）。为了能够支持所允许的最大数量的远程网络，对于与 IPSec 终止节点相对应的计算位置，请分配超过 500 Mbps 的带宽。

一个计算位置最多可以有 200 个 IPSec 终止节点。每个 IPSec 终止节点可为您提供最多 1000 Mbps 的带宽。如果您为计算地点分配超过 1,000 Mbps 的带宽，Prisma Access 会为您提供额外的 IPSec 终止节点。

- **IPSec** 终止节点和 **3.2** 之前版本的升级—在 3.2 版本之前，在计算位置中，每分配 500 Mbps 带宽，就会分配一个 IPSec 终止节点。如果您的远程网络部署版本低于 3.2，并升级到 3.2.1 或更高版本，且如果远程网络位置为其相应的计算位置分配了超过 500 Mbps，则与 IPSec 终止节点关联的每个远程网络都可以支持高达 1,000 Mbps 的带宽。升级到 3.2 或更高版本后，Prisma Access 每分配 1000 Mbps 带宽就会部署一个 IPSec 终止节点。对于现有的远程网络，Prisma Access 可以使用自动扩展机制来增加远程网络的带宽，当远程网络上的带宽消耗需要额外容量时，就会触发该机制。有关详细信息，请参阅 Prisma Access (Panorama Managed) 发行说明中的默认行为的更改。

  升级到 3.2 后，当前 IPSec 终止节点到远程网络的映射保持不变，并且 IPSec 终止节点的数量仍然相同。仅当您增加或减少现有计算位置的带宽或者为远程网络接入新的计算位置时，才会添加或删除 IPSec 终止节点。

- 服务连接—如果您的远程网络位置需要访问公司总部的基础设施来验证用户身份，或者要允许访问关键网络资产，则必须创建服务连接，以便总部和远程网络位置连通。如果远程网络位置是自主的并且不需要访问其他位置的基础设施，则无需设置服务连接（除非您的移动用户需要访问）。
- 模板—Prisma Access会自动为适用于网络的 Prisma Access 创建模板堆栈 (Remote_Network_Template_Stack) 和顶层模板 (Remote_Network_Template)。要接入并配置远程网络，您需要从头开始配置顶级模板，或者利用现有配置（如果您已经在本地运行 Palo Alto Networks 防火墙）。此模板需要用于建立 IPSec 隧道和互联网密钥交换 (IKE) 配置（用于远程网络位置和适用于网络的 Prisma Access 之间的协议协商）的设置、可以在安全策略中引用的区域以及日志转发配置文件（以便可以将日志从适用于远程网络的 Prisma Access 转发到 Strata Logging Service）。
- **IPSec** 隧道配置—如果您已有一个包含 IPSec 隧道、隧道监控和 IPSec 加密配置文件 配置的模板，您可以将该模板添加到 Remote_Network_Template_Stack 中，以简化创建 IPSec 隧道的流程。或者，您可以编辑自动创建的 Remote_Network_Template 并创建在创建返回公司站点的 IPSec 隧道时所需的 IPSec 配置。Prisma Access 还提供一组适用于常用网络设备的预定义 IPSec 模板，以及适用于预定义模板中未包含的任何设备的一个通用模板。配置远程网络隧道时，请务必遵循 IPSec 隧道建议。
- 确定路由方法（静态或动态）—为了让 Prisma Access 将流量路由到您的远程网络，您必须提供使用 Prisma Access 进行安全防护的子网的路由信息。可以通过多种方式来实现这一点。既可以在远程网络位置为每个子网定义静态路由，也可以在服务连接位置与 Prisma Access 之间配置 BGP，或者同时使用这两种方法。如果配置两条静态路由并启用 BGP，则静态路由优先。如果您的远程网络位置只有几个子网，使用静态路由可能会很方便，但在大型部署中，很多远程网络的子网彼此重叠，在这种情况下，使用 BGP 将使您能够更轻松地扩展。
- 父设备组—适用于网络的 Prisma Access 要求您指定一个父设备组，该组将包括您的安全策略、安全配置文件和其他策略对象（例如应用程序组和对象以及地址组）以及身份验证策略，这样一来，适用于网络的 Prisma Access 可能够以一致方式对经由 IPSec 隧道路由到适用于网络

 ©2025 Palo Alto Networks, Inc.

的 Prisma Access 的流量实施策略。您需要在 Panorama 上定义策略规则和对象，或者使用现有设备组来保护远程网络位置的用户。



如果您使用引用区域的现有设备组，请确保将定义区域的相应模板添加到 *Remote_Network_Template_Stack*。这样做将允许您在接入和配置远程网络时完成区域映射。

 ©2025 Palo Alto Networks, Inc.

分配远程网络带宽

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

远程网络用于保护远程网络位置（如分支机构）以及这些分支机构中的用户。

远程网络按流量计费，这意味着需要为计算地点分配特定的带宽量，并且分配的带宽会产生相关费用。

当您准备将远程网络连接到 Prisma Access 时，您需要知道将加入的站点数量以及每个站点的带宽要求。

了解如何分配远程网络带宽。

- Strata Cloud Manager
- Panorama

分配远程网络带宽 (Strata Cloud Manager)

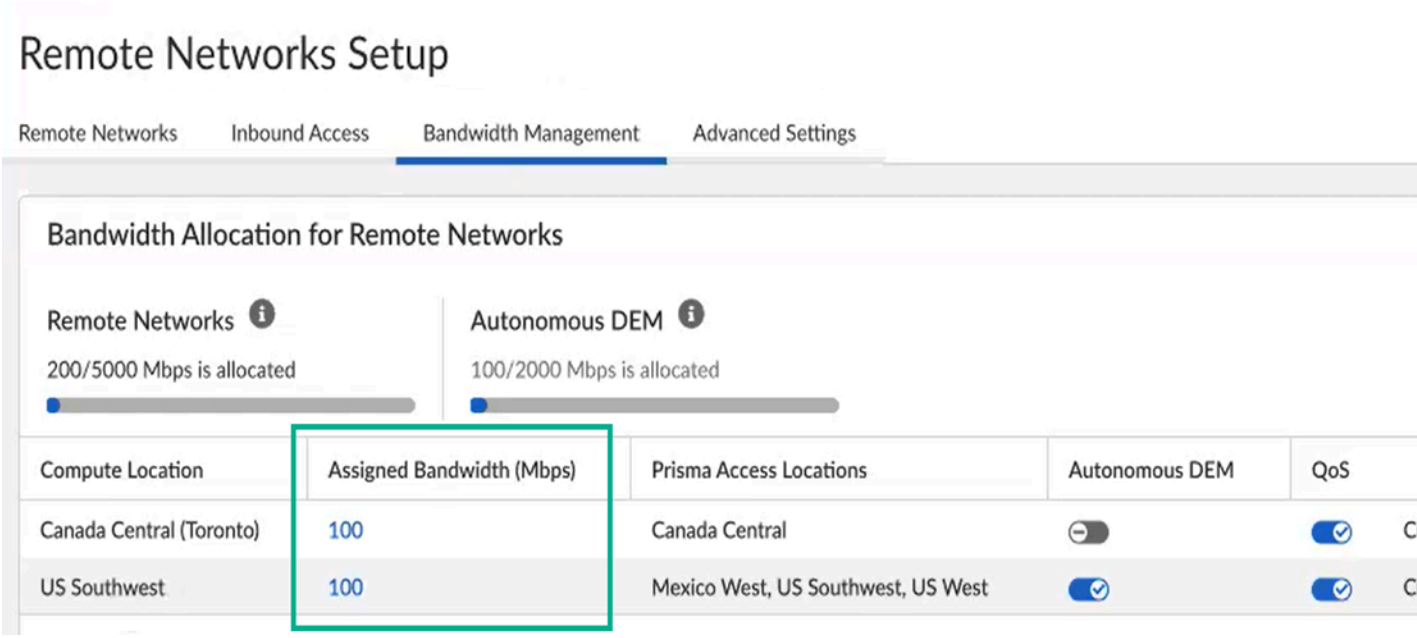
在地理位置上彼此相近的至少两个（通常更多）Prisma Access 地点被分组为计算地点。这是您分配带宽的级别，而不是为个别 Prisma Access 地点或特定的远程网络站点分配带宽。这意味着 Prisma Access 可以根据负载或需求向计算地点中的站点动态分配带宽。

例如，您需要使用位于新加坡、泰国和越南的远程网络加入四个分支机构。所有这些地点都映射到亚洲东南部的计算地点。如果您为亚洲东南部的计算地点分配 200 Mbps 带宽，则 Prisma Access 会将 200 Mbps 带宽分配给您在该地点加入的四个分支机构。如果您还添加了香港的地点，您会注意到香港映射到香港计算地点，并且需要向该计算地点增加带宽。将每个计算地点的最小带宽指定为 50 Mbps。

Prisma Access 根据每个地点的负载或需求动态分配带宽。使用前面的示例，其中四个站点总共使用高达 200 Mbps 的带宽，如果一个或多个站点使用的带宽不如其他站点那么多，Prisma Access 会为需求量较大的地点提供更多带宽，以便您更有效地利用分配的带宽。此外，如果其中一个站点出现故障，则 Prisma Access 会在该计算地点仍处于正常运行状态的其他站点之间重新分配带宽。

首先，请转到 **Workflows**（工作流） > **Prisma Access** 设置 > **Remote Networks**（远程网络） > **Bandwidth Management**（带宽管理）。

 ©2025 Palo Alto Networks, Inc.



当您根据地点分配带宽时，仍要考虑每个站点所需的带宽量

为了帮助您确定特定站点所需的带宽量，请考虑每个地点的 ISP 提供的带宽。计算某个站点所需的带宽量时，请考虑带宽使用情况，包括远程网络连接的出站流量和入站流量。

跨地点分配带宽时，不支持远程网络站点的安全入站访问和远程网络的服务质量 *(QoS)*。

分配远程网络带宽 (Panorama)

要配置按计算地点分配带宽的 Prisma Access 远程网络部署，请完成以下步骤。

如果您需要加入多个远程网络（最多 *1,000* 个），则可以使用以下步骤加入远程网络，然后将远程网络配置导出到 CSV 文件，将要加入的其他远程网络添加到 *CSV* 文件中，然后导入 *CSV* 文件以将配置保存到 *Prisma Access* 中。

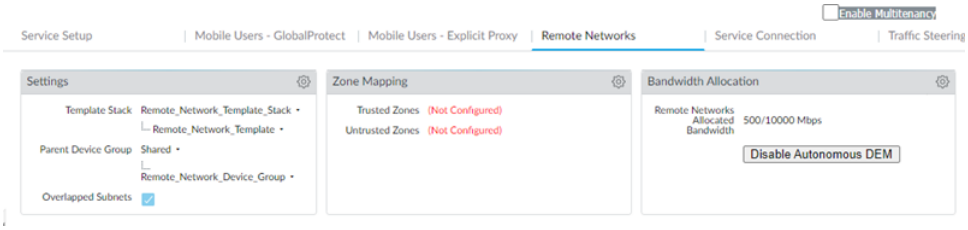
STEP 1 | 选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Remote Networks**（远程网络）。

 ©2025 Palo Alto Networks, Inc.

STEP 2 | 单击 **Bandwidth Allocation**（带宽分配）区域中的齿轮图标，为您要加入的地点分配带宽。

您可以按计算地点在聚合级别分配带宽。有关详细信息，请参阅Prisma Access 远程网络。

如果您删除了作为附加程序许可证的自主 DEM，或者从许可证中删除了远程网络的自主 *DEM*，请选择 ***Disable Autonomous DEM***（禁用自主 ***DEM***）。如果您删除远程网络的自主 *DEM* 且未禁用自主 *DEM*，则在提交时会收到错误。



如果现有远程网络部署当前按地点加入远程网络，则会显示一个弹出窗口，询问您是否要迁移到聚合带宽模型。单击 **Migrate**（迁移）继续，或单击 **Cancel**（取消）取消迁移。

迁移到聚合带宽模型是永久性且不可逆的过程。迁移之前，请查看迁移前检查清单。必须 ***Commit and Push***（提交并推送）您的更改，才能使其生效。

当您将部署迁移到聚合带宽模型时，**Service IP Address**（服务 **IP** 地址）（用于远程网络连接的 IPSec 隧道的 Prisma Access 端的 公共 IP 地址）不会更改，并且不需要重新配置 IPSec 隧道。

STEP 3 | 输入与您要加入的 **Prisma Access** 地点相关联的每个 **Compute Location**（计算地点）所需的 **Bandwidth Allocation**（带宽分配）。

要验证您输入的带宽量，请选中带宽量旁边的复选标记；要取消该带宽量，请选择 **x**。

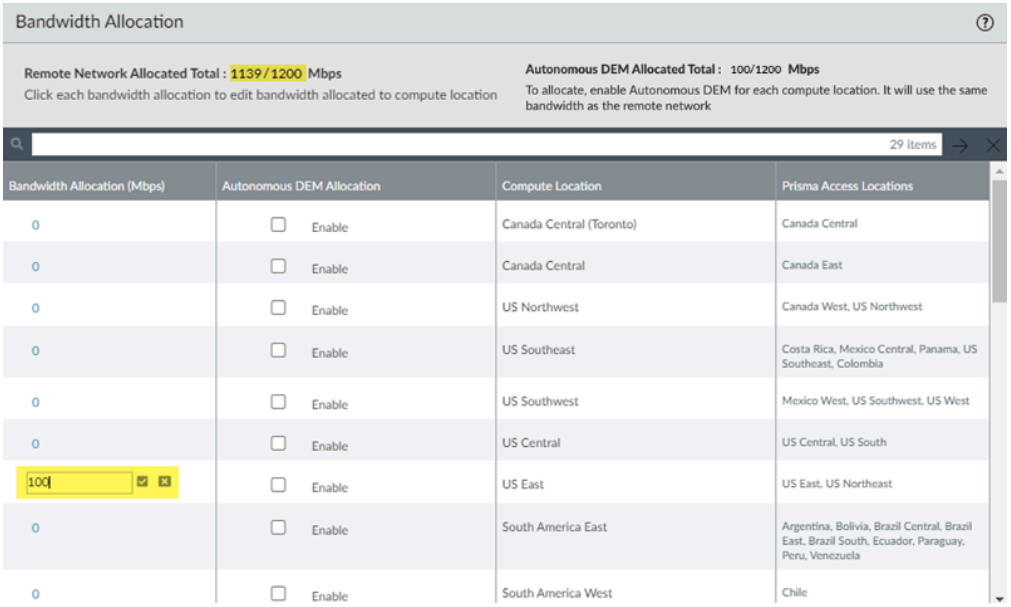
指定最小带宽为 50 Mbps，最大带宽为最大剩余许可带宽。

STEP 4 | （可选，仅限具有远程网络许可证的自主 DEM 的部署）为您分配带宽的计算地点 **Enable**（启用）**Autonomous DEM Allocation**（自主 **DEM** 分配）。

如果为计算地点启用自主 DEM，则自主 DEM 许可证使用的带宽量与您为计算地点指定的带宽量相同。**Autonomous DEM Allocated Total**（自主 **DEM** 分配的总带宽量）显示自主 DEM 使用的带宽量以及剩余的带宽量。有关详细信息，请参阅自主 DEM 指南。

©2025 Palo Alto Networks, Inc.

STEP 5 | 等待带宽反映在页面顶部的 **Allocated Total**（分配的总带宽量）字段中；然后单击 **OK**（确定）。



STEP 6 | （可选）如果您想要配置远程网络以提供对远程网络位置的安全入站访问，请单击 **Inbound Access Remote Networks**（入站访问远程网络）选项卡，按照工作流程为远程网络配置安全入站访问。

STEP 7 | **Add**（添加）远程网络并指定 **Name**（名称）。

输入远程网络位置的名称后，您无法更改该名称。请确保您了解远程网络的命名方案，然后再开始加入该远程网络。

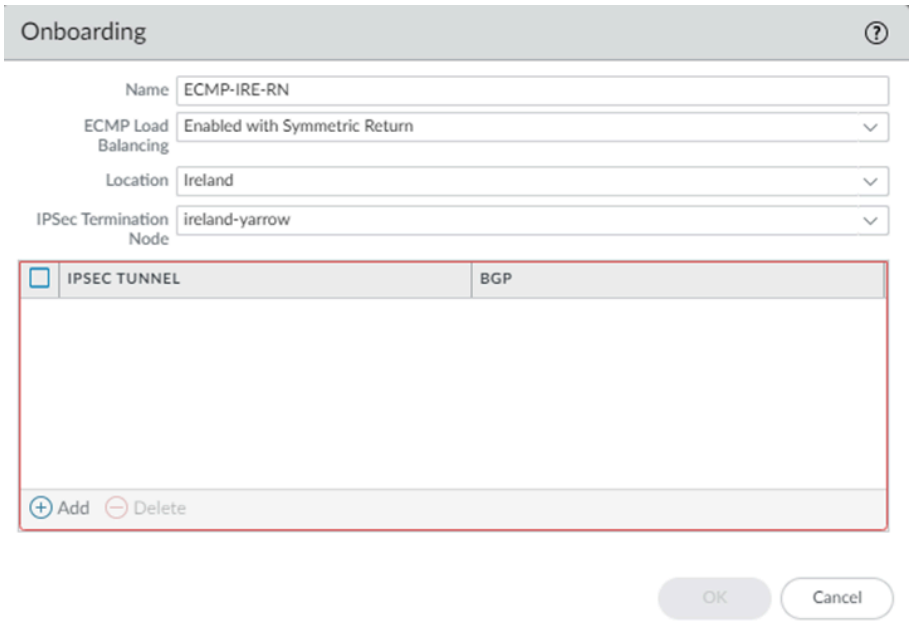
 ©2025 Palo Alto Networks, Inc.

STEP 8 | （可选，仅限 BGP 部署）创建配置，以便远程网络连接可以使用最多四个 IPSec 隧道进行流量传输（**ECMP Load Balancing**（**ECMP** 负载均衡））。

不支持静态路由（需要 BGP），并且如果配置了 QoS，则无法更改 ECMP 链路的分配比例。如果您的部署使用一个 IPSec 隧道进行远程网络连接或使用静态路由，请为 **ECMP Load Balancing**（**ECMP** 负载均衡）选择 **None**（无），然后继续执行步骤 11。

1. 选择其中一个选项来启用或禁用 ECMP 负载均衡。
   - **None**（无）— 不使用 ECMP 负载均衡（使用一个远程网络隧道进行此次远程网络连接）。这是静态路由的唯一选择；ECMP 负载均衡需要 BGP。
   - **Enabled with Symmetric Return**（启用对称返回）— 为此远程网络连接指定最多四个 IPSec 隧道，并强制 Prisma Access 使用与发送流量相同的链路来传输返回流量。

     如果您使用一个或多个隧道作为仅在其中一个主隧道断开时使用的备用隧道，请选择此选项。如果链路发生故障，Prisma Access 会使用其他隧道之一来对称地发送和接收流量。



2. 为远程网络连接 **Add**（添加）IPSec 隧道并指定以下值：
   - **Enable**（启用）— 为 IPSec 隧道启用 BGP。

     此选项不可配置；您必须启用 BGP 才能配置 ECMP。
   - **Summarize Mobile User Routes before advertising**（在通告之前汇总移动用户路由）— 通过汇总移动用户 IP 子网，减少通过 BGP 向您的客户终端设备 (CPE) 通告的移动用户 IP 子网的数量。

     默认情况下，Prisma Access 以 /24 子网的形式通告移动用户的 IP 地址池；如果将它们汇总起来，Prisma Access 会根据您指定的子网来通告该池。例如，Prisma Access 使用 /20 子网通告公共用户移动 IP 池 10.8.0.0/20，而不是在通告之前将池划分为 10.8.1.0/24、10.8.2.0/24、10.8.3.0/24 等子网。汇总这些通告可以减少 CPE 路由表

 ©2025 Palo Alto Networks, Inc.

中存储的路由数量。例如，您可以将 IP 池汇总与可接受有限数量路由的云 VPN 网关（虚拟专用网关 (VGW) 或传输网关 (TGW)）结合使用。

如果为使用 *ECMP* 的位置启用路由汇总，则必须在指向该位置的所有链路上启用路由汇总，否则您将在提交期间收到错误。

Prisma Access 将聚合移动用户路由的社区字符串设置为 `0xFFFE:0xFFF0`。

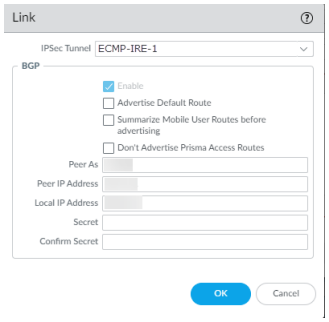
- **Advertise Default Route**（通告默认路由）—Prisma Access 使用 eBGP 为远程网络发起默认路由通告。

  确保您的网络没有由 *BGP* 通告的其他默认路由，否则可能会在网络中引入路由问题。

- 不通告 **Prisma Access** 路由 — 防止 Prisma Access BGP 对等体将路由转发到您组织的网络中。

  默认情况下，Prisma Access 通告所有 BGP 路由信息，包括本地路由以及它从其他服务连接、远程网络和移动用户子网收到的所有前缀。选中此复选框可防止 Prisma Access 发送任何 BGP 通告，但仍使用其收到的 BGP 信息从其他 BGP 邻居学习路由。

  如果您选择此选项，Prisma Access 不会发送 BGP 通告，因此您必须在本地设备上配置静态路由以建立返回 Prisma Access 的路由。



- **Peer AS**（对等 **AS**）— 指定远程网络中的防火墙、虚拟路由器或 BGP 路由器所属的自治系统 (AS)。
- **Peer IP Address**（对等体 **IP** 地址）— 输入为您要配置此连接的远程网络上的 eBGP 路由器的路由器 ID 分配的 IP 地址。
- **Local IP Address**（本地 **IP** 地址）（可选）— 输入 Prisma Access 用作 BGP 的本地 IP 地址的地址。指定要在隧道的 Prisma Access 端使用的 IP 地址。

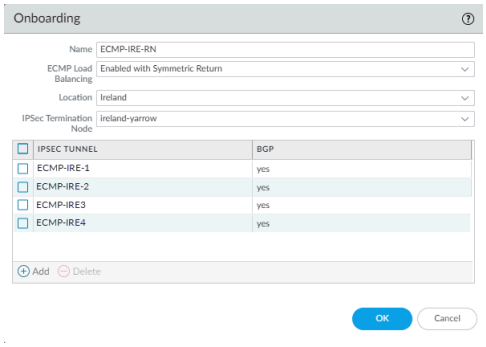
  当连接另一端的设备（例如 Amazon Web Service (AWS) 虚拟专用网关）需要特定的本地 IP 地址才能成功进行 BGP 对等连接时，指定**Local Address**（本地地址）很有

 ©2025 Palo Alto Networks, Inc.

用。确保您指定的地址与基础架构子网或远程网络中的子网中的 IP 地址不冲突或重叠。

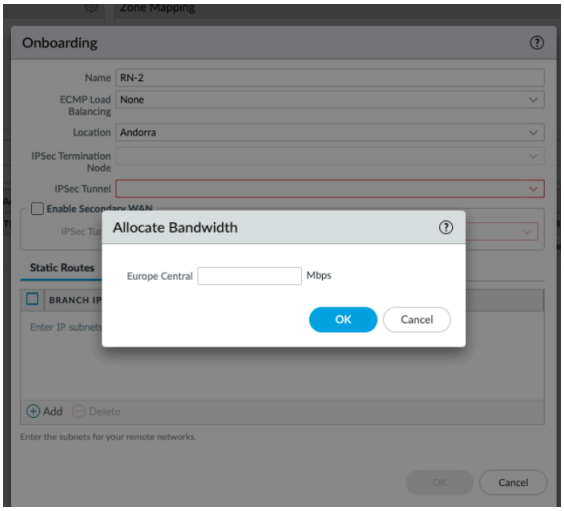
- **Secret**（密码）和 **Confirm Secret**（确认密码）（可选）— 输入并确认密码以验证 BGP 对等体通信。

3. 重复上一步，以添加最多四个隧道用于远程网络连接。



STEP 9 | 选择 Prisma Access 将在其中部署保护远程网络位置所需的基础架构的 **Location**（位置）。此区域在地理位置上应靠近您的远程网络位置。

如果您尚未为该位置映射到的计算地点分配带宽， Prisma Access 会提示您输入该计算地点的带宽。



STEP 10 | 选择您要用于此远程网络的 **IPSec Termination Node**（**IPSec** 终止节点）。

Prisma Access 使用此节点将远程网络位置与计算地点相关联。

STEP 11 | （仅限静态路由或单隧道部署）选择或添加新的 **IPSec Tunnel**（**IPSec** 隧道）配置，以访问公司位置的防火墙、路由器或 SD-WAN 设备：

- 在 Remote_Network_Template 中选择一个预定义的 IPSec 模板，或者，如果您已向 Remote_Network_Template_Stack 添加包含 IPSec 隧道配置的模板（或修改了预定义的 Remote_Network_Template），请从下拉列表中选择该 **IPSec Tunnel**（**IPSec** 隧道）。请

 ©2025 Palo Alto Networks, Inc.

注意，您为每个远程网络连接创建的隧道会将 Prisma Access 连接到每个分支机构位置支持 IPSec 的设备。

配置 IPSec 隧道时，请遵循以下准则：

- IKE 网关配置中的对等地址对于每个隧道都必须是唯一的。但是，您可以重用其他一些常见的配置元素，例如加密配置文件。
- 从模板中选择的 IPSec 隧道必须仅使用自动密钥交换和 IPv4。
- IPSec 隧道、IKE 网关和加密配置文件名称不能超过 31 个字符。
- 如果将多个远程网络上线到具有动态 IKE 对等设备的同一位置，则必须对所有远程网络配置使用相同的 IKE 加密配置文件。

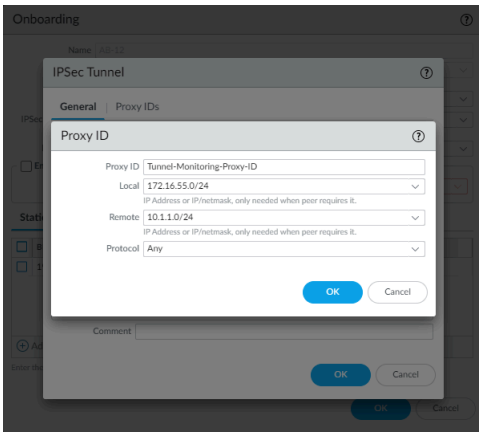
- 要创建新的 IPSec 隧道配置，请单击 **New IPSec Tunnel**（新建 **IPSec** 隧道），为其指定一个 **Name**（名称），然后配置 IKE 网关、IPSec 加密配置文件和隧道监控设置。
  - 如果分支机构中支持 IPSec 的设备使用基于策略的 VPN，请在 **Proxy IDs**（代理 **ID**）选项卡上，**Add**（添加）与本地 IPSec 设备上配置的设置匹配的代理 ID，以确保 Prisma Access 可以成功建立与本地设备的 IPSec 隧道。
- 保持 **Enable Replay Protection**（启用重放保护）选中状态以检测重放攻击并使其无效。
- 选择 **Copy ToS Header**（复制 **ToS** 标头），将封装数据包的内部 IP 标头中的服务类型 (ToS) 标头复制到其外部 IP 标头中，以保留原始 ToS 信息。

©2025 Palo Alto Networks, Inc.

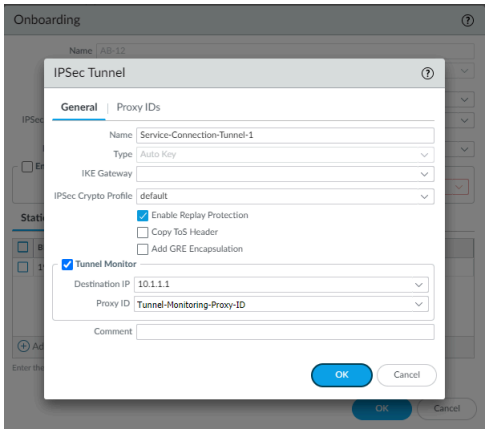
- 要为服务连接启用隧道监视，请选择 **Tunnel Monitor**（隧道监视器）。
  - 输入 **Destination**（目标）IP 地址。

    在分支机构位置指定一个 IP 地址，Prisma Access 可以向该地址发送 IPSec 隧道监控的验证请求。请确保整个 Prisma Access 基础架构子网都可以通过 ICMP 访问此地址。
  - 如果对使用多个代理 ID 的对等设备使用隧道监控，请指定一个 **Proxy ID**（代理 **ID**）或添加一个 **New Proxy ID**（新代理 **ID**），以允许从基础架构子网访问分支机构位置。

    下图显示了一个代理 ID，其中服务基础架构子网（本示例中为 172.16.55.0/24）作为 **Local**（本地）IP 子网，分支机构位置的子网（本示例中为 10.1.1.0/24）作为 **Remote**（远程）子网。



    下图显示了您创建的代理 ID，该代理 ID 通过在 **Proxy ID**（代理 **ID**）字段中指定而应用于隧道监视器配置。



您必须在 *CPE* 上配置一个到隧道监视器 *IP* 地址的静态路由，以使隧道监视正常工作。要查找用于从分支机构位置到 *Prisma Access* 的隧道监控的目标 *IP* 地址，请选择 ***Panorama > Cloud Services***（云服务）***> Status***（状态）***> Network Details***（网络详细信息），并单击 ***Service Infrastructure***（服务基础架构）单选按钮，然后找到 ***Tunnel Monitor IP Address***（隧道监控 *IP* 地址）。

 ©2025 Palo Alto Networks, Inc.

STEP 12 | 如果在此位置有辅助 WAN 链路，请选择 **Enable Secondary WAN**（启用辅助 **WAN**）。

确保为每个远程网络的辅助 *WAN* 创建唯一的 *IPSec* 隧道；*Prisma Access* 不支持对多个远程网络中的辅助 *WAN* 重用相同的 *IPSec* 隧道。

以下部署不支持配置辅助 WAN：

- 如果您的辅助 WAN 的主 IPSec 隧道设置为主动-主动模式。
- 如果您的客户端设备 (CPE) 的主 IPSec 隧道和辅助 IPSec 隧道设置为等价多路径 (ECMP) 配置。

如果您使用静态路由，隧道故障转移时间从检测时间算起不超过 15 秒，具体取决于您的 WAN 提供商。

如果您配置了 BGP 路由并启用了隧道监视，则确定安全参数索引 (SPI) 失败的最短默认保持时间是使用隧道监视器，当它检测到连续 15 秒的隧道失败时，将删除指向对等设备的所有路由。通过这种方式，隧道监控器确定 BGP 路由的行为。如果未配置隧道监控，保持计时器将确定在删除路由之前隧道关闭的时间。Prisma Access 使用 RFC 4271 定义的默认 BGP HoldTime 值 90 秒，这是 Prisma Access 删除非活动 SPI 的路由之前的最长等待时间。如果对等 BGP 设备的配置保持时间较短，BGP 保持计时器将使用较低的值。

成功安装辅助隧道后，辅助路由将优先使用，直到主隧道恢复。如果主路由和辅助路由都已启动，则主路由优先。

如果您使用不同的 *BGP* 对等设备进行辅助（备份）连接，*Prisma Access* 不会接受 *CPE* 通告的 *Multi-Exit Discriminator (MED)* 属性。如果您在远程网络连接或服务连接上使用多个 *BGP* 对等设备，则此警告适用。

 ©2025 Palo Alto Networks, Inc.

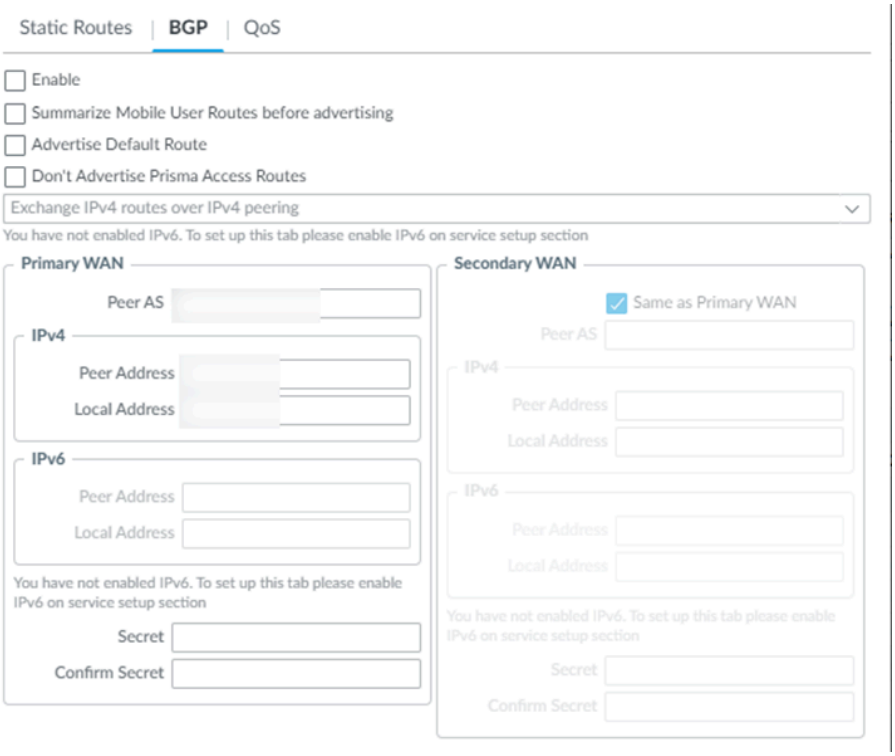
STEP 13 | 启用到用户需要访问的远程网络站点的子网或单个 IP 地址的路由。

Prisma Access 使用此信息将请求路由到适当的站点。每个站点的网络不能相互重叠，也不能与您为服务基础架构或适用于用户的 Prisma Access IP 池指定的 IP 地址池重叠。您可以配置 **Static Routes**（静态路由）、**BGP** 或两者的组合。

- 要配置 **Static Routes**（静态路由）：
  1. 在 **Static Routes**（静态路由）选项卡上，单击 **Add**（添加）并输入子网地址（例如，172.168.10.0/24）或资源的单个 IP 地址，例如远程用户需要访问的 DNS 服务器（例如，10.32.5.1/32）。
  2. 对 Prisma Access 在此位置需要访问的所有子网或 IP 地址重复此操作。



- 要配置 **BGP**：
  1. 选择 **BGP** 选项卡。
  2. （可选）选择 **ECMP Load Balancing**（**ECMP** 负载均衡）选项。请参阅步骤 8。
  3. 如果为 **ECMP Load Balancing**（**ECMP** 负载均衡）选择 **None**（无），请输入 BGP 选项。



 ©2025 Palo Alto Networks, Inc.

4. 要为远程网络连接启用 BGP，请选择 **Enable**（启用）。

   启用 BGP 后，Prisma Access 会将外部 BGP (eBGP) 的生存时间 (TTL) 值设置为 8，以适应 Prisma Access 基础架构和终止 eBGP 连接的客户终端设备 (CPE) 之间可能发生的任何额外跳数。

5. 要通过汇总移动用户 IP 子网以减少通过 BGP 向您的客户终端设备 (CPE) 通告的移动用户 IP 子网的数量，请选择 **Summarize Mobile User Routes before advertising**（在通告之前汇总移动用户路由）。

   默认情况下，Prisma Access 以 /24 子网的形式通告移动用户的 IP 地址池；如果将它们汇总起来，Prisma Access 会根据您指定的子网来通告该池。例如，Prisma Access 使用 /20 子网通告公共用户移动 IP 池 10.8.0.0/20，而不是在通告之前将池划分为 10.8.1.0/24、10.8.2.0/24、10.8.3.0/24 等子网。汇总这些通告可以减少 CPE 路由表中

 ©2025 Palo Alto Networks, Inc.

存储的路由数量。例如，您可以将 IP 池汇总与可接受有限数量路由的云 VPN 网关（虚拟专用网关 (VGW) 或传输网关 (TGW)）结合使用。

Prisma Access 将聚合移动用户路由的社区字符串设置为 `0xFFFE:0xFFF0`。

6. 要允许 Prisma Access 使用 eBGP 为远程网络通告默认路由，请选择 **Advertise Default Route**（通告默认路由）。

   如果选择 **Advertise Default Route**（通告默认路由），请确保您的网络没有由 BGP 通告的其他默认路由，否则可能会在网络中引入路由问题。

   > 您必须先发布默认路由，然后才能进行此选择以通告默认路由。此外，确保您的网络没有由 *BGP* 通告的其他默认路由，否则可能会在网络中引入路由问题。

7. 要防止 Prisma Access 防火墙上的 BGP 对等体将路由转发到您组织的网络中，请选择不通告 **Prisma Access** 路由。

   默认情况下，Prisma Access 通告所有 BGP 路由信息，包括本地路由以及它从其他服务连接、远程网络和移动用户子网收到的所有前缀。选中此复选框可防止 Prisma Access 发送任何 BGP 通告，但仍使用其收到的 BGP 信息从其他 BGP 邻居学习路由。

   如果您选择此选项，Prisma Access 不会发送 BGP 通告，因此您必须在本地设备上配置静态路由以建立返回 Prisma Access 的路由。

8. 输入 **Peer AS**（对等 **AS**），即远程网络中的防火墙、虚拟路由器或 BGP 路由器所属的自治系统 (AS)。
9. 输入为您要配置此连接的远程网络上的 eBGP 路由器的路由器 ID 分配的 IP 地址作为 **Peer Address**（对等体 **IP** 地址）。
10. （可选）输入 Prisma Access 用作 BGP 的本地 IP 地址的地址。

    当连接另一端的设备（例如 Amazon Web Service (AWS) 虚拟专用网关）需要特定的本地 IP 地址才能成功进行 BGP 对等连接时，指定**Local Address**（本地地址）很有用。确保您指定的地址与基础架构子网或远程网络中的子网中的 IP 地址不冲突或重叠。

    > 您必须在 *CPE* 上配置到 *BGP **Local Address***（本地地址）的静态路由。

11. （可选）输入并确认密码以验证 BGP 对等体通信。
12. （可选）如果您配置了 **Secondary WAN**（辅助广域网），并且需要更改辅助（备份）BGP 对等体的 **Peer Address**（对等体地址）或 **Local Address**（本地地址），请取消

 ©2025 Palo Alto Networks, Inc.

选择 **Same as Primary WAN**（与主广域网相同），然后输入唯一的对等体，或者输入辅助广域网的本地 IP 地址。

如果您在远程网络部署中使用 IPv6 网络，则可以配置 **IPv6** 地址以及 **IPv4** 地址。您还需要在 Prisma Access 基础架构中全局启用 IPv6 网络，然后才能使用 IPv6 寻址。

在某些部署中（例如，当使用 BGP 与 AWS VPN 网关对等时），主广域网和辅助广域网的 BGP 对等体可能有所不同。在这些情况下，您可以选择为辅助广域网设置不同的 BGP 对等体。

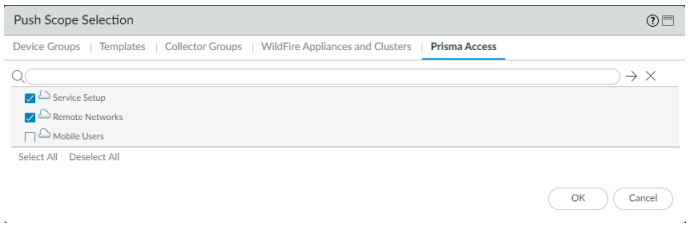
对于具有辅助广域网的 *BGP* 部署，*Prisma Access* 将主隧道和辅助隧道都设置为 ***UP*** 状态，但遵循网络流量的正常 *BGP* 主动备份行为。*Prisma Access* 将主隧道设置为活动状态，并仅通过该隧道发送和接收流量；如果主隧道发生故障，*Prisma Access* 将使用 *BGP* 规则检测故障，将辅助隧道设置为活动状态，并且仅使用辅助隧道发送和接收流量。

STEP 14 | （可选）为该位置启用 **QoS** 并指定 **QoS Profile**（**QoS** 配置文件）。

您可以在 **Settings**（设置）中根据计算地点指定 QoS 选项和整体设置；但是，您可以在此处根据位置启用或禁用 QoS 或更改 QoS 配置文件。

STEP 15 | 将配置更改提交给 Panorama，并将配置推送到适用于网络的 Prisma Access。

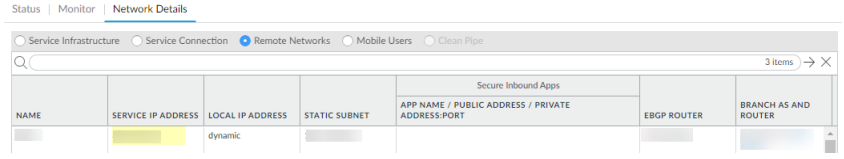
1. 单击 **Commit**（提交） > **Commit to Panorama**（提交到 **Panorama**）。
2. 单击 **Commit**（提交） > **Commit and Push**（提交并推送）。单击 **Edit Selections**（编辑选择） > **Prisma Access**，然后选择适用于网络的 Prisma Access 和适用于服务设置的 Prisma Access，以将配置推送到服务。



3. 单击 **OK**（确定）和 **Push**（推送）。

STEP 16 | 在远程网络位置配置支持 IPSec 的设备，以便与适用于网络的 Prisma Access 建立 IPSec 连接。

1. 要查找此远程网络连接的 **Service IP Address**（服务 **IP** 地址），请选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息），单击 **Remote Networks**（远程网络）单选按钮，并查看 **Service IP Address**（服务 **IP** 地址）字段。适用于网络的 Prisma Access 基础架构已为 Prisma Access 远程网络连接分配了此 IP 地址，您必须将其配置为对等 IP 地址，以在远程网络位置和适用于网络的 Prisma Access 之间建立 IPSec 隧道。



2. 在 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息） > **Remote Networks**（远程网络）页面上，查看远程网络位置上该设备的 **Local**

 ©2025 Palo Alto Networks, Inc.

IP address（本地 **IP** 地址）。如果您在远程网络位置执行 NAT，则 **Local IP address**（本地 **IP** 地址）将显示设备 NAT 后的 IP 地址。

STEP 17 | 为了保护远程网络位置的流量，您必须创建安全策略规则。

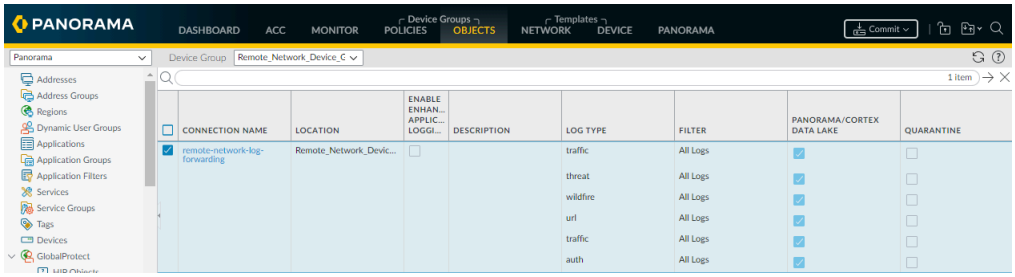
1. 选择 **Policies**（策略）。
2. 选择要添加策略规则的 **Device Group**（设备组）。您可以选择 Remote_Network_Device_Group，或您为保护远程网络位置定义策略时所选择的父设备组。
3. 创建安全策略规则。确保您没有定义允许将流量从任何区域传输到任何区域的安全策略规则。在安全策略规则中，使用您在模板中定义的区域。

   如果您网络上的用户被拒绝访问某个网站，请在向 Palo Alto Networks 开立工单之前报告网站访问问题。

STEP 18 | 启用将日志记录到 Strata Logging Service 的功能。您必须创建日志转发配置文件，并将其附加到想要转发日志所用的每个策略规则。

1. 选择 **Objects**（对象）> **Log Forwarding**（日志转发）。
2. 选择添加了策略规则的 **Device Group**（设备组），例如 Remote_Network_Device_Group。
3. **Add**（添加）日志转发配置文件在日志转发配置文件匹配列表中，**Add**（添加）您想要转发的每种 **Log Type**（日志类型）。
4. 选择 **Panorama/Strata Logging Service** 作为转发方法，使 Prisma Access 能够将日志转发到 Strata Logging Service。您将能够监控日志并从 Panorama 生成报告。Strata Logging Service 提供无缝集成来存储日志，而无需将其回传到公司总部的 Panorama，并且 Panorama 可以根据需要查询 Strata Logging Service。

   以下示例展示如何将流量、威胁预防、WildFire 提交、URL 过滤、数据过滤和身份验证日志转发到 Strata Logging Service。



5. 选择 **Policies**（策略）> **Security**（安全）并编辑策略规则。在 **Actions**（操作）中，选择您创建的日志转发配置文件。

STEP 19 | 将所有更改提交到 Panorama 并将配置更改推送到 Prisma Access。

1. 单击 **Commit**（提交）> **Commit and Push**（提交并推送）。
2. **Edit Selections**（编辑选择），在 **Prisma Access** 选项卡中，确保在 **Push Scope**（推送范围）中选择适用于网络的 **Prisma Access**，然后单击 **OK**（确定）。
3. **Commit and Push**（提交并推送）更改。

©2025 Palo Alto Networks, Inc.

STEP 20 | 检查远程网络状态。

有关详细信息，请参阅验证远程网络是否已连接到 Prisma Access。

©2025 Palo Alto Networks, Inc.

规划向新模式的迁移

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

新的 Prisma Access 远程网络部署的带宽在每个计算位置的聚合级别分配，也称为聚合带宽模型。在计算位置级别分配带宽可让您更灵活地分配许可的远程网络带宽，因为 Prisma Access 会根据负载或需求动态为每个位置分配带宽。

如果您的现有部署是按 Prisma Access 位置分配带宽，则可以迁移到聚合带宽模型。您还可以迁移远程网络 QoS 部署。当您迁移时，所有远程网络都使用聚合带宽模型。

使用以下检查清单来规划向聚合带宽模型的迁移：

- ❑ 请注意，以下远程网络组件在迁移后保持不变：
  - 数据平面没有任何更改。流量继续流经 Prisma Access 数据平面，不会对现有配置进行任何更改。
  - 迁移不会影响现有隧道。

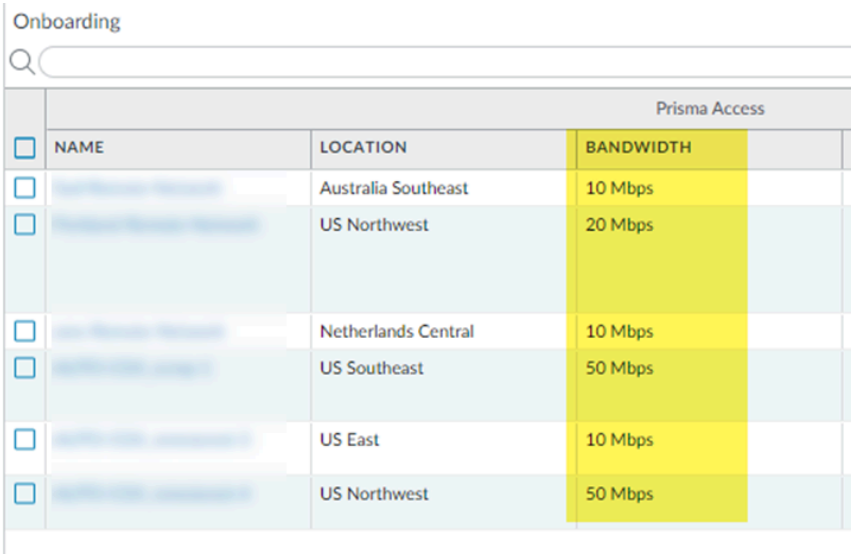
    无需重新配置 IPSec 隧道参数。IKE 网关、IKE 和 IPSec 加密配置文件以及 IPSec 隧道配置保持不变。
  - 将部署迁移到聚合带宽模型时，远程网络的服务 **IP** 地址（用于远程网络连接的 IPSec 隧道 Prisma Access 端的 公共 IP 地址）不会更改。
- ❑ Prisma Access 指定 IPSec 终止节点，并在迁移到聚合带宽模型期间为远程网络分配带宽。在迁移之前，您应该了解此模型的工作原理。

  如果要在迁移后将现有远程网络重新分配到另一个 *IPSec* 终止节点，则在您提交并推送更改后，*Prisma Access* 将为远程网络分配另一个服务 ***IP*** 地址。在这种情况下，您需要重新配置 *CPE* 以指向远程网络隧道的新 *IP* 地址。
- ❑ 如果您有不受支持的配置，则不会看到“Bandwidth Allocation（带宽分配）”选项卡，也不会查看用于迁移的横幅。以下配置不支持迁移到聚合带宽模型：
  - 带宽为 **1000 Mbps** 的远程网络。
  - Prisma SD-WAN CloudBlade 集成的 Prisma Access 版本低于 3.0。
  - 远程网络配置，为低于 2.1 Innovation 的远程网络站点的应用程序提供安全入站访问。

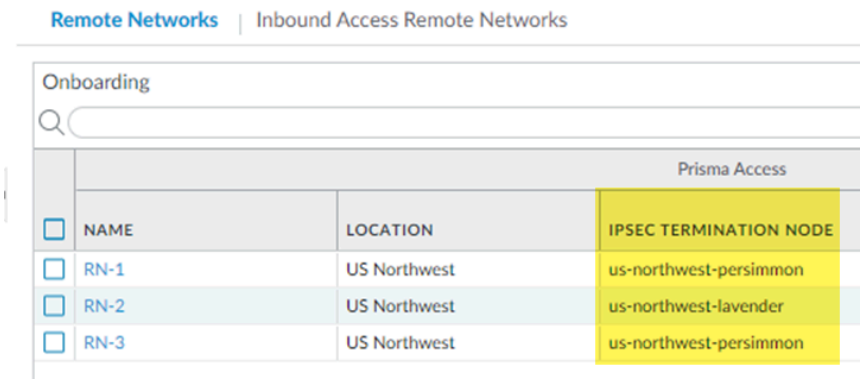
  如果您的远程网络使用 QoS，请确保在迁移之前遵循 QoS 迁移指南。

©2025 Palo Alto Networks, Inc.

- 如果您不确定您的部署使用的是哪种模式，请选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Remote Networks**（远程网络）。
  - 如果在远程网络区域看到 **Bandwidth**（带宽）字段，说明您正按 Prisma Access 位置分配带宽，此时您可迁移至聚合带宽模式。



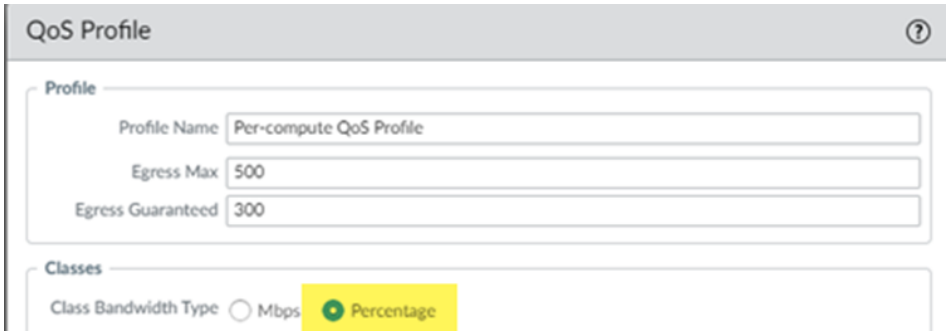
  - 如果您看到 **IPSec Termination Node**（**IPSec** 终止节点），则表示您已经迁移到聚合带宽模型。



- 在您迁移到聚合带宽模型后，此更改是永久性的，并且无法再恢复到按 Prisma Access 位置分配带宽的部署方式。
- 要迁移到聚合带宽模型，必须至少具有 50 Mbps 的可用带宽。

©2025 Palo Alto Networks, Inc.

- 如果要在迁移后实施 QoS，请了解为聚合带宽部署配置 QoS 的不同之处。
  - 请确保在您的服务质量（QoS）配置文件中使用 类别带宽类型（**Class Bandwidth Type**）为 **Percentage**（百分比），而非 **Mbps**。对于按计算位置分配带宽的部署，Prisma Access 不支持在 QoS 配置文件中使用 **Mbps** 这种带宽类型。



  - 了解如何指定保证带宽比率以及如何自定义每个站点的带宽。

    使用保证带宽比率，您可以在计算位置中分配总分配带宽的百分比。Prisma Access 将保证带宽除以计算位置中 IPSec 终止节点的数量。

    通过自定义每个站点的带宽，您可以在远程网络的 **Settings**（设置）中为站点应用单个 IPSec 终止节点的分配比率，并指定每个站点的 QoS 配置文件。或者，您也可以在远程网络配置期间指定 QoS 配置文件，方法是选择远程网络并在 **QoS** 选项卡中指定 QoS 配置文件。

- 如果您已将远程网络配置为提供对远程网络位置的安全入站访问，则支持所有现有的入站访问功能，例如启用辅助 WAN 链路（**Enable Secondary WAN**（启用辅助 **WAN**））、BGP、QoS 和源 NAT 选项。此外，Prisma Access 设备所分配的公共 IP 地址所消耗的带宽也不会发生变化（5 个 IP 地址会从您的远程网络许可证分配中占用 150 Mbps 带宽，10 个 IP 地址则会占用 300 Mbps 带宽）。

  如果您在迁移后需要配置入站访问，请使用特定于聚合带宽模型的入站访问过程。

- Palo Alto Networks 建议您在迁移前记下现有的带宽设置和总许可带宽。

  虽然 *Prisma Access* 在迁移期间迁移了带宽；但作为最佳实践，您应该记下当前设置，并在迁移后对计算位置带宽进行任何调整。

  - 要检查现有的带宽设置，请选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Remote Networks**（远程网络），并记下每个远程网络连接可用的现有 **Bandwidth**（带宽）。
  - 导航到 **Panorama** > **Licenses**（许可证），检查远程网络的总许可带宽 (Mbps)。此信息位于在 **Prisma AccessNet Capacity**（网络容量）或 **GlobalProtect Cloud Service for Mobile Users**（适用于移动用户的 **GlobalProtect** 云服务）下面，具体取决于您的许可证类型。

迁移后，请注意部署中的以下差异：

- 您将使用聚合带宽远程网络接入程序来接入所有新的远程网络。
- 在查看带宽使用统计信息时，您可以在每个 IPSec 终止节点级别查看这些信息。

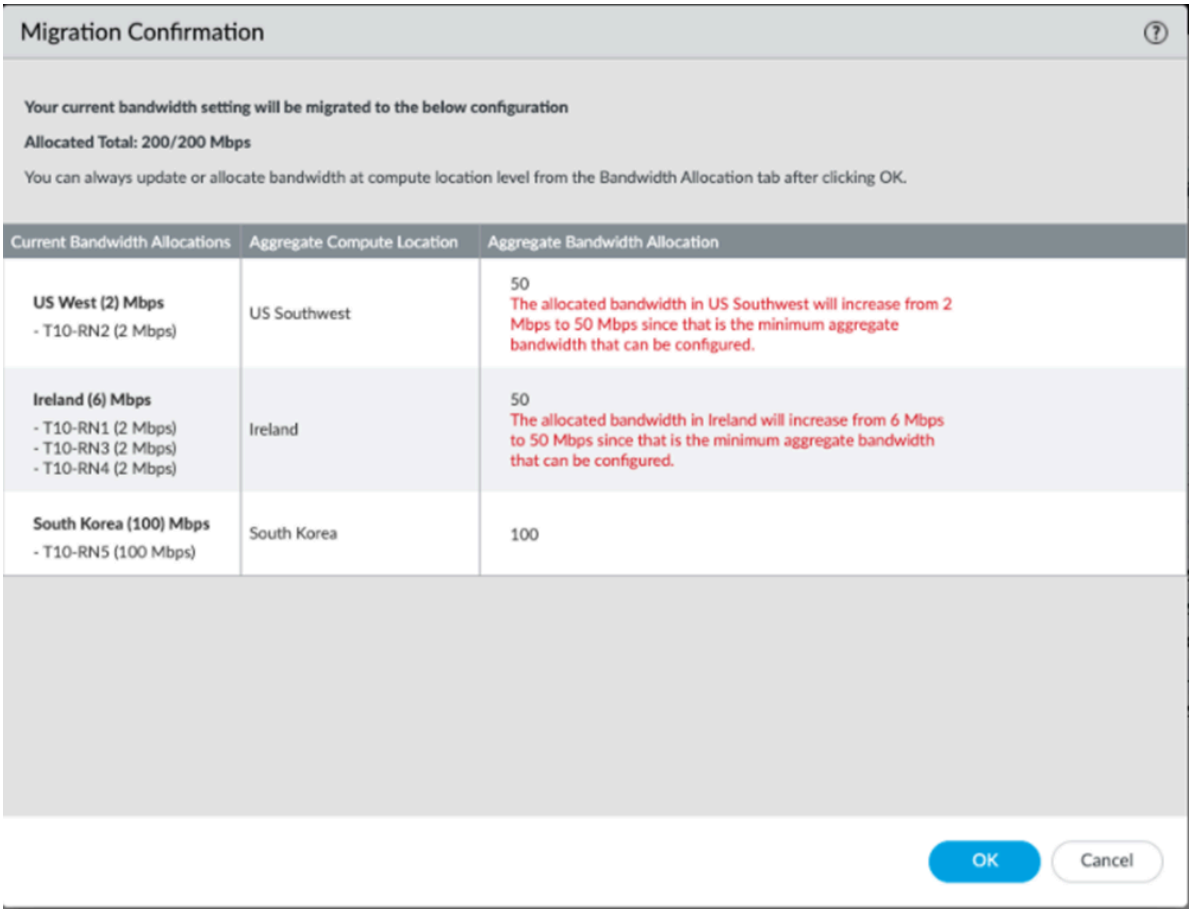
©2025 Palo Alto Networks, Inc.

迁移后聚合带宽部署的带宽分配

如果您的部署按 Prisma Access 位置分配带宽，Prisma Access 会在您迁移到聚合带宽模型后进行以下更改：

- Prisma Access 将给定计算位置中所有位置的带宽相加，并将相加后的带宽分配给该计算位置。

  例如，您在墨西哥西部、美国西南部和美国西部有三个位置（位置 **1**、位置 **2** 和位置 **3**），每个现有位置都有 50 Mbps 带宽。由于每个位置都位于美国西南计算位置，因此 Prisma Access 会将三个位置的带宽相加，并为美国西南位置分配 150 Mbps 的带宽。
- 如果计算位置中所有位置的总带宽小于 50 Mbps，则 Prisma Access 会将该计算位置的带宽增加到 50 Mbps。Prisma Access 为您提供在迁移过程中需要增加带宽的地点。



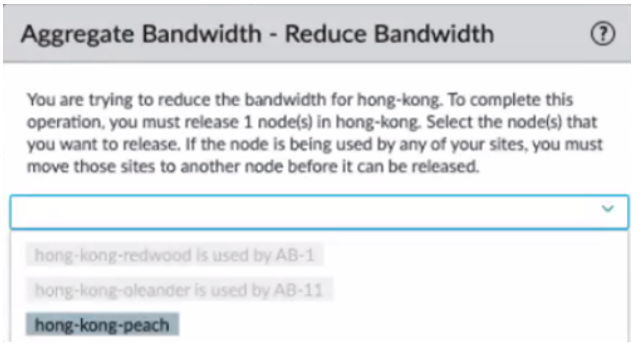
 ©2025 Palo Alto Networks, Inc.

- 在聚合带宽部署中，Prisma Access 使用 IPSec 终止节点。在迁移过程中，Prisma Access 设备会为每个计算位置按每分配 1000 Mbps 带宽配备一个 IPSec 终止节点。例如，如果您在计算位置分配了 1500 Mbps 的带宽，Prisma Access 会为该位置提供两个 IPSec 终止节点。

  在远程网络接入期间，您将 IPSec 终止节点分配给远程网络。在聚合带宽迁移中，Prisma Access 在迁移期间将 IPSec 终止节点与远程网络相关联。以下列表提供了迁移的 IPSec 终止节点关联的几个示例：

  - 如果您有四个远程网络位于同一计算位置，并且这些位置各有 50 Mbps 带宽，则 Prisma Access 会为该计算位置分配 200 Mbps 带宽，为该计算位置提供单个 IPSec 终止节点，并将该 IPSec 终止节点与所有四个远程网络相关联。
  - 如果您在同一计算位置有三个远程网络，每个网络有 100 Mbps，则 Prisma Access 会为该计算位置分配 300 Mbps 带宽，为该计算位置提供单个 IPSec 终止节点，并将该 IPSec 终止节点与所有三个远程网络相关联。
  - 如果您在同一个计算位置有七个远程网络，其中两个远程网络各有 500 Mbps，五个远程网络各有 100 Mbps，则 Prisma Access 会为该计算位置分配 1500 Mbps 的带宽。由于该计算位置中分配的总带宽大于 1000 Mbps，因此 Prisma Access 分配两个 IPSec 终止节点并进行以下关联：
    - 为两个 500 Mbps 远程网络分配一个 IPSec 终止节点（为每 1000 Mbps 远程网络分配一个节点）。
    - 五个 100 Mbps 远程网络被分配一个 IPSec 终止节点。

  迁移后，您可以更改 IPSec 终止节点关联以增大位置的带宽。例如，假设某个计算位置有两个 IPSec 终止节点，您可以将单个 IPSec 终止节点重新分配到单个位置，并将另一个 IPSec 终止节点重新分配到其余位置，这样实际上能让那个不与其他位置共享 IPSec 终止节点的位置获得更多带宽。
- 如果您大幅降低带宽，可能就必须得释放一个 IPSec 终止节点。例如，如果您将计算位置的带宽从 1500 Mbps 减少到 800 Mbps，则需要删除某个现有的 IPSec 终止节点。如果现有位置正在使用其中任何节点，则必须在删除 IPSec 终止节点之前重新分配 IPSec 终止节点。



QoS迁移指南

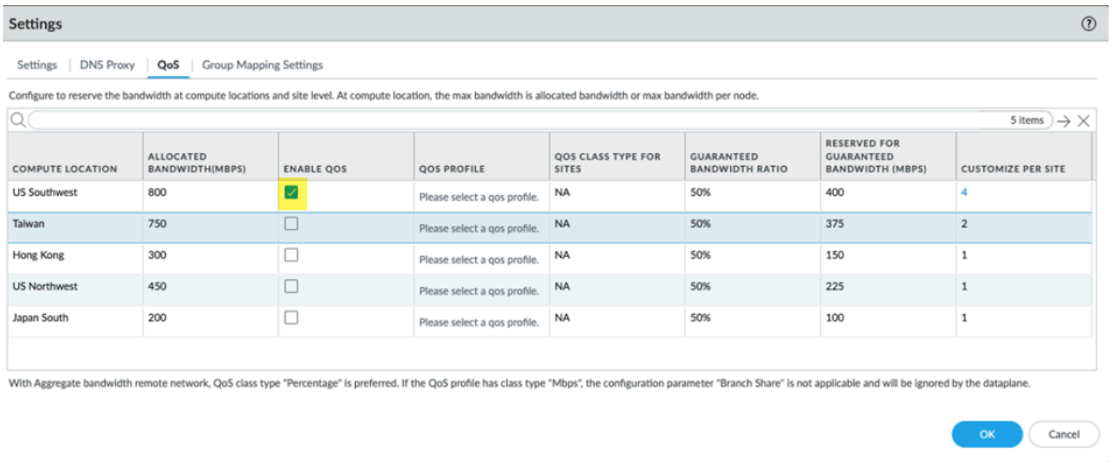
如果将 QoS 用于当前的 Prisma Access 远程网络部署，并且按位置分配带宽，则可以迁移到聚合带宽部署，同时仍保留现有 QoS 策略和配置文件。

使用聚合带宽模型，您可以为每个计算位置分配聚合级别的带宽，Prisma Access 会根据每个位置的负载或需求动态分配带宽。

 ©2025 Palo Alto Networks, Inc.

迁移后，**QoS** 选项卡将显示远程网络设置中的 QoS 配置（**Panorama** > **Cloud Services**（云服务）> **Configuration**（配置） > **Remote Networks**（远程网络） > **Settings**（设置））。任何映射到已启用 QoS 位置的计算位置，都会选中 **Enable QoS**（启用 **QoS**）；如果任何计算位置映射到未启用 QoS 位置的位置，都会取消选中 **Enable QoS**（启用 **QoS**）。

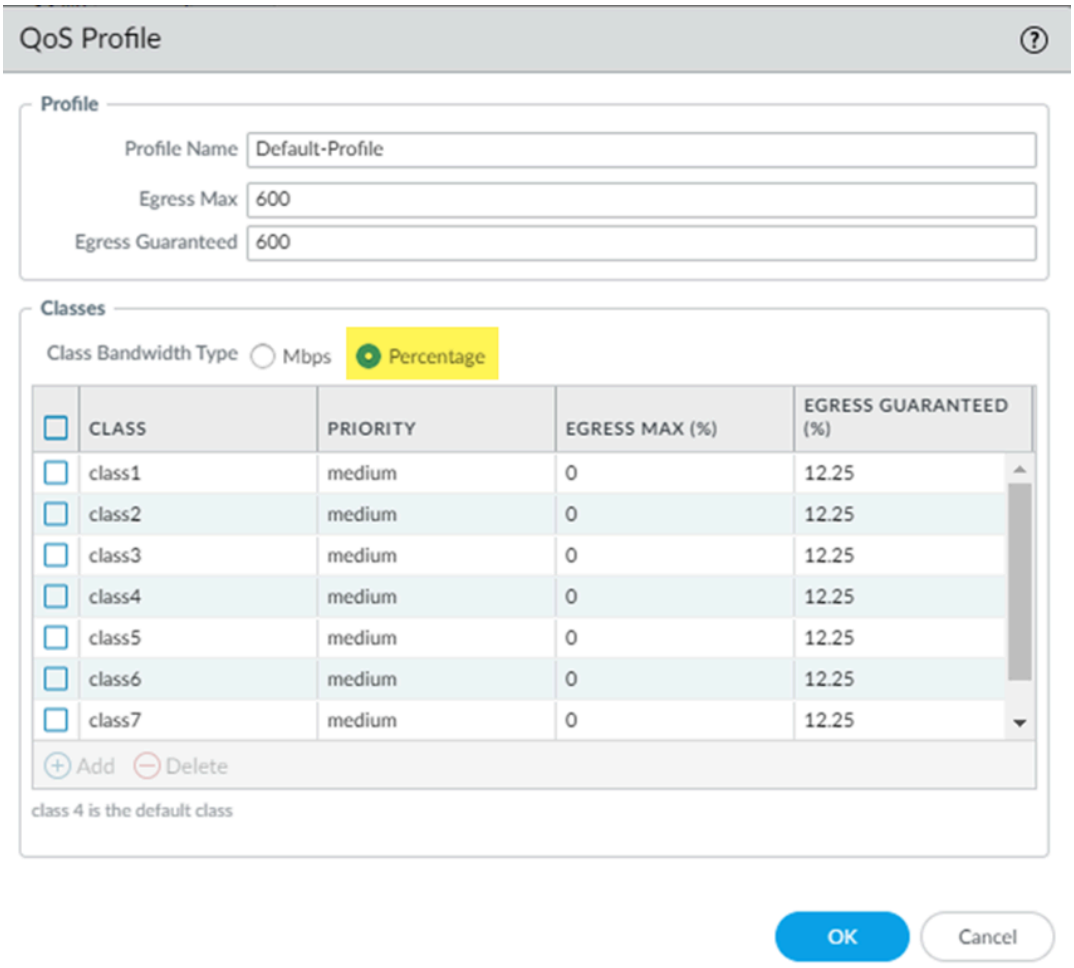
以下屏幕截图显示了迁移后的 QoS 选项卡示例。美国西部位置的远程网络启用了 QoS，其他位置未启用 QoS。由于美国西部位置映射到美国西南部计算位置，因此 **QoS** 选项卡显示为美国西南部计算位置启用的 QoS。



Palo Alto Networks 对聚合带宽部署中的 QoS 有以下建议和要求。

©2025 Palo Alto Networks, Inc.

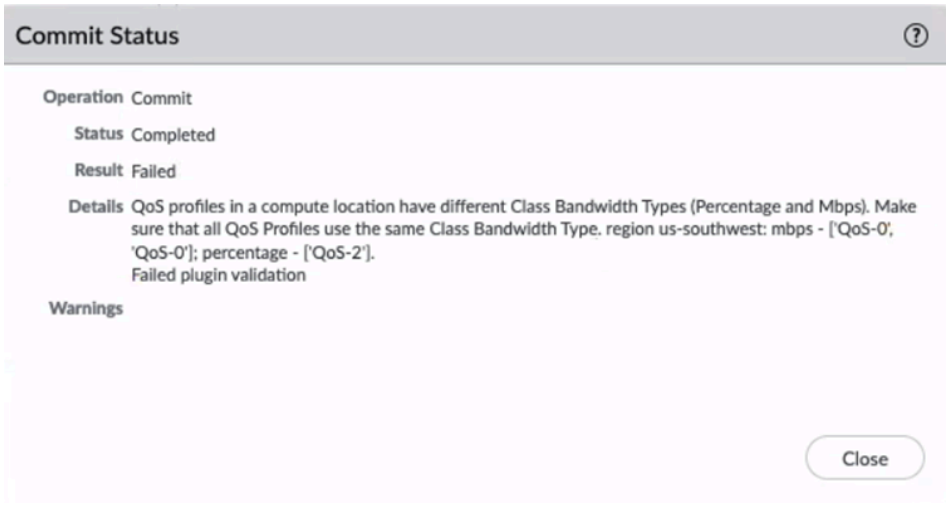
- 因为带宽是为单个计算位置中的所有位置共享的，所以应将 **Class Bandwidth Type**（类别带宽类型） 从 **Mbps** 更改为 **Percentage**（百分比）。仅当您已有一个按位置分配带宽的现有部署，并且随后迁移到聚合带宽部署时，才支持使用 **Mbps** 这种带宽类型。



- 您不能根据配置文件中的 Mbps 调整 QoS 带宽分配；对于使用 **Percentage**（百分比）带宽类型的配置文件，通过调整“Guaranteed Bandwidth Ratio（保证带宽比率）”和自定义每个站点的 QoS 配置文件便可以更改每个位置的 QoS 带宽。

 ©2025 Palo Alto Networks, Inc.

- 不能在计算位置混合带宽类型；如果混合，则在提交期间会收到错误消息。

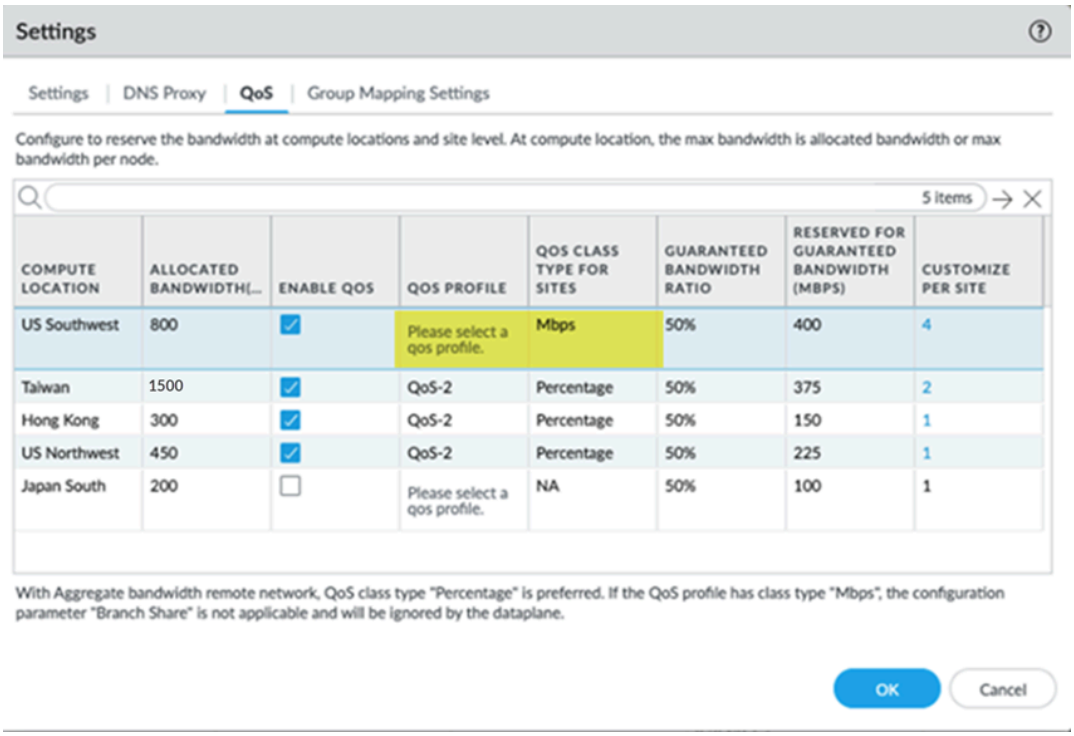


- 如果添加新位置，并且这些位置属于新的计算位置，则只能在新的计算位置中创建 **Class Bandwidth Type**（类别带宽类型）为 **Percentage**（百分比）的配置文件。
- 如果保留 **Class Bandwidth Type**（类别带宽类型）为 **Mbps** 的 QoS 配置文件，那么您对“Class Bandwidth Type（类别带宽类型）”所做的任何更改，或针对每个站点对 QoS 配置文件进行的自定义设置都将被忽略。
- 迁移后，如果有任何位置所使用的 QoS 配置文件将 **Class Bandwidth Type**（类别带宽类型）设置为 **Mbps**，则都会在 **QoS** 选项卡中为其相应的计算位置显示 **QoS Class Type For Sites**（站点的 **QoS** 类别类型）为 **Mbps**。**Class Bandwidth Type**（类别带宽类型）为 **Percentage**（百分比）的 QoS 配置文件显示**QoS Class Type For Sites**（站点的 **QoS** 类别类型）为 **Percentage**（百分比）。

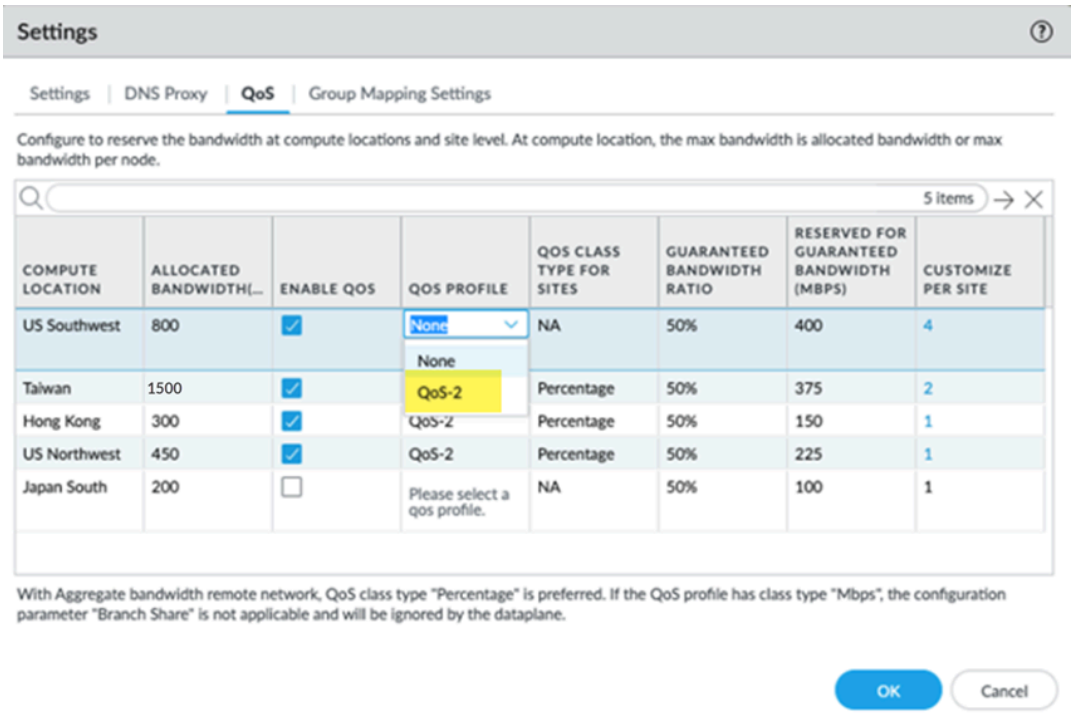
  此外，您不能选择 **Class Bandwidth Type**（类别带宽类型）为 **Mbps** 的任何 QoS 配置文件。以下屏幕截图显示了美国西南地区使用 QoS 配置文件的计算位置，该配置文件的 **Class**

 ©2025 Palo Alto Networks, Inc.

Bandwidth Type（类别带宽类型）为 **Mbps**。在 **QoS Profile**（**QoS** 配置文件）区域的下拉框中，无法选择此选项。

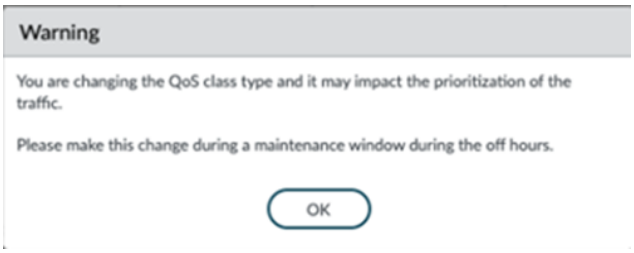


但是，您可以选择 **Class Bandwidth Type**（类别带宽类型）为 **Mbps** 的 QoS 配置文件（在本示例中为 QoS-2）。

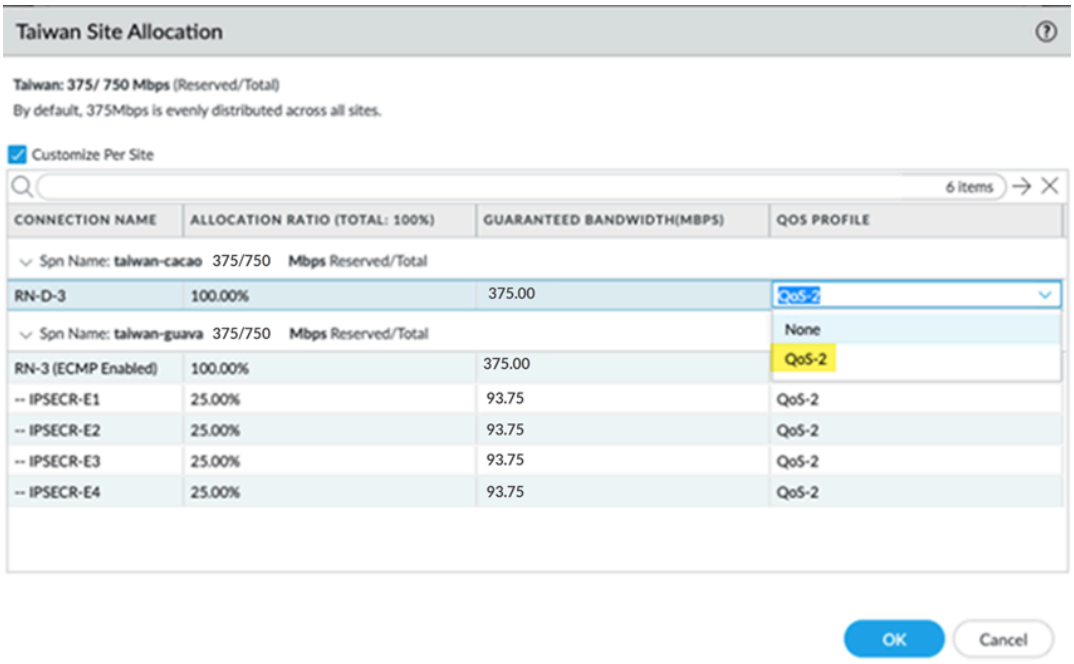


 ©2025 Palo Alto Networks, Inc.

- 如果将计算位置的 QoS 配置文件的 **Class Bandwidth Type**（类别带宽类型）从 **Mbps** 更改为 **Percentage**（百分比），则应在维护窗口或非高峰时段进行更改。更改 QoS 配置文件可能会更改流量优先级。



- 在自定义每个站点的 QoS 配置文件时，只能选择 **Class Bandwidth Type**（类别带宽类型）为 **Percentage**（百分比）的 QoS 配置文件。



迁移您的带宽管理设置

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

学习如何迁移您的带宽管理设置。

如果您有按位置分配带宽的 Prisma Access 远程网络部署，则 Prisma Access 允许您通过迁移到按计算位置分配带宽的部署（聚合带宽模型），使您的部署更加灵活和可伸缩。查看迁移规划清单后，使用以下步骤迁移到聚合带宽模型。您还可以迁移远程网络 QoS 部署。当您迁移时，所有远程网络都使用聚合带宽模型。

©2025 Palo Alto Networks, Inc.

在迁移带宽设置之前，请记住以下几点：

- 以下远程网络组件在迁移后保持不变：
  - Prisma Access 数据平面。
  - 对现有隧道没有影响。
  - 不会重新配置 IPSec 隧道参数。
  - IKE 网关、IKE 和 IPSec 加密配置文件以及 IPSec 隧道配置保持不变。
  - 每个远程网络的 **Service IP Address**（服务 **IP** 地址）不会改变。
- Prisma Access 指定 IPSec 终端节点，并在迁移到聚合带宽模型期间为远程网络分配带宽。
- 如果您有不受支持的配置，则不会看到“Bandwidth Allocation（带宽分配）”选项卡，也不会查看用于迁移的横幅。
- 如果您的远程网络具有 QoS，请确保在迁移之前遵循 QoS 迁移指南。
- 在您迁移到聚合带宽模型后，此更改是永久性的，并且无法再恢复到按 Prisma Access 位置分配带宽的部署方式。
- 要迁移到聚合带宽模型，必须至少具有 50 Mbps 的可用带宽。
- 如果要在迁移后实施 QoS，请了解为聚合带宽部署配置 QoS 的不同之处。
- 迁移完成后，您将使用聚合带宽远程网络接入程序来接入所有新的远程网络。
- 迁移后，在查看带宽使用统计信息时，您可以在每个 IPSec 终端节点级别查看这些信息。
- 不要使用 CLI 执行迁移。仅使用 UI 进行迁移。
- Strata Cloud Manager
- Panorama

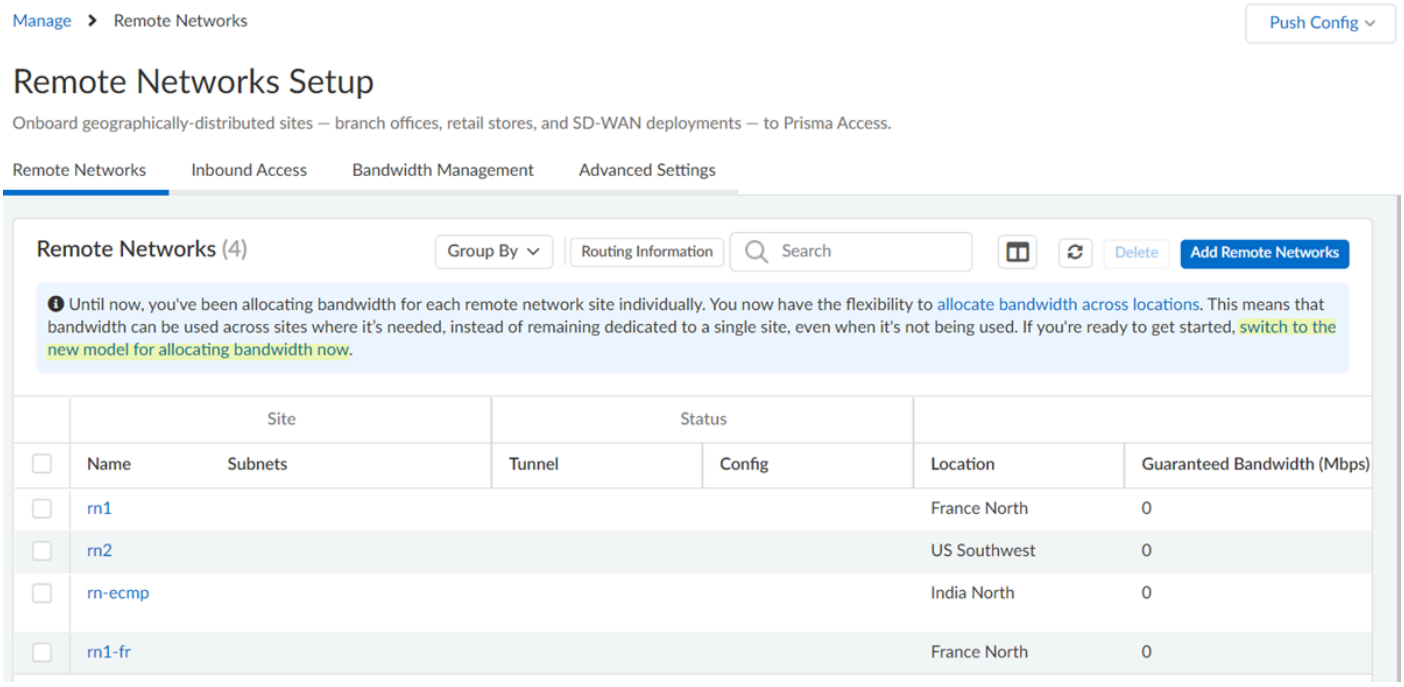
迁移您的带宽管理设置 (Strata Cloud Manager)

如果您有按位置分配带宽的 Prisma Access 远程网络部署，则 Prisma Access 允许您通过迁移到按计算位置分配带宽的部署（聚合带宽模型），使您的部署更加灵活和可伸缩。查看迁移规划清单后，使用以下步骤迁移到聚合带宽模型。

STEP 1 | 选择 **Workflows**（工作流） > **Prisma Access** 设置 > **Remote Networks**（远程网络）。

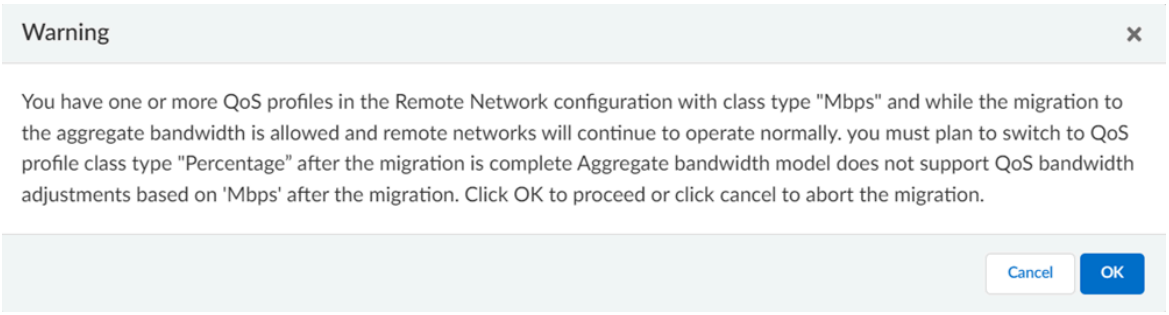
©2025 Palo Alto Networks, Inc.

STEP 2 | 现在切换到分配带宽的新模式。

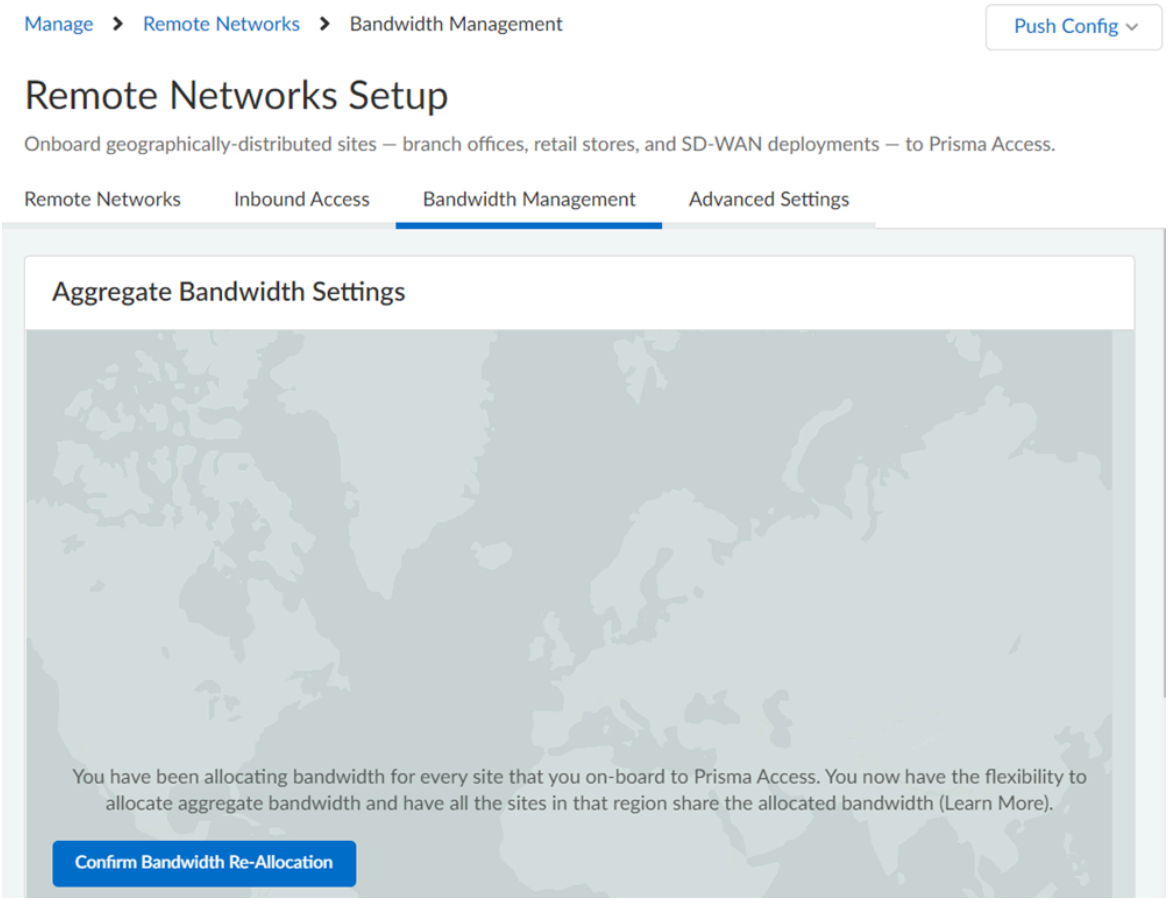


©2025 Palo Alto Networks, Inc.

- 如果您的 QoS 配置文件的 ***Class Bandwidth Type***（类带宽类型）设置为 ***Mbps***，则 *Prisma Access* 会通知您，您应该计划将这些配置文件的 ***Class Bandwidth Type***（类带宽类型）设置为 ***Percentage***（百分比）。



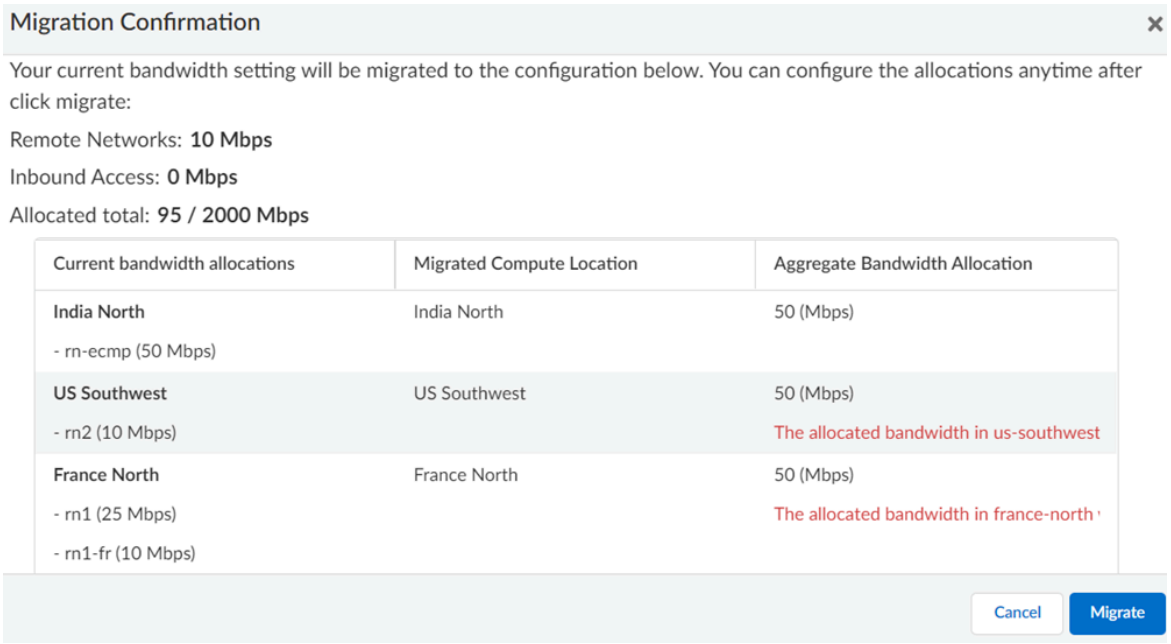
- 或者，在 ***Bandwidth Management***（带宽管理）选项卡中，选择 ***Confirm Bandwidth Re-Allocation***（确认带宽重新分配）。



 ©2025 Palo Alto Networks, Inc.

STEP 3 | 查看相关信息，然后在显示的弹出窗口中选择 **Migrate**（迁移）。

如果计算位置中所有位置的总带宽小于 *50 Mbps*，则 *Prisma Access* 会将该计算位置的带宽增加到 *50 Mbps*。*Prisma Access* 为您提供在迁移过程中需要增加带宽的位置。



迁移到聚合带宽模型是永久性且不可逆的过程。迁移之前，请查看迁移前检查清单。必须 ***Commit and Push***（提交并推送）您的更改，才能使其生效。

Prisma Access 会将分配的远程网络带宽迁移到聚合带宽模型。

STEP 4 | **Commit and Push**（提交并推送）更改。

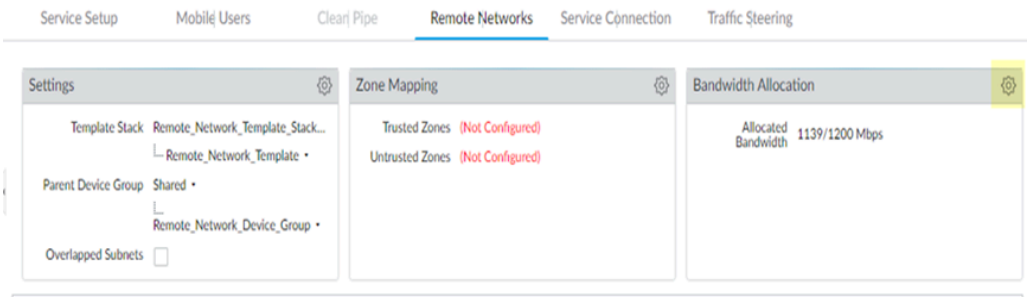
迁移您的带宽管理设置 (Panorama)

如果您有按位置分配带宽的 Prisma Access 远程网络部署，则 Prisma Access 允许您通过迁移到按计算位置分配带宽的部署（聚合带宽模型），使您的部署更加灵活和可伸缩。查看迁移规划清单后，使用以下步骤迁移到聚合带宽模型。

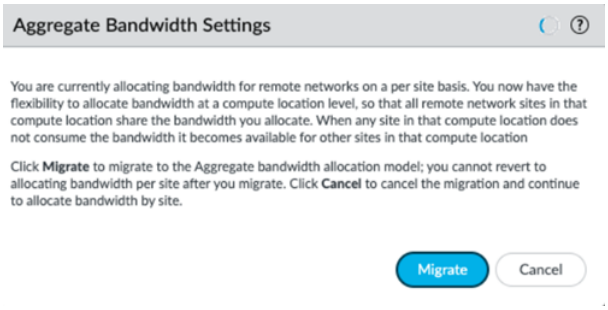
STEP 1 | 选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Remote Networks**（远程网络）。

 ©2025 Palo Alto Networks, Inc.

STEP 2 | 通过单击 **Bandwidth Allocation**（带宽分配）区域中的齿轮图标来编辑设置。

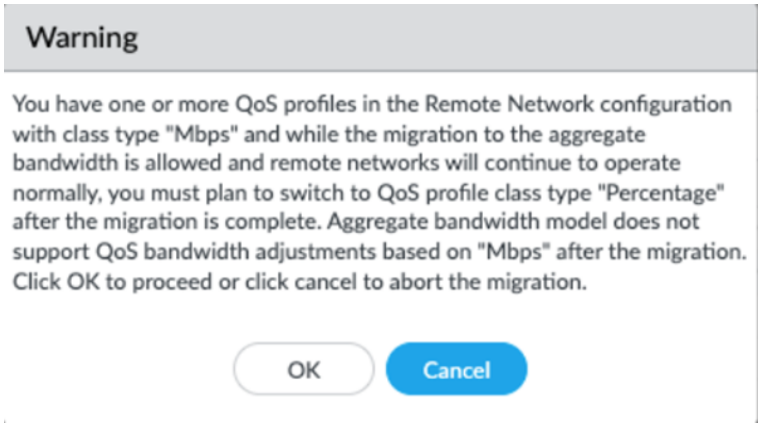


STEP 3 | 在显示的弹出窗口中选择 **Migrate**（迁移）。



迁移到聚合带宽模型是永久性且不可逆的过程。迁移之前，请查看迁移前检查清单。必须 ***Commit and Push***（提交并推送）您的更改，才能使其生效。

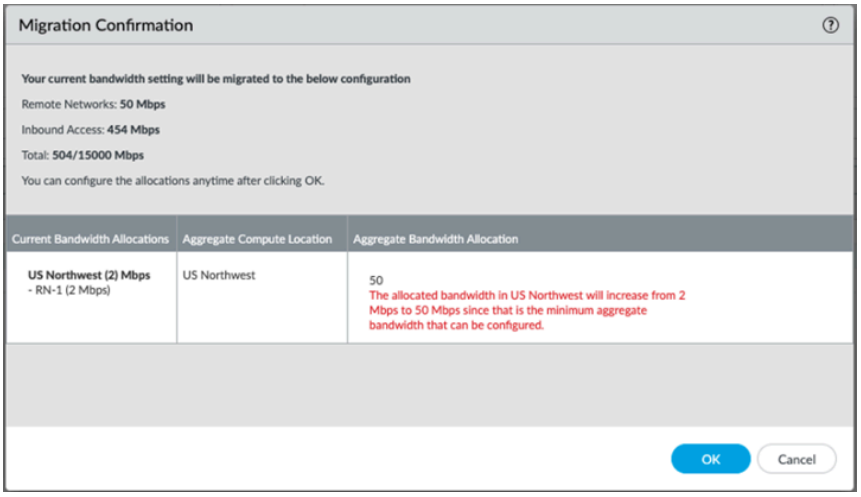
如果您的 *QoS* 配置文件的 ***Class Bandwidth Type***（类带宽类型）设置为 ***Mbps***，则 *Prisma Access* 会通知您，您应该计划将这些配置文件的 ***Class Bandwidth Type***（类带宽类型）设置为 ***Percentage***（百分比）。



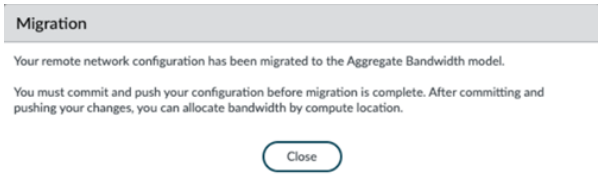
 ©2025 Palo Alto Networks, Inc.

STEP 4 | 查看 **Migration Confirmation**（迁移确认）窗口中的信息；然后，单击 **OK**（确定）。

如果计算位置中所有位置的总带宽小于 *50 Mbps*，则 *Prisma Access* 会将该计算位置的带宽增加到 *50 Mbps*。*Prisma Access* 为您提供在迁移过程中需要增加带宽的位置。



Prisma Access 会将分配的远程网络带宽迁移到聚合带宽模型并显示确认窗口。单击 **Close**（关闭）以关闭窗口。



STEP 5 | **Commit and Push**（提交并推送）更改。

 ©2025 Palo Alto Networks, Inc.

加入远程网络

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

规划好远程网络后，即可开始配置过程。这包括加入远程网络、将远程网络站点连接到 Prisma Access 以及为远程网络启用路由和 QoS。对于要使用 Prisma Access 保护网络的每个远程网络，将所需的策略配置推送到 Prisma Access 并加入每个远程网络，以便可以开始通过 IPSec 隧道将流量从远程站点发送到 Prisma Access。根据您的带宽分配类型，使用以下步骤之一来加入远程网络：

了解如何加入远程网络。

- Strata Cloud Manager
- Panorama

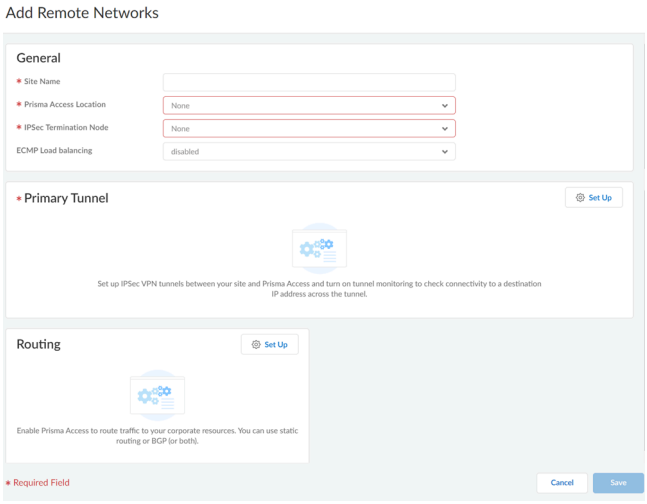
接入远程网络 (Strata Cloud Manager)

下面介绍如何将新的远程网络站点添加到 Prisma Access。首先要指定位置并定义要分配给连接的带宽量。

STEP 1 | 启动 Prisma Access (Managed by Strata Cloud Manager)。

STEP 2 | 确保您已为将要部署远程网络的位置分配带宽。请参阅远程网络规划清单。

STEP 3 | 转至 **Workflows**（工作流） > **Prisma Access** 设置 > **Remote Networks**（远程网络） > **Add Remote Networks**（添加远程网络）。



STEP 4 | 为远程网络提供一个描述性的 **Site Name**（站点名称）。

©2025 Palo Alto Networks, Inc.

STEP 5 | 选择站点所在的 **Region**（区域），然后选择最近的位置 Prisma Access **Location**（位置）。

STEP 6 | （仅当您计划使用 BGP 进行动态路由时）启用 **ECMP Load Balancing**（**ECMP** 负载均衡），以便远程网络站点可以使用多达四个 IPSec 隧道。

BGP 是 ECMP 负载均衡所必需的；不支持 QoS 和静态路由。

启用 ECMP 时，远程网络流量将在您配置的隧道上进行负载均衡。

STEP 7 | 配置 **Advanced Settings**（高级设置）。

- （可选）使用 **Static Entries**（静态条目）将 FQDN 解析为特定 IP 地址。

  如果您的组织有访客互联网服务，并且您希望访客安全地使用搜索引擎，防止他们搜索可能不当或冒犯的资料（这可能违反公司政策），则这个功能将非常有用。要做到这一点，请分别在 **Name**（名称）、**FQDN** 和 **Address**（地址）为静态条目规则输入唯一名称、FQDN 以及应将 FQDN 请求定向到的 IP 地址。



- 如果您希望 Prisma Access 代理 DNS 请求，请为 **UDP Queries Retries**（**UDP** 查询重试次数）配置相关值（**Interval (Sec)**（间隔时间（秒）），即重试查询的时间间隔（以秒为单位），以及要执行的重试次数（在 **Attempts**（次数）中配置）。

STEP 8 | 将远程网络站点连接到 Prisma Access，您将在其中创建 IPSec VPN 隧道以将远程网络站点连接到 Prisma Access。

STEP 9 | 配置静态路由。

1. 如果使用静态路由来路由往返于总部或数据中心的流量，请选择 **Add**（添加）以添加要在分支机构保护的 IP 子网或 IP 地址。

   如果对总部或数据中心网络上的 IP 子网进行任何更改，则必须手动更新静态路由。

STEP 10 | 配置动态路由。

1. 如果使用动态路由来通告总部或数据中心子网，请选择 **Enable BGP for Dynamic Routing**（为动态路由启用 **BGP**）。
2. （可选）选择 **MRAI Timer**（**MRAI** 计时器）值。

   BGP 路由提供一个计时器，您可以使用它来定制网络中的 BGP 路由收敛，称为最小路由通告间隔 *(MRAI)*。MRAI 用于对每个目标的更新进行速率限制，BGP 路由器至少需等待所配置的 MRAI 时间，然后才能发送前缀相同的通告。数字越小，收敛时间就越快，但能在网络中创建的通告也越多。数字越大，可发送的通告数量就越少，但也会使路由收敛

 ©2025 Palo Alto Networks, Inc.

速度变慢。由您来决定在网络中输入的具体数字，以便在更快的路由收敛和更少的通告数量之间取得最佳平衡。

将 MRAI 范围配置为 1 到 600 秒，默认值为 30 秒。

3. 要减少通过 BGP 向客户终端设备 (CPE) 通告的移动用户 IP 子网的数量，请选择 **Summarize Mobile User Routes before advertising**（在通告之前汇总移动用户路由），以指定 Prisma Access 在通告之前汇总子网。

   默认情况下，Prisma Access 以 /24 子网的形式通告移动用户的 IP 地址池；如果将它们汇总起来，Prisma Access 会根据您指定的子网来通告该池。例如，Prisma Access 使用 /20 子网通告公共用户移动 IP 池 10.8.0.0/20，而不是在通告之前将池划分为 10.8.1.0/24、10.8.2.0/24、10.8.3.0/24 等子网。汇总这些通告可以减少 CPE 路由表中存储的路由数量。例如，您可以将 IP 池汇总与可接受有限数量路由的云 VPN 网关（虚拟专用网关 (VGW) 或传输网关 (TGW)）结合使用。

4. （可选）要让 Prisma Access 使用 eBGP 为远程网络发起默认路由通告，请选择 **Advertise the Default Route**（通告默认路由）。确保您的网络没有由 BGP 通告的其他默认路由，否则可能会在网络中引入路由问题。

5. （可选）如果您配置了辅助广域网，并且需要更改辅助（备份）BGP 对等体的对等体地址，请选择 **Use different BGP Peer for Secondary Tunnel**（使用不同的 **BGP** 对等体作为辅助隧道），然后输入唯一的对等体，或者输入辅助广域网的本地 IP 地址。

6. （自选）选择 **Do Not Export Routes**（不导出路由），以防止 Prisma Access 将路由转发到总部或数据中心。

   默认情况下，Prisma Access 通告所有 BGP 路由信息，包括本地路由以及它从其他服务连接、远程网络和移动用户子网收到的所有前缀。选中此复选框可防止 Prisma Access 发送任何 BGP 通告，但仍使用其收到的 BGP 信息从其他 BGP 邻居学习路由。

   如果您选择此选项，*Prisma Access* 不会发送 *BGP* 通告，因此您必须在本地设备上配置静态路由以建立返回 *Prisma Access* 的路由。

7. 输入分配给总部或数据中心网络上的 eBGP 路由器作为路由器 ID 的 **Peer IP Address**（对等体 **IP** 地址）。

8. 输入 **Peer AS**（对等 **AS**），即您网络的自治系统 (AS)。

   使用符合 RFC 6996 标准的 BGP 私有 AS 编号。

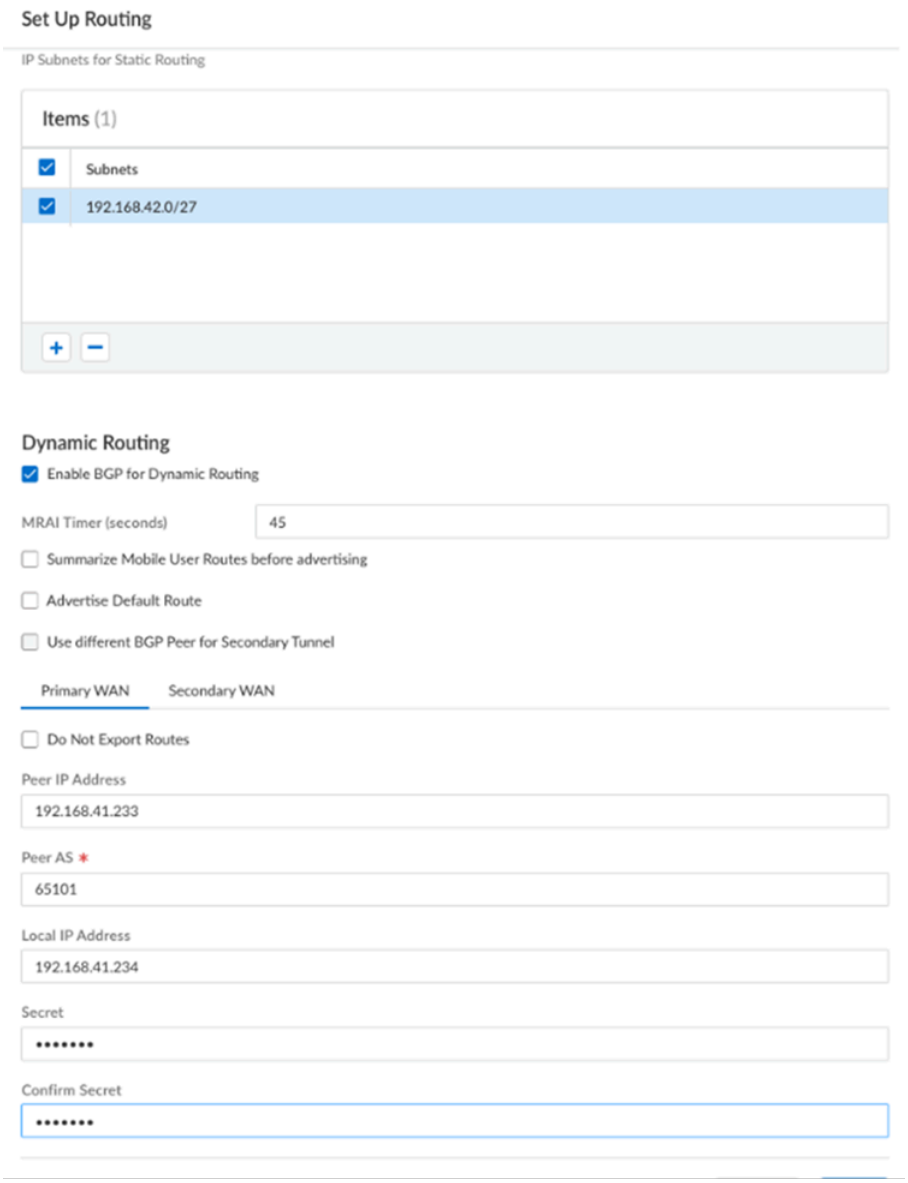
9. 输入 Prisma Access 用作 BGP 的本地 IP 地址的 **Local IP Address**（本地 **IP** 地址）。

   仅当总部或数据中心设备需要本地地址才能成功建立 BGP 对等互连时，才需要本地地址。确保指定的地址不会与基础设施子网或远程网络中的子网中的 IP 地址产生冲突或重叠。

10. 输入用于对 BGP 对等体通信进行身份验证的 **Secret**（机密）密码。

©2025 Palo Alto Networks, Inc.

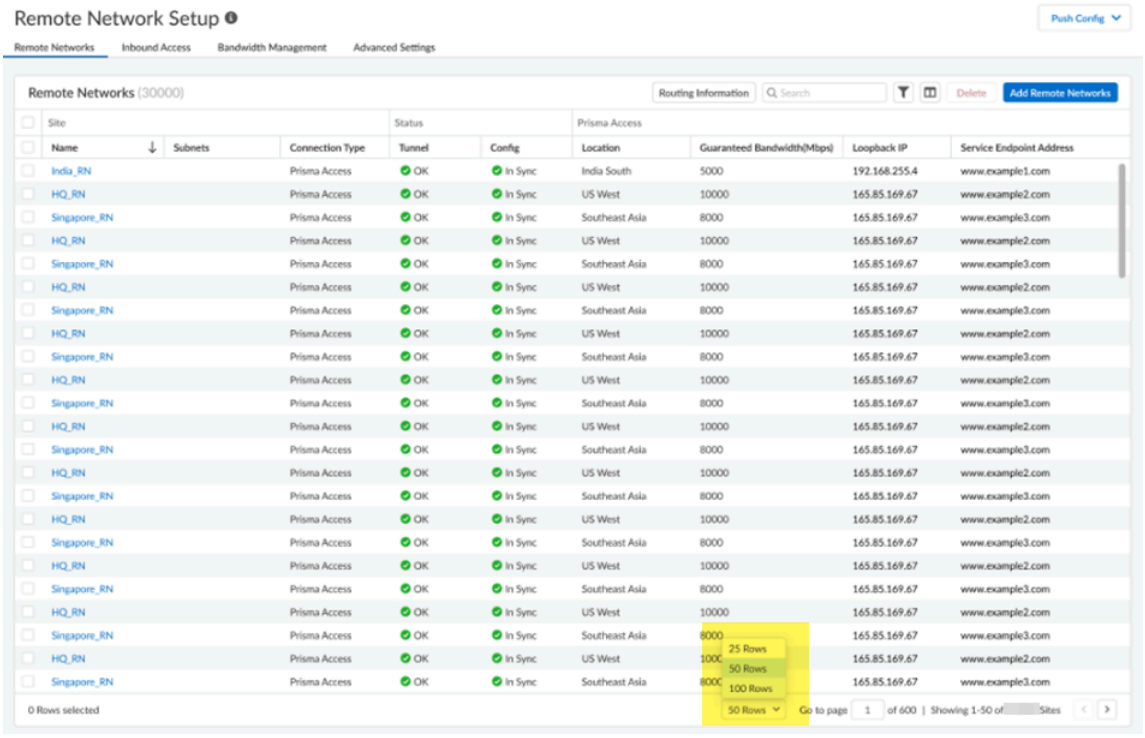
11. 选择 **Confirm Secret**（确认机密）。



从 *Prisma Access 5.2* 开始，在 *Prisma Access* 部署中，每个租户最多可以接入 *25,000* 个远程网络和 *50,000* 个 *IKE* 网关。为了适应这一增强功能，对 *Strata Cloud Manager Web* 界面进行了以下更改：

- 启用了分页，您可以选择在给定页面中显示多少行。

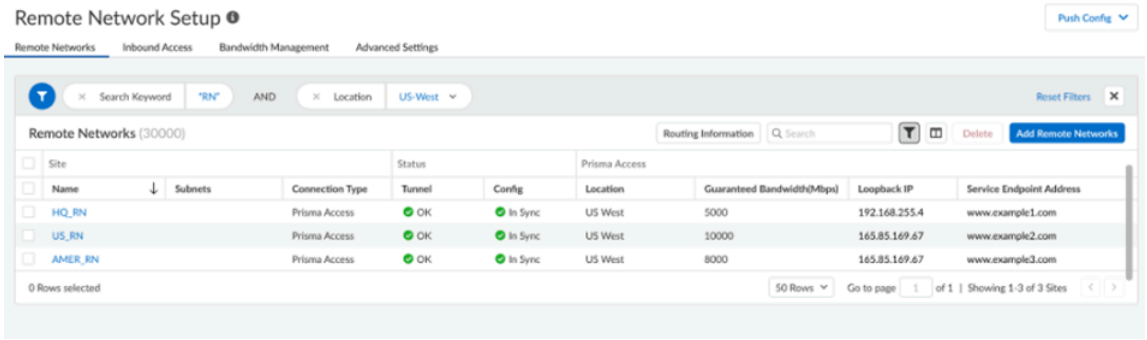
©2025 Palo Alto Networks, Inc.



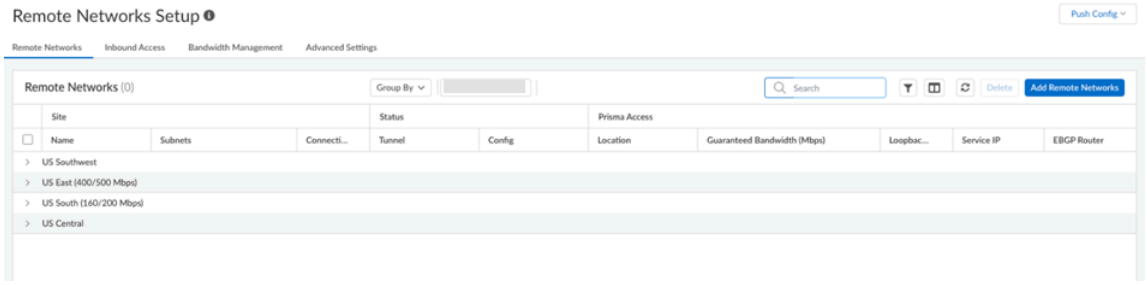
 ©2025 Palo Alto Networks, Inc.

- 支持对远程网络进行过滤。

  应用过滤后，您可以按名称对生成的输出进行排序。



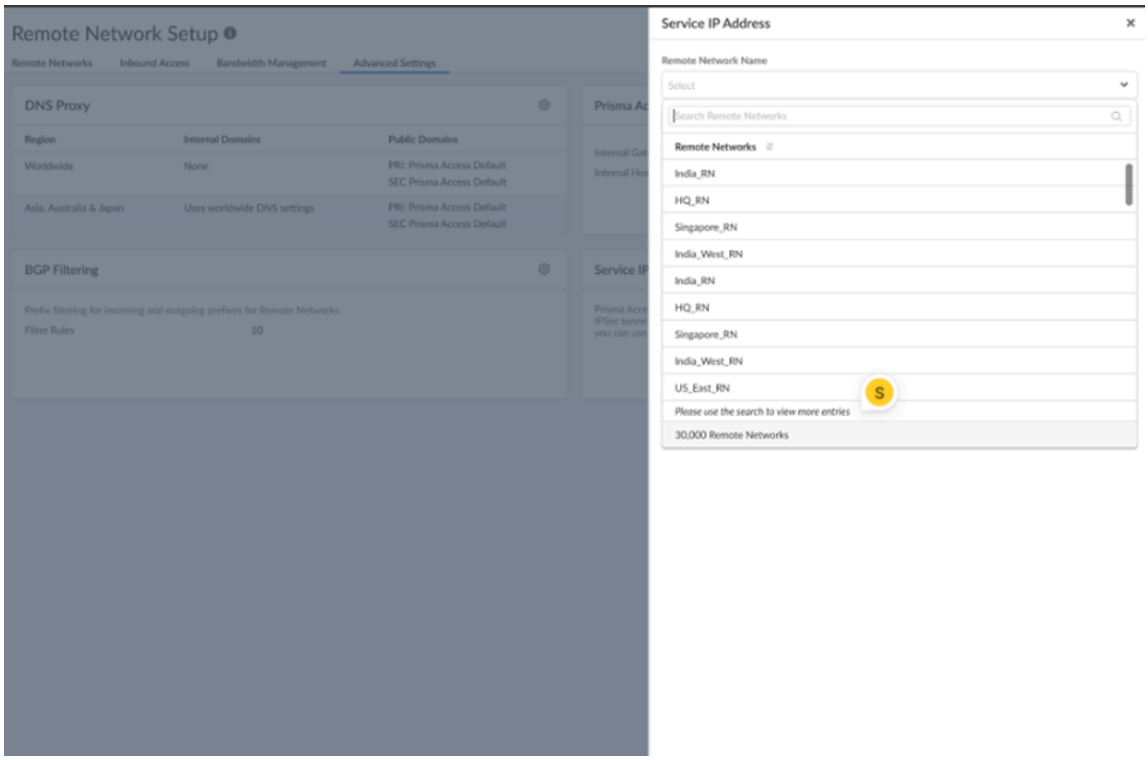
- 新增了 **Group By**（分组依据）字段。如果您选择按 **Compute Location**（计算位置）进行分组，则会显示所有组（但处于折叠状态），并且您选择的页面大小适用于这些组。如果您选择了一个计算位置以将其展开，则将根据您选择的页面大小显示行。



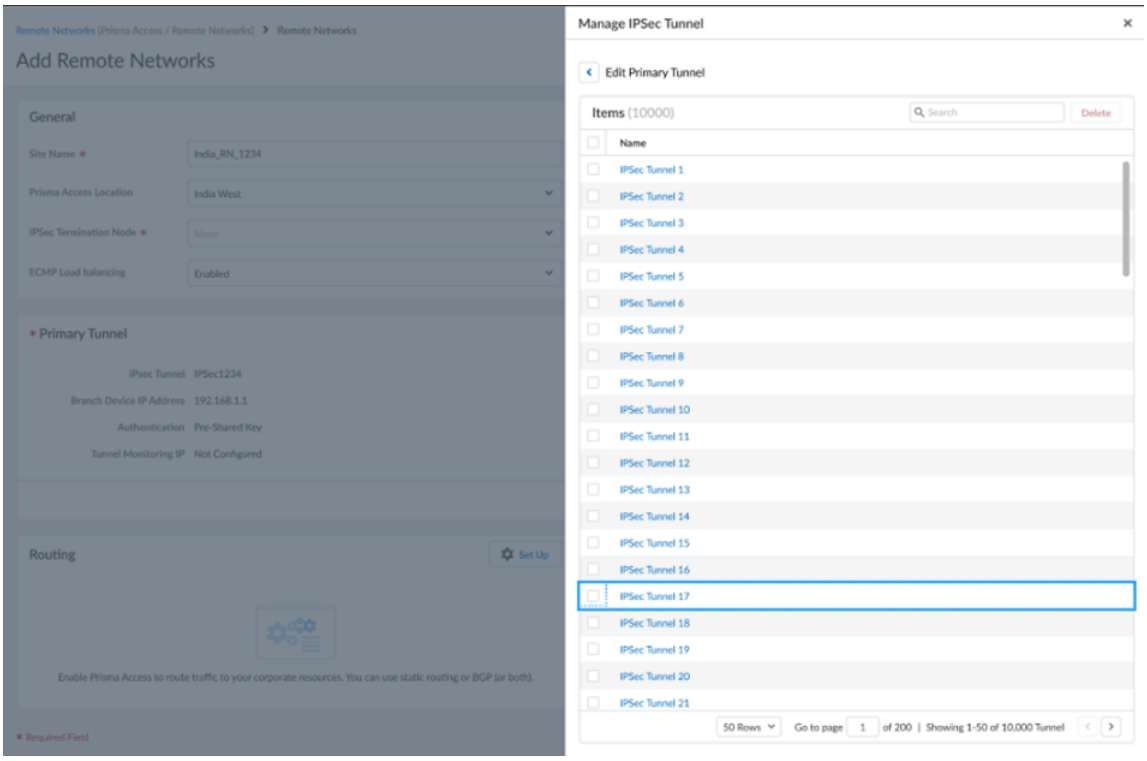
- 当远程网络显示在下拉菜单中时，UI 会显示前 500 个项目。通过在文本框中键入内容，便可以在列表中找到所需的远程网络。

  此外，还会显示远程网络的总数。

©2025 Palo Alto Networks, Inc.

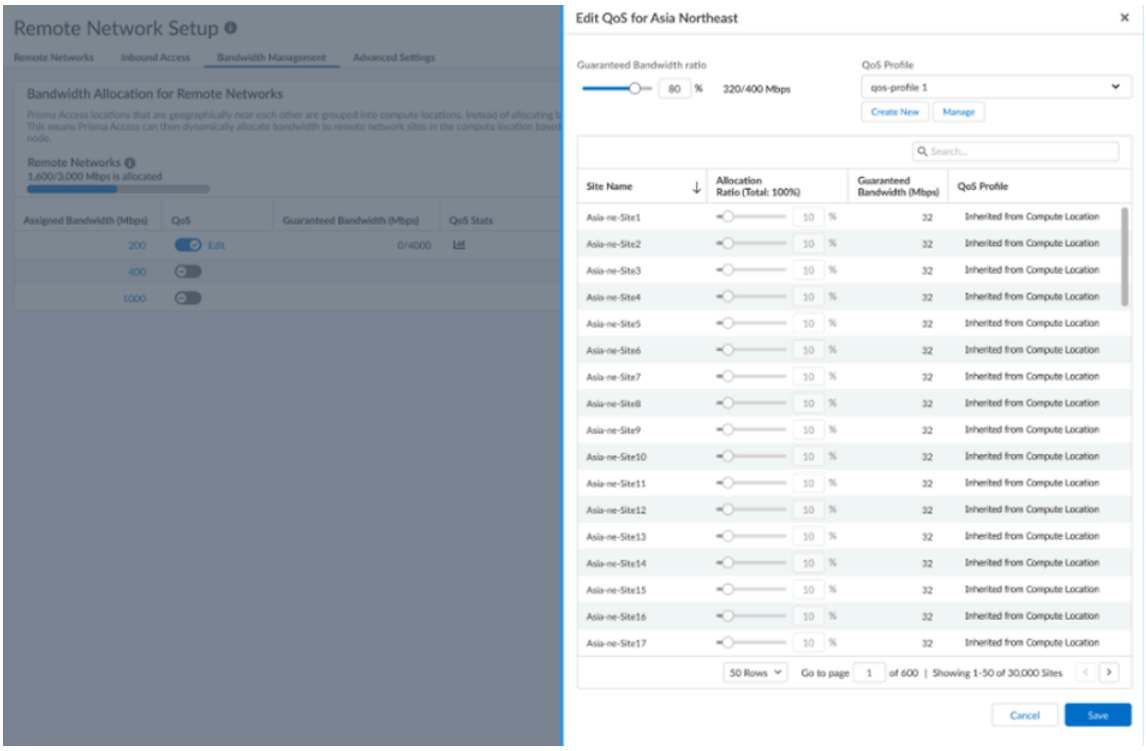


- 以下附加页面已应用分页：
  - IPSec Tunnels（IPSec 隧道）：

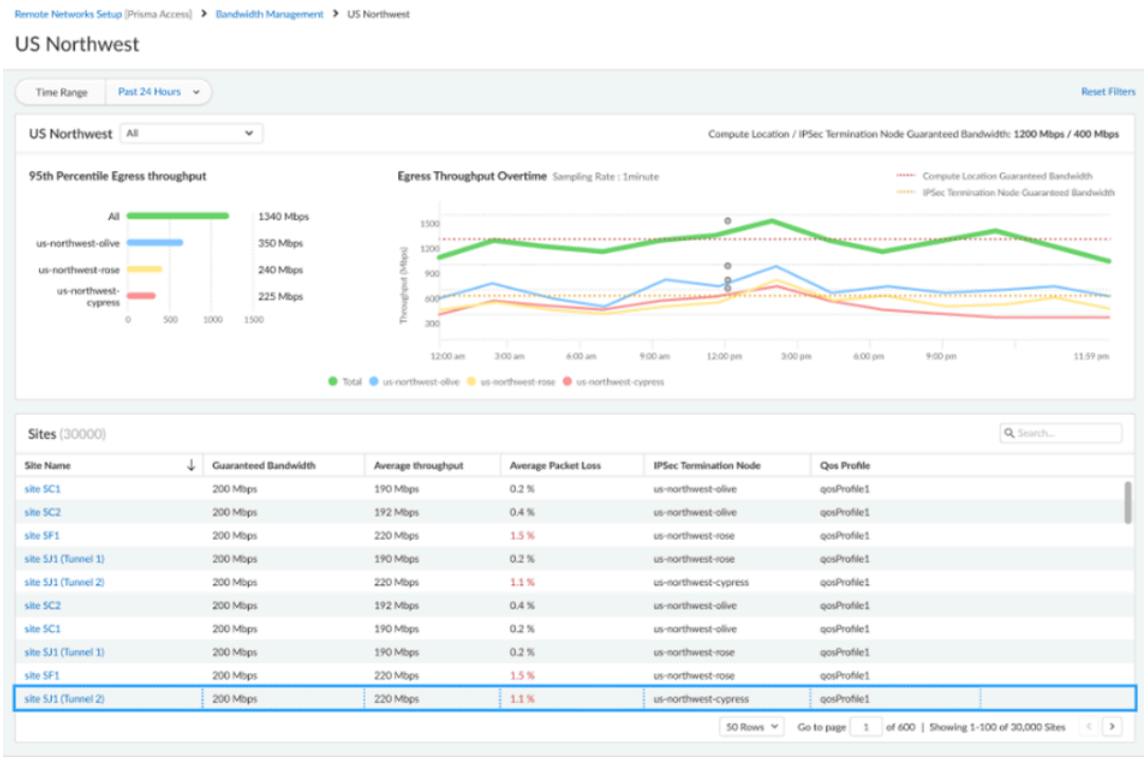


  - QoS：

 ©2025 Palo Alto Networks, Inc.

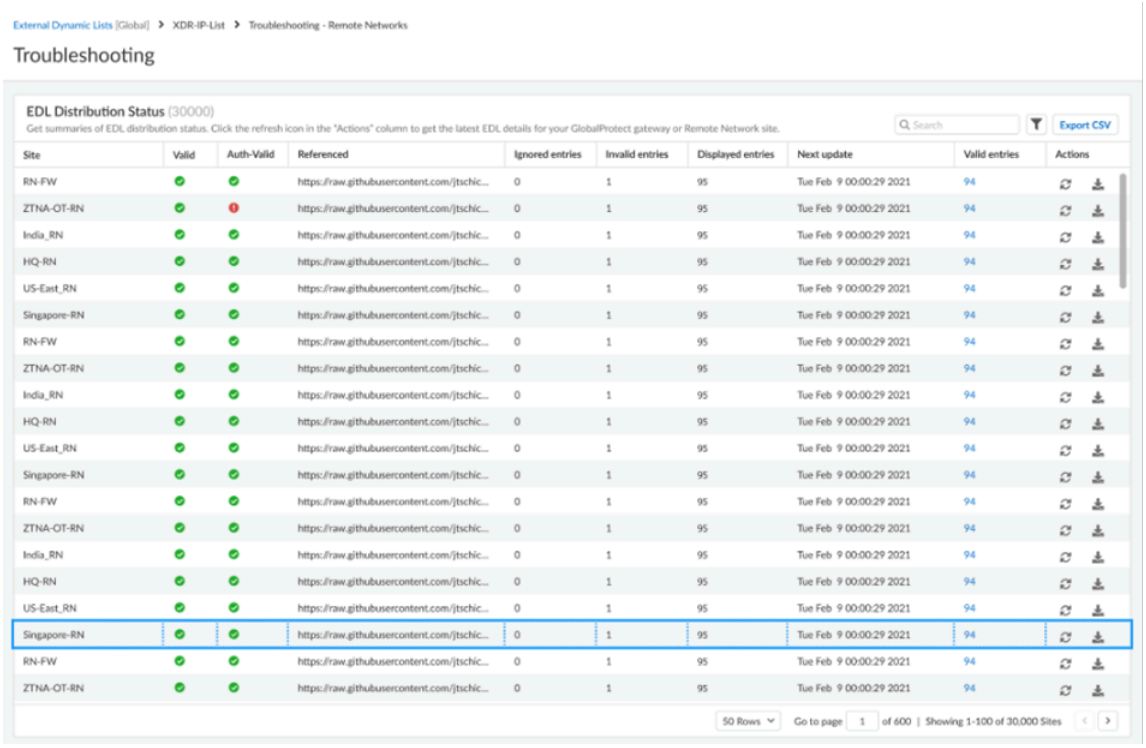


- QoS Statistics（QoS 统计信息）：



- **External Dynamic Lists**（外部动态列表）下面的 **Troubleshooting**—**Remote Networks**（故障排除 - 远程网络）：

 ©2025 Palo Alto Networks, Inc.



接入远程网络 (Panorama)

要配置按计算地点分配带宽的 Prisma Access 远程网络部署，请完成以下步骤。

如果您需要加入多个远程网络（最多 *1,000* 个），则可以使用以下步骤加入远程网络，然后将远程网络配置导出到 CSV 文件，将要加入的其他远程网络添加到 *CSV* 文件中，然后导入 *CSV* 文件以将配置保存到 *Prisma Access* 中。

STEP 1 | 选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Remote Networks**（远程网络），然后单击 **Settings**（设置）区域中的齿轮图标以编辑设置。

1. 在“Templates（模板）”部分，选择 **Add**（添加）可添加任何模板，但其中必须包含您想要推送到适用于网络的 Prisma Access 的配置。例如，如果您已有包含区域配置或 IPSec 隧道、IKE 网关或加密配置文件设置的模板，您可以将这些模板添加到预定义的 Remote_Network_Template_Stack 中，以简化接入流程。

   您可以在该模板堆栈中 添加（**Add**）多个模板，然后使用 上移（**Move Up**）和 下移（**Move Down**）功能对它们进行适当排序。这一点很重要，因为 Panorama 在堆栈中从上到下进行评估，堆栈中较高模板中的设置优先于堆栈中较低模板中指定的相同设置。请注意，您无法将默认模板从模板堆栈的顶部移走。

   尽管您可以从插件中将现有的模板添加到模板堆栈中，但无法通过该插件创建新的模板。相反，请使用添加新模板的工作流。

2. 为适用于远程网络的 Prisma Access 选择 **Parent Device Group**（父设备组）。您可以选择现有设备组，也可以使用 **Shared**（共享）。

   您将推送所有配置，包括安全策略、安全配置文件以及其他策略对象（如应用程序组和对象、地址组）、主机完整性策略对象和配置文件以及身份验证策略，适用于网络的

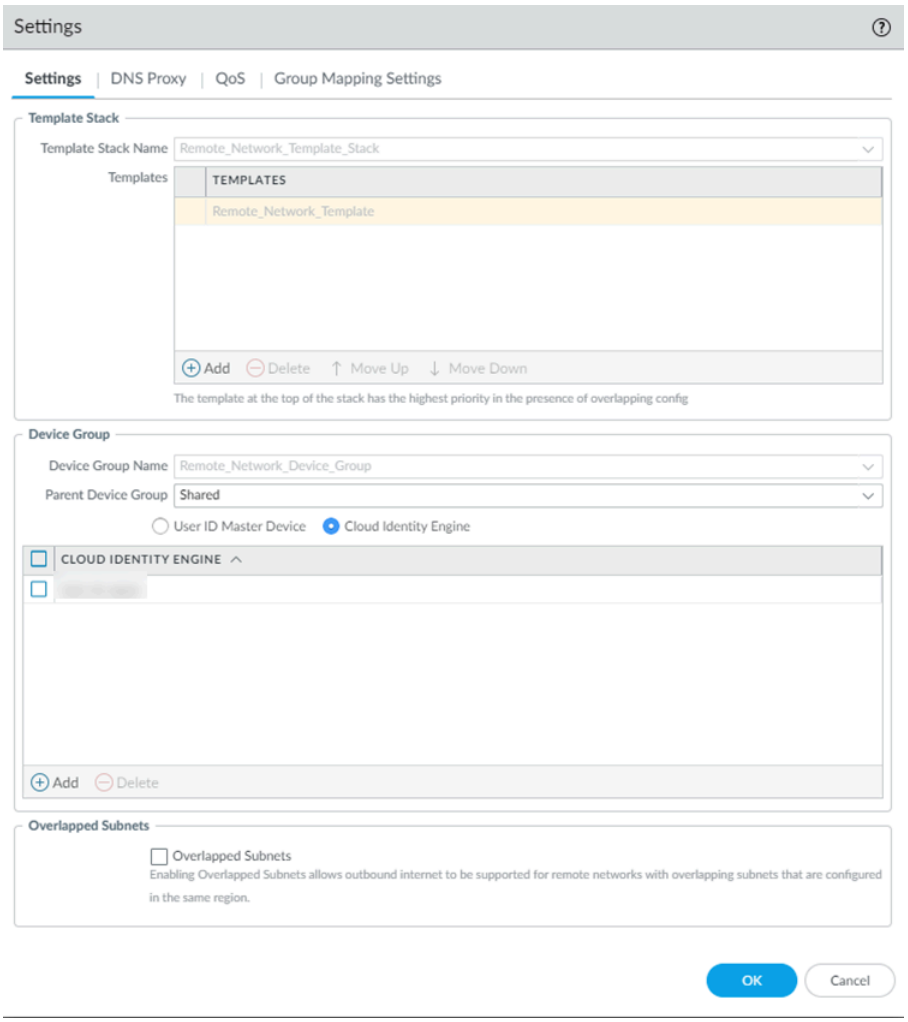
 ©2025 Palo Alto Networks, Inc.

Prisma Access 需要使用您在此处指定的 设备组层次结构，向您的远程网络用户实施一致的策略。

现在还不需要定义要推送到远程网络的所有策略。相反，请配置设置以接入远程站点。然后，您可以返回并添加具有完整配置的模板和设备组，以将一致的策略推送到您的远程网络。

3. （可选）如果您已将新一代防火墙配置为主设备，或者添加了 Cloud Identity Engine 配置文件以便使用户和组信息在安全策略中变为可选，请选择 **User-ID Master Device**（**User-ID** 主设备）或 **Cloud Identity Engine**；然后，选择您所创建的主设备或 Cloud Identity Engine 配置文件。
4. 如果您将配置的远程网络中存在子网重叠情况，请选中 **Overlapped Subnets**（重叠子网）复选框，从而为这些位置启用出站互联网访问功能。

   虽然配置 Remote Network Locations with Overlapping Subnets（带有重叠子网的远程网络位置）会带来一些限制，但在某些情况下（例如，您想要在零售商店位置添加一个访客网络），这是可以接受的。



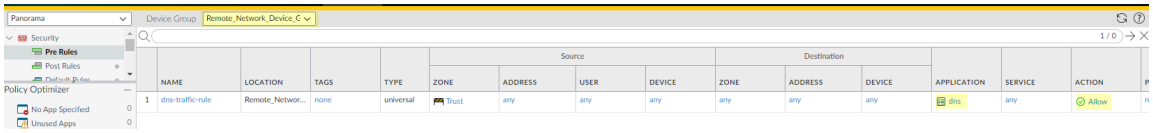
 ©2025 Palo Alto Networks, Inc.

STEP 2 | （可选）为远程网络配置 **DNS Proxy**（**DNS** 代理）设置。

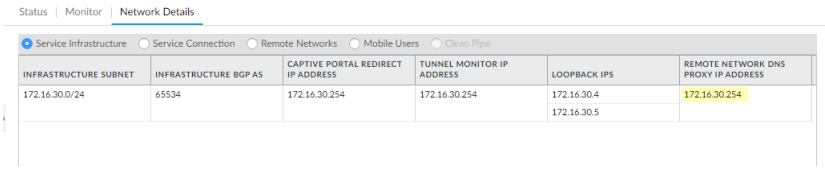
Prisma Access 允许您指定 DNS 服务器来解析组织内部域和外部域。如果未指定任何设置，则 Prisma Access 不会代理远程网络的 DNS 请求。

1. 在 **Remote_Network_Device_Group** 设备组中，选择 **Policies**（策略） > **Security**（安全），然后选择 **Add**（添加）以添加一条安全策略规则，其 **Application**（应用程序）设置为 **DNS**，**Action**（操作）设置为 **Allow**（允许），以便允许 DNS 流量。

   如果没有允许 DNS 流量的安全策略规则，则不会进行 DNS 解析。



2. 如果配置 Prisma Access 以代理来自远程网络的 DNS 请求，请更新该网络中所有终结点上的 DNS 设置，以使用 Prisma Access 远程网络 **DNS** 代理 **IP** 地址作为主 DNS 服务器，并使用您的 DNS 服务器作为辅助 DNS 服务器。您可以从 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详情） > **Service Infrastructure**（服务基础设施）中获取此 DNS 代理 IP。



3. 选择 添加（**Add**）以添加一个或多个 **DNS Proxy**（**DNS** 代理）设置，并输入以下值：

   - 从窗口顶部的下拉列表中选择 **Region**（区域）。

     选择 **Worldwide**（全球）以便在全球范围内应用 DNS 设置，或者选择特定大区，又或者选择按位置组（规模小于大区的一组位置）来设置。如果您添加了多个设置，那么首先会应用位置组设置，其次是大区设置，最后是全球范围的设置。Prisma Access 会按列表从上到下的顺序来评估这些规则。

   - **Add**（添加）一条或多条规则来配置 **Internal Domains**（内部域）的 DNS 设置。
     - 在 **Rule Name**（规则名称）中输入规则的唯一名称。
     - 如果您希望内部 DNS 服务器仅解析您指定的域，请在 **Domain Lists**（域列表）中输入要解析的域。在域前面指定一个星号；例如 *.acme.com。最多可以指定 1024 个域条目。
     - 如果您具有可以访问内部域的 **Custom DNS server**（自定义 **DNS** 服务器），请指定 **Primary DNS**（主 **DNS**）和 **Secondary DNS**（辅助 **DNS**）服务器的 IP 地址，或

 ©2025 Palo Alto Networks, Inc.

选择 **Use Cloud Default**（使用云默认设置）以使用 Prisma Access 的默认 DNS 服务器。

- 指定 **Public Domains**（公共域）的 DNS 设置。
  - **Use Cloud Default**（使用云默认值）—使用默认的 Prisma Access DNS 服务器。
  - **Same as Internal Domains**（与内部域相同）—使用您用于解析内部域的同一服务器。选择此选项时，用于解析公共域的 DNS 服务器与 **Internal Domains**（内部域）部分中第一条规则配置的服务器相同。
  - **Custom DNS server**（自定义 **DNS** 服务器）—如果您有可以访问公共（外部）域的 DNS 服务器，请在该字段中输入主 DNS 服务器地址。

  （可选）您可以依次选择 **Add**（添加）和 **DNS Suffix**（**DNS** 后缀）来添加客户端 DNS 后缀列表，以指定在用户输入了客户端无法解析的不合格主机名时应该在本地使用的后缀（例如 acme.local）。请勿在域名后缀前输入通配符 **(*)** 字符（例如 acme.com）。可以添加多个后缀。
- 如果您希望 Prisma Access 代理 DNS 请求，请为 UDP 查询配置相关值（**Interval**（间隔时间），即重试查询的时间间隔（以秒为单位），以及要执行的重试次数（在 **Attempts**（次数）中配置）。

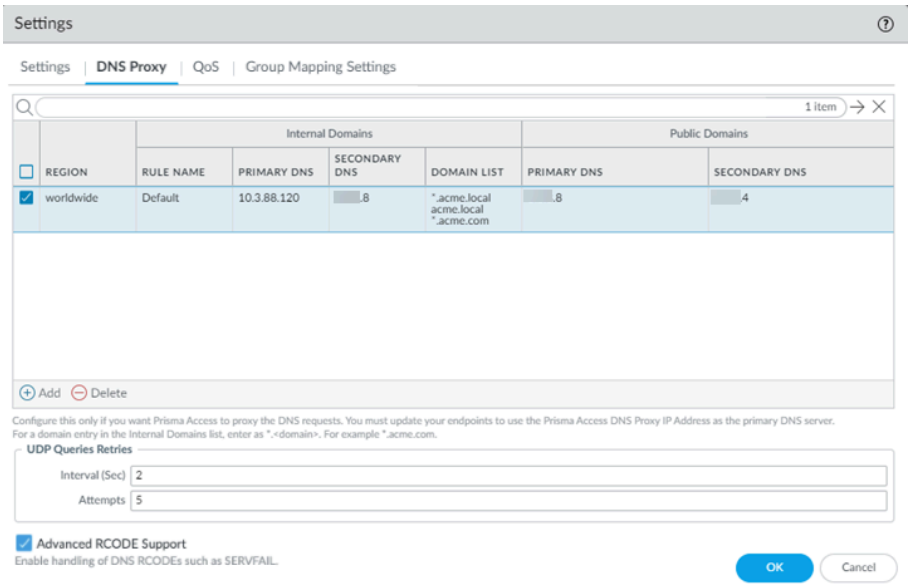
  如果您希望 Prisma Access 为您的 GlobalProtect 用户代理 DNS 请求，您必须更新端点，以使用 远程网络 **DNS** 代理 **IP** 地址（**Remote Network DNS Proxy IP Address**）作为主 DNS 服务器（**Panorama** > **Cloud Services**（云服务） >

 ©2025 Palo Alto Networks, Inc.

Status（状态） > **Network Details**（网络详细信息） > 服务基础设施（**Service Infrastructure**））。

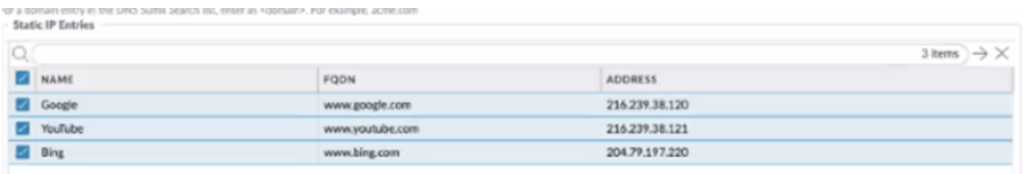
4. （可选）选择 Advanced RCODE Support（高级 RCODE 支持）可在收到 RCODE 2 (SERVFAIL) 和 RCODE 5 (REFUSED) DNS 返回码的情况下让主 DNS 服务器故障转移到辅助 DNS 服务器。

   DNS 响应代码 SERVFAIL 表示与主 DNS 服务器的通信错误，DNS 响应代码 REFUSED 表示主 DNS 服务器拒绝提供请求的信息。在这两种情况下，服务都会故障切换到辅助 DNS 服务器。



5. （可选）使用 **Static Entries**（静态条目）以将 FQDN 解析为特定的 IP 地址。

   如果您的组织有访客互联网服务，并且您希望访客安全地使用搜索引擎，防止他们搜索可能不当或冒犯的资料（这可能违反公司政策），则这个功能将非常有用。要做到这一点，请分别在 **Name**（名称）、**FQDN** 和 **Address**（地址）为静态条目规则输入唯一名称、FQDN 以及应将 FQDN 请求定向到的 IP 地址。



STEP 3 | （可选）为您的远程网络部署启用 **QoS**，并指定 **QoS Profile**（服务质量配置文件）、**Guaranteed Bandwidth Ratio**（保证带宽比率）、**Reserved for Guaranteed Bandwidth (Mbps)**（为保证带宽预留的值 **(Mbps)**），并且可选择按位置自定义站点选项（**Customize Per Site**（按站点自定义））。

在计算位置级别启用 QoS；但当您在后面的步骤中添加远程网络时，您可以指定启用或禁用每个站点的 QoS，并可指定每个站点的 QoS 配置文件。在配置 QoS 前，您应当理解 QoS 如何作用于按计算位置分配带宽的远程网络，包括指定保证带宽和按站点定制带宽。

©2025 Palo Alto Networks, Inc.

STEP 4 | （可选）配置 **Group Mapping Settings**（组映射设置），以使 Prisma Access 能够利用 Cloud Identity Engine 的目录同步组件来检索用户和组信息。

在使用 **Group Mapping Settings**（组映射设置）在 Prisma Access 中启用组映射之前，必须将 Cloud Identity Engine 配置为从 Active Directory (AD) 检索用户和组信息。

STEP 5 | 在模板堆栈中的其中一个模板里创建新区域（**Network**（网络）**> Zones**（区域）**> Add**（添加）），或者将堆栈内现有模板引用的区域映射为可信或不可信。在 Panorama 上，策略规则在设备组中定义，区域在模板中定义。因此，您需要确保将引用策略规则中包含的区域的模板添加到模板堆栈中。

在 Palo Alto Networks® 新一代防火墙上，安全策略在区域之间实施，这些区域映射到防火墙上的物理或虚拟接口。但由于适用于网络的 Prisma Access 只有两个区域，即信任和不信任，因此您需要将流量绑定到互联网的任何区域（包括您认可的 SaaS 应用程序）映射为不信任，并将所有内部区域映射为信任。

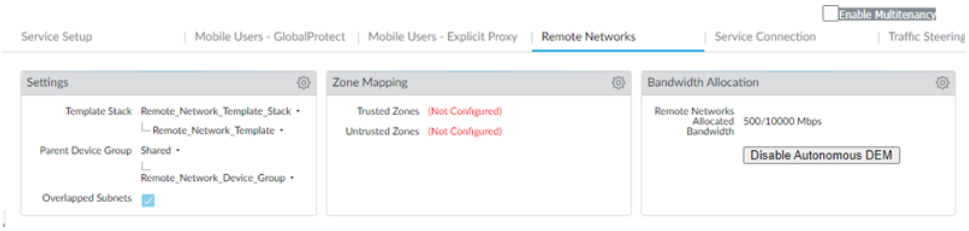
1. （可选）编辑区域映射设置。

   默认情况下，适用于网络的 Prisma Access 的模板堆栈 A 中的所有区域都分类为不受信任的区域。如果尚未定义区域，或者 Remote_Network_Template_Stack 中的模板没有区域配置，则可以在将策略推送到 Prisma Access 时返回并添加这些配置。
2. 对于要指定为受信任的每个区域，请选择这些区域，然后单击 **Add**（添加）以将其移动到 **Trusted Zones**（可信区域）。
3. 单击 **OK**（确定）保存映射。

STEP 6 | 单击 **Bandwidth Allocation**（带宽分配）区域中的齿轮图标，为您要加入的地点分配带宽。

您可以按计算位置在聚合级别分配带宽。有关详细信息，请参阅Prisma Access 远程网络。

如果您删除了作为附加程序许可证的自主 DEM，或者从许可证中删除了远程网络的自主 *DEM*，请选择 ***Disable Autonomous DEM***（禁用自主 ***DEM***）。如果您删除远程网络的自主 *DEM* 且未禁用自主 *DEM*，则在提交时会收到错误。



如果现有远程网络部署当前按地点加入远程网络，则会显示一个弹出窗口，询问您是否要迁移到聚合带宽模型。单击 **Migrate**（迁移）继续，或单击 **Cancel**（取消）取消迁移。

迁移到聚合带宽模型是永久性且不可逆的过程。迁移之前，请查看迁移前检查清单。必须 ***Commit and Push***（提交并推送）您的更改，才能使其生效。

当您将部署迁移到聚合带宽模型时，**Service IP Address**（服务 **IP** 地址）（用于远程网络连接的 IPSec 隧道的 Prisma Access 端的 公共 IP 地址）不会更改，并且不需要重新配置 IPSec 隧道。

©2025 Palo Alto Networks, Inc.

STEP 7 | 输入与您要加入的 **Prisma Access** 地点相关联的每个 **Compute Location**（计算地点）所需的 **Bandwidth Allocation**（带宽分配）。

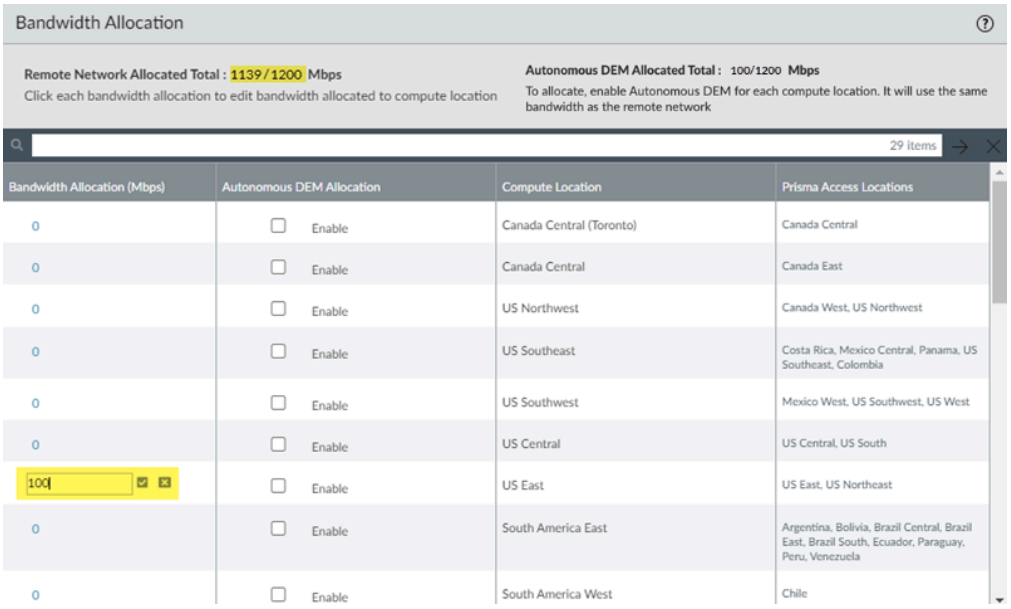
要验证您输入的带宽量，请选中带宽量旁边的复选标记；要取消该带宽量，请选择 **x**。

指定最小带宽为 50 Mbps，最大带宽为最大剩余许可带宽。

STEP 8 | （可选，仅限具有远程网络许可证的自主 DEM 的部署）为您分配带宽的计算地点 **Enable**（启用）**Autonomous DEM Allocation**（自主 **DEM** 分配）。

如果为计算地点启用自主 DEM，则自主 DEM 许可证使用的带宽量与您为计算地点指定的带宽量相同。**Autonomous DEM Allocated Total**（自主 **DEM** 分配的总带宽量）显示自主 DEM 使用的带宽量以及剩余的带宽量。有关详细信息，请参阅自主 DEM 指南。

STEP 9 | 等待带宽反映在页面顶部的 **Allocated Total**（分配的总带宽量）字段中；然后单击 **OK**（确定）。



STEP 10 | （可选）如果您想要配置远程网络以提供对远程网络位置的安全入站访问，请单击 **Inbound Access Remote Networks**（入站访问远程网络）选项卡，按照工作流为远程网络配置安全入站访问。

STEP 11 | **Add**（添加）远程网络并指定 **Name**（名称）。

输入远程网络位置的名称后，您无法更改该名称。请确保您了解远程网络的命名方案，然后再开始加入该远程网络。

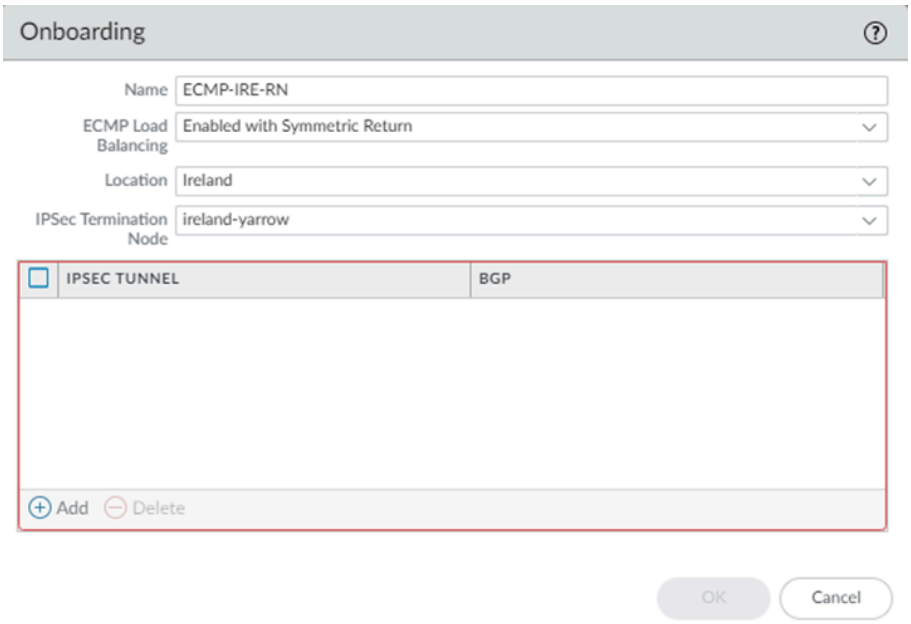
©2025 Palo Alto Networks, Inc.

STEP 12 | （可选，仅限 BGP 部署）创建配置，以便远程网络连接可以使用最多四个 IPSec 隧道进行流量传输（**ECMP Load Balancing**（**ECMP** 负载均衡））。

不支持静态路由（需要 BGP），并且如果配置了 QoS，则无法更改 ECMP 链路的分配比例。如果您的部署使用一个 IPSec 隧道进行远程网络连接或使用静态路由，请为 **ECMP Load Balancing**（**ECMP** 负载均衡）选择 **None**（无），然后继续执行步骤 15。

1. 选择其中一个选项来启用或禁用 ECMP 负载均衡。
   - **None**（无）—不使用 ECMP 负载均衡（使用一个远程网络隧道进行此次远程网络连接）。这是静态路由的唯一选择；ECMP 负载均衡需要 BGP。
   - **Enabled with Symmetric Return**（启用对称返回）—为此远程网络连接指定最多四个 IPSec 隧道，并强制 Prisma Access 使用与发送流量相同的链路来传输返回流量。

     如果您使用一个或多个隧道作为仅在其中一个主隧道断开时使用的备用隧道，请选择此选项。如果链路发生故障，Prisma Access 会使用其他隧道之一来对称地发送和接收流量。



2. 为远程网络连接 **Add**（添加）IPSec 隧道并指定以下值：
   - **Enable**（启用）—为 IPSec 隧道启用 BGP。

     此选项不可配置；您必须启用 BGP 才能配置 ECMP。
   - **Summarize Mobile User Routes before advertising**（在通告之前汇总移动用户路由）—通过汇总移动用户 IP 子网，减少通过 BGP 向您的客户终端设备 (CPE) 通告的移动用户 IP 子网的数量。

     默认情况下，Prisma Access 以 /24 子网的形式通告移动用户的 IP 地址池；如果将它们汇总起来，Prisma Access 会根据您指定的子网来通告该池。例如，Prisma Access 使用 /20 子网通告公共用户移动 IP 池 10.8.0.0/20，而不是在通告之前将池划分为 10.8.1.0/24、10.8.2.0/24、10.8.3.0/24 等子网。汇总这些通告可以减少 CPE 路由表

©2025 Palo Alto Networks, Inc.

中存储的路由数量。例如，您可以将 IP 池汇总与可接受有限数量路由的云 VPN 网关（虚拟专用网关 (VGW) 或传输网关 (TGW)）结合使用。

如果为使用 *ECMP* 的位置启用路由汇总，则必须在指向该位置的所有链路上启用路由汇总，否则您将在提交期间收到错误。

Prisma Access 将聚合移动用户路由的社区字符串设置为 `0xFFFE:0xFFF0`。

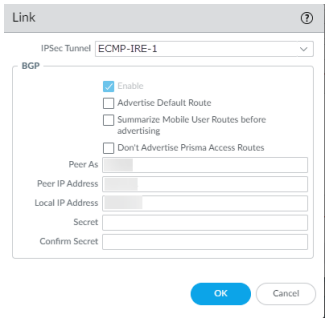
- **Advertise Default Route**（通告默认路由）—Prisma Access使用 eBGP 为远程网络发起默认路由通告。

  确保您的网络没有由 *BGP* 通告的其他默认路由，否则可能会在网络中引入路由问题。

- 不通告 **Prisma Access** 路由—防止 Prisma Access BGP 对等体将路由转发到您组织的网络中。

  默认情况下，Prisma Access 通告所有 BGP 路由信息，包括本地路由以及它从其他服务连接、远程网络和移动用户子网收到的所有前缀。选中此复选框可防止 Prisma Access 发送任何 BGP 通告，但仍使用其收到的 BGP 信息从其他 BGP 邻居学习路由。

  如果您选择此选项，Prisma Access 不会发送 BGP 通告，因此您必须在本地设备上配置静态路由以建立返回 Prisma Access 的路由。



- （可选）选择 **MRAI** 计时器值。

  GP 路由提供一个计时器，您可以使用它来定制网络中的 BGP 路由收敛，称为最小路由通告间隔 *(MRAI)*。MRAI 用于对每个目标的更新进行速率限制，BGP 路由器至少需等待所配置的 MRAI 时间，然后才能发送前缀相同的通告。数字越小，收敛时间就越快，但能在网络中创建的通告也越多。数字越大，可发送的通告数量就越少，但也会

 ©2025 Palo Alto Networks, Inc.

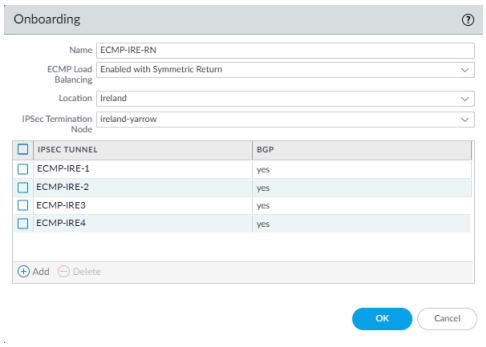
使路由收敛速度变慢。由您来决定在网络中输入的具体数字，以便在更快的路由收敛和更少的通告数量之间取得最佳平衡。

将 MRAI 范围配置为 1 到 600 秒，默认值为 30 秒。

- **Peer AS**（对等 **AS**）—指定远程网络中的防火墙、虚拟路由器或 BGP 路由器所属的自治系统 (AS)。
- **Peer IP Address**（对等体 **IP** 地址）—输入为您要配置此连接的远程网络上的 eBGP 路由器的路由器 ID 分配的 IP 地址。
- 本地 **IP** 地址（可选）输入 Prisma Access 用作 BGP 的本地 IP 地址的地址。指定要在隧道的 Prisma Access 端使用的 IP 地址。

  当连接另一端的设备（例如 Amazon Web Service (AWS) 虚拟专用网关）需要特定的本地 IP 地址才能成功进行 BGP 对等连接时，指定**Local Address**（本地地址）很有用。确保您指定的地址与基础设施子网或远程网络中的子网中的 IP 地址不冲突或重叠。
- **Secret**（密码）和 **Confirm Secret**（确认密码）（可选）—输入并确认密码以验证 BGP 对等体通信。

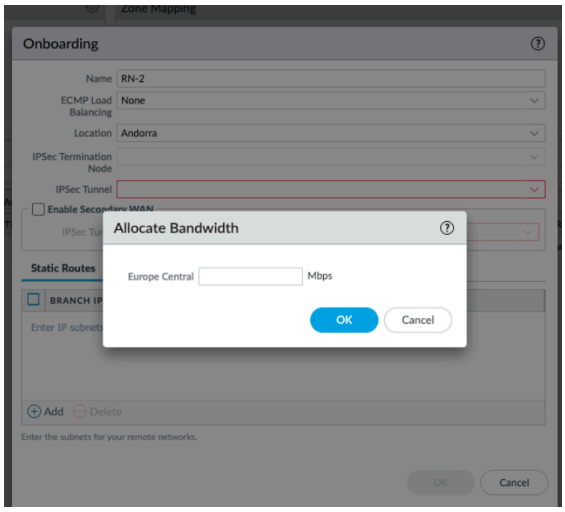
3. 重复上一步，以添加最多四个隧道用于远程网络连接。



 ©2025 Palo Alto Networks, Inc.

STEP 13 | 选择 Prisma Access 将在其中部署保护远程网络位置所需的基础设施的 **Location**（位置）。此区域在地理位置上应靠近您的远程网络位置。

如果您尚未为该位置映射到的计算地点分配带宽， Prisma Access 会提示您输入该计算地点的带宽。



标有两个星号的位置是 **Local Zones**（本地服务区）。这些位置将计算、存储、数据库和基础设施服务置于人口密集和工业中心附近；然而，它们也存在一些局限性。要添加本地服务区，请联系您的 Palo Alto Networks 代表。

STEP 14 | 选择您要用于此远程网络的 **IPSec Termination Node**（**IPSec** 终止节点）。

Prisma Access 使用此节点将远程网络位置与计算地点相关联。

STEP 15 | （仅限静态路由或单隧道部署）选择或添加新的 **IPSec Tunnel**（**IPSec** 隧道）配置，以访问公司位置的防火墙、路由器或 SD-WAN 设备：

- 在 Remote_Network_Template 中选择一个预定义的 IPSec 模板，或者，如果您已向 Remote_Network_Template_Stack 添加包含 IPSec 隧道配置的模板（或修改了预定义的 Remote_Network_Template），请从下拉列表中选择该 **IPSec Tunnel**（**IPSec** 隧道）。请注意，您为每个远程网络连接创建的隧道会将 Prisma Access 连接到每个分支机构位置支持 IPSec 的设备。

  配置 IPSec 隧道时，请遵循以下准则：

  - IKE 网关配置中的对等地址对于每个隧道都必须是唯一的。但是，您可以重用其他一些常见的配置元素，例如加密配置文件。
  - 从模板中选择的 IPSec 隧道必须仅使用自动密钥交换和 IPv4。
  - IPSec 隧道、IKE 网关和加密配置文件名称不能超过 31 个字符。
  - 如果将多个远程网络上线到具有动态 IKE 对等设备的同一位置，则必须对所有远程网络配置使用相同的 IKE 加密配置文件。

 ©2025 Palo Alto Networks, Inc.

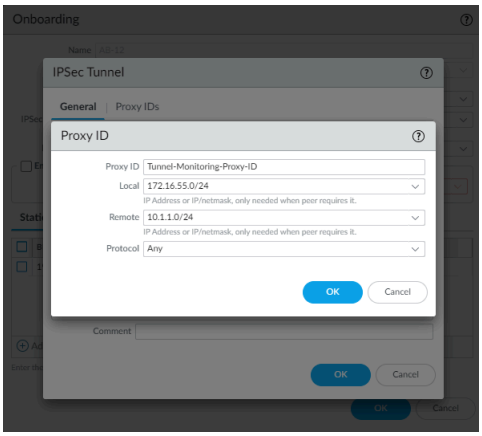
- 要创建新的 IPSec 隧道配置，请单击 **New IPSec Tunnel**（新建 **IPSec** 隧道），为其指定一个 **Name**（名称），然后配置 IKE 网关、IPSec 加密配置文件和隧道监控设置。
  - 如果分支机构中支持 IPSec 的设备使用基于策略的 VPN，请在 **Proxy IDs**（代理 **ID**）选项卡上，**Add**（添加）与本地 IPSec 设备上配置的设置匹配的代理 ID，以确保 Prisma Access 可以成功建立与本地设备的 IPSec 隧道。
- 保持 **Enable Replay Protection**（启用重放保护）选中状态以检测重放攻击并使其无效。
- 选择 **Copy ToS Header**（复制 **ToS** 标头），将封装数据包的内部 IP 标头中的服务类型 (ToS) 标头复制到其外部 IP 标头中，以保留原始 ToS 信息。

©2025 Palo Alto Networks, Inc.

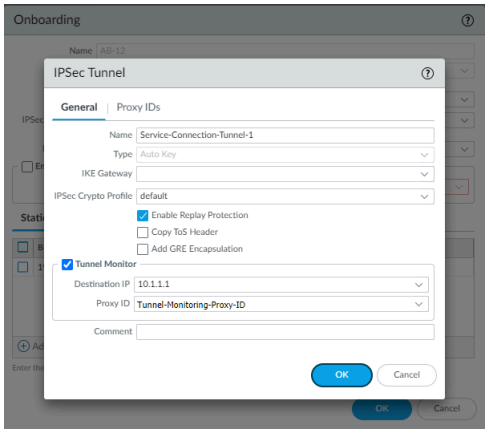
- 要为服务连接启用隧道监视，请选择 **Tunnel Monitor**（隧道监视器）。
  - 输入 **Destination**（目标）IP 地址。

    在分支机构位置指定一个 IP 地址，Prisma Access 可以向该地址发送 IPSec 隧道监控的验证请求。请确保整个 Prisma Access 基础设施子网都可以通过 ICMP 访问此地址。
  - 如果对使用多个代理 ID 的对等设备使用隧道监控，请指定一个 **Proxy ID**（代理 **ID**）或添加一个 **New Proxy ID**（新代理 **ID**），以允许从基础设施子网访问分支机构位置。

    下图显示了一个代理 ID，其中服务基础设施子网（本示例中为 172.16.55.0/24）作为 **Local**（本地）IP 子网，分支机构位置的子网（本示例中为 10.1.1.0/24）作为 **Remote**（远程）子网。



    下图显示了您创建的代理 ID，该代理 ID 通过在 **Proxy ID**（代理 **ID**）字段中指定而应用于隧道监视器配置。





您必须在 *CPE* 上配置一个到隧道监视器 *IP* 地址的静态路由，以使隧道监视正常工作。要查找用于从分支机构位置到 *Prisma Access* 的隧道监控的目标 *IP* 地址，请选择 ***Panorama > Cloud Services***（云服务）***> Status***（状态）***> Network Details***（网络详细信息），并单击 ***Service Infrastructure***（服务基础设施）单选按钮，然后找到 ***Tunnel Monitor IP Address***（隧道监控 ***IP*** 地址）。

 ©2025 Palo Alto Networks, Inc.

STEP 16 | 如果在此位置有辅助 WAN 链路，请选择 **Enable Secondary WAN**（启用辅助 **WAN**）。

确保为每个远程网络的辅助 *WAN* 创建唯一的 *IPSec* 隧道；*Prisma Access* 不支持对多个远程网络中的辅助 *WAN* 重用相同的 *IPSec* 隧道。

以下部署不支持配置辅助 WAN：

- 如果您的辅助 WAN 的主 IPSec 隧道设置为主动-主动模式。
- 如果您的客户端设备 (CPE) 的主 IPSec 隧道和辅助 IPSec 隧道设置为等价多路径 (ECMP) 配置。

如果您使用静态路由，隧道故障转移时间从检测时间算起不超过 15 秒，具体取决于您的 WAN 提供商。

如果您配置了 BGP 路由并启用了隧道监视，则确定安全参数索引 (SPI) 失败的最短默认保持时间是使用隧道监视器，当它检测到连续 15 秒的隧道失败时，将删除指向对等设备的所有路由。通过这种方式，隧道监控器确定 BGP 路由的行为。如果未配置隧道监控，保持计时器将确定在删除路由之前隧道关闭的时间。Prisma Access 使用 RFC 4271 定义的默认 BGP HoldTime 值 90 秒，这是 Prisma Access 删除非活动 SPI 的路由之前的最长等待时间。如果对等 BGP 设备的配置保持时间较短，BGP 保持计时器将使用较低的值。

成功安装辅助隧道后，辅助路由将优先使用，直到主隧道恢复。如果主路由和辅助路由都已启动，则主路由优先。

如果您使用不同的 *BGP* 对等设备进行辅助（备份）连接，*Prisma Access* 不会接受 *CPE* 通告的 *Multi-Exit Discriminator (MED)* 属性。如果您在远程网络连接或服务连接上使用多个 *BGP* 对等设备，则此警告适用。

 ©2025 Palo Alto Networks, Inc.

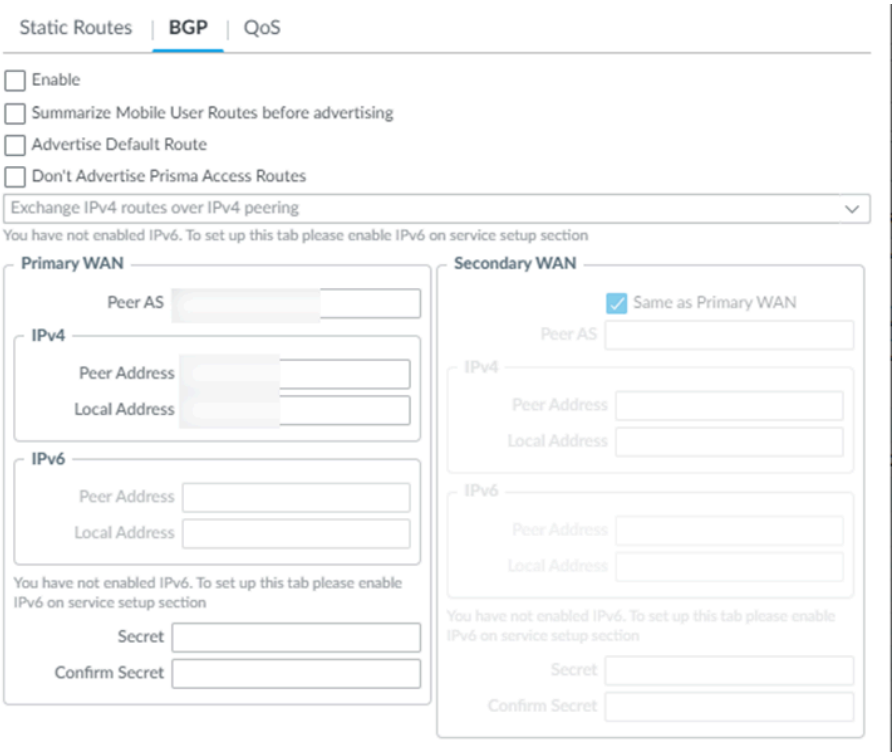
STEP 17 | 启用到用户需要访问的远程网络站点的子网或单个 IP 地址的路由。

Prisma Access 使用此信息将请求路由到适当的站点。每个站点的网络不能相互重叠，也不能与您为服务基础设施或适用于用户的 Prisma Access IP 池指定的 IP 地址池重叠。您可以配置 **Static Routes**（静态路由）、**BGP** 或两者的组合。

- 要配置 **Static Routes**（静态路由）：
  1. 在 **Static Routes**（静态路由）选项卡上，单击 **Add**（添加）并输入子网地址（例如，172.168.10.0/24）或资源的单个 IP 地址，例如远程用户需要访问的 DNS 服务器（例如，10.32.5.1/32）。
  2. 对 Prisma Access 在此位置需要访问的所有子网或 IP 地址重复此操作。



- 要配置 **BGP**：
  1. 选择 **BGP** 选项卡。
  2. （可选）选择 **ECMP Load Balancing**（**ECMP** 负载均衡）选项。请参阅步骤 12。
  3. 如果为 **ECMP Load Balancing**（**ECMP** 负载均衡）选择 **None**（无），请输入 BGP 选项。



 ©2025 Palo Alto Networks, Inc.

4. 要为远程网络连接启用 BGP，请选择 **Enable**（启用）。

   启用 BGP 后，Prisma Access 会将外部 BGP (eBGP) 的生存时间 (TTL) 值设置为 8，以适应 Prisma Access 基础设施和终止 eBGP 连接的客户终端设备 (CPE) 之间可能发生的任何额外跳数。

5. 要通过汇总移动用户 IP 子网以减少通过 BGP 向您的客户终端设备 (CPE) 通告的移动用户 IP 子网的数量，请选择 **Summarize Mobile User Routes before advertising**（在通告之前汇总移动用户路由）。

   默认情况下，Prisma Access 以 /24 子网的形式通告移动用户的 IP 地址池；如果将它们汇总起来，Prisma Access 会根据您指定的子网来通告该池。例如，Prisma Access 使用 /20 子网通告公共用户移动 IP 池 10.8.0.0/20，而不是在通告之前将池划分为 10.8.1.0/24、10.8.2.0/24、10.8.3.0/24 等子网。汇总这些通告可以减少 CPE 路由表中

©2025 Palo Alto Networks, Inc.

存储的路由数量。例如，您可以将 IP 池汇总与可接受有限数量路由的云 VPN 网关（虚拟专用网关 (VGW) 或传输网关 (TGW)）结合使用。

Prisma Access 将聚合移动用户路由的社区字符串设置为 `0xFFFE:0xFFF0`。

6. 要允许 Prisma Access 使用 eBGP 为远程网络通告默认路由，请选择 **Advertise Default Route**（通告默认路由）。

   如果选择 **Advertise Default Route**（通告默认路由），请确保您的网络没有由 BGP 通告的其他默认路由，否则可能会在网络中引入路由问题。

   您必须先发布默认路由，然后才能进行此选择以通告默认路由。此外，确保您的网络没有由 *BGP* 通告的其他默认路由，否则可能会在网络中引入路由问题。

7. 要防止 Prisma Access 防火墙上的 BGP 对等体将路由转发到您组织的网络中，请选择不通告 **Prisma Access** 路由。

   默认情况下，Prisma Access 通告所有 BGP 路由信息，包括本地路由以及它从其他服务连接、远程网络和移动用户子网收到的所有前缀。选中此复选框可防止 Prisma Access 发送任何 BGP 通告，但仍使用其收到的 BGP 信息从其他 BGP 邻居学习路由。

   如果您选择此选项，Prisma Access 不会发送 BGP 通告，因此您必须在本地设备上配置静态路由以建立返回 Prisma Access 的路由。

8. 输入 **Peer AS**（对等 **AS**），即远程网络中的防火墙、虚拟路由器或 BGP 路由器所属的自治系统 (AS)。
9. 输入为您要配置此连接的远程网络上的 eBGP 路由器的路由器 ID 分配的 IP 地址作为 **Peer Address**（对等体 **IP** 地址）。
10. （可选）输入 Prisma Access 用作 BGP 的本地 IP 地址的地址。

    当连接另一端的设备（例如 Amazon Web Service (AWS) 虚拟专用网关）需要特定的本地 IP 地址才能成功进行 BGP 对等连接时，指定**Local Address**（本地地址）很有用。确保您指定的地址与基础设施子网或远程网络中的子网中的 IP 地址不冲突或重叠。

    您必须在 *CPE* 上配置到 *BGP **Local Address***（本地地址）的静态路由。

11. （可选）输入并确认密码以验证 BGP 对等体通信。
12. （可选）如果您配置了 **Secondary WAN**（辅助广域网），并且需要更改辅助（备份）BGP 对等体的 **Peer Address**（对等体地址）或 **Local Address**（本地地址），请取消

©2025 Palo Alto Networks, Inc.

选择 **Same as Primary WAN**（与主广域网相同），然后输入唯一的对等体，或者输入辅助广域网的本地 IP 地址。

如果您在远程网络部署中使用 IPv6 网络，则可以配置 **IPv6** 地址以及 **IPv4** 地址。您还需要在 Prisma Access 基础设施中全局启用 IPv6 网络，然后才能使用 IPv6 寻址。

在某些部署中（例如，当使用 BGP 与 AWS VPN 网关对等时），主广域网和辅助广域网的 BGP 对等体可能有所不同。在这些情况下，您可以选择为辅助广域网设置不同的 BGP 对等体。

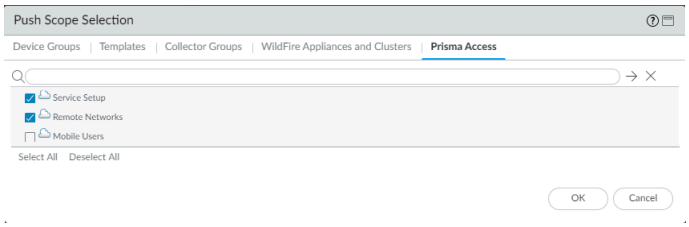
对于具有辅助广域网的 *BGP* 部署，*Prisma Access* 将主隧道和辅助隧道都设置为 ***UP*** 状态，但遵循网络流量的正常 *BGP* 主动备份行为。*Prisma Access* 将主隧道设置为活动状态，并仅通过该隧道发送和接收流量；如果主隧道发生故障，*Prisma Access* 将使用 *BGP* 规则检测故障，将辅助隧道设置为活动状态，并且仅使用辅助隧道发送和接收流量。

STEP 18 | （可选）为该位置启用 **QoS** 并指定 **QoS Profile**（**QoS** 配置文件）。

您可以在 **Settings**（设置）中根据计算地点指定 QoS 选项和整体设置；但是，您可以在此处根据位置启用或禁用 QoS 或更改 QoS 配置文件。

STEP 19 | 将配置更改提交给 Panorama，并将配置推送到适用于网络的 Prisma Access。

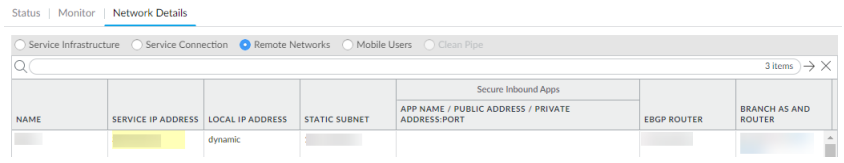
1. 单击 **Commit**（提交） > **Commit to Panorama**（提交到 **Panorama**）。
2. 单击 **Commit**（提交） > **Commit and Push**（提交并推送）。单击 **Edit Selections**（编辑选择） > **Prisma Access**，然后选择适用于网络的 Prisma Access 和适用于服务设置的 Prisma Access，以将配置推送到服务。



3. 单击 **OK**（确定）和 **Push**（推送）。

STEP 20 | 在远程网络位置配置支持 IPSec 的设备，以便与适用于网络的 Prisma Access 建立 IPSec 连接。

1. 要查找此远程网络连接的 **Service IP Address**（服务 **IP** 地址），请选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息），单击 **Remote Networks**（远程网络）单选按钮，并查看 **Service IP Address**（服务 **IP** 地址）字段。适用于网络的 Prisma Access 基础设施已为 Prisma Access 远程网络连接分配了此 IP 地址，您必须将其配置为对等 IP 地址，以在远程网络位置和适用于网络的 Prisma Access 之间建立 IPSec 隧道。



2. 在 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息） > **Remote Networks**（远程网络）页面上，查看远程网络位置上该设备的 **Local**

 ©2025 Palo Alto Networks, Inc.

IP address（本地 **IP** 地址）。如果您在远程网络位置执行 NAT，则 **Local IP address**（本地 **IP** 地址）将显示设备 NAT 后的 IP 地址。

STEP 21 | 为了保护远程网络位置的流量，您必须创建安全策略规则。

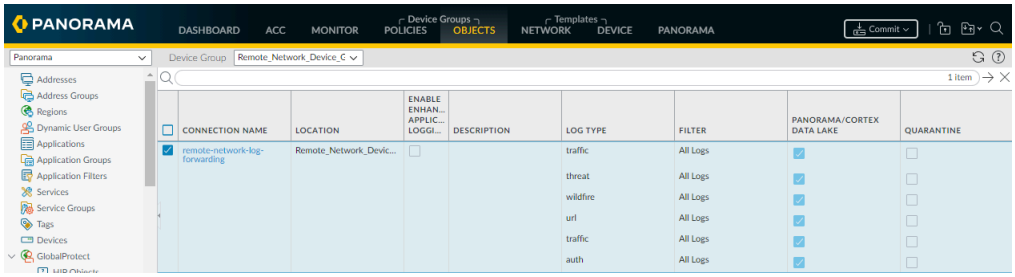
1. 选择 **Policies**（策略）。
2. 选择要添加策略规则的 **Device Group**（设备组）。您可以选择 Remote_Network_Device_Group，或您为保护远程网络位置定义策略时所选择的父设备组。
3. 创建安全策略规则。确保您没有定义允许将流量从任何区域传输到任何区域的安全策略规则。在安全策略规则中，使用您在模板中定义的区域。

   如果您网络上的用户被拒绝访问某个网站，请在向 Palo Alto Networks 开立工单之前报告网站访问问题。

STEP 22 | 启用将日志记录到 Strata Logging Service 的功能。您必须创建日志转发配置文件，并将其附加到想要转发日志所用的每个策略规则。

1. 选择 **Objects**（对象）> **Log Forwarding**（日志转发）。
2. 选择添加了策略规则的 **Device Group**（设备组），例如 Remote_Network_Device_Group。
3. **Add**（添加）日志转发配置文件在日志转发配置文件匹配列表中，**Add**（添加）您想要转发的每种 **Log Type**（日志类型）。
4. 选择 **Panorama/Strata Logging Service** 作为转发方法，使 Prisma Access 能够将日志转发到 Strata Logging Service。您将能够监控日志并从 Panorama 生成报告。Strata Logging Service 提供无缝集成来存储日志，而无需将其回传到公司总部的 Panorama，并且 Panorama 可以根据需要查询 Strata Logging Service。

   以下示例展示如何将流量、威胁预防、WildFire 提交、URL 过滤、数据过滤和身份验证日志转发到 Strata Logging Service。



5. 选择 **Policies**（策略）> **Security**（安全）并编辑策略规则。在 **Actions**（操作）中，选择您创建的日志转发配置文件。

STEP 23 | 将所有更改提交到 Panorama 并将配置更改推送到 Prisma Access。

1. 单击 **Commit**（提交）> **Commit and Push**（提交并推送）。
2. **Edit Selections**（编辑选择），在 **Prisma Access** 选项卡中，确保在 **Push Scope**（推送范围）中选择适用于网络的 **Prisma Access**，然后单击 **OK**（确定）。
3. **Commit and Push**（提交并推送）更改。

©2025 Palo Alto Networks, Inc.

STEP 24 | 检查远程网络状态。

有关详细信息，请参阅验证远程网络连接状态。

©2025 Palo Alto Networks, Inc.

将远程网络站点连接到 Prisma Access

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 许可证

设置 IPSec VPN 隧道以将您的远程网络站点连接到 Prisma Access。您必须从分支 IPSec 设备创建到 Prisma Access 的 IPSec 隧道。

您创建的第一个隧道是远程网络站点的主隧道。然后，您可以重复此工作流，以选择性地设置辅助隧道。当两个隧道都打开时，主隧道优先于辅助隧道。如果远程网络站点的主隧道发生故障，则远程网络将回退到辅助隧道，直到主隧道恢复正常。

根据您用于在远程网络站点建立隧道的 IPSec 设备，Prisma Access 提供推荐的内置 IKE 和 IPSec 安全设置。您可以使用建议的设置快速入门，也可以根据您的环境需要进行自定义。

- 添加主要和辅助 IPSec VPN 隧道
- 更多 IKE 选项
- 更多 IPSec 选项

添加主要和辅助 IPSec VPN 隧道

STEP 1 | 启动 Prisma Access。

STEP 2 | 转到 **Workflows**（工作流） > **Prisma Access** 设置 > **Remote Networks**（远程网络） > **Add Remote Networks**（添加远程网络），然后 **Set Up**（设置）主隧道。如果您已设置主隧道，则可以继续在此处添加辅助隧道。

1. 为隧道指定一个描述性 **Name**（名称）。
2. 为用于与 Prisma Access 建立隧道的远程网络站点上的 IPSec 设备选择 **Branch Device Type**（分支设备类型）。
3. 对于 **Branch Device IP Address**（分支设备 **IP** 地址），选择使用标识隧道端点的静态 **IP** 地址或 **Dynamic**（动态）IP 地址。

   如果将 **Branch Device IP Address**（分支设备 **IP** 地址）设置为 **Dynamic**（动态），则还必须添加远程网络站点的 IKE ID（**IKE Local Identification**（**IKE** 本地标识））或添加 Prisma Access 的 IKE ID（**IKE Peer Identification**（**IKE** 对等体标识）），以使 IPSec 对等体能够进行身份验证。

   由于在远程网络完全部署之前，您没有用于 Prisma Access IKE ID（**IKE Peer Identification**（**IKE** 对等体标识））的值，因此您通常希望为远程网络站点设置 IKE ID（**IKE Local Identification**（**IKE** 本地标识）），而不是 Prisma Access IKE ID。

©2025 Palo Alto Networks, Inc.

STEP 3 | **Turn on Tunnel Monitoring**（打开隧道监控）。

输入远程网络上的隧道监控 **Destination IP**（目标 **IP**）地址，以便 Prisma Access 用于确定隧道是否开启，并且如果分支 IPSec 设备使用基于策略的 VPN，请输入关联的代理 **ID**。

您输入的隧道监控 IP 地址将自动添加到分支子网列表中。

STEP 4 | **Save**（保存）隧道设置。

要继续：

- 为 IKE 和 IPSec 设置和自定义高级加密设置。请参阅 更多 IKE 选项 和 更多 IPSec 选项。
- 为远程网络启用路由.

更多 IKE 选项

根据您选择的 IPSec 设备类型，Prisma Access 为远程网络站点设备和 Prisma Access 之间的 IKE 第 1 阶段密钥交换过程提供一组建议的密码和密钥有效期。您可以使用建议的设置，也可以根据环境需要自定义设置。

为分支设备和 Prisma Access 选择用于 IKE 协商的 **IKE Protocol Version**（**IKE** 协议版本）。

如果选择 **IKEv1 Only Mode**（仅限 **IKEv1** 模式），Prisma Access 只能使用 IKEv1 协议进行协商。如果选择 **IKEv2 Only Mode**（仅限 **IKEv2** 模式），Prisma Access 只能使用 IKEv2 协议进行协商。如果选择 **IKEv2 Preferred Mode**（**IKEv2** 首选模式），则仅当分支 IPSec 设备也支持 IKEv2 时，Prisma Access 才会使用 IKEv2 协议。如果分支 IPSec 设备不支持 IKEv2，Prisma Access 将回退到 IKEv1 协议。

 ©2025 Palo Alto Networks, Inc.

添加 **IKEv1 Crypto Profile**（**IKEv1** 加密配置文件）以自定义 IKE 加密设置，这些设置定义用于 IKE 阶段 1 中密钥交换过程的加密和身份验证算法。

Prisma Access 根据用于建立此隧道的 **Branch Device Type**（分支设备类型）自动使用默认 IKE 加密配置文件。

- **Encryption**（加密） — 指定 IKE SA 协商中使用的加密算法。

  Prisma Access 支持以下加密算法：3DES（168 位）、AES-128-CBC（128 位）、AES-192-CBC（192 位）、AES-256-CBC（256 位）和 DES（56 位）。还可以选择 Null（不加密）。
- 身份验证 — 指定 IKE SA 协商中使用的身份验证算法。

  Prisma Access 支持以下身份验证算法：sha1（160 位）、sha256（256 位）、sha384（384 位）、sha512（512 位）和 md5（128 位）。还可以选择 Null（无身份验证）。
- **DH Group**（**DH** 组） — 指定用于在 IKE SA 协商中为 IKE 生成对称密钥的 Diffie-Hellman (DH) 组。Diffie-Hellman 算法使用一方的私钥和另一方的公钥创建共享机密，即两个 VPN 隧道对等设备共享的加密密钥。

  Prisma Access 支持以下 DH 组：组 1（768 位）、组 2（1024 位 — 默认）、组 5（1536 位）、组 14（2048 位）、组 19（256 位椭圆曲线组）、组 20（384 位椭圆曲线组）。要获得最强的安全性，请选择数字最高的组。
- **Lifetime**（有效期） — 指定 IKE 阶段 1 密钥有效的单位和时间长度（默认值为 8 小时）。对于 IKEv1，在密钥有效期到期之前，不会主动重新生成安全关联 (SA) 的密钥。IKEv1 阶段 1 重新生成密钥仅在 SA 过期时触发。对于 IKEv2，必须在密钥有效期到期之前重新生成 SA 密钥。如果 SA 在到期时未重新生成密钥，则 SA 必须开始新的第 1 阶段密钥。
- **IKEv2 Authentication Multiple**（**IKEv2** 身份验证倍数） — 指定密钥有效期的乘数值（范围为 0-50；默认为 0）以确定身份验证计数。身份验证计数是安全处理节点在必须开始重新进行 IKEv2 身份验证之前可以执行 IKEv2 IKE SA 重新生成密钥操作的次数。默认值 0 会禁用重新验证身份功能。

启用 **IKE Passive Mode**（**IKE** 被动模式），以便 Prisma Access 仅响应 IKE 连接，而不启动它们。

默认情况下，**IKE NAT Traversal**（**IKE NAT** 遍历）处于打开状态。

这意味着 UDP 封装用于 IKE 和 UDP 协议，使它们能够通过 IPSec VPN 隧道端点之间的网络地址转换 (NAT) 设备。

更多 IPSec 选项

根据您选择的 IPSec 设备类型，Prisma Access 提供一组建议的 IPsec 协议和密钥有效期设置，以在 IKE 第 2 阶段保护分支设备与 Prisma Access 之间的 IPSec 隧道内的数据，从而实现安全关联 (SA)。您可以使用建议的设置，也可以根据环境需要自定义设置。

 ©2025 Palo Alto Networks, Inc.

自定义 **IPSec Crypto Profile**（**IPsec** 加密配置文件），以定义在 IKE 第 2 阶段自动密钥 IKE 自动为 IKE SA 生成密钥时，如何保护隧道内的数据。

Prisma Access 会根据 **Branch Device Type**（分支设备类型）供应商自动配置默认 IPsec 加密配置文件。您可以使用默认配置文件或创建自定义配置文件。

- **IPsec** 协议 — 保护通过 VPN 隧道传输的数据。封装式安全措施负载 **(ESP)** 协议会加密数据、对源进行身份验证并验证数据完整性。身份验证标头 **(AH)** 协议对源进行身份验证并验证数据的完整性。

  如果使用 **ESP** 作为 IPsec 协议，还要指定 IPsec SA 协商中使用的 **Encryption**（加密）算法。

  Prisma Access 支持以下加密算法：aes-256-gcm（256 位）、aes-256-cbc（256 位）、aes-192-cbc（192 位）、aes-128-gcm（128 位）、aes-128-cbc （128 位）、3des（168 位）和 des（56 位）。还可以选择 Null（不加密）。

Authentication（身份验证）— 指定 IPsec SA 协商中使用的身份验证算法。

Prisma Access 支持以下身份验证算法：sha1（160 位）、sha256（256 位）、sha384（384 位）、sha512（512 位）和 md5（128 位）。如果将 IPSec 协议设置为 ESP，您还可以选择无（不进行身份验证）。

DH Group（**DH** 组）— 在 IPsec 安全关联 (SA) 协商中为 IKE 指定 Diffie-Hellman (DH) 组。

Prisma Access 支持以下 DH 组：组 1（768 位）、组 2（1024 位 — 默认）、组 5（1536 位）、组 14（2048 位）、组 19（256 位椭圆曲线组）、组 20（384 位椭圆曲线组）。要获得最强的安全性，请选择数字最高的组。如果您不想续订 Prisma Access 在 IKE 第 1 阶段创建的密钥，请选择 **no-pfs**（没有完美的向前保密）。如果选择此选项，Prisma Access 将重复使用当前密钥进行 IPsec SA 协商。

Lifetime（有效期）— 指定协商密钥有效的单位和时间长度（默认为一小时）。

Lifesize（数据量） — 指定密钥可用于加密的数据单位和数量。

 ©2025 Palo Alto Networks, Inc.

为远程网络启用路由

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 许可证

要使 Prisma Access 将流量路由到您的远程网络，必须为要使用 Prisma Access 保护的子网提供路由信息。可以通过多种方式来实现这一点。既可以在远程网络站点为每个子网定义静态路由，也可以在服务连接位置与 Prisma Access 之间配置 BGP，或者同时使用这两种方法。

如果配置两条静态路由并启用 BGP，则静态路由优先。如果您的远程网络位置只有几个子网，使用静态路由可能会很方便，但在大型部署中，很多远程网络的子网彼此重叠，在这种情况下，使用 BGP 将使您能够更轻松地扩展。

- 静态路由 — 要启用远程站点到 Prisma Access 的静态路由，请标识远程站点上您希望 Prisma Access 保护的子网或单个 IP 地址（对于入站和出站流量）。每个站点的子网不能相互重叠，不能与您为 Prisma Access for Users 指定的 IP 池重叠，也不能与基础设施子网重叠。
- **BGP** — 如果您想要启用 BGP 来动态路由往返于远程网络的流量，则需要为分支机构的 eBGP 路由器提供 BGP 信息：
  - 分支路由器自治系统 **(AS)** 编号 — 远程网络中的 eBGP 路由器所属的 AS。这被称为对等 **AS**。
  - 路由器 **ID** — 分配给远程网络上 eBGP 路由器作为路由器 ID 的 IP 地址。这被称为对等地址。

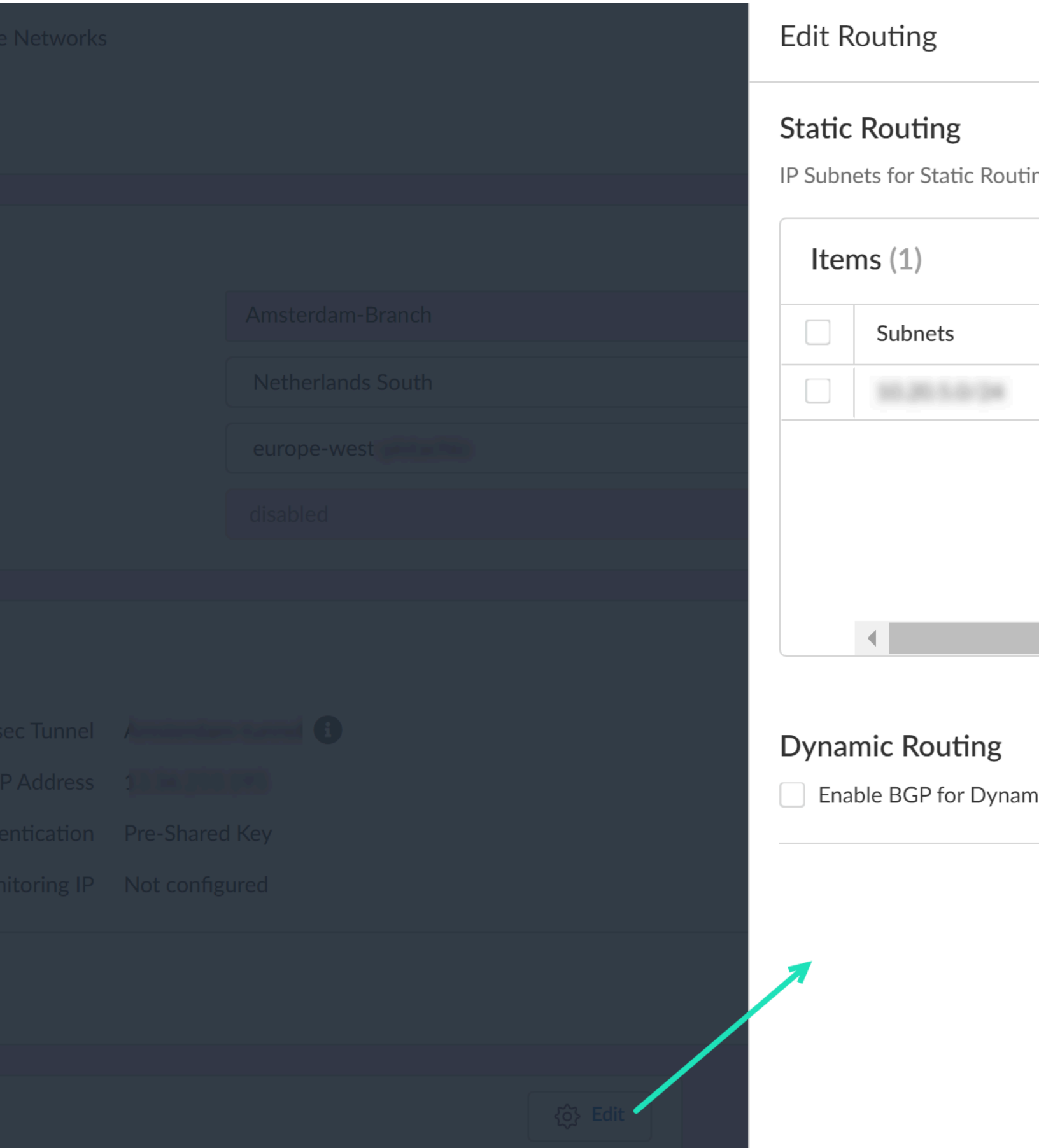
  如果同时配置静态路由和 BGP 路由，则静态路由优先。

以下介绍了如何为远程网络站点配置路由设置。

 ©2025 Palo Alto Networks, Inc.

要添加或调整路由设置，请转到 **Workflows**（工作流程） > **Prisma Access** 设置 > **Remote Networks**（远程网络），然后添加或编辑远程网络站点。

 ©2025 Palo Alto Networks, Inc.



©2025 Palo Alto Networks, Inc.

配置静态路由。

如果您使用静态路由来路由往返于分支机构的流量，则选择 **Add**（添加）以添加要在分支机构保护的 IP 子网或 IP 地址。请注意，如果对分支机构的 IP 子网进行任何更改，则必须手动更新静态路由。

配置动态路由。

要使用动态路由来通告您的分支子网，则选择 **Enable BGP for Dynamic Routing**（为动态路由启用 **BGP**），然后配置以下设置：

- **Do Not Export Routes**（不导出路由） — 防止 Prisma Access 将路由转发到您的远程网络。

  默认情况下，Prisma Access 通告所有 BGP 路由信息，包括本地路由以及它从其他服务连接、远程网络和移动用户子网收到的所有前缀。选中此复选框可防止 Prisma Access 发送任何 BGP 通告，但仍使用其收到的 BGP 信息从其他 BGP 邻居学习路由。

  如果您选择此选项，*Prisma Access* 不会发送 *BGP* 通告，因此您必须在本地设备上配置静态路由以建立返回 *Prisma Access* 的路由。
- **Peer IP Address**（对等 **IP** 地址） — 输入分配给远程网络上 eBGP 路由器作为路由器 ID 的 IP 地址。
- **Peer AS**（对等 **AS**） — 输入对等 AS，即您网络的自治系统 (AS)。

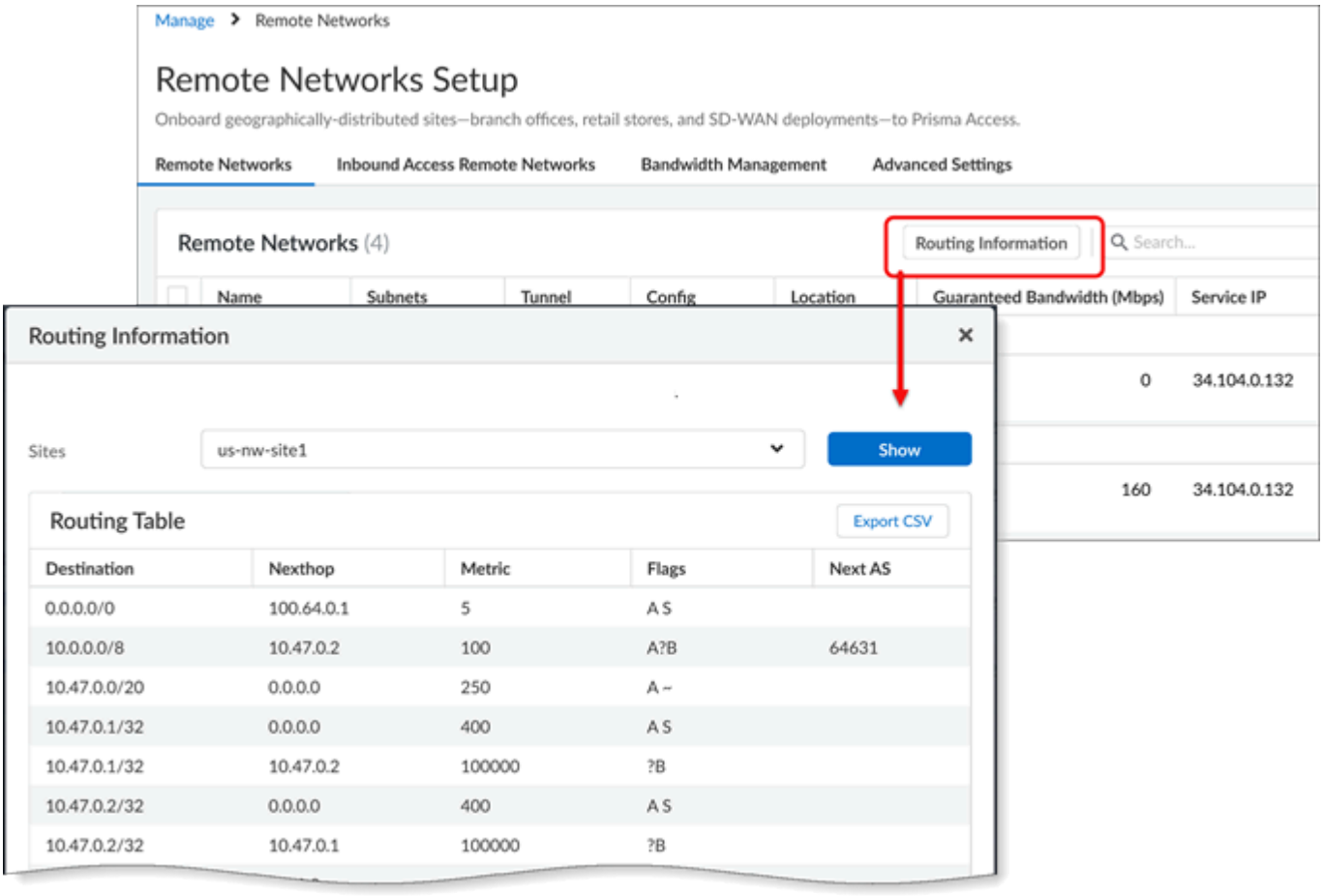
  必须使用符合 RFC 6996 标准的 BGP 私有 AS 编号。
- **Local IP Address**（本地 **IP** 地址） — 输入 Prisma Access 用作其 BGP 本地 IP 地址的 IP 地址。

  仅当您的远程站点设备需要本地地址才能成功实现 BGP 对等时，才需要本地地址。要确保指定的地址不会与基础设施子网或远程网络中的子网中的 IP 地址产生冲突或重叠。
- **Secret**（机密） — 输入用于对 BGP 对等通信进行身份验证的机密，然后选择 **Confirm Secret**（确认机密）。

站点连接故障排除

为了排除故障，您现在可以查看远程网络站点或服务连接站点的路由表。在远程网络或服务连接指示板上找到 **Routing Information**（路由信息）按钮。

 ©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.

接入多个远程网络

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	• Prisma Access 许可证

要简化接入和配置远程网络的过程，您可以选择接入至少一个远程网络，然后将这些设置导出到逗号分隔值 (CSV) 文本文件。该 CSV 文件包含了为导出而选择的网络的 IPSec 隧道和 IKE 网关设置值，然后可以编辑这些设置，并使它们对于可能想要纳入的每个新网络而言都是独一无二的。您可以修改 CSV 文件以包含 100 个新的远程网络，然后将 CSV 文件导入回去，以加快接入新远程网络位置的过程。

CSV 文件不包括密钥或密码，例如 BGP 共享机密、IKE 预共享密钥、代理 ID、IKE 加密配置文件、IPSec 加密配置文件。因此，IPSec 隧道和 IKE 网关设置所需的任何密钥和密码都是从您在启动 CSV 文件导入时选择的网络继承的。

使用这一批量导入过程时，您必须等待 Prisma Access 部署用于保护这些位置的基础设施。

STEP 1 | 选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Remote Networks**（远程网络）（在“Onboarding（接入）”部分中）。

STEP 2 | 选择一个位置，然后选择 **Export**（导出）以导出以前接入的远程网络的配置。

如果您尚未添加任何位置，则需要选择 **Add**（添加）以添加一个位置，然后下载其配置。您必须选择一个远程网络，然后单击 **Export**（导出）.包含设置的 CSV 文件将下载到您的计算机。

STEP 3 | (仅按计算位置分配带宽的部署) 确保您已为要接入的位置分配了带宽。

您的每个接入位置都有一个为其分配带宽的相应计算位置。

1. 选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Remote Networks**（远程网络），并单击 **Bandwidth Allocation**（带宽分配）区域中的齿轮图标。
2. 在显示的表中检查 **Bandwidth Allocation**（带宽分配）字段。

   此区域中的表显示了计算位置到 Prisma Access 位置的映射。您必须为与要接入的位置关联的计算位置分配带宽。例如，要接入 Japan Central（日本中部）位置，请确保您已在 Asia Northeast（东南亚）计算位置分配了带宽。
3. 如果您尚未为与要接入的位置关联的计算位置分配带宽，请立即添加。

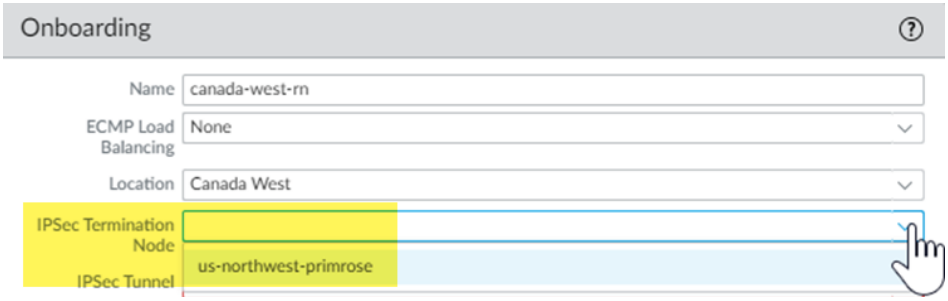
 ©2025 Palo Alto Networks, Inc.

STEP 4 | （仅按计算位置分配带宽的部署）找到与您想要接入的一个或多个位置相关联的 **IPSec Termination Node**（**IPSec** 终止节点）。

将某个 *IPSec* 终止节点添加到远程网络，然后在 CSV 文件的 **spn-name** 列中输入此值。每个 IPSec 终端节点可提供高达 1000 Mbps 的带宽。

要查找 IPSec 终止节点，请执行下列操作之一：

- 选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Remote Networks**（远程网络），单击 **Add**（添加）以添加一个远程网络，然后选择您想要接入的位置，并记下接入区域中的 IPSec 终止节点选项。



- 使用管理 Prisma Access 的 Panorama 打开一个命令行界面 (CLI) 会话，然后输入 `show plugins cloud_services remote-networks agg-bandwidth region` *compute-location-name*，其中 *compute-location-name* 是与您想要接入的位置相关联的计算位置。IPSec 终止节点显示在 `spn-name-list` 字段中。

STEP 5 | 修改 CSV 文件以添加远程网络的配置。

有关此文件中的字段和可能值的说明，请参见远程网络表中的字段。

您必须重命名导出文件中列出的网络。如果文件名称重复，则导入将失败。

STEP 6 | 选择 **Import**（导入）以导入 CSV 文件。

文件中的配置将显示在屏幕上。您选择用于导入文件的远程网络将用作模型配置，并且文件中列出的远程网络将从该网络中继承密钥和任何不需要唯一的缺失值。

STEP 7 | 提交并推送更改。

1. 依次选择 **Commit**（提交） > **Commit and Push**（提交并推送）以提交并推送更改。
2. 单击 **OK**（确定）和 **Push**（推送）。

远程网络表中的字段

下表对远程网络表中的字段进行了说明。在 **Required**（必填）这一行中，标记为 **Y**（是）的字段为必填字段，标记为 **N**（否）的字段为可选字段。

©2025 Palo Alto Networks, Inc.

字段	说明	Required? (Y/N)（必填？（是/否））
名称	远程网络的名称。	Y
bandwidth	（仅按位置分配带宽的部署）远程网络的已分配带宽。可接受的值为： • 2 Mbps • 5 Mbps • 10 Mbps • 20 Mbps • 25 Mbps • 50 Mbps • 100 Mbps • 150 Mbps • 300 Mbps • 500 Mbps • 1000 Mbps  *1000 Mbps* 带宽选项处于预览模式。预览期间的吞吐量是在尽力而为的基础上提供的，实际性能将根据流量混合而变化。	Y
区域	远程网络的位置。 输入与本文档中完全相同的位置（例如，**US West**（美国西部）或 **Japan South**（日本南部））。	Y
subnets	远程网络 LAN 端的静态路由子网。用逗号分隔多个子网。	N
bgp_peer_as	远程网络对等设备的 BGP 自治系统编号 (ASN)。	N
bgp_peer_address	远程网络对等设备的 BGP 对等地址。	N
tunnel_name	IPSec 隧道配置的名称。值必须唯一。	Y
gateway_name	IKE 网关配置的名称。值必须唯一。	Y
peer_ip_address	Prisma Access 对等设备的 IP 地址。	N

©2025 Palo Alto Networks, Inc.

字段	说明	Required? (Y/N)（必填？（是/否））
local_id_type	Prisma Access 提供给对等设备的 IKE ID 的类型。如果在要导入此文件的远程网络中使用证书，则所有指定的导入类型都将引用已配置的证书值。	N
local_id_value	Prisma Access 提供给对等设备的 IKE ID 的值。如果在要导入此文件的远程网络中使用证书，则所有指定的导入类型都将引用已配置的证书值。	N
peer_id_type	对等设备提供给 Prisma Access 的 IKE ID 的值。如果在要导入此文件的远程网络中使用证书，则所有指定的导入类型都将引用对等设备证书值。	N
peer_id_value	Prisma Access 提供给对等设备的 IKE ID 的值。如果在要导入此文件的远程网络中使用证书，则所有指定的导入类型都将引用对等设备证书值。	N
monitor_ip	云将使用该隧道监控 IP 地址来确定 IPSec 隧道已启用且对等网络是可访问的。 不能导出隧道监视器的 *proxy-ID* 值。	N
proxy_ids	为对等设备配置的代理 ID。对于基于路由的 VPN，请将此字段留空。按以下 CSV 配置格式指定代理 ID： [{"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	指定是否启用辅助 IPSec 隧道。可接受的值为 yes 和 no。	N
sec_tunnel_name	辅助 IPSec 隧道配置的名称。如果指定辅助隧道，则值必须唯一。	N
sec_gateway_name	辅助 IKE 网关配置的名称。如果指定辅助隧道，则值必须唯一。	N

©2025 Palo Alto Networks, Inc.

字段	说明	Required? (Y/N)（必填？（是/否））
sec_peer_ip_address	辅助 IPSec 隧道的 Prisma Access 对等设备的 IP 地址。	N
sec_local_id_type	Prisma Access 提供给对等设备以用于辅助 IPSec 隧道的 IKE ID 类型。如果在要导入此文件的远程网络中使用证书，则所有指定的导入类型都将引用已配置的证书值。	N
sec_local_id_value	Prisma Access 提供给对等设备以用于辅助 IPSec 隧道的 IKE ID 值。如果在要导入此文件的远程网络中使用证书，则所有指定的导入类型都将引用已配置的证书值。	N
sec_peer_id_type	对等设备提供给 Prisma Access 以用于辅助 IPSec 隧道的 IKE ID 值。如果在要导入此文件的远程网络中使用证书，则所有指定的导入类型都将引用对等设备证书值。	N
sec_peer_id_value	Prisma Access 提供给对等设备以用于辅助 IPSec 隧道的 IKE ID 值。如果在要导入此文件的远程网络中使用证书，则所有指定的导入类型都将引用对等设备证书值。	N
sec_monitor_ip	云将该隧道监控 IP 地址用于辅助 IPSec 隧道，以确定 IPSec 隧道已启用且对等网络是可访问的。 不能导出隧道监视器的 *proxy-ID* 值。	N
sec_proxy_ids	为辅助 IPSec 隧道的对等设备配置的代理 ID。对于基于路由的 VPN，请将此字段留空。按以下 CSV 配置格式指定代理 ID： [{"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
ecmp_link_1_tunnel_name	（仅限 ECMP 部署）ECMP 隧道 1 的 IPSec 隧道配置的名称。值必须唯一。	

©2025 Palo Alto Networks, Inc.

字段	说明	Required? (Y/N)（必填？（是/否））
ecmp_link_1_gateway_name	（仅限 ECMP 部署）ECMP 隧道 1 的 IKE 网关配置的名称。值必须唯一。	
ecmp_link_1_peer_ip_address	（仅限 ECMP 部署）ECMP 隧道 1 的 Prisma Access 对等设备的 IP 地址。	
ecmp_link_1_local_id_type	（仅限 ECMP 部署）Prisma Access 提供给对等设备以用于 ECMP 隧道 1 的 IKE ID 类型。如果在要导入此文件的远程网络中使用证书，则所有指定的导入类型都将引用已配置的证书值。	
ecmp_link_1_local_id_value	（仅限 ECMP 部署）Prisma Access 提供给对等设备以用于 ECMP 隧道 1 的 IKE ID 值。如果在要导入此文件的远程网络中使用证书，则所有指定的导入类型都将引用已配置的证书值。	
ecmp_link_1_peer_id_type	（仅限 ECMP 部署）对等设备提供给 Prisma Access 以用于 ECMP 隧道 1 的 IKE ID 值。如果在要导入此文件的远程网络中使用证书，则所有指定的导入类型都将引用对等设备证书值。	
ecmp_link_1_peer_id_value	（仅限 ECMP 部署）Prisma Access 提供给对等设备以用于 ECMP 隧道 1 的 IKE ID 值。如果在要导入此文件的远程网络中使用证书，则所有指定的导入类型都将引用对等设备证书值。	
ecmp_link_1_monitor_ip	（仅限 ECMP 部署）隧道监控 IP 地址，云将使用该地址来确定 IPSec 隧道是否打开，以及 ECMP 隧道 1 是否可以访问对等网络。 不能导出隧道监视器的 *proxy-ID* 值。	
ecmp_link_1_proxy_ids	（仅限 ECMP 部署）为 ECMP 隧道 1 的对等设备配置的代理 ID。对于基于路由的 VPN，请将此字段留空。按以下 CSV 配置格式指定代理 ID： [{"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.

字段	说明	Required? (Y/N)（必填？（是/否））
ecmp_link_1_bgp_peer_as	（仅限 ECMP 部署）ECMP 隧道 1 的远程网络对等设备的 BGP 自治系统编号 (ASN)。	
ecmp_link_1_bgp_peer_address	（仅限 ECMP 部署）ECMP 隧道 1 的远程网络对等设备的 BGP 对等地址。	
ecmp_link_2_tunnel_name	（仅限 ECMP 部署）ECMP 隧道 2 的 IPSec 隧道配置的名称。值必须唯一。	
ecmp_link_2_gateway_name	（仅限 ECMP 部署）ECMP 隧道 2 的 IKE 网关配置的名称。值必须唯一。	
ecmp_link_2_peer_ip_address	（仅限 ECMP 部署）ECMP 隧道 2 的 Prisma Access 对等设备的 IP 地址。	
ecmp_link_2_local_id_type	（仅限 ECMP 部署）Prisma Access 提供给对等设备以用于 ECMP 隧道 2 的 IKE ID 类型。如果在要导入此文件的远程网络中使用证书，则所有指定的导入类型都将引用已配置的证书值。	
ecmp_link_2_local_id_value	（仅限 ECMP 部署）Prisma Access 提供给对等设备以用于 ECMP 隧道 2 的 IKE ID 值。如果在要导入此文件的远程网络中使用证书，则所有指定的导入类型都将引用已配置的证书值。	
ecmp_link_2_peer_id_type	（仅限 ECMP 部署）对等设备提供给 Prisma Access 以用于 ECMP 隧道 2 的 IKE ID 值。如果在要导入此文件的远程网络中使用证书，则所有指定的导入类型都将引用对等设备证书值。	
ecmp_link_2_peer_id_value	（仅限 ECMP 部署）Prisma Access 提供给对等设备以用于 ECMP 隧道 2 的 IKE ID 值。如果在要导入此文件的远程网络中使用证书，则所有指定的导入类型都将引用对等设备证书值。	
ecmp_link_2_monitor_ip	（仅限 ECMP 部署）隧道监控 IP 地址，云将使用该地址来确定 IPSec 隧道是否打开，以及 ECMP 隧道 2 是否可以访问对等网络。 不能导出隧道监视器的 *proxy-ID* 值。	

©2025 Palo Alto Networks, Inc.

字段	说明	Required? (Y/N)（必填？（是/否））
ecmp_link_2_proxy_ids	（仅限 ECMP 部署）为 ECMP 隧道 2 的对等设备配置的代理 ID。对于基于路由的 VPN，请将此字段留空。按以下 CSV 配置格式指定代理 ID： [{"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_2_bgp_peer_as	（仅限 ECMP 部署）ECMP 隧道 2 的远程网络对等设备的 BGP 自治系统编号 (ASN)。	
ecmp_link_2_bgp_peer_address	（仅限 ECMP 部署）ECMP 隧道 2 的远程网络对等设备的 BGP 对等地址。	
ecmp_link_3_tunnel_name	（仅限 ECMP 部署）ECMP 隧道 3 的 IPSec 隧道配置的名称。值必须唯一。	
ecmp_link_3_gateway_name	（仅限 ECMP 部署）ECMP 隧道 3 的 IKE 网关配置的名称。值必须唯一。	
ecmp_link_3_peer_ip_address	（仅限 ECMP 部署）ECMP 隧道 3 的 Prisma Access 对等设备的 IP 地址。	
ecmp_link_3_local_id_type	（仅限 ECMP 部署）Prisma Access 提供给对等设备以用于 ECMP 隧道 3 的 IKE ID 类型。如果在要导入此文件的远程网络中使用证书，则所有指定的导入类型都将引用已配置的证书值。	
ecmp_link_3_local_id_value	（仅限 ECMP 部署）Prisma Access 提供给对等设备以用于 ECMP 隧道 3 的 IKE ID 值。如果在要导入此文件的远程网络中使用证书，则所有指定的导入类型都将引用已配置的证书值。	
ecmp_link_3_peer_id_type	（仅限 ECMP 部署）对等设备提供给 Prisma Access 以用于 ECMP 隧道 3 的 IKE ID 值。如果在要导入此文件的远程网络中使用证书，则所有指定的导入类型都将引用对等设备证书值。	
ecmp_link_3_peer_id_value	（仅限 ECMP 部署）Prisma Access 提供给对等设备以用于 ECMP 隧道 3 的 IKE ID 值。如果在	

 ©2025 Palo Alto Networks, Inc.

字段	说明	Required? (Y/N)（必填？（是/否））
	要导入此文件的远程网络中使用证书，则所有指定的导入类型都将引用对等设备证书值。	
ecmp_link_3_monitor_ip	（仅限 ECMP 部署）隧道监控 IP 地址，云将使用该地址来确定 IPSec 隧道是否打开，以及 ECMP 隧道 3 是否可以访问对等网络。 不能导出隧道监视器的 *proxy-ID* 值。	
ecmp_link_3_proxy_ids	（仅限 ECMP 部署）为 ECMP 隧道 3 的对等设备配置的代理 ID。对于基于路由的 VPN，请将此字段留空。按以下 CSV 配置格式指定代理 ID： [{"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	（仅限 ECMP 部署）ECMP 隧道 3 的远程网络对等设备的 BGP 自治系统编号 (ASN)。	
ecmp_link_3_bgp_peer_address	（仅限 ECMP 部署）ECMP 隧道 3 的远程网络对等设备的 BGP 对等地址。	
ecmp_link_4_tunnel_name	（仅限 ECMP 部署）ECMP 隧道 4 的 IPSec 隧道配置的名称。值必须唯一。	
ecmp_link_4_gateway_name	（仅限 ECMP 部署）ECMP 隧道 4 的 IKE 网关配置的名称。值必须唯一。	
ecmp_link_4_peer_ip_address	（仅限 ECMP 部署）ECMP 隧道 4 的 Prisma Access 对等设备的 IP 地址。	
ecmp_link_4_local_id_type	（仅限 ECMP 部署）Prisma Access 提供给对等设备以用于 ECMP 隧道 4 的 IKE ID 类型。如果在要导入此文件的远程网络中使用证书，则所有指定的导入类型都将引用已配置的证书值。	
ecmp_link_4_local_id_value	（仅限 ECMP 部署）Prisma Access 提供给对等设备以用于 ECMP 隧道 4 的 IKE ID 值。如果在	

 ©2025 Palo Alto Networks, Inc.

字段	说明	Required? (Y/N)（必填？（是/否））
	要导入此文件的远程网络中使用证书，则所有指定的导入类型都将引用已配置的证书值。	
ecmp_link_4_peer_id_type	（仅限 ECMP 部署）对等设备提供给 Prisma Access 以用于 ECMP 隧道 4 的 IKE ID 值。如果在要导入此文件的远程网络中使用证书，则所有指定的导入类型都将引用对等设备证书值。	
ecmp_link_4_peer_id_value	（仅限 ECMP 部署）Prisma Access 提供给对等设备以用于 ECMP 隧道 4 的 IKE ID 值。如果在要导入此文件的远程网络中使用证书，则所有指定的导入类型都将引用对等设备证书值。	
ecmp_link_4_monitor_ip	（仅限 ECMP 部署）隧道监控 IP 地址，云将使用该地址来确定 IPSec 隧道是否打开，以及 ECMP 隧道 4 是否可以访问对等网络。 不能导出隧道监视器的 *proxy-ID* 值。	
ecmp_link_4_proxy_ids	（仅限 ECMP 部署）为 ECMP 隧道 4 的对等设备配置的代理 ID。对于基于路由的 VPN，请将此字段留空。按以下 CSV 配置格式指定代理 ID： [{"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	（仅限 ECMP 部署）ECMP 隧道 4 的远程网络对等设备的 BGP 自治系统编号 (ASN)。	
ecmp_link_4_bgp_peer_address	（仅限 ECMP 部署）ECMP 隧道 4 的远程网络对等设备的 BGP 对等地址。	
spn-name	（仅按计算位置分配带宽的部署）IPSec 终止节点的名称。对于按计算位置分配带宽的部署，此字段为必填。	

 ©2025 Palo Alto Networks, Inc.

验证远程网络是否已连接到 Prisma Access

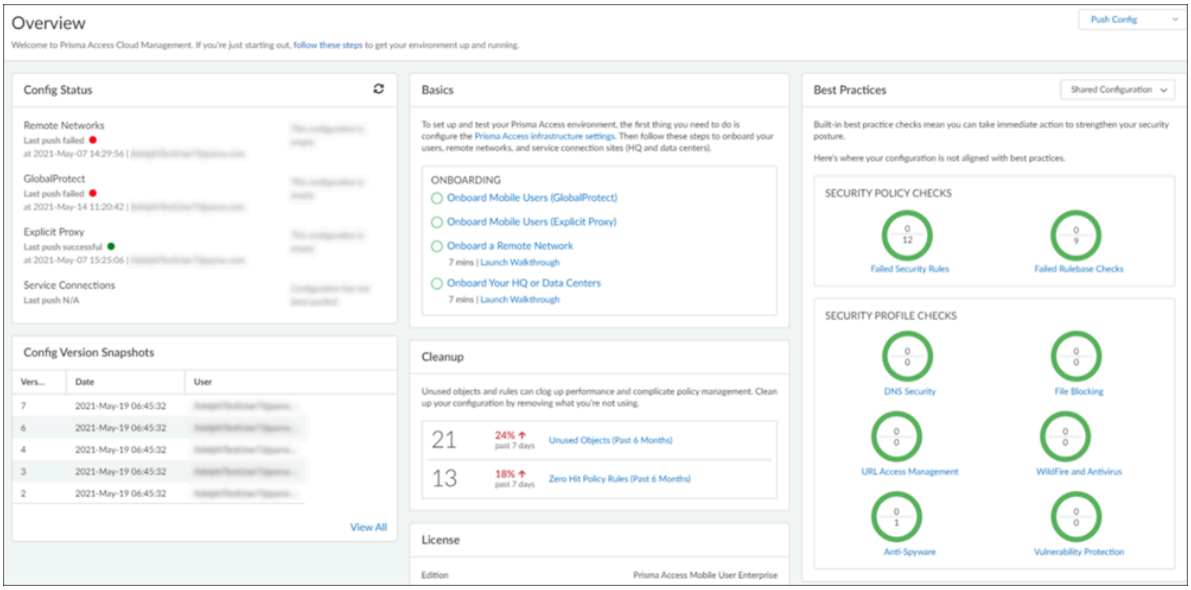
在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证

在远程网络上配置 IPSec VPN 设备后，请验证隧道状态。验证远程网络的状态时，请记住以下几点：

- 验证远程网络的 IPSec 隧道的状态。
- 验证远程网络的最后一步是查看日志并确保流量正在流经 Prisma Access。如果有错误或警告，请检查 Prisma Access 中的系统日志以及远程网络设备上的本地日志。请先解决所有错误或警告，然后继续配置。
- 根据需要继续添加远程网络。
- Strata Cloud Manager
- Panorama

验证远程网络是否已连接到 Prisma Access (Strata Cloud Manager)

选择 **Manage**（管理） > **Configuration**（配置） > **NGFW** 和 **Prisma Access**，将 **Configuration Scope**（配置范围）更改为 **Prisma Access**然后选择 **Prisma Access Sync Status**（同步状态） > **Remote Networks**（远程网络）。



 ©2025 Palo Alto Networks, Inc.

验证远程网络是否已连接 Prisma Access (Panorama)

STEP 1 | > > > 选择Panorama云服务状态以验证远程网络连接是否已成功部署。

部署状态区域允许您在入职和部署作业完成之前查看进度，以及查看有关已完成作业状态的更多信息。

STEP 2 | > > > 要显示一张地图，显示您所选择区域中远程网络的位置，请选择Panorama云服务状态监视器，然后点击远程网络选项卡。

STEP 3 | 选择一个区域以获取该区域的更多详细信息。

©2025 Palo Alto Networks, Inc.

STEP 4 | 单击地图下方的选项卡以查看其他远程网络统计信息。

状态标签

- 位置—您远程网络部署的位置。
- 远程对等体 — 远程网络与之建立IPSec隧道连接的对等体。
- IPSec 终止节点—与远程网络关联的 IPSec 终止节点。此字段仅在您按计算位置分配带宽时显示。
- ECMP—您是否在此远程网络连接上启用了 ECMP 负载均衡。
- 配置状态 - 您上次向服务推送的配置状态。如果您在本地进行了更改，但尚未将配置推送到云端，则状态显示为不同步。将鼠标悬停在状态指示器上以获取更详细的信息。在将配置提交并推送到 Prisma Access 后，配置状态更改为同步。
- BGP 状态—显示有关远程网络位置和 Prisma Access 的防火墙或路由器之间 BGP 状态的信息。尽管您可能会暂时看到状态经过各种 BGP 状态（空闲、活动、打开发送、打开挂起、打开确认），但最常见的 BGP 状态显示：
  - 连接 — 远程网络位置的路由器正在尝试建立与 Prisma Access 的BGP对等关系。
  - 已建立 — BGP对等关系已建立。

    此字段还将显示BGP连接是否处于错误状态：
  - 警告—超过八分钟没有BGP状态更新。这可能表示防火墙出现故障。
  - 错误—BGP状态未知。
- Prisma Access隧道状态—与远程网络之间连接的操作状态。

Statistics（统计信息）选项卡：

- 位置—您远程网络部署的位置。
- 远程对等体 — 此远程网络正在建立 IPSec 隧道的公司位置。
- 入口带宽 (Mbps) — 从远程网络位置到 Prisma Access

  对于入口带宽、入口峰值带宽、传出带宽和传出峰值带宽字段，当远程网络的带宽消耗超过分配带宽的*80%*时，数字将以红色显示。
- 入口峰值带宽（Mbps）— 从远程网络位置到云服务的峰值负载。
- 传出带宽（Mbps）— 从 Prisma Access 到远程网络位置的带宽。
- 传出峰值带宽（Mbps）—从 Prisma Access 到远程网络位置的峰值负载。

要查找该地区位置的统计信息，请选择带宽使用情况。

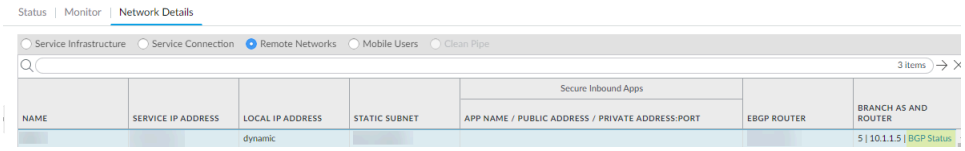
选择一个位置的勾选标记以查看详细的带宽使用情况。对于按计算位置分配带宽的部署，选择一个IPSec终止节点以查看该节点的统计信息。Prisma Access 使用第95百分位标准来收集统计数据，该标准跟踪峰值利用率的带宽，并忽略前5%的利用率峰值和大幅度的突发。

 ©2025 Palo Alto Networks, Inc.

验证远程连接 BGP 状态

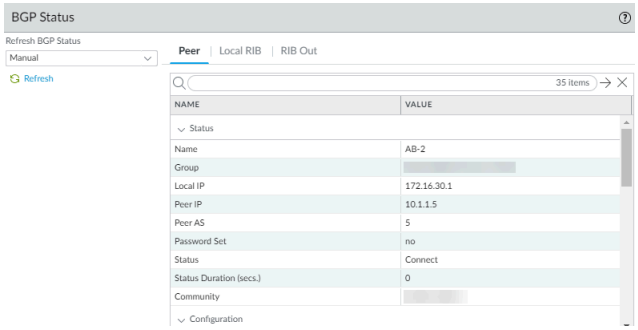
在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

如果您配置了 BGP，则可以通过选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details** >（网络详细信息） > **Remote Networks**（远程网络） > **BGP Status**（**BGP** 状态）来检查其状态。

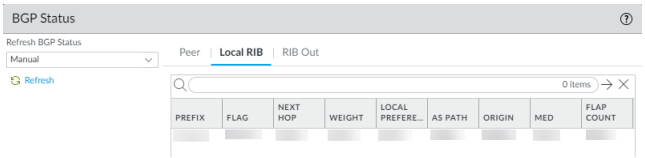


此时将显示 BGP 状态对话框。该表为您提供以下信息：

- 对等体 — BGP 对等体的路由信息，包括状态、路由总数、配置以及运行时统计信息和计数器。路由总数显示在 **bgpAfiIpv4-unicast Counters**（**bgpAfiIpv4-unicast** 计数器）区域、**Incoming Total**（传入总数）和 **Outgoing Total**（传出总数）字段中。



- 本地 **RIB** — 从不同对等体接收并存储在路由信息库 (RIB) 中的路由信息。



- 外部 **RIB** — Prisma Access 通过 BGP 更新消息向其对等体通告的路由信息。有关此表的示例以及有关 BGP 如何利用您为移动用户创建的 IP 地址池的信息，请参阅BGP 如何为服务连接和远程网络连接通告移动用户 IP 地址池。

 ©2025 Palo Alto Networks, Inc.

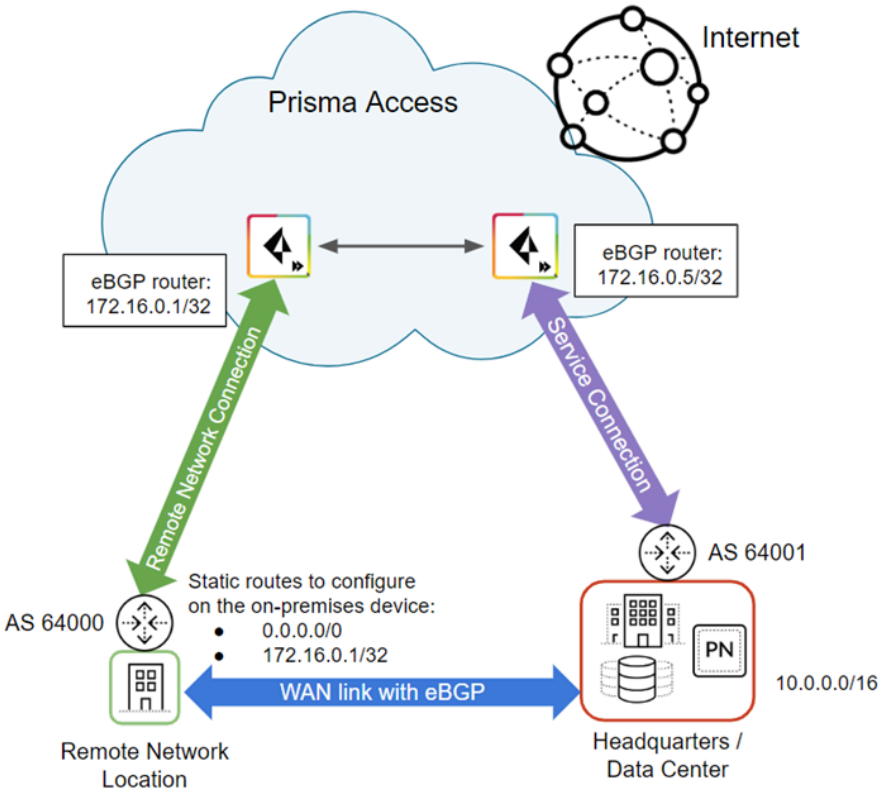
配置通过 WAN 链路连接的远程网络和服务连接

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

如果部署中的远程网络位置和具有服务连接的总部或数据中心通过 WAN 链路直接连接，为了确保最佳路由（使用 eBGP），您必须执行以下操作：

- 向 eBGP 路由器地址添加静态路由。除了将所有流量发送到 Prisma Access 的默认路由之外，您还必须在远程网络中支持 IPSec 的设备或路由器上本地添加静态路由。
- 筛选从总部支持 IPSec 的设备或路由器通告到其他直连位置的 eBGP 对等体的路由。最佳实践是，将总部的 BGP 路由器配置为仅通告您希望允许通过 WAN 链路访问的路由；确保总部的 eBGP 路由器不会将其从 Prisma Access 学习到的路由通告到由 Prisma Access 保护的其他远程网络位置。在此示例中，总部的 eBGP 路由器仅通告分支机构办公室的员工连接到总部的服务器（子网）所需的路由。

下图显示的是一家零售企业，它有两条路径可访问总部的服务器。一条路径是为访问总部服务器的员工提供直接连接的 WAN 链路，另一条路径则保护此位置的其他用户生成的流量。例如，客户通过 Wi-Fi 访问零售商的网站或使用分支机构办公室的自助服务终端查看库存时所产生的流量。这些流量通过隧道发送到远程网络，然后发送到总部。

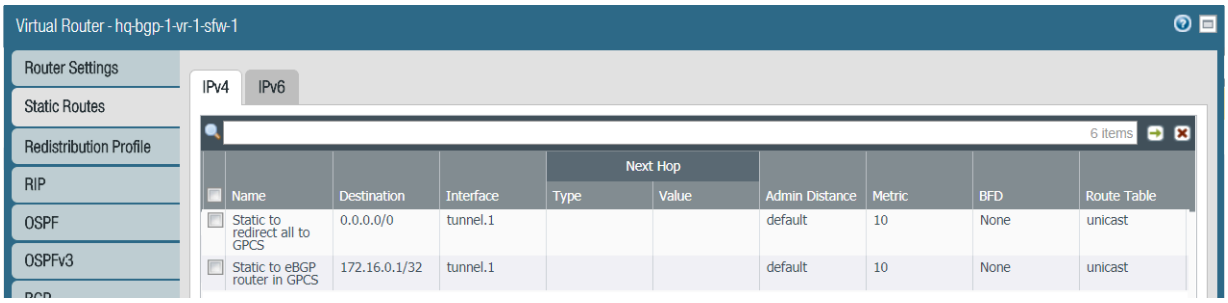


要设置此配置，请创建远程网络连接并创建服务连接，以加入远程网络和总部位置。以下详细信息展示了如何设置每个位置的路由器配置以确保最佳路由：

 ©2025 Palo Alto Networks, Inc.

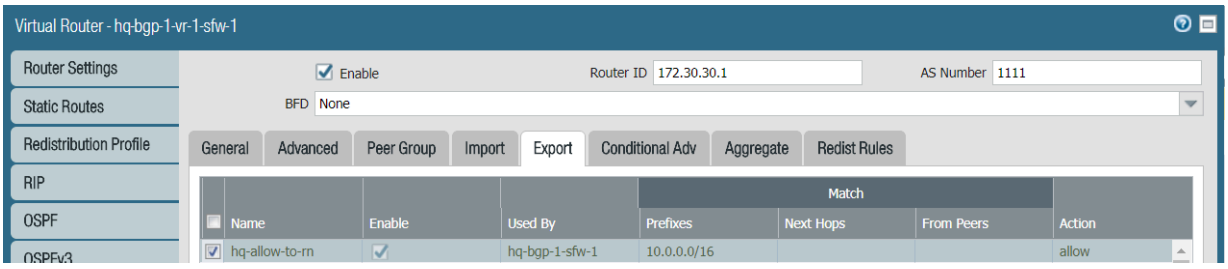
STEP 1 | 在远程网络位置的路由器或本地支持 IPSec 的设备上添加静态路由。

如果 WAN 链路的边缘部署有 Palo Alto Networks 防火墙，请在 **Network**（网络） > **Virtual Routers**（虚拟路由器） > **Static Routes**（静态路由）上 **Add**（添加）静态路由：



STEP 2 | 配置您希望通过 WAN 链路通告到另一个直连位置的路由。

在此示例中，您需要在总部位置配置此设置。如果 WAN 链路的边缘部署有本地 Palo Alto Networks 防火墙，您可以设置路由重新分发，并在 **Network**（网络） > **Virtual Routers**（虚拟路由器） > **BGP** 上配置要导出的 BGP 路由。



 ©2025 Palo Alto Networks, Inc.

远程网络的 QoS

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证 ❑ Minimum Required Prisma Access Version：首选 3.0

新 Prisma Access 部署通过计算地点为远程网络提供带宽。要在远程网络中使用 QoS，您需要在计算地点级别启用或禁用 QoS，并指定保证带宽。不过，您仍然可以通过为每个站点自定义带宽，在每个地点级别调整 QoS 和保证带宽。

Prisma Access 使用 *IPSec 终止节点*划分计算地点带宽。每个 IPSec 终止节点可为您提供最多 1000 Mbps 的带宽。如果您为计算地点分配超过 1,000 Mbps 的带宽，Prisma Access 会为您提供额外的 IPSec 终止节点。

- Strata Cloud Manager
- Panorama

远程网络的 QoS (Strata Cloud Manager)

使用 QoS 对远程网络中的关键流量进行优先级排序，并为计算地点中的远程网络站点设置最大和保证带宽。

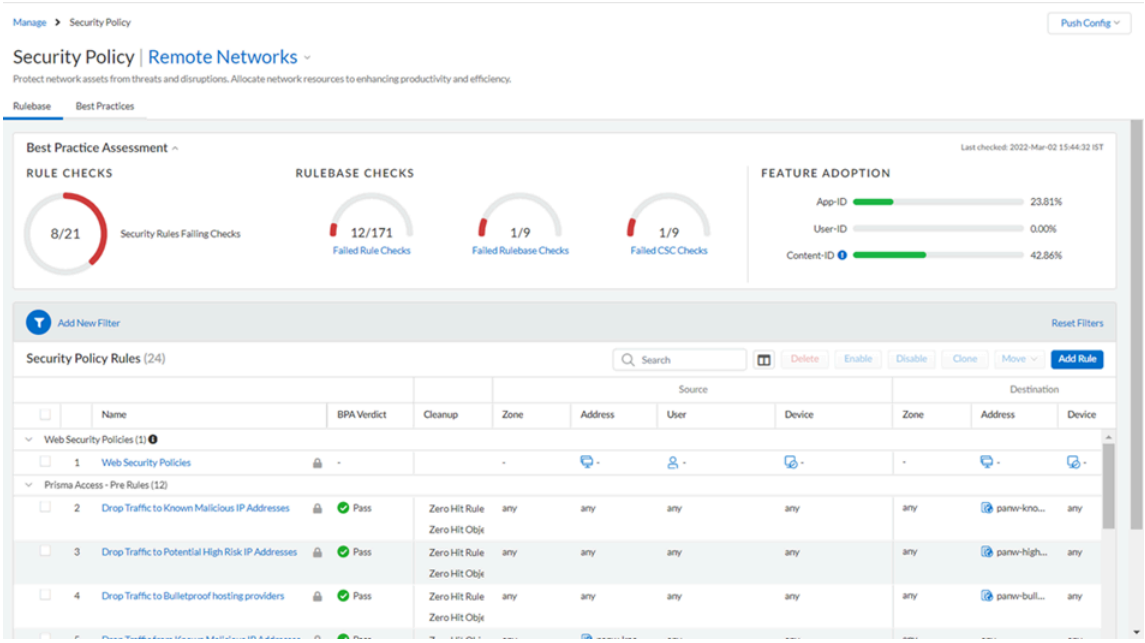
©2025 Palo Alto Networks, Inc.

STEP 1 | 标记要进行 QoS 处理的流量。

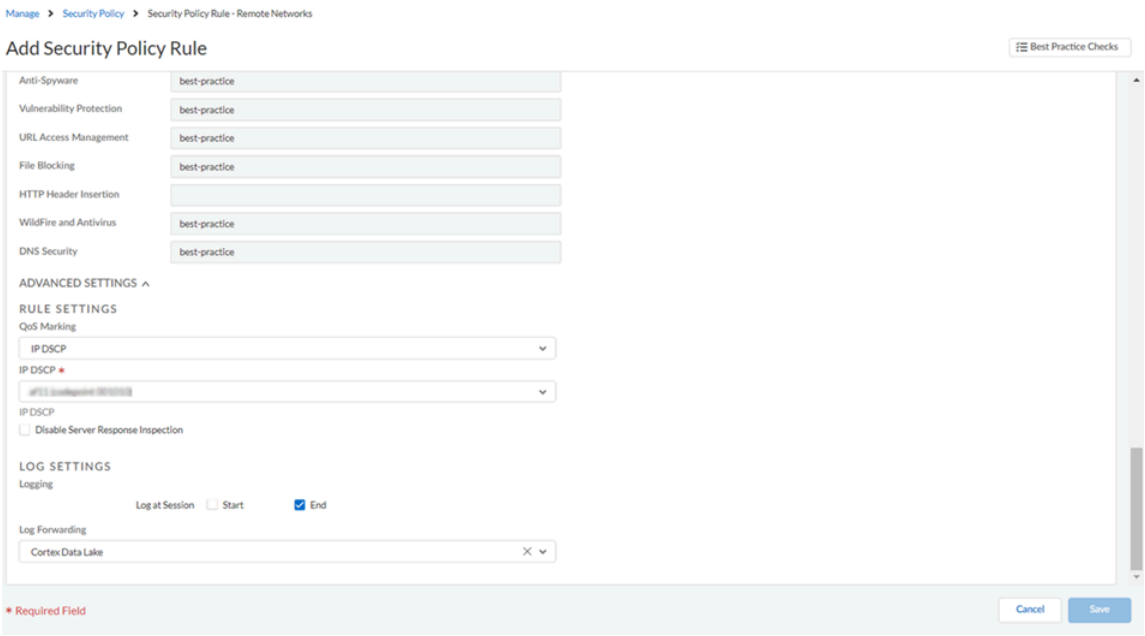
1. 选择 **Manage**（管理） > **Configuration**（配置） > **NGFW** 和 **Prisma Access** > **Security Services**（安全服务） > **Security Policy**（安全策略）。

   确保您正在为远程网络创建策略。

2. **Add Rule**（添加规则）。



3. 通过在 **Advanced Settings**（高级设置）中分配 DSCP 值来标记传入流量并保存该策略。

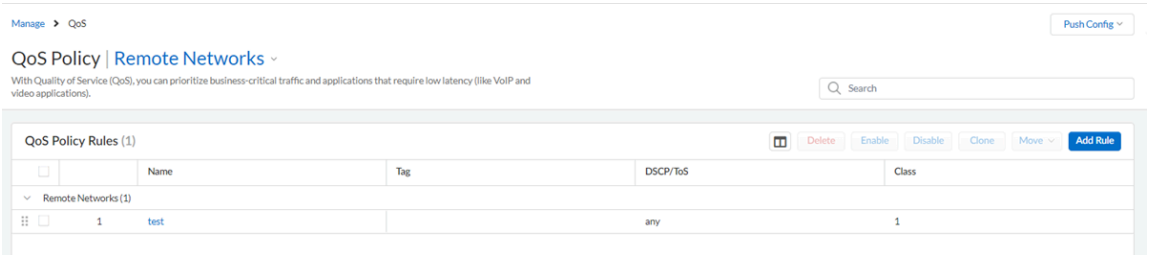


 ©2025 Palo Alto Networks, Inc.

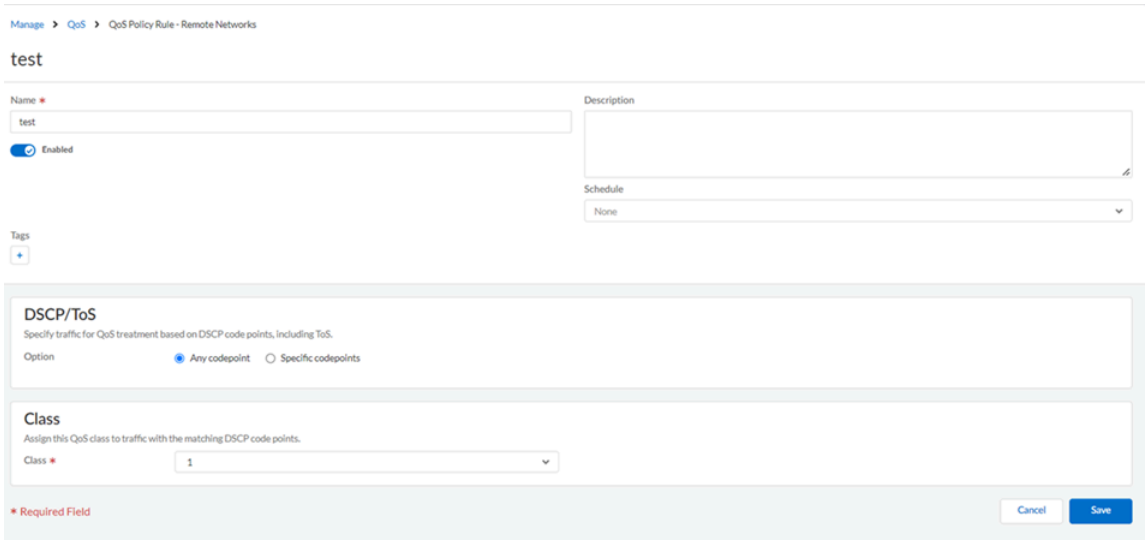
STEP 2 | 添加一个或多个 QoS 策略规则。

您使用 QoS 策略将 DSCP 标记绑定到八个可用类之一。您将在后续步骤中定义 QoS 类所接受的处理。QoS 类确定与 QoS 策略规则匹配的流量的优先级和带宽。

1. 选择 **Monitor**（监控） > **Network Services**（网络服务） > **QoS**。
2. **Add Rule**（添加规则）。



3. 输入值并保存策略。



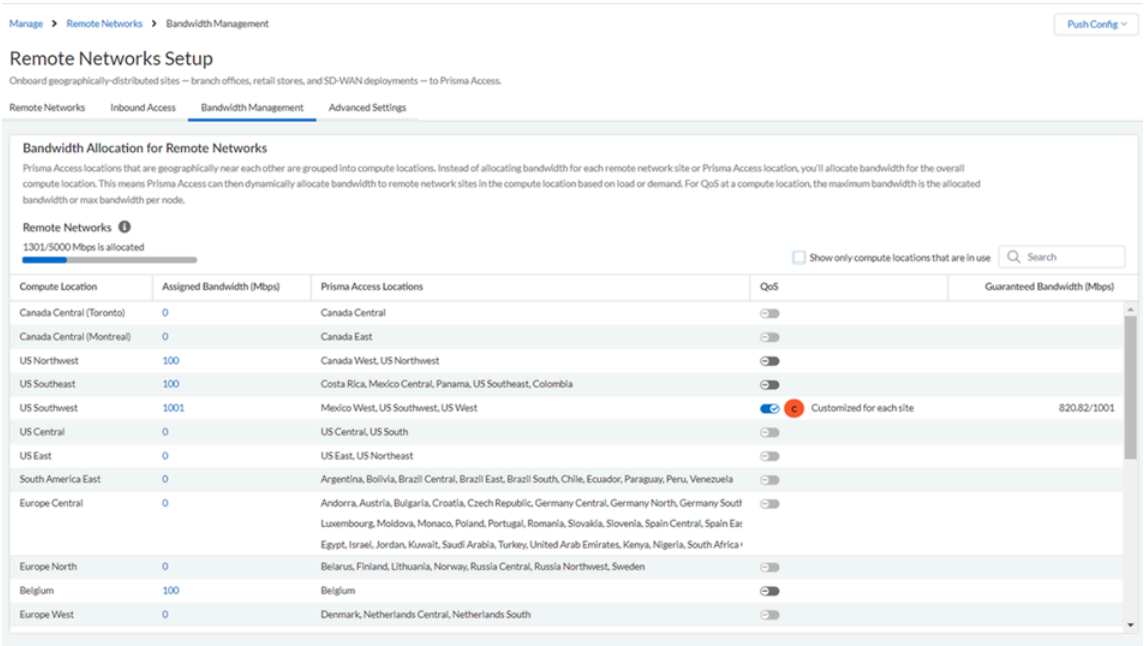
 ©2025 Palo Alto Networks, Inc.

STEP 3 | 为您的远程网络地点启用 QoS。

1. 选择 **Manage**（管理） > **Service Setup**（服务设置） > **Remote Networks**（远程网络） > **Bandwidth Management**（带宽管理）。
2. 确定要部署 QoS 的 Prisma Access 地点；然后找到与每个 Prisma Access 地点对应的计算地点。

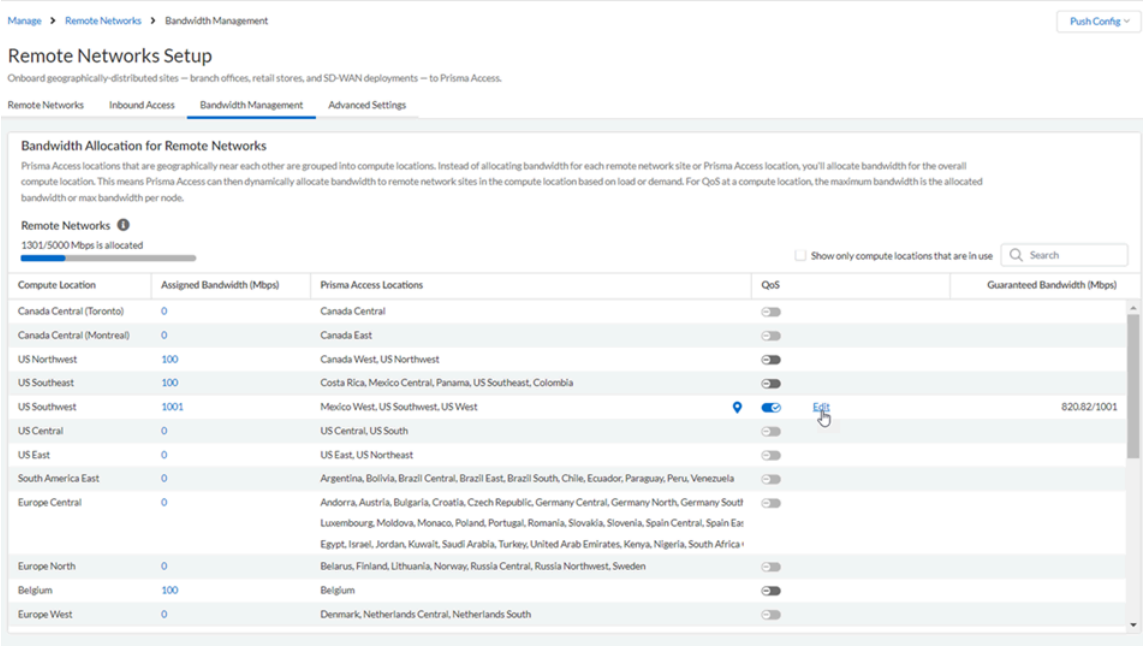
   每个 Prisma Access 地点根据其计算地点分配带宽，并且您必须知道要分配 QoS 的地点的计算地点的名称。
3. 在 **QoS** 列中启用计算地点级别的 **QoS**。

   您输入的任何设置都可应用于与此计算地点对应的所有地点。



 ©2025 Palo Alto Networks, Inc.

STEP 4 | **Edit**（编辑）该计算地点的 QoS 设置。



1. 选择保证的带宽比率，该比率基于为计算地点分配的整个带宽。

   例如，如果您为美国西南部计算地点分配了 1001 Mbps 的带宽，并且在 **Guaranteed Bandwidth Ratio**（保证的带宽比率）中输入 82%，则该计算地点的保证带宽为 820.82 Mbps。

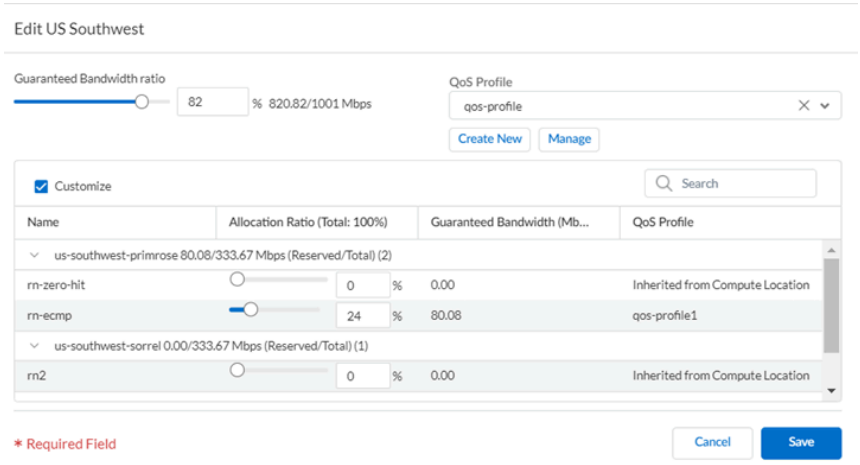
   默认情况下，每个远程网络的百分比等于连接的数量。例如，假设某个计算地点有 4 个连接，总保证带宽为 820.82 Mbps，则每个地点将获得 25% 的带宽或 205.2 Mbps 的带宽。

   如果启用了 AIOps 支持的 ADEM 许可证，则自动为所有计算地点启用该许可证。

2. **Create New**（新建）QoS 配置文件或 **Manage**（管理）现有 QoS 配置文件。

   您可以使用 QoS 配置文件来实现对出口点流量的整形。

3. （可选）为计算地点中的远程网络站点自定义 QoS 设置。如果每个计算地点有多个远程网络，并且想要更改每个远程网络的带宽比率或 QoS 配置文件，请选择 **Customize**（自定义）并更改带宽分配比率、QoS 配置文件或两者。



 ©2025 Palo Alto Networks, Inc.

如果选择 ***Customize***（自定义），然后在同一个 *IPSec* 终止节点中加入其他远程网络，则新加入的站点获得的分配比率为 *0*，并且您必须通过手动方式重新平衡现有站点和新加入站点之间的分配比率。

STEP 5 | **Save**（保存）更改。

STEP 6 | **Push**（推送）配置。

远程网络的 QoS (Panorama)

通过完成以下任务在 Prisma Access 中配置服务质量。

STEP 1 | 为远程网络和移动用户添加一个或多个安全策略规则，以标记 QoS 的入口流量。

您可以使用这些策略来匹配流量并为其分配所选的 DSCP 值。

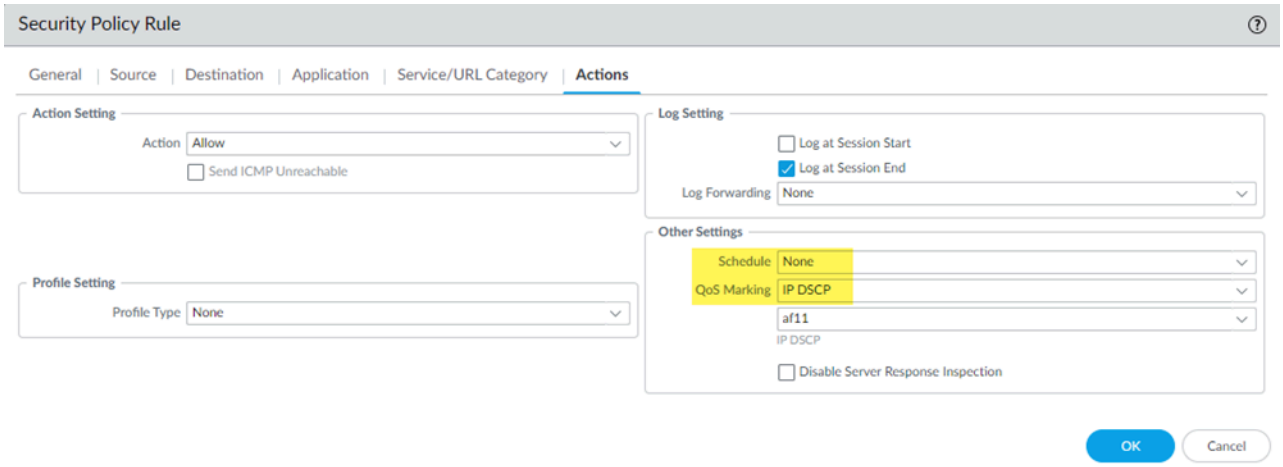
1. 选择 **Policys**（策略） > **Security**（安全） > **Pre Rules**（前导规则）。

   或者，选择 **Policies**（策略） > **Security**（安全） > **Post Rules**（后置规则），以在规则顺序的底部添加规则，在预规则之后评估该规则。

   确保您选择正确的 ***Device Group***（设备组）。要为远程网络创建安全规则，请选择远程网络的设备组（例如，***Remote_Network_Device_Group***）；对于移动用户，请选择移动用户的设备组（例如，***Mobile_User_Device_Group***）。
2. **Add**（添加）安全策略规则。
3. 输入规则的 **Name**（名称）。
4. 为数据包中的源或目标字段定义匹配条件。

   有关详细信息，请参阅创建安全策略规则。
5. 单击 **Actions**（操作），然后在 **QoS Marking**（**QoS** 标记）中选择**IP DSCP** 或 **IP Precedence**（**IP** 优先级）。
6. 以二进制形式输入 QoS 值，或从下拉列表中选择值。

   以下屏幕截图显示了与标记有 **IP DSCP** 值 **af11** 的流量匹配的安全策略规则。



 ©2025 Palo Alto Networks, Inc.

STEP 2 | 添加一个或多个 QoS 策略规则。

您使用 QoS 策略将 DSCP 标记绑定到八个可用类之一。稍后在创建一个或多个 QoS 配置文件时使用这些类。

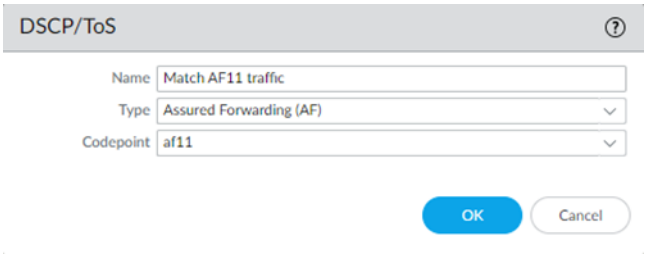
1. 选择 **Policies**（策略） > **QoS** > **Pre Rules**（预规则）。

   或者，使用后置规则（**Policies**（策略） > **QoS** > **Post Rules**（后置规则）），以在规则顺序的底部添加规则，在预规则之后评估该规则。

   服务连接不支持 QoS 后置规则；仅在服务连接中使用预规则。

   确保为服务连接选择正确的 **Device Group**（设备组）（例如，**Service_Conn_Device_Group**），或为远程网络连接选择正确的设备组（例如，**Remote_Network_Device_Group**）。如果共享设备组中的规则定义了除 **General**（常规）、**DSCP/ToS** 和 **Other**（其他）设置区域中的值以外的值，则 Prisma Access 不会在远程网络和服务连接上应用该规则。
2. **Add**（添加）QoS 策略规则。
3. 单击 **General**（常规）并输入策略规则的名称。
4. 单击 **DSCP/ToS** 选项卡，然后单击 **Codepoints**（代码点），并 **Add**（添加）一个或多个新的代码点。

   对于 Clean Pipe 部署，您可以在策略中指定其他 QoS 设置，例如源、目标或应用程序。
5. 为 DSCP/ToS 规则指定 **Name**（名称），然后选择 **Type**（类型）和 **Codepoint**（代码点）。



   或者，保留默认值（**Any**（任意）），以允许策略匹配通信，而不考虑为流量定义的差分服务代码点 (DSCP) 值或 IP 优先级/服务类型 (ToS)。
6. 单击 **Other Settings**（其他设置）选项卡，然后选择要分配给该规则的 QoS **Class**（类）。

   您可以在 QoS 配置文件中定义类特性。
7. 单击 **OK**（确定）。



 ©2025 Palo Alto Networks, Inc.

STEP 3 | 创建一个或多个 QoS 配置文件，以实现服务连接和远程网络连接的出口 QoS 流量的整形。

通过定义 QoS 类并为其分配带宽，可以使用配置文件实现对出口点的流量的整形。为 Prisma Access 启用 QoS 时，您必须选择现有 QoS 配置文件或创建新的 QoS 配置文件。

1. 为您要创建的配置文件选择正确的模板（**Remote_Network_Template** 或 **Service_Conn_Template**）；然后，选择 **Network**（网络）> **Network Profiles**（网络配置文件）> **QoS Profile**（**QoS** 配置文件）。
2. **Add**（添加）配置文件。
3. 输入配置文件 **Name**（名称）。
4. 为 QoS 配置文件规则设置总宽带限制。
   - 输入 **Egress Max**（出口最大）值，表示从服务连接或远程网络连接传出的流量的最大吞吐量（以 Mbps 为单位）。
     - 对于服务连接，请指定不超过 1 Gbps (1,000 Mbps) 的数字。

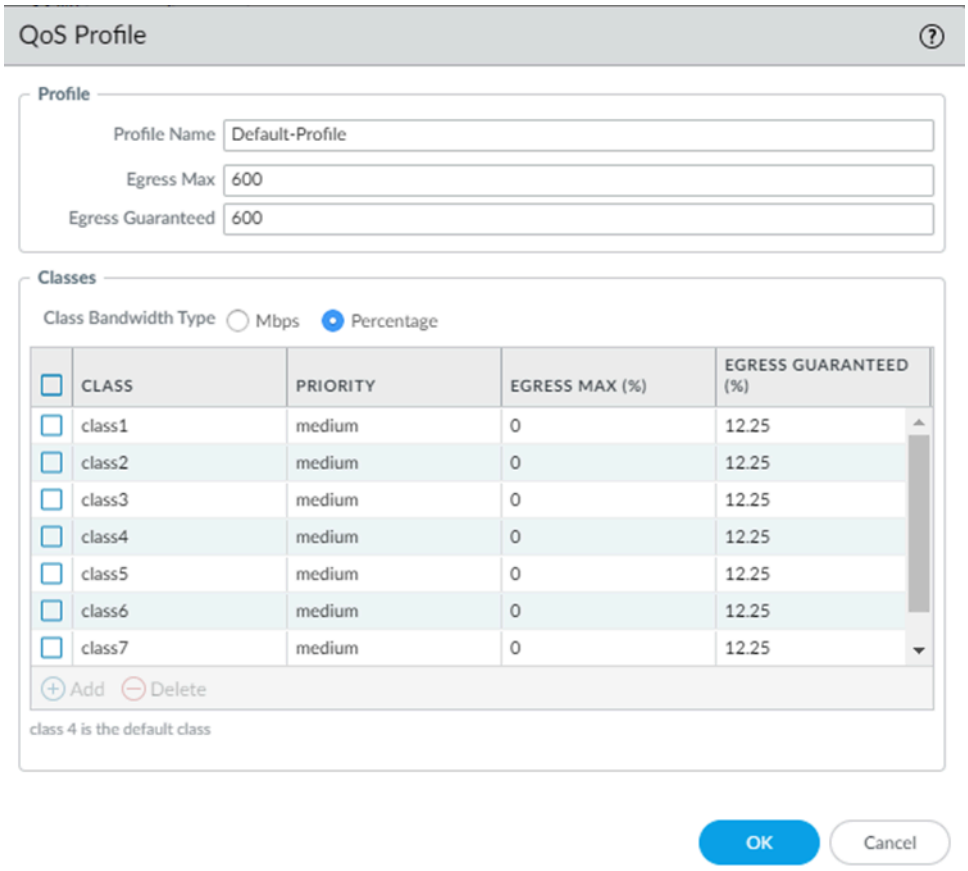
       请勿输入大于 *1 Gbps* 的数字；*Prisma Access* 会计算每个服务连接 *IPSec* 隧道的服务连接带宽，而不是跨多个隧道累计计算。
   - 对于远程网络连接，请输入 **0** 值。
   - 输入 **Egress Guaranteed**（出口保证）值，为此配置文件设置保证带宽（以 Mbps 为单位）。
     - 对于服务连接，输入 **Egress Guaranteed**（出口保证）带宽，即此配置文件的保证带宽（以 Mbps 为单位）。

       任何超过出口保证值的流量都会得到尽可能地处理，但是并不保证效果。保证带宽如不使用，将继续对所有流量保持可用状态。
     - 对于远程网络连接，请输入 **0** 值。
5. 在“类”部分中，**Add**（添加）一个或多个类，并指定如何标记最多 8 个单独的 QoS 类。
   - 对于按计算地点分配带宽的远程网络使用的 QoS 配置文件，将 **Class Bandwidth Type**（类带宽类型）更改为 **Percentage**（百分比），并输入您在此区域中输入的 **Egress Max**（出口最大）和 **Egress Guaranteed**（出口保证）值的百分比。
   - 对于按地点分配带宽的服务连接或远程网络使用的 QoS 配置文件，请指定 **Mbps** 类型。
   - 选择该类的 **Priority**（优先级）（**real-time**（实时）、**high**（高）、**medium**（中）或 **low**（低））。
   - 输入分配给您创建的每个 QoS 类的流量的 **Egress Max**（出口最大）值。
     - 对于按计算地点分配带宽的远程网络，请输入 **0**。
     - 对于基于带宽的 QoS 配置文件（由按地点分配带宽的服务连接或远程网络使用），请输入以 Mbps 为单位的值。QoS 类的出口最大值必须小于或等于 QoS 配置文件的出口最大值。
   - 输入每个 QoS 类的 **Egress Guaranteed**（出口保证）百分比或带宽（以 Mbps 为单位）。对于远程网络的 QoS 配置文件，请输入百分比。

 ©2025 Palo Alto Networks, Inc.

分配给某个类别的保证带宽并非为该类别保留的带宽，如不使用，则将继续对所有流量保持可用状态。当某类流量超出出口保证带宽时，Prisma Access 会尽量让流量通过。

- 输入该配置文件的 **Class Bandwidth Type**（类带宽类型）。



6. 单击 **OK**（确定）。

STEP 4 | （仅限服务连接）为服务连接启用 QoS 并将 QoS 配置文件应用于该连接。

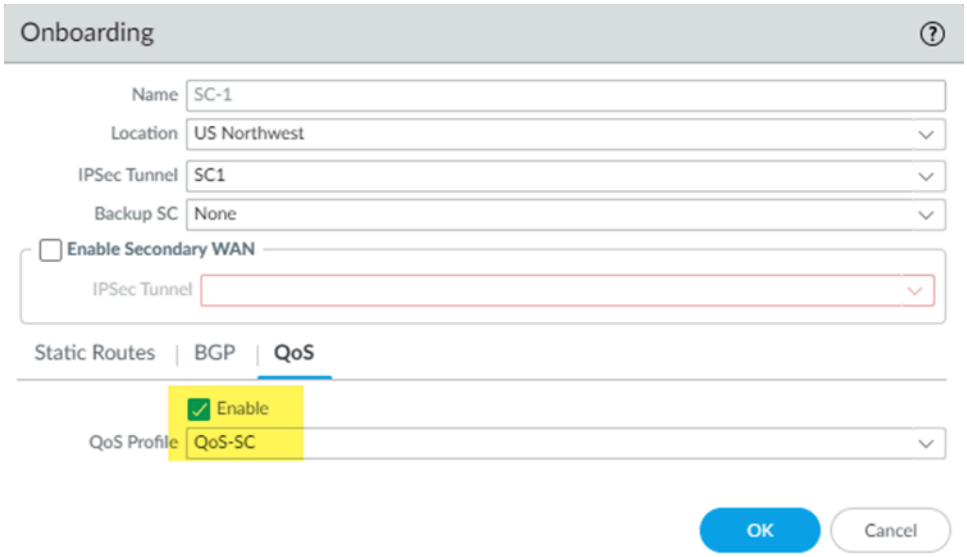
1. 启用 QoS，方法是选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Service Setup**（服务设置），选择 **Connection Name**（连接名称），单击 **QoS** 选项卡；然后 **Enable**（启用）QoS。

   如果您通过 Prisma Access 远程网络 而不是按计算地点分配远程网络带宽，请以与服务连接相同的方式配置 QoS。选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Remote Networks**（远程网络），选择远程网络连接

 ©2025 Palo Alto Networks, Inc.

Name（名称）的超文本，单击 **QoS** 选项卡，然后 **Enable**（启用）QoS。如果按计算地点分配带宽（默认方法），请继续执行步骤 5，为远程网络配置 QoS。

2. 选择一个 QoS 配置文件，然后单击 **OK**（确定）。



STEP 5 | （仅限按计算地点分配带宽的远程网络部署）为远程网络位置启用 QoS。

1. 确定要部署 QoS 的 Prisma Access 地点；然后找到与每个地点对应的计算地点。

   每个地点根据其计算地点分配带宽，并且您必须知道要分配 QoS 的地点的计算地点的名称。有关计算地点到地点的映射列表，请参阅 Prisma Access 位置，或选择 **Panorama > Cloud Services**（云服务） > **Configuration**（配置） > **Remote Networks**（远程网络） > **Aggregate Bandwidth**（聚合带宽），并单击齿轮图标；映射会显示在 **Compute Location**（计算地点）和 **Prisma Access Location**（**Prisma Access** 地点）列中。

2. 选择 **Panorama > Cloud Services**（云服务） > **Configuration**（配置） > **Remote Networks**（远程网络） > **Settings**（设置），单击齿轮图标以编辑设置，然后选择 **QoS**。

3. 在计算地点级别 **Enable QoS**（启用 **QoS**）。

   您输入的任何设置都可应用于与此计算地点对应的所有地点。

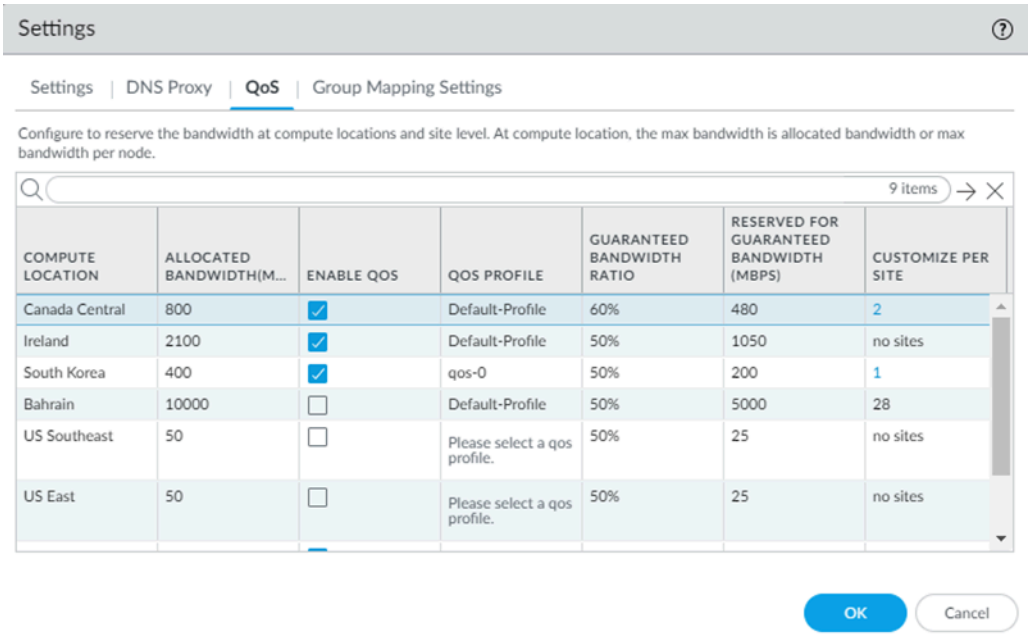
 ©2025 Palo Alto Networks, Inc.

4. 输入 **QoS Profile**（**QoS** 配置文件）、**Guaranteed Bandwidth Ratio**（保证的带宽比率）和 **Reserved for Guaranteed Bandwidth (Mbps)**（为保证带宽预留 **(Mbps)**）。
   - 输入要用于此计算地点的 **QoS Profile**（**QoS** 配置文件）。

     如果要为每个远程网络使用不同的 QoS 配置文件，请使用后面步骤中所述的 **Customize Per Site**（按站点自定义）。
   - 输入保证的带宽比率，该比率基于为计算地点分配的整个带宽。

     例如，如果您为加拿大中部计算地点分配了 800 Mbps 的带宽，并且在 **Guaranteed Bandwidth Ratio**（保证的带宽比率）中输入 **60%**，则该计算地点的保证带宽为 480 Mbps。
   - 为所选 QoS 配置文件和计算地点输入 **Reserved for Guaranteed Bandwidth (Mbps)**（为保证带宽预留 **(Mbps)**）的带宽量。

   以下屏幕截图显示为加拿大中部、爱尔兰和韩国计算地点启用的 QoS。



5. （可选）如果每个计算地点有多个远程网络连接，并且您想要更改每个地点的带宽比率或 QoS 配置文件，请加入远程网络地点；然后选择 **Customize Per Site**（按站点自定义）并更改带宽分配比率、QoS 配置文件或两者。
   - 要自定义保证带宽，请单击 **Customize Per Site**（按站点自定义）区域中的数字，选择 **Customize Per Site**（按站点自定义）“，然后更改 **Allocation Ratio**（分配比率）。

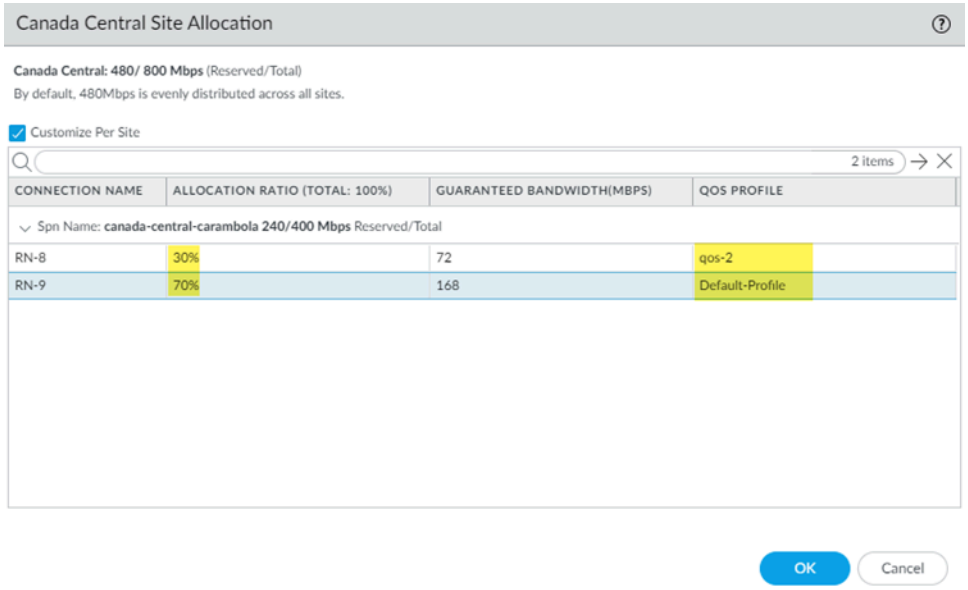
     默认情况下，每个远程连接的百分比等于连接的数量。例如，假设某个计算地点有 4 个连接，总保证带宽为 100 Mbps，则每个地点将获得 25% 的带宽或 25 Mbps 的带宽。

©2025 Palo Alto Networks, Inc.

如果选择 ***Customize Per Site***（按站点自定义），然后在同一个 *IPSec* 终止节点中加入其他远程网络，则新加入的站点获得的分配比率为 ***0***，并且您必须通过手动方式重新平衡现有站点和新加入站点之间的分配比率。

如果未选择 ***Customize Per Site***（按站点自定义），则添加远程网络时，带宽百分比会自动重新平衡。例如，如果您未选择 ***Customize Per Site***（按站点自定义），并且加入了四个远程网络，则每个远程网络的分配比率为 *25%*。如果添加第五个远程网络，则会重新平衡这五个站点的带宽百分比，每个站点将获得 *20%* 的保证带宽。

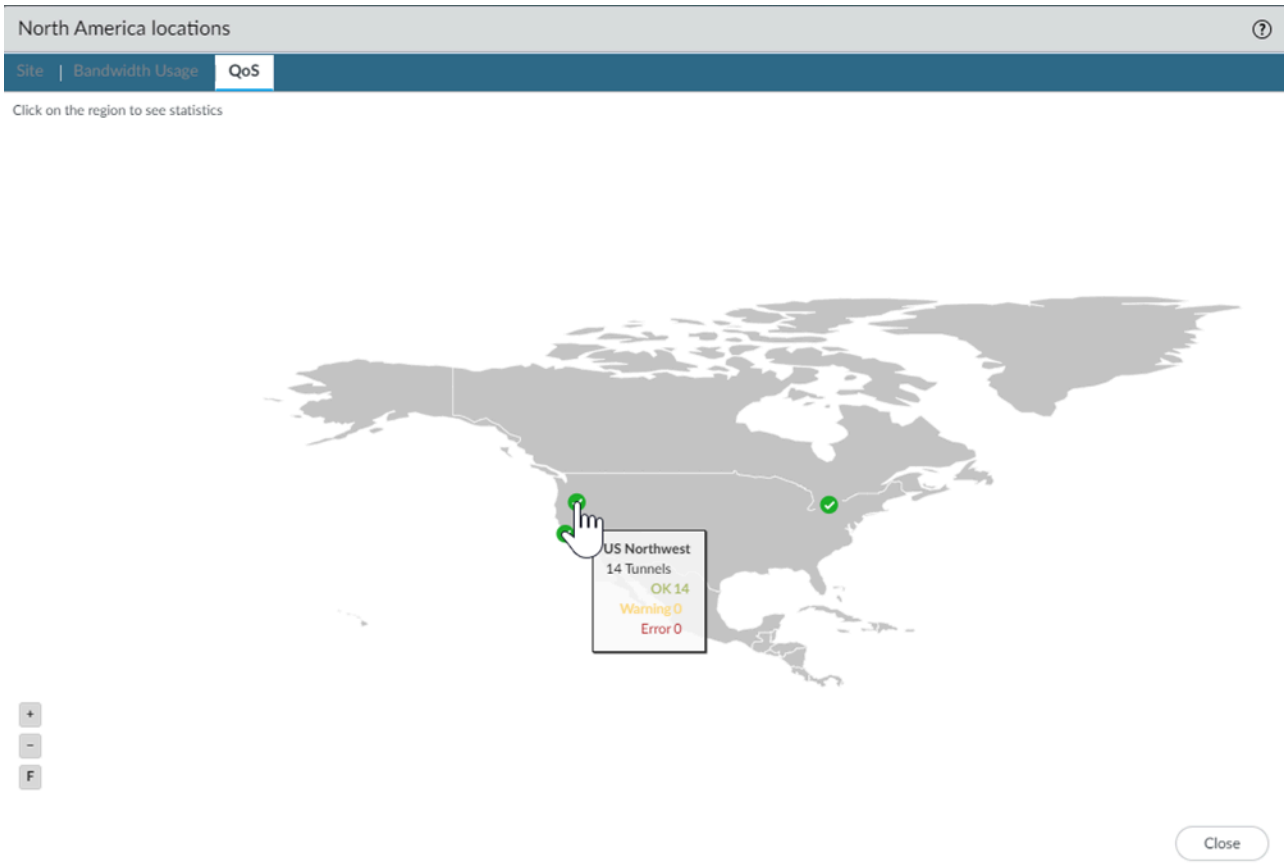
- 如果要在每个远程网络级别指定 QoS 配置文件，请为远程网络选择不同的 **QoS Profile**（**QoS** 配置文件）。



 ©2025 Palo Alto Networks, Inc.

STEP 6 | 检查 QoS 状态。

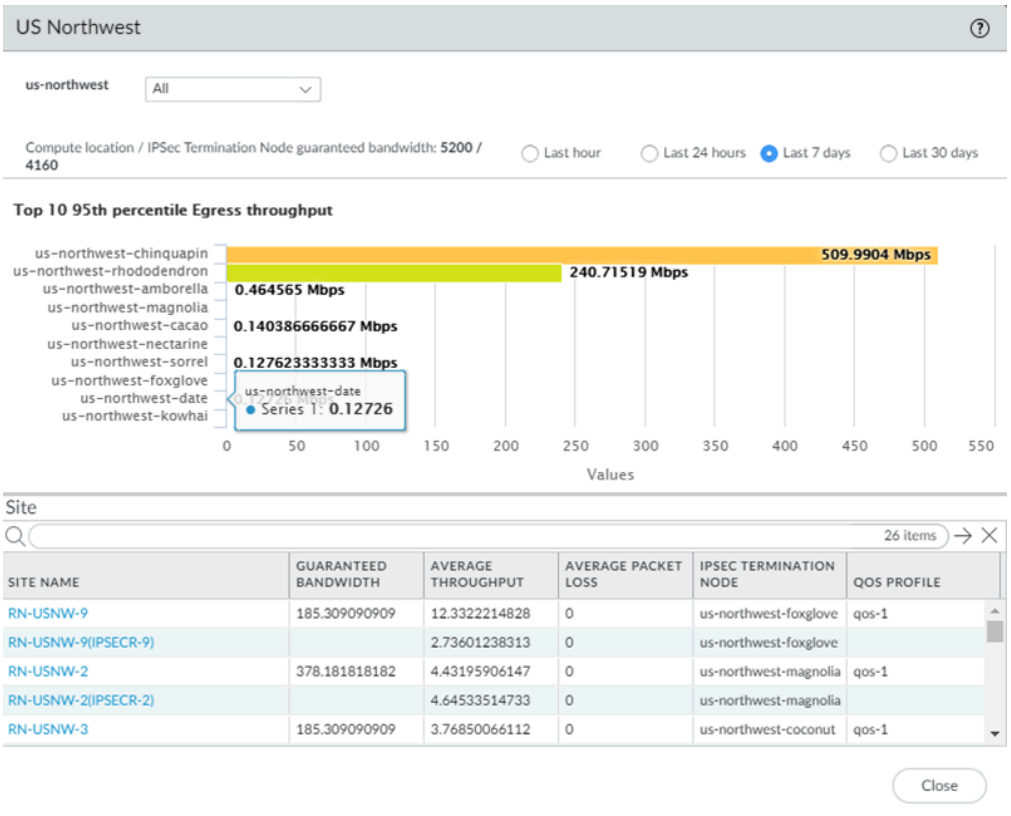
- 对于远程网络，选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Monitor**（监控） > **Remote Networks**（远程网络），从地图中选择一个区域，选择 **QoS**，然后选择一个地点。



远程网络统计信息显示吞吐量最高的 10 个 IPSec 终止节点。Prisma Access 使用第 95 百分位数标准来收集统计信息，该标准跟踪利用率达到峰值时的带宽，并忽略前 5% 的利用率峰值和大量突发。

选择时间范围（**Last hour**（过去 **1** 小时）、**Last 24 hours**（过去 **24** 小时）、**Last 7 days**（过去 **7** 天）或 **Last 30 days**（过去 **30** 天）），以查看该时间段的统计信息。

©2025 Palo Alto Networks, Inc.

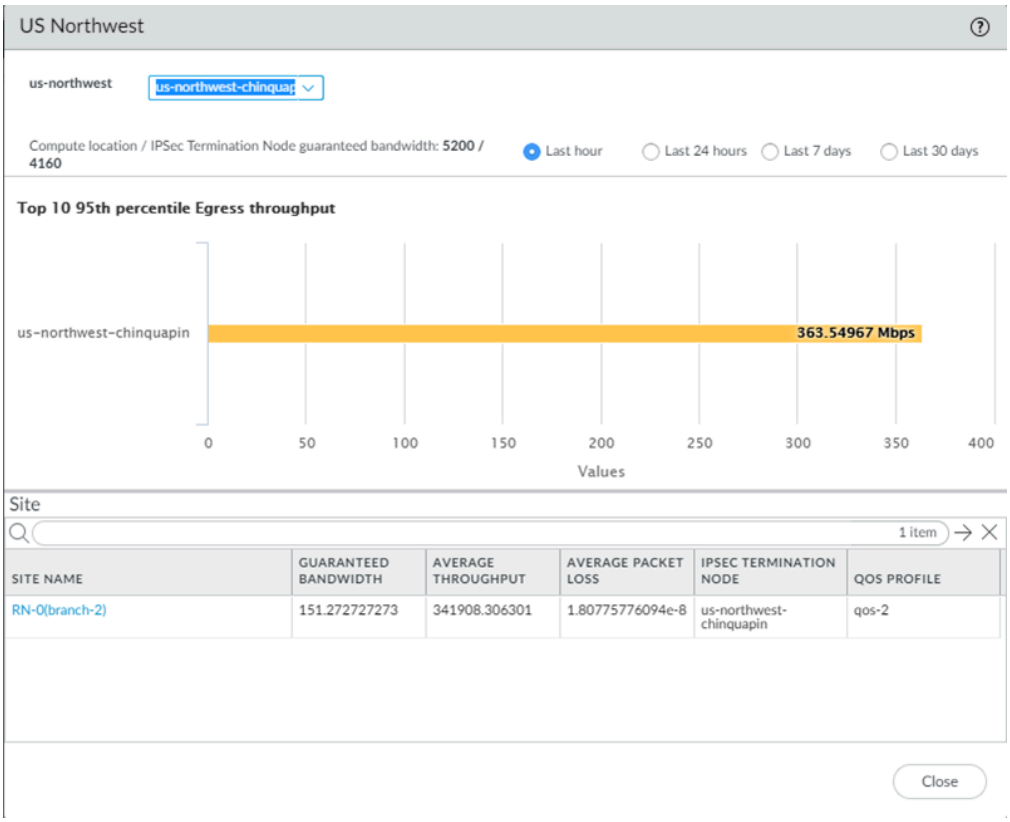


Site（站点）区域将显示出口带宽使用率最高的远程网络，远程网络地点的 **Guaranteed Bandwidth**（保证带宽）、**Average Throughput**（平均吞吐量）、**Average Packet Loss**（平均数据包丢失）的统计信息，以及远程网络使用的 **IPSec Termination**

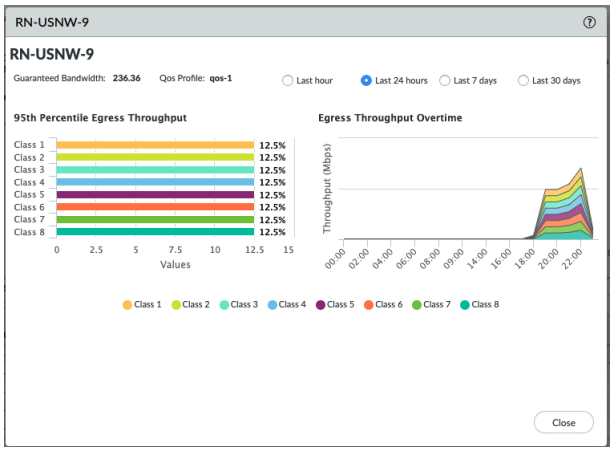
 ©2025 Palo Alto Networks, Inc.

Node（**IPSec** 终止节点）和 **QoS Profile**（**QoS** 配置文件）。您还可以 **Search**（搜索）地点。

要查看与特定 IPSec 终止节点关联的远程网络，请将页面顶部的下拉菜单从 **All**（全部）更改为特定 IPSec 终止节点，以查看该 IPSec 终止节点和该站点的远程网络的统计信息。

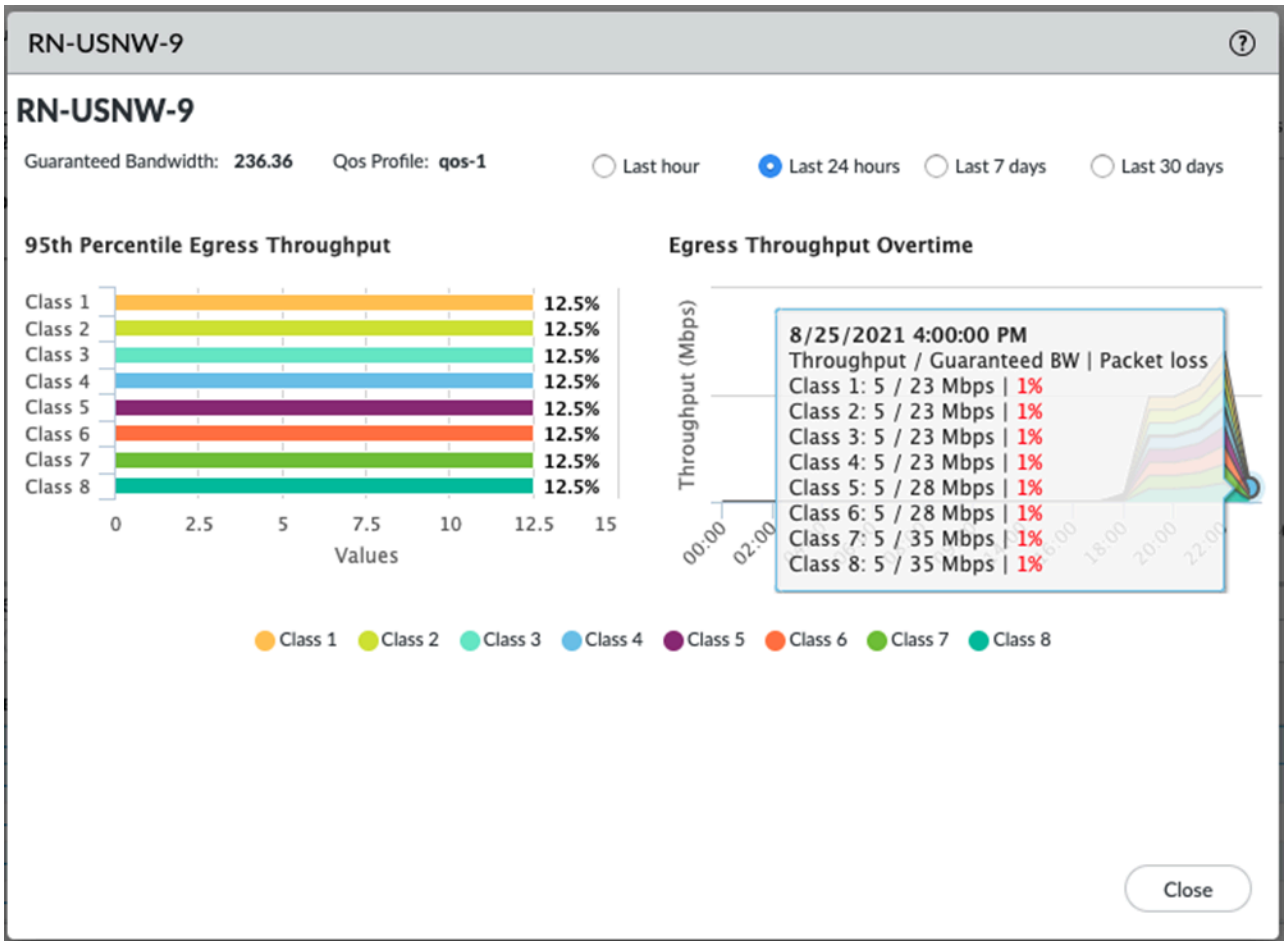


要查看按 QoS 类排序的站点特定流量，请单击 **Site Name**（站点名称）。系统将显示远程网络站点的保证带宽、出口吞吐量以及随时间变化的吞吐量。您还可以按过去 1 小时、过去 24 小时、过去 7 天或过去 30 天对这些信息进行排序。



将鼠标悬停在右侧图表上，以获取特定时间段的详细信息。

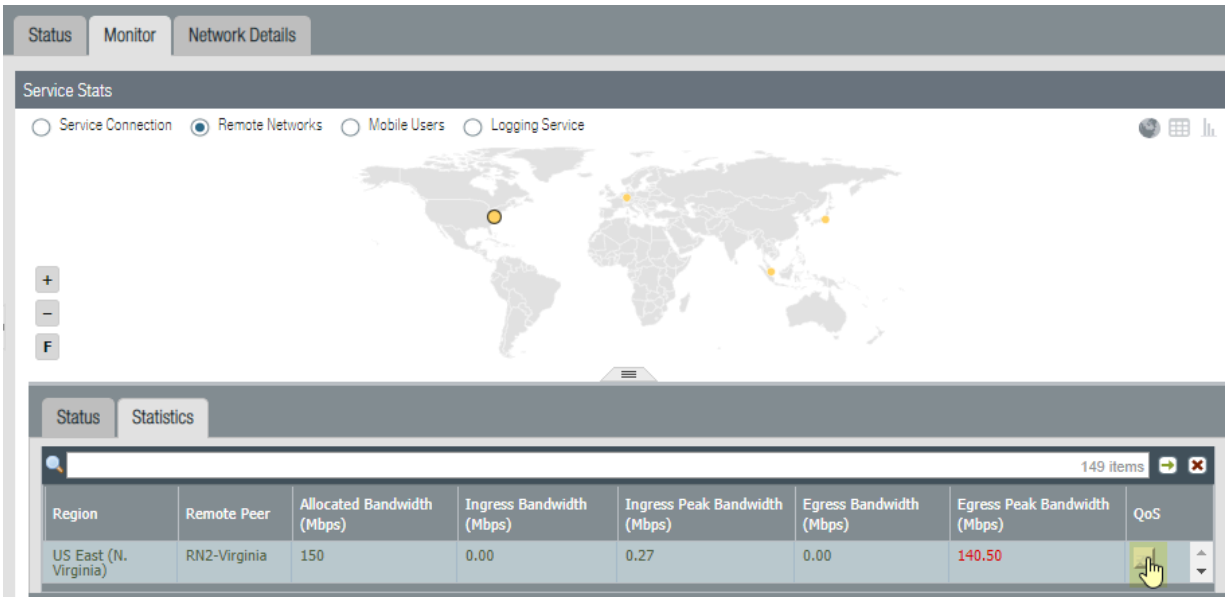
©2025 Palo Alto Networks, Inc.



- 对于服务连接，请选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Monitor**（监控） > **Service Connection**（服务连接），选择一个区域，然后 **Monitor**（监控）**Statistics**（统计信息）。

单击 **QoS** 以查看包含 QoS 统计信息的页面。

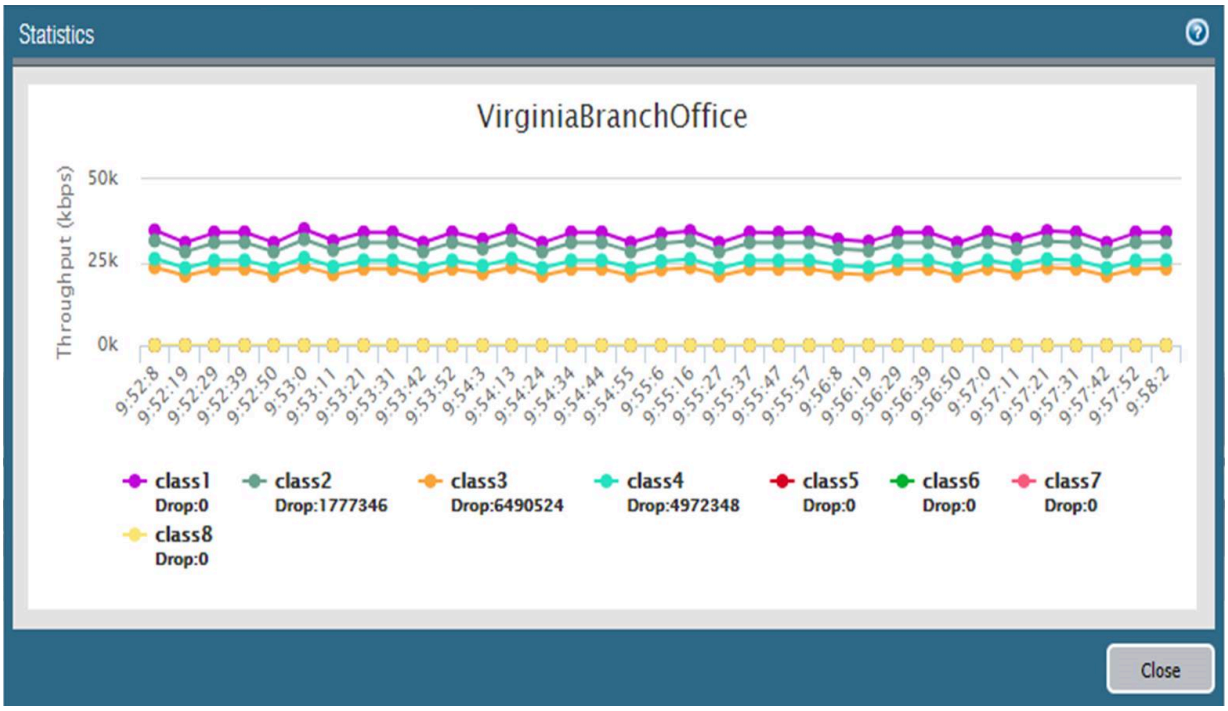
©2025 Palo Alto Networks, Inc.



此页面显示一个图表，其中包含实时和历史 QoS 统计信息，包括每个类别的丢弃数据包数。此图表仅显示启用了 QoS 的服务连接或远程网络连接，显示连接的网络活动最后五分钟的统计信息，每 10 秒刷新一次。

下图显示了 1、2、3 和 4 类的流量传递情况。图表下方的数据根据 2、3 和 4 类的 QoS 配置显示丢包数。

©2025 Palo Alto Networks, Inc.



更改保证带宽

更改保证带宽

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

如果您有多个远程网络位置与一个 IPSec 终止节点相关联，则可以更改每个站点的保证带宽。在以下示例中，您希望加拿大东部地点获得比加拿大中部地点更多的带宽；为此，请完成以下步骤。

STEP 1 | 选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Remote Networks**（远程网络） > **Settings**（设置）。

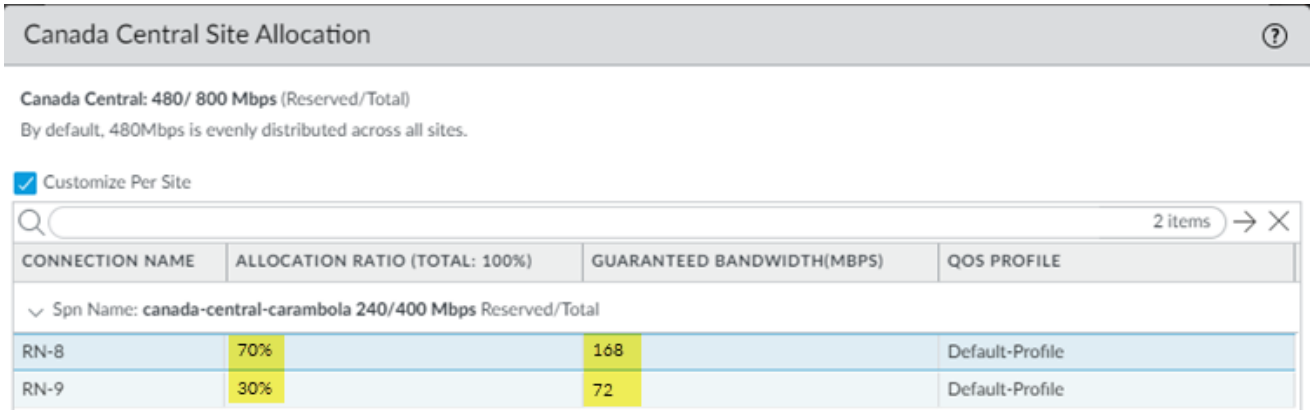
STEP 2 | 单击齿轮以编辑设置，然后选择 **QoS**。

STEP 3 | **Enable QoS**（启用 **QoS**），为加拿大中部计算地点分配一个 **QoS Profile**（**QoS** 配置文件）（在此示例中为 **Default-Profile**（默认配置文件））和 **Guaranteed Bandwidth Ratio**（保证的带宽比率）。

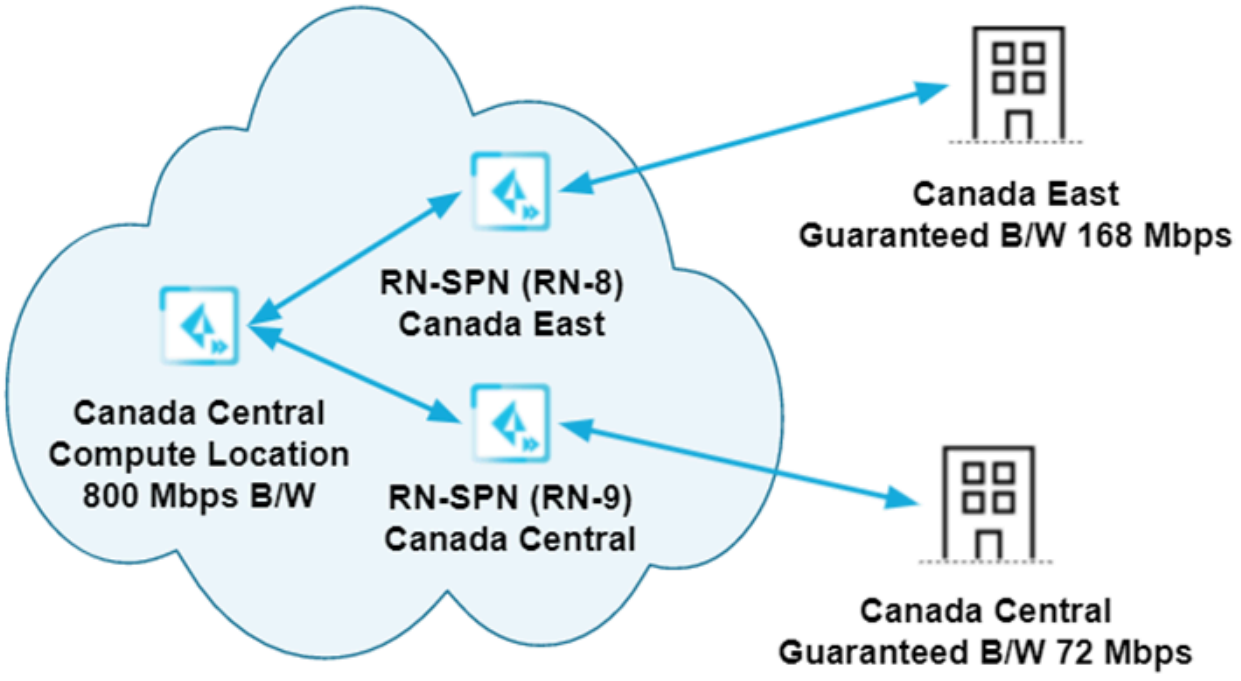
 ©2025 Palo Alto Networks, Inc.

STEP 4 | 选择 **Customize Per Site**（按站点自定义），启用 **Customize Per Site**（按站点自定义），然后向 RN-8 远程网络（用于加拿大东部地点）应用比 RN-9 远程网络（用于加拿大中部地点）更高的带宽 **Allocation Ratio**（分配比例）。

以下示例显示了 **Allocation Ratio**（分配比例）：RN-8 为 70%，RN-9 为 30%。**Guaranteed Bandwidth (Mbps)**（保证带宽 **(Mbps)**）会相应地更改，显示新的保证带宽量。



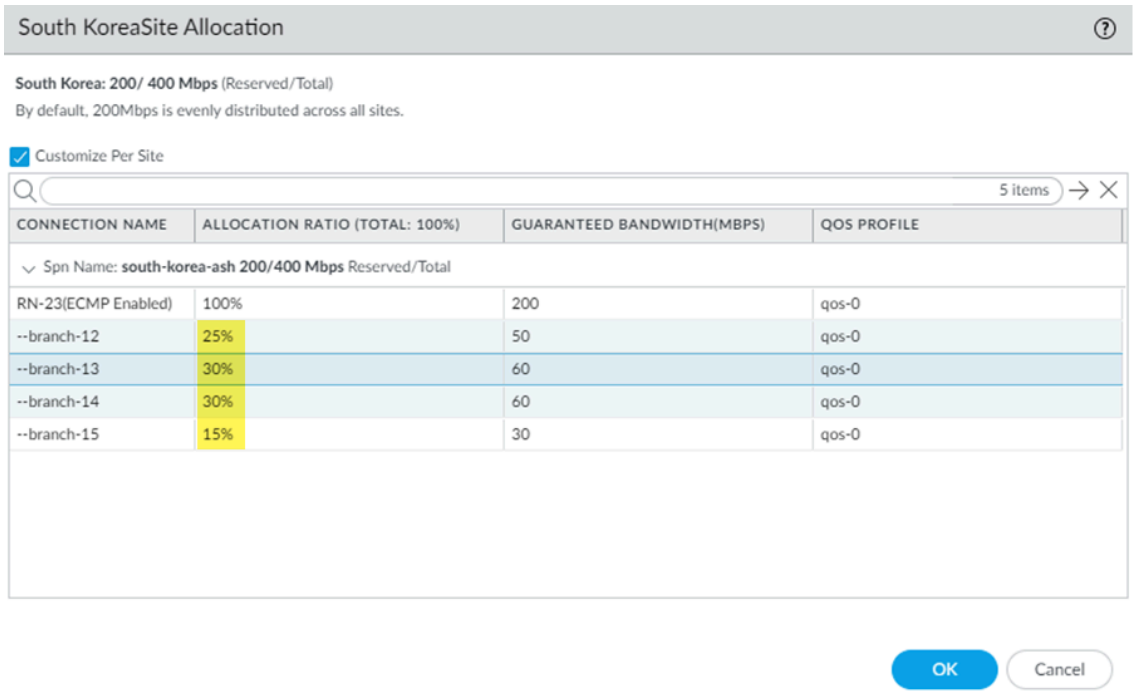
完成后，您的配置将为这两个站点分配以下保证带宽。



您还可以为每个远程网络位置分配不同的 QoS 配置文件。要分配不同的配置文件，请启用 **Customize Per Site**（按站点自定义）功能，并为每个远程网络位置选择不同的 QoS 配置文件。

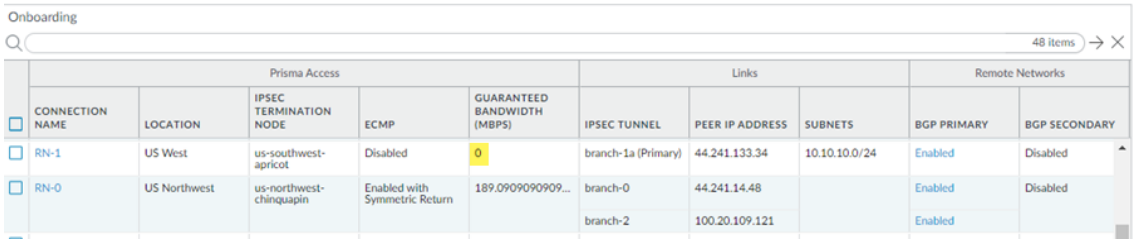
如果您的远程网络启用了 ECMP 以将多个 IPSec 隧道用于单个远程网络，则可以更改用于该远程网络位置的 IPSec 隧道的 **Allocation Ratio**（分配比例）。

©2025 Palo Alto Networks, Inc.



STEP 5 | 保存并提交更改。

保证带宽值显示在 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Monitor**（监控） > **Remote Networks**（远程网络）区域的 **Guaranteed Mbps**（保证 **Mbps**）区域中。如果您未指定带宽，则显示为 0。



 ©2025 Palo Alto Networks, Inc.

远程网络 — 高性能

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证 这是一个限制发布的版本。要激活此功能，请联系您的 *Palo Alto Networks* 客户代表。

随着业务规模扩大，您的分支机构位置在地理上会变得分散，Prisma Access 远程网络使您能够快速接入您的分支站点，并为您的用户提供一流的安全性。要为一个高带宽的分支站点进行接入，Prisma Access 提供了远程网络—高性能部署解决方案。

要接入“远程网络—高性能”部署，您需要指定分支站点的位置，然后 Prisma Access 会选择离该站点最近的位置。您可以选择为网站设置一个备用位置，以实现冗余和弹性。高性能远程网络为每 3 Gbps 带宽使用一个单一的服务 IP 地址，消除了在每个远程位置配置和管理多个 IPSec 设备的复杂性。

Prisma Access (Managed by Panorama) 部署不支持二级位置。

在您为“远程网络-高性能”部署进行规划后，就可以开始配置过程，包括将高性能远程网络接入 Prisma Access 并启用 QoS 和路由。

“远程网络—高性能”部署的性能和指南

高性能远程网络为您提供以下核心功能：

- 每个计算区域每个节点最高可达 3 Gbps 的总带宽
- 每个远程站点的远程网络隧道可达 2 Gbps 带宽
- 每个服务IP地址最多可支持 500 个远程分支，适用于 Prisma SD-WAN 和扩展（第三方）CPE 部署

在为分支站点配置高性能远程网络时，请注意以下指南以及站点和远程网络之间的差异：

- **Prisma Access** 地点 — “远程网络—高性能”支持部分 Prisma Access 地点。
- 服务质量 **(QoS)** — 对于分支站点，Prisma Access 支持按站点级别的 QoS，您选择的 QoS 配置文件适用于整个站点。
- 承诺信息速率 **(CIR)** — 为了确保和承诺每个站点使用的带宽量，请指定一个 CIR。如果在一个计算位置有多个共享带宽的远程网络，当与该计算位置的其他站点发生争用时，“远程网络—高性能”至少会接收到 CIR 中指定的带宽。

©2025 Palo Alto Networks, Inc.

- **IPSec** 终止节点 — 与远程网络不同，在部署时您无需在介入过程中为 Prisma Access (Managed by Strata Cloud Manager) 部署选择 IPSec 终止节点。Prisma Access 自动为远程网络连接实现负载均衡，以最大化分配给站点的带宽。

  您仍然需要为从 Panorama 导入的远程网络选择一个 IPSec 终止节点。
- 隧道和计算位置冗余以及每个站点的最大隧道数 — 高性能远程网络让您可以配置位置和 IPSec 冗余。
  - 位置冗余（在一个计算位置指定 **Primary**（主要）位置，在另一个计算位置指定 **Secondary**（次要）位置）。

    配置次要位置是可选的，并且次要位置必须位于与主位置不同的计算位置。
  - IPSec 隧道冗余（将隧道指定为 **Active/Active**（主动/主动）或 **Active/Passive**（主动/被动））。

  此表提供每个隧道的最小和最大位置数量。

地点部署类型	隧道部署类型	的最小数量	隧道的最大数量
仅主动	主动/被动	1	2
仅主动	主动/主动	2	4
主要和次要	主动/被动	2	4
主要和次要	主动/主动	4	8

- 基于部署类型的服务 **IP** 地址分配 — 您收到的服务IP地址数量取决于您是否在单个位置设置了高性能远程网络，或者是否在主要和次要部署中使用两个不同的位置设置了它们。
  - 如果您在单个位置设置了高性能远程网络，并且没有备用位置，Prisma Access 将为您提供一个单一的服务 IP 地址。
  - 如果您在主配置和辅助配置中设置计算位置冗余，Prisma Access 将为您提供两个服务 IP 地址（每个配置一个）。

  如果您在主动/被动配置中设置 IPSec 隧道，Prisma Access 将为两个隧道提供一个单一的服务 IP 地址（与标准 Prisma Access 远程网络配置相同）。
- 基于带宽的服务 **IP** 地址分配 — Prisma Access 为您在每计算位置提供 3 Gbps 带宽的单个 IP 地址或 FQDN。
- 每个计算位置的带宽 — 您为每个计算位置分配带宽的方式与为标准远程网络分配带宽的方式相同。在开始配置之前或在高性能远程网络创建期间，您可以规划和分配带宽。
- **IPv6** 支持 — “远程网络—高性能”部署不支持 IPv6。

根据您的带宽分配类型，使用以下步骤之一来加入远程网络：

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

 ©2025 Palo Alto Networks, Inc.

Strata Cloud Manager

下面介绍如何使用 Strata Cloud Manager 添加“远程网络 - 高性能”版本。

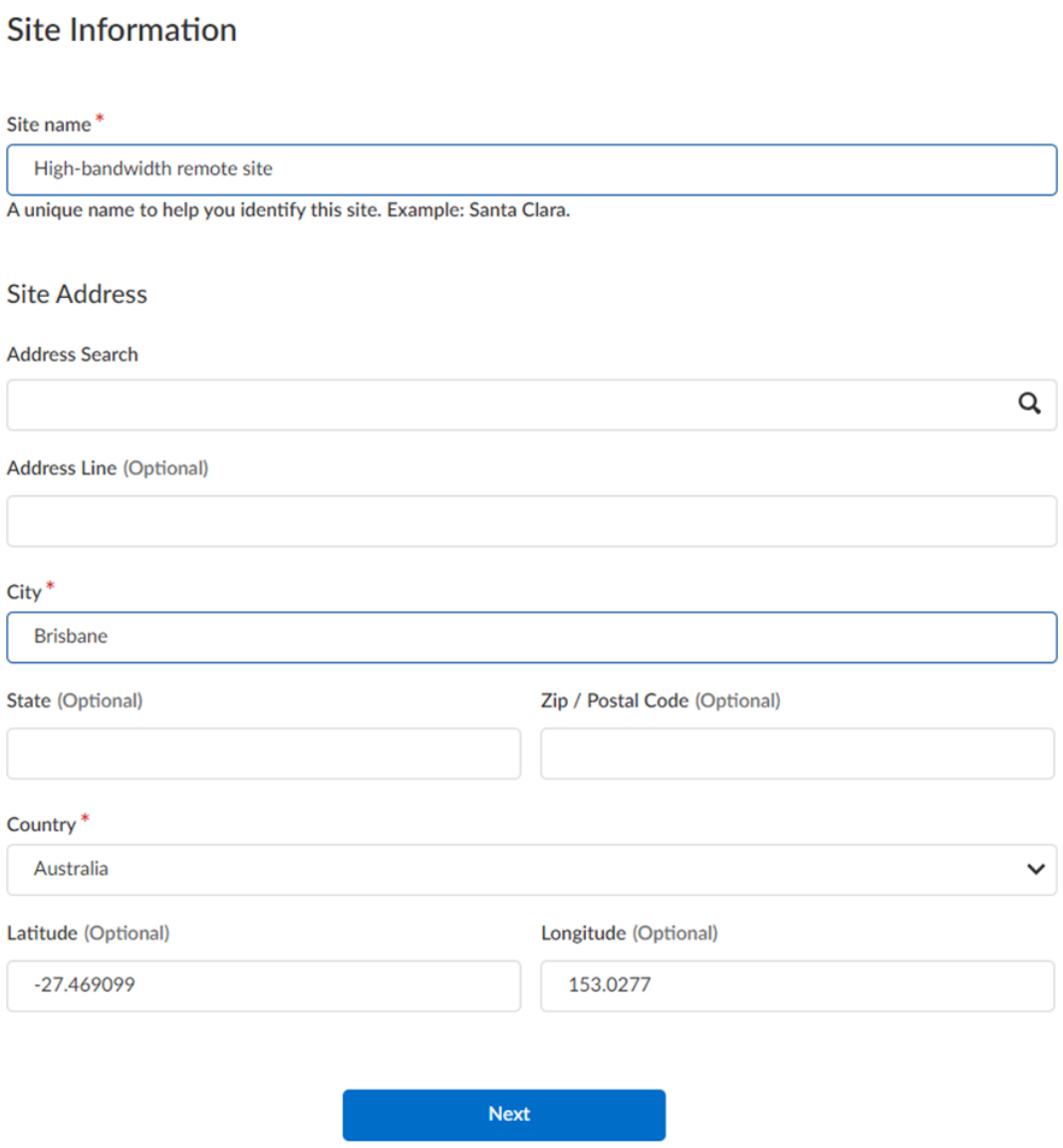
STEP 1 | 从 Strata Cloud Manager 中转到 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Branch Sites**（分支机构站点）。

此选择表示您为分支机构站点创建的隧道由您的 CPE（Palo Alto Networks 新一代防火墙或第三方 CPE）终止。

STEP 2 | **Add Site**（添加站点）并为远程网络提供一个描述性的 **Site Name**（站点名称）。

STEP 3 | 选择站点的 **City**（城市）和 **Country**（国家/地区）。

为了更精确地进行搜索，请添加一个地址。



STEP 4 | 单击 **Next**（下一步）。

 ©2025 Palo Alto Networks, Inc.

STEP 5 | 请输入 **QoS CIR (Committed Information Rate)**（**QoS CIR**（承诺信息速率）），单位为 Mbps。

如果您在一个计算位置有多个共享带宽的远程网络，并且与该计算位置的其他站点争用带宽，则“远程网络 — 高性能”版本至少接收 CIR 中指定的带宽。

如果您配置主站点和辅助站点，则需要指定不同的计算区域，辅助区域将获得 20% 的 CIR。例如，如果您为一个站点配置 100 Mbps 的CIR，则 Prisma Access 会为主站点提供 100 Mbps 的CIR，并为次站点提供 20 Mbps 的 CIR。

如果 CIR 为 500 Mbps，并且计算位置的所有剩余带宽都被其他站点使用，则 Prisma Access 会丢弃超过 500 Mbps 的任何带宽。然而，如果其他站点没有使用带宽，高性能远程网络的带宽可以超过 500 Mbps，达到在计算位置分配的带宽。

输入的最低 CIR 为 1 Mbps，最高为 2000 Mbps。请不要超过为计算区域指定的带宽。

STEP 6 | 选择 **Primary Prisma Access Location**（**Prisma Access** 主位置）。

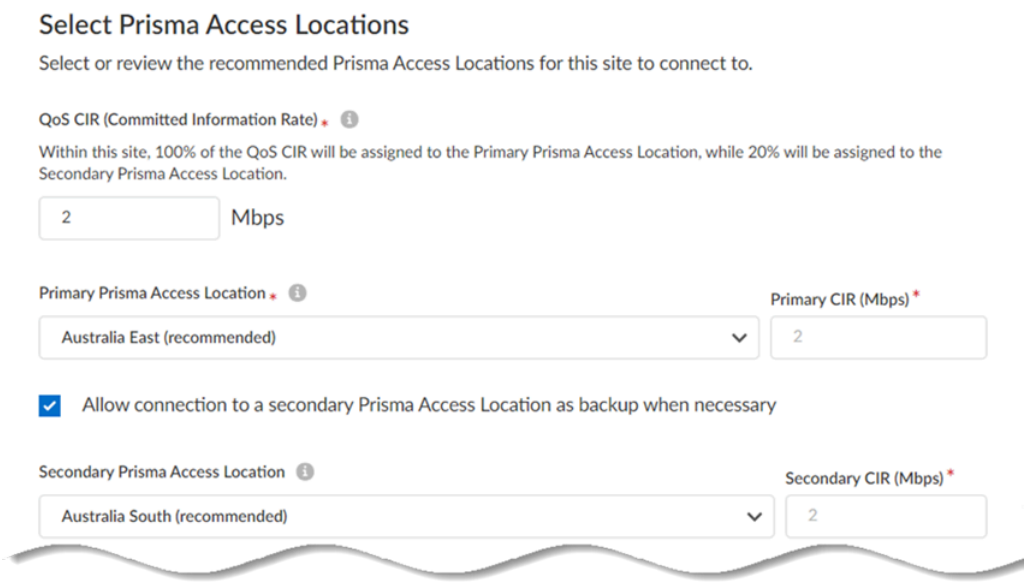
如果列表中 **Recommended**（推荐）多个位置，请选择最适合您部署的位置。

STEP 7 | （可选）要创建一个次要（备份）站点，请选择**Allow connection to a secondary Prisma Access Location as backup when necessary**（在必要时允许连接到次要 **Prisma Access** 位置

 ©2025 Palo Alto Networks, Inc.

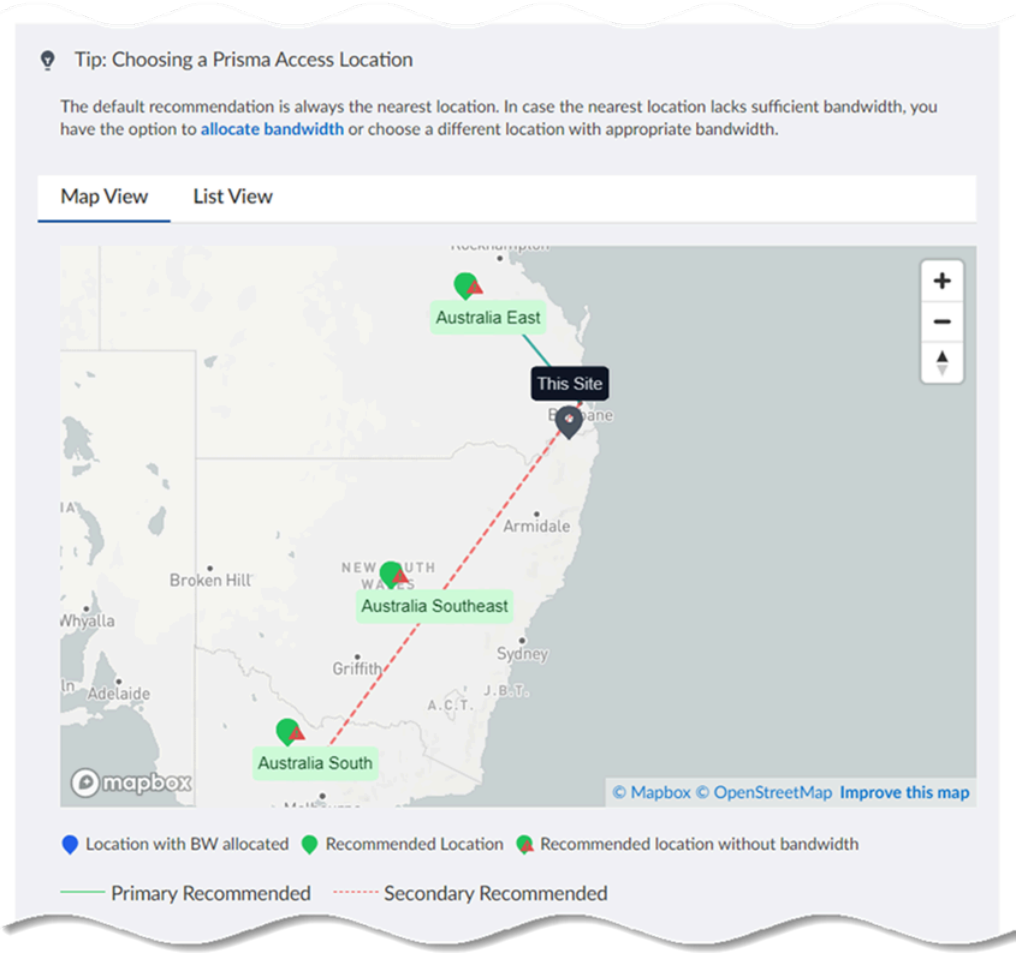
以作为备份），然后选择一个 **Secondary Prisma Access Location**（次要 **Prisma Access** 位置）。

如果您选择此选项，Prisma Access 将预填充最佳次要位置或与主要位置位于不同计算位置的位置。如果 **Recommended**（推荐）多个位置，请选择最适合您部署的位置。



Prisma Access 会提供一个包含建议位置的地图，以便帮助您做出选择。

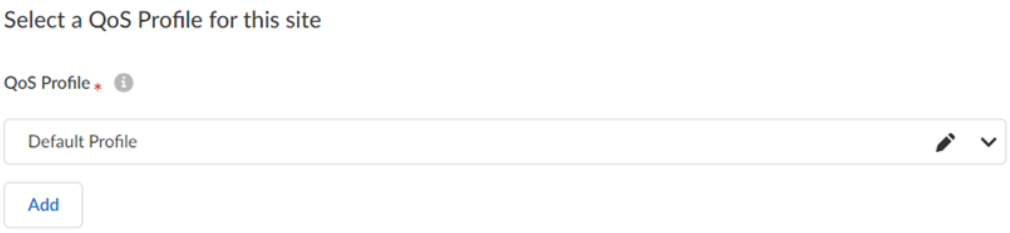
 ©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.

STEP 8 | 选择要用于此站点的 **QoS Profile**（**QoS** 配置文件）。

远程网络 — 高性能使用单一 QoS 配置文件。

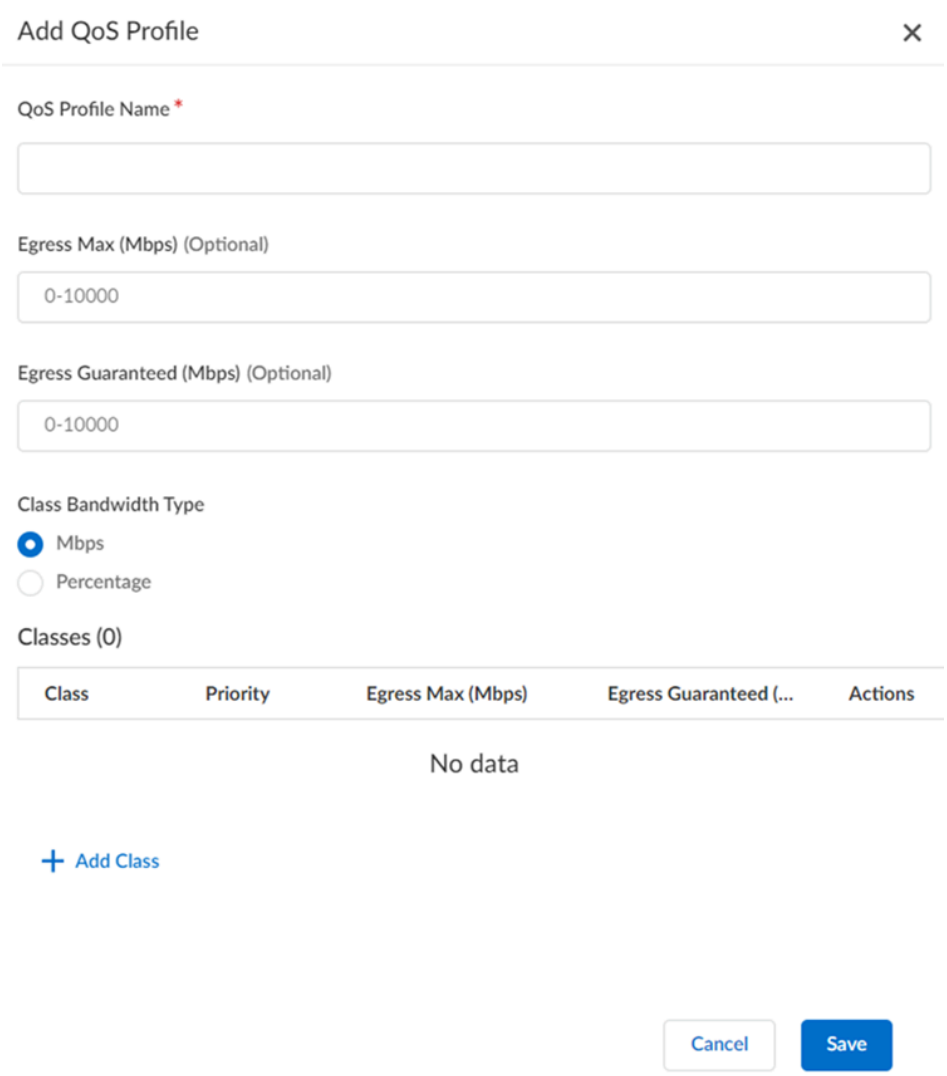


如果您尚未创建 QoS 配置文件，请 **Add**（添加）QoS 配置文件，并指定以下值：

- 输入唯一 **QoS Profile Name**（**QoS** 配置文件名称）。
- （可选）输入一个表示服务连接或远程网络连接中流出流量的最大吞吐量 (Mbps) 的**Egress Max (Mbps)**（传出最大值 **(Mbps)**）。
- （可选）输入一个 **Egress Guaranteed (Mbps)**（传出保证值 **(Mbps)**），表示此配置文件的保证带宽 (Mbps)。
- 输入一个 **Class Bandwidth Type**（类带宽类型），即 **Percentage**（百分比）或 **Mbps**。

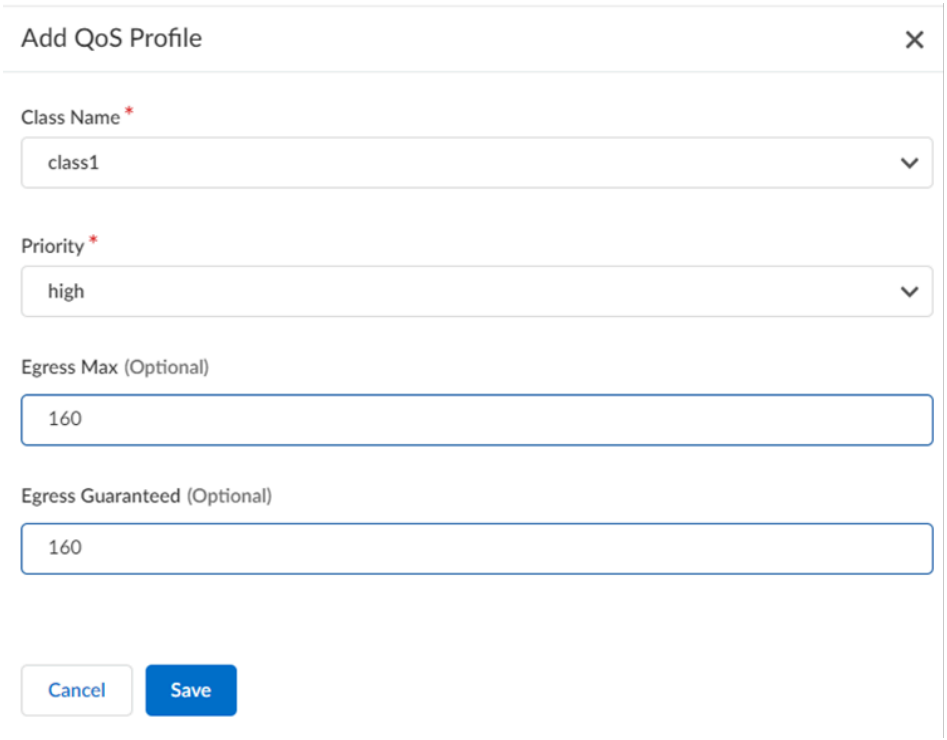
  远程网络的 QoS — 高性能不使用保证带宽比。

 ©2025 Palo Alto Networks, Inc.



- 在“类”部分中，**Add Class**（添加类）并指定如何标出八个单独的 QoS 类。
  - 输入一个 **Class Name**（类名称）。
  - 为类选择 **Priority**（优先级）（**real-time**（实时）、**high**（高）、**medium**（中）或 **low**（低））。
  - 输入一个 **Egress Max**（传出最大值），表示离开服务连接或远程网络连接的最大吞吐量（以 Mbps 为单位）。
  - 输入一个 **Egress Guaranteed**（传出保证值），表示此配置文件的保证带宽（以 Mbps 为单位）。
- **Save**（保存）更改。

©2025 Palo Alto Networks, Inc.

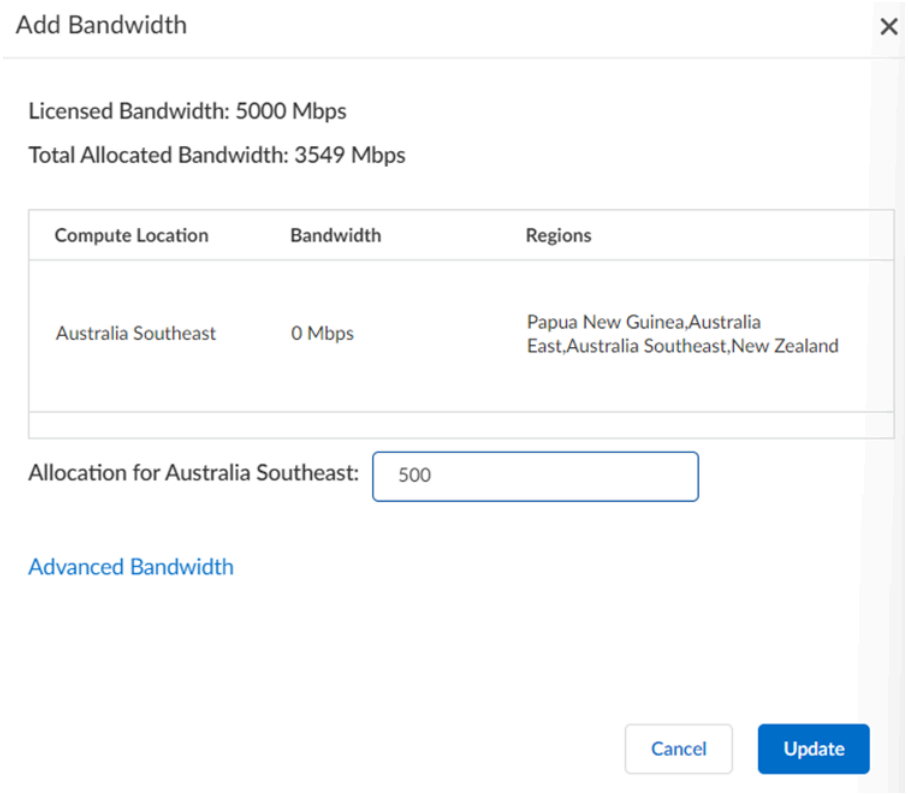


STEP 9 | 如果您尚未分配带宽，Prisma Access 会提示您为与选择的位置相关联的计算位置 **Allocate**（分配）带宽。指定每个计算位置的最低带宽为 50 Mbps。



 ©2025 Palo Alto Networks, Inc.

STEP 10 | 如果您尚未为选择的位置分配带宽，请分配带宽；然后，**Update**（更新）您的更改。



STEP 11 | 单击 **Next**（下一步）。

STEP 12 | 定义 **Tunnel & Circuit Settings**（隧道和电路设置）。

1. 选择 **Tunnel Mode**（隧道模式）：**Active/Active**（主动/主动）或 **Active/Passive**（主动/被动）。

   隧道模式指定您希望为高性能远程网络利用多少个 ISP 电路。

   - 如果您选择 **Active/Active**（主动/主动），则 Prisma Access 会利用四个 ISP 电路创建两个或四个活动隧道。
   - 如果您选择 **Active/Passive**（主动/被动），则 Prisma Access 会利用两个 ISP 电路创建两个活动隧道。如果活动隧道断开，备用隧道将变为活动状态。

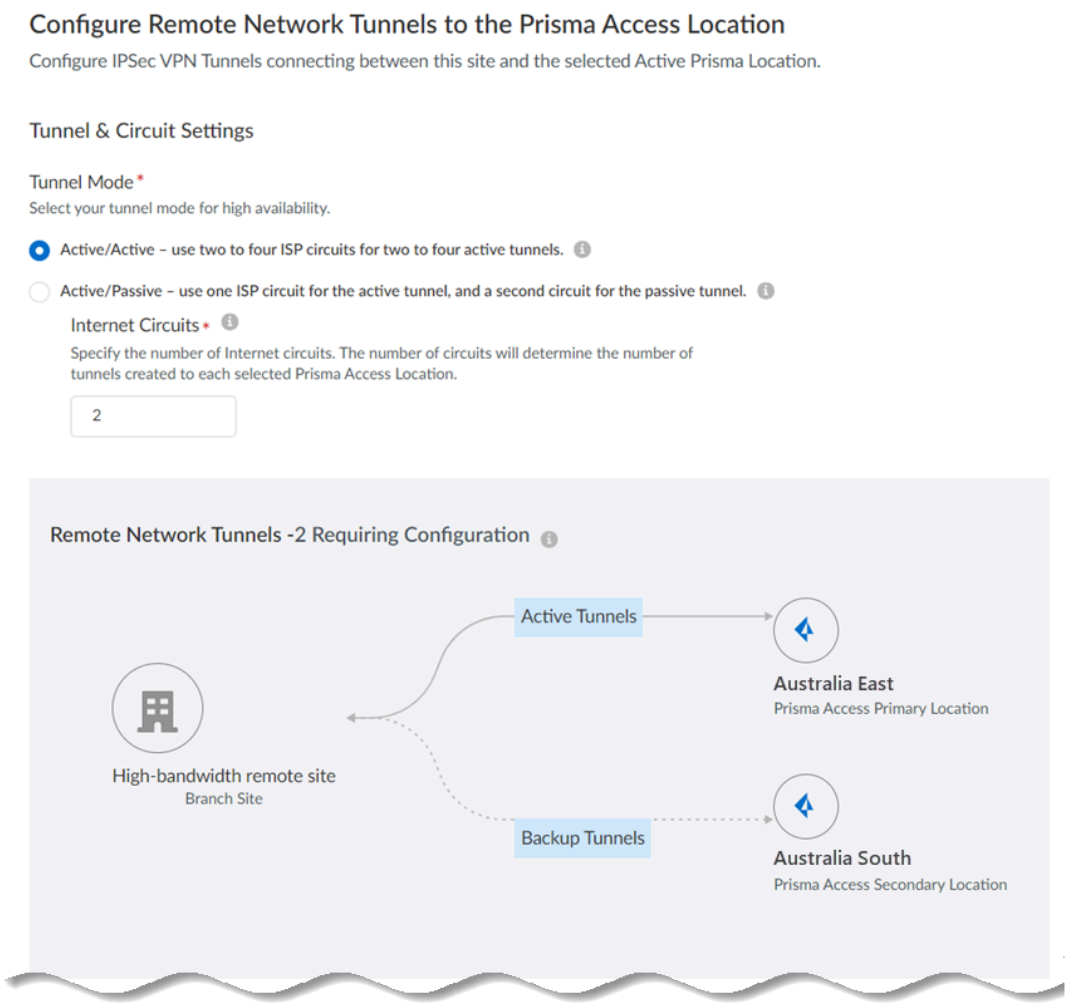
2. 选择要使用的 **Internet Circuits**（互联网电路）数量。

   Prisma Access 根据您在此处指定的电路数量以及您的部署是主动/主动还是主动/被动来分配隧道，如下表所示。

电路数量	部署类型	隧道数量
1	主动/被动	1（一个用于活动隧道）。
2	主动/主动	2（每个活动隧道一个）。

©2025 Palo Alto Networks, Inc.

电路数量	部署类型	隧道数量
		如果您选择主要和次要位置，则 Prisma Access 为主要位置创建一个活动隧道，为次要位置创建一个活动隧道。
2	主动/被动	2（每个活动隧道一个）。 如果您选择主要和次要位置，则 Prisma Access 为主要位置创建一个活动和被动隧道，并为次要位置创建一个活动和被动隧道。如果活动隧道出现故障，则 Prisma Access 对变为活动的被动隧道使用相同的服务 IP 地址或 FQDN。
4	主动/主动	4（每个活动隧道一个）。 如果您选择主要和次要位置，则 Prisma Access 为主要位置创建两个活动隧道，为次要位置创建两个活动隧道。

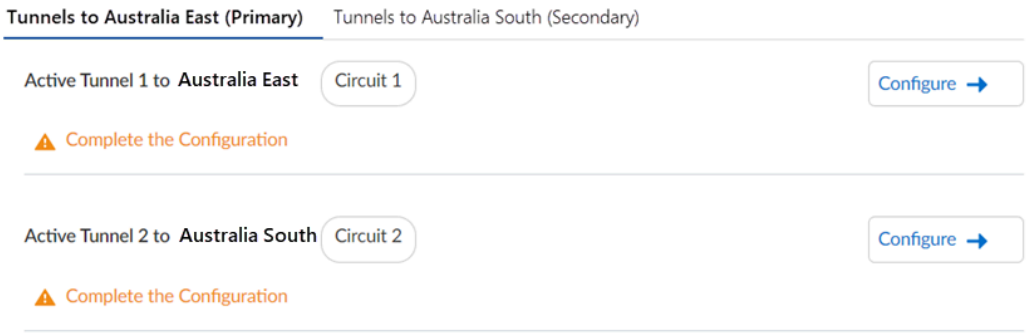


 ©2025 Palo Alto Networks, Inc.

3. （可选）**Configure**（配置）您的 IPSec 隧道设置。

   Prisma Access 为您提供默认的 IPSec 隧道设置。这些设置决定远程网络隧道的 IPSec 和 IKE 加密设置。如果您想更改它们，请选择 **Primary Tunnel**（主要隧道）并 **Edit**（编辑）设置。

   如果您指定了一个次要位置，Prisma Access 会将主隧道的值自动填充到次要隧道；要编辑次要隧道，请选择该隧道并 **Edit**（编辑）设置。



   请记下这些设置；您必须在终止您站点的 IPSec 隧道的 CPE 上匹配这些设置。

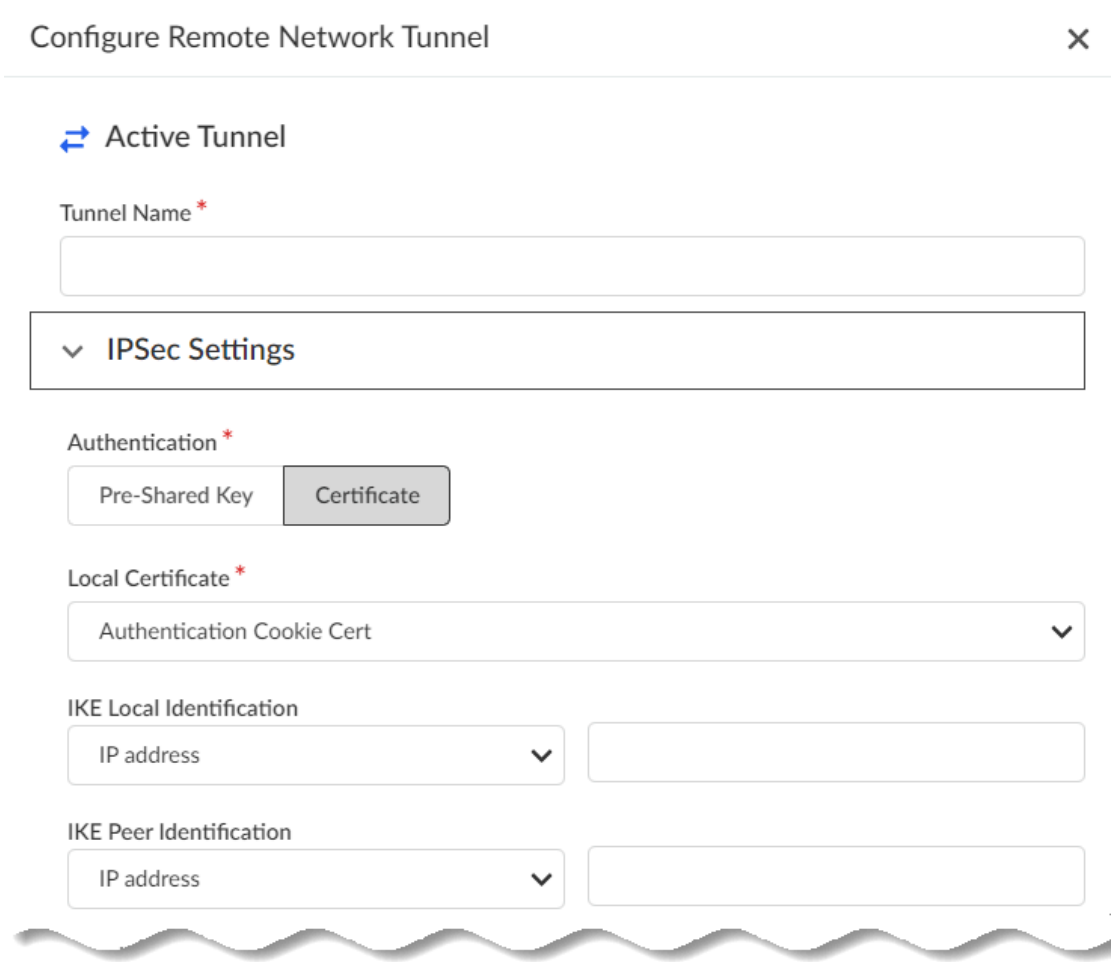
   - 给活动隧道分配一个唯一的 **Tunnel Name**（隧道名称）。
   - 指定 **IPSec Settings**（IPSec 设置）。
     - 指定 **Authentication**（身份验证）类型（（预共享密钥或证书））。

       如果您指定预共享密钥，请输入并确认预共享密钥。

       如果您指定证书，请输入要使用的本地证书。此证书必须在 Strata Cloud Manager 中已存在。
     - 指定 **IKE Local Identification**（IKE 本地标识）（**IP Address**（IP 地址）、**Distinguished Name (Subject)**（专有名称（主题））、**User FQDN (email address)**（用户 FQDN（电子邮件地址））或 **FQDN (hostname)**（FQDN（主机名））。
     - 指定 **IKE Peer Identification**（IKE 对端设备标识）（**IP Address**（IP 地址）、**Distinguished Name (Subject)**（专有名称（主题））、**User FQDN (email**

 ©2025 Palo Alto Networks, Inc.

address)（用户 **FQDN**（电子邮件地址））或 **FQDN (hostname)**（**FQDN**（主机名））

- 

- 指定对等设备 ID 检查的类型：
  - **Exact**（精确）— 确保本地设置和对等设备 IKE ID 有效负载精确匹配。
  - **Wildcard**（通配符）— 允许对等设备标识只匹配通配符 (*) 之前的每个字符。不需要匹配通配符后面的字符。
- （可选）单击 **Permit peer identification and certificate payload identification mismatch**（允许对等设备标识和证书有效内容标识不匹配），这样，即使对端设备标识与证书中的对端设备标识不匹配，IKE 安全关联 (SA) 仍会成功。
- 创建 **Certificate Profile**（证书配置文件）。证书配置文件包含有关如何验证对等设备网关的信息。
- （可选）要严格控制密钥的使用方式，请单击 **Enable strict validation of peer's extended key use**（启用对等设备扩展密钥使用的严格验证）。
- 选择 **Branch Device IP Address**（分支设备 **IP** 地址）（**Static**（静态）或 **Dynamic**（动态））。
  - 如果选择 **Static**（静态），请输入要用于 IPSec 隧道的 **Static IP Address**（静态 **IP** 地址）。

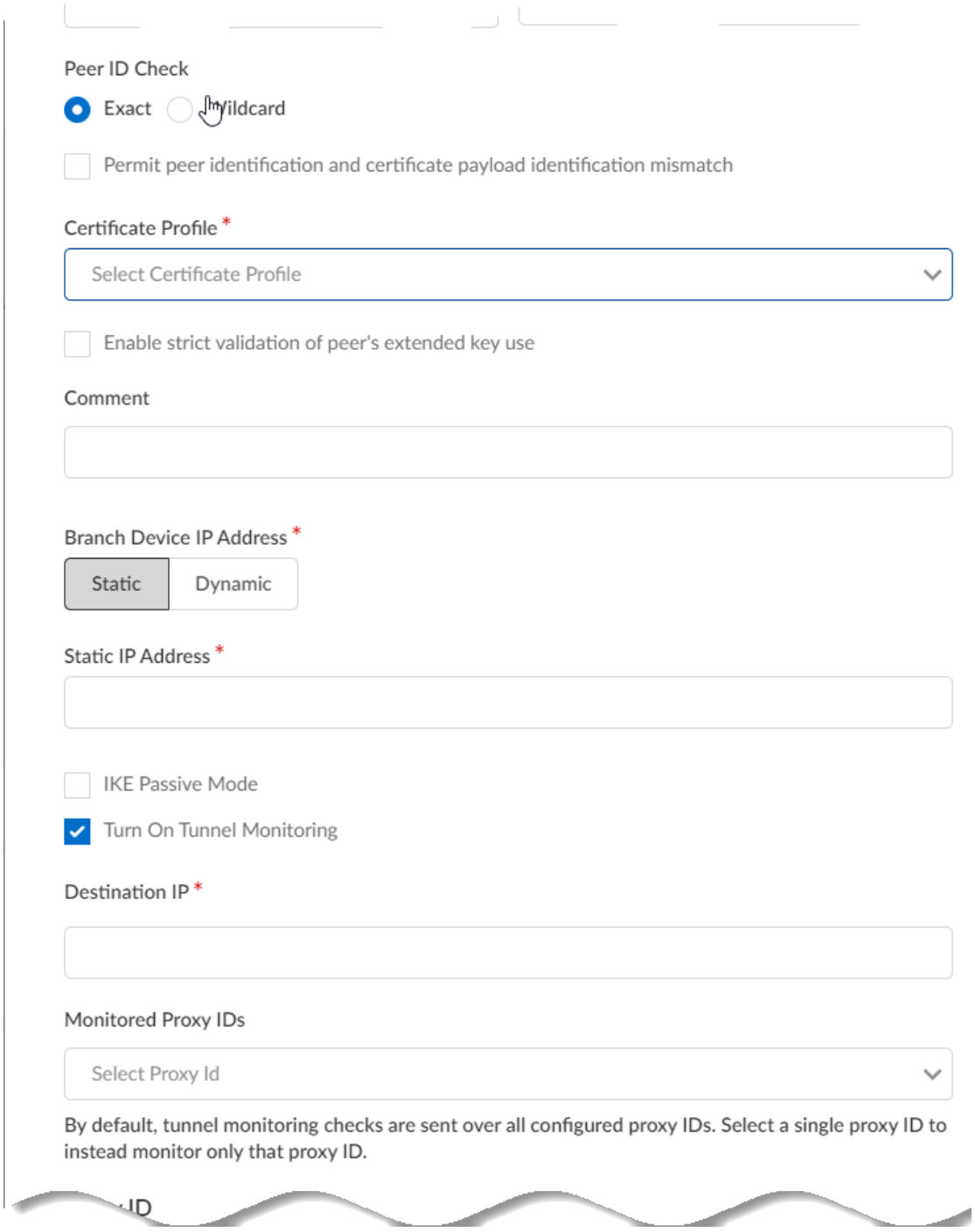
©2025 Palo Alto Networks, Inc.

  - 指定 **Dynamic**（动态）可自动获取 IP 地址。
- 可选，推荐）启用 **IKE Passive Mode**（**IKE** 被动模式），以便让 Prisma Access 响应 IKE 连接但不启动它们。

  虽然不是必需的，但建议使用 **IKE Passive Mode**（**IKE** 被动模式）。
- （可选）**Turn on Tunnel Monitoring**（打开隧道监控）。

  在 Prisma Access 的远程网络上输入隧道监控 **Destination IP**（目标 **IP**）以确定隧道是否开启，如果分支 IPSec 设备使用基于策略的 VPN，请输入相关联的 **Proxy ID**（代理 **ID**）作为 **Monitored Proxy ID**（监控代理 **ID**）。

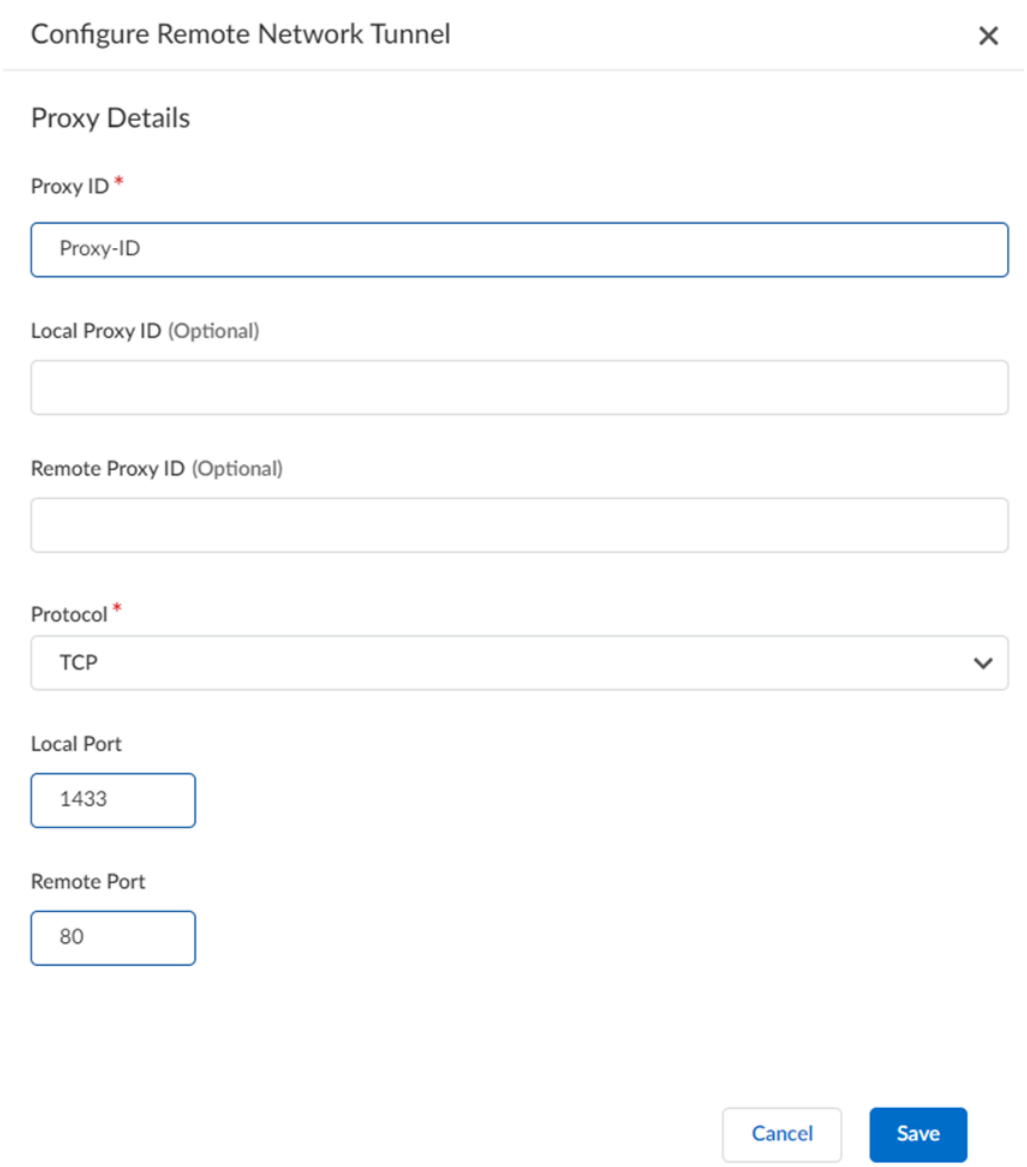
 ©2025 Palo Alto Networks, Inc.



- 可选）如果您需要代理 ID：
  - **Add Proxy ID**（添加代理 **ID**）并输入 **Proxy ID**（代理 **ID**）。
  - 选择输入 **Local Proxy ID**（本地代理 **ID**）和 **Remote Proxy ID**（远程代理 **ID**）。
  - 输入要用于代理 ID 的 **Protocol**（协议）。输入一个 **Number**（编号）、**TCP** 或 **UDP**。
  - 为 TCP 或 UDP 指定 **Local Port**（本地端口）和 **Remote Port**（远程端口），或者指定

 ©2025 Palo Alto Networks, Inc.

- **Save**（保存）更改。



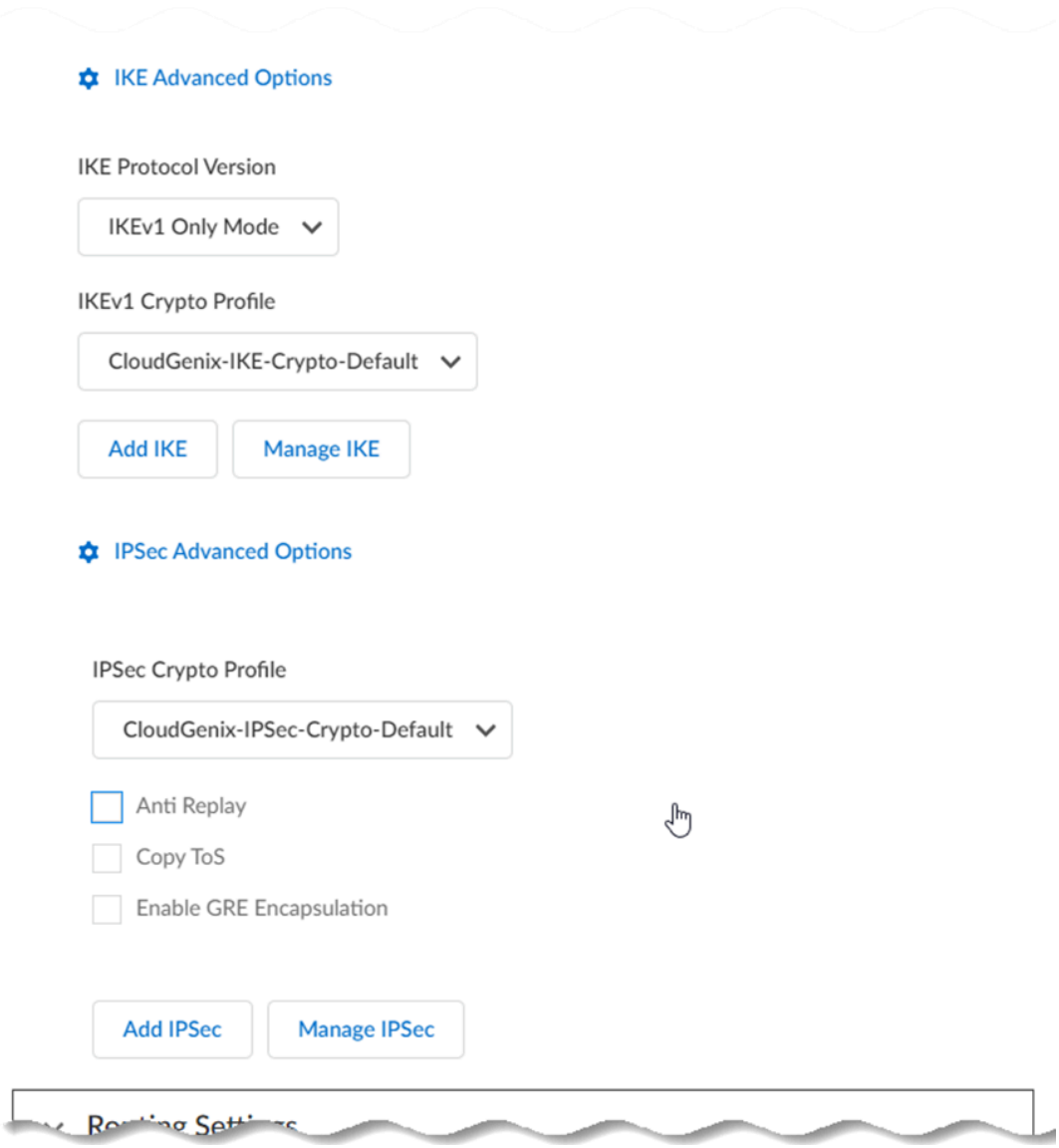
- 指定 **IKE Advanced Options**（**IKE** 高级选项）。
  - 选择 **IKE Protocol Version**（**IKE** 协议版本）。
  - 选择 **IKEv1 Crypto Profile**（**IKEv1** 加密配置文件）。

    要添加加密配置文件，请 **Add IKE**（添加 **IKE**）。要管理现有 IKE 配置文件，请单击 **Manage IKE**（管理 **IKE**）并选择要编辑的配置文件。
  - 选择 **IKEv2 Crypto Profile**（**IKEv2** 加密配置文件）。

    要添加加密配置文件，请 **Add IKE**（添加 **IKE**）。要管理现有 IKE 配置文件，请单击 **Manage IKE**（管理 **IKE**）并选择要编辑的配置文件。
- 指定 **IPSec Advanced Options**（**IPsec** 高级选项）。
  - 选择 **IPSec Crypto Profile**（**IPSec** 加密配置文件）。

©2025 Palo Alto Networks, Inc.

要添加加密配置文件，请 **Add IPSec**（添加 **IPSec**）。要管理现有的 IPSec 配置文件，请单击 **Manage IPSec**（管理 **IPSec**）并选择要编辑的配置文件。

- 

- 选择 **Routing Settings**（路由设置）。
  - 选择 **Routing Type**（路由类型）（**Static**（静态）或 **Dynamic**（动态））。

    如果选择 **Static**（静态），请 **Add**（添加）要在站点保护的 IP 子集或 IP 地址。

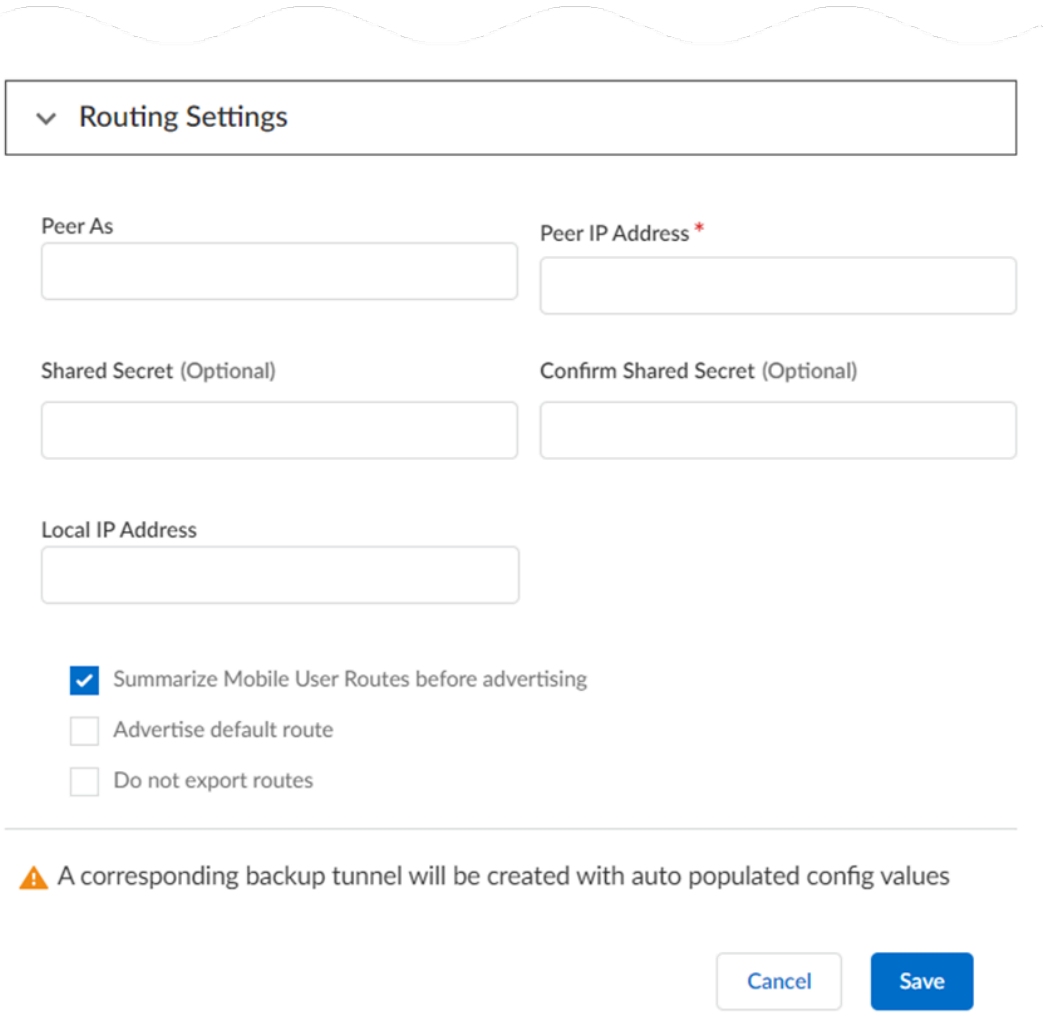
    如果选择 **Dynamic**（动态）：
    - 输入 **Peer AS**（对端 **AS**）（网络的自治系统 (AS)）。

      使用符合 RFC 6996 的 BGP 私有 AS 编号。
    - 输入分配的 **Peer IP Address**（对端 **IP** 地址）作为总部或数据中心网络上 eBGP 路由器的路由器 ID。
    - 可选）输入 **Shared Secret**（共享机密）密码来对 BGP 对端通信进行身份验证。

 ©2025 Palo Alto Networks, Inc.

- 输入 Prisma Access 为用作 BGP 的本地 IP 地址的 **Local IP Address**（本地 **IP** 地址）。
- 可选）选中 **Summarize Mobile User Routes before advertising**（在通告之前汇总移动用户路由），以便在通告之前通过 Prisma Access 来汇总子网，以减少通过 BGP 向您的客户本地设备 (CPE) 通告的移动用户 IP 子网的数量。
- 可选）选择 **Advertise Default Route**（通告默认路由），以便让 Prisma Access 使用 eBGP 为远程网络发起默认路由通告。确保您的网络没有其他由 BGP 通告的默认路由，否则您可能会在网络中引入路由问题。
- 可选）选择 **Don't Export Routes**（不导出路由），以阻止 Prisma Access 将路由转发到总部或数据中心。

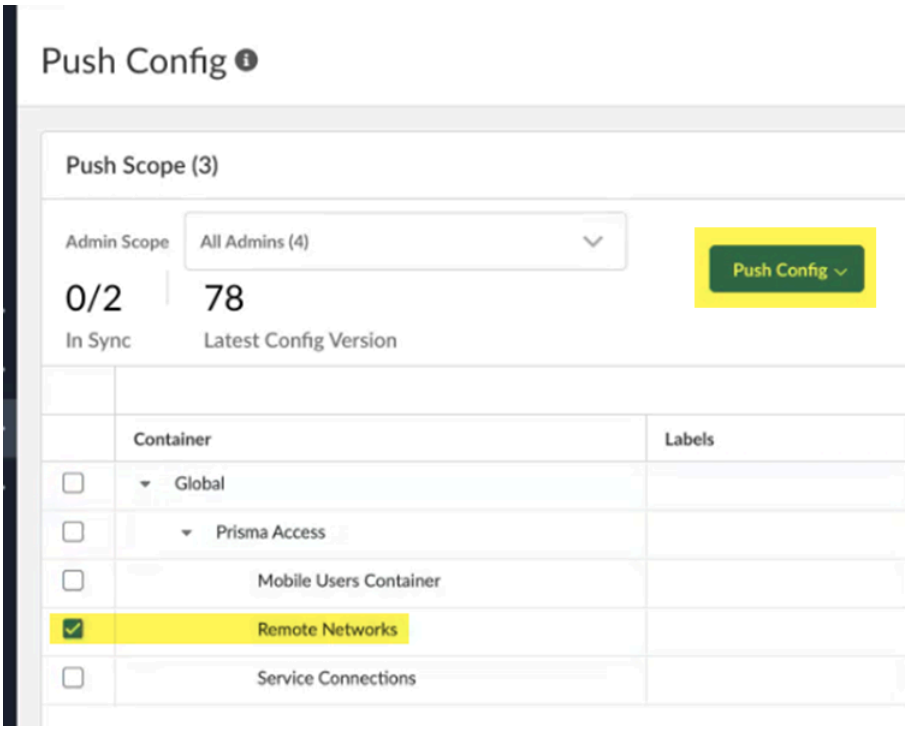
4. **Save**（保存）您的 IPSec 隧道更改。



STEP 13 | 保存并退出。

 ©2025 Palo Alto Networks, Inc.

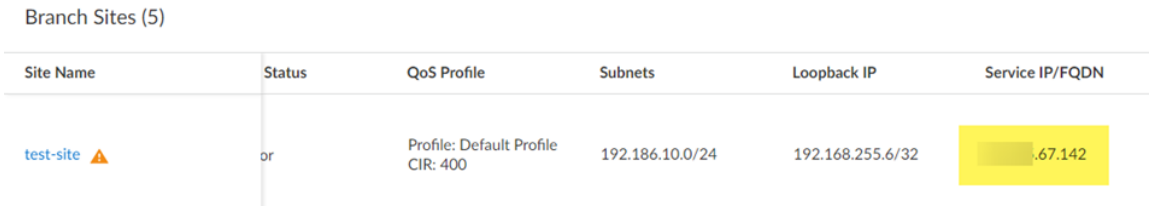
STEP 14 | **Push Configuration**（推送配置）以保存配置更改，确保在 **Push Scope**（推送范围）中选择 **Remote Networks**（远程网络）。



STEP 15 | 在您的 CPE 上找到指定的 **Service IP**（服务 **IP**）地址。

当您设置远程网络时，请使用服务 IP 地址作为您 CPE 上的对等 IP 地址，以终止 IPSec 隧道。

1. 转到 **Workflows**（工作流） > **Prisma SASE Setup**（**Prisma SASE** 设置） > **Branch Site Management**（分支站点管理） > **Extended CPE Site**（扩展 **CPE** 站点）。
2. 找到 **Service IP/FQDN**（服务 **IP/FQDN**）地址。



Panorama

在 Prisma Access (Managed by Panorama) 中，配置“远程网络—高性能”的步骤与载入标准远程网络的步骤相同，包括在载入时选择 **IPSec Termination Node**（**IPsec** 终止节点）。

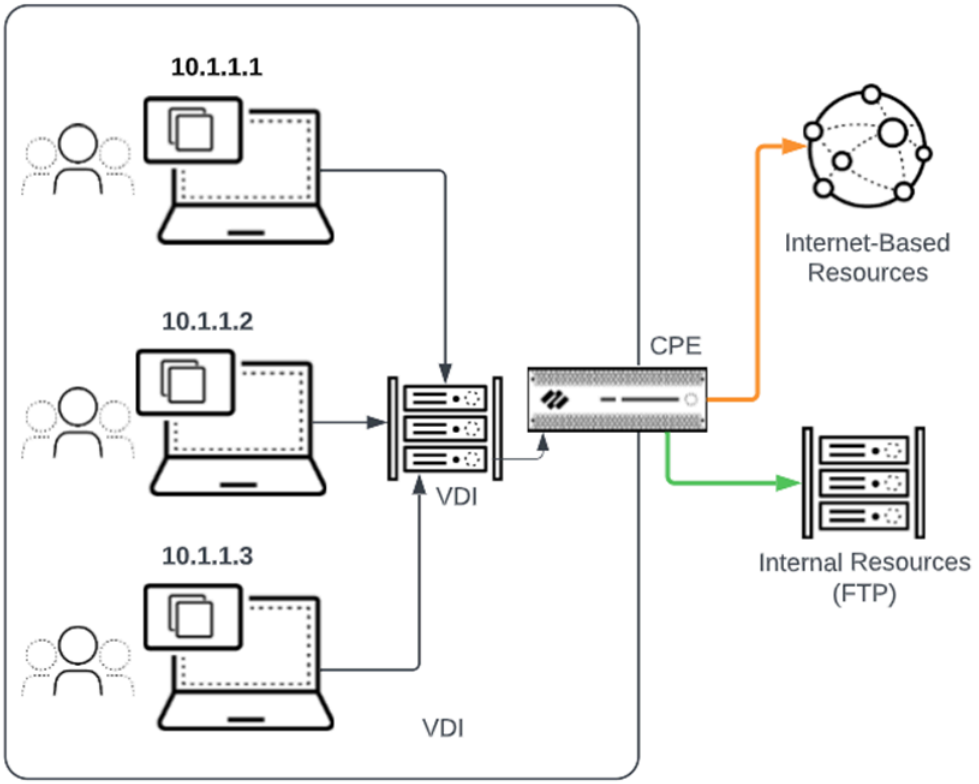
 ©2025 Palo Alto Networks, Inc.

使用终端服务器将共享桌面 VDI 与 Prisma Access 集成

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 许可证

虚拟桌面基础设施 (VDI) 是一种使用虚拟机来配置和管理虚拟桌面的技术。VDI 使用托管服务器来部署桌面环境，并根据请求将其部署给最终用户。最终用户可以从其配置的 VDI 桌面访问他们所需的资源，例如基于互联网的公共应用程序和资源或可通过 FTP 连接获取的私有应用程序和资源。

可以使用共享或专用桌面来实现 VDI 拓扑。如果共享桌面，则多个用户将位于单个 IP 地址后面，并使用端口来区分用户。



如果你的 VDI 部署采用了共享桌面实施，Prisma Access 提供了一种解决方案，允许最终用户通过一次登录即可安全访问互联网和 FTP 资源，同时保护你所在机构的 VDI 用户以及内部和外部资源。此解决方案使用在 VDI 服务器上安装的 Palo Alto Networks TS 代理。

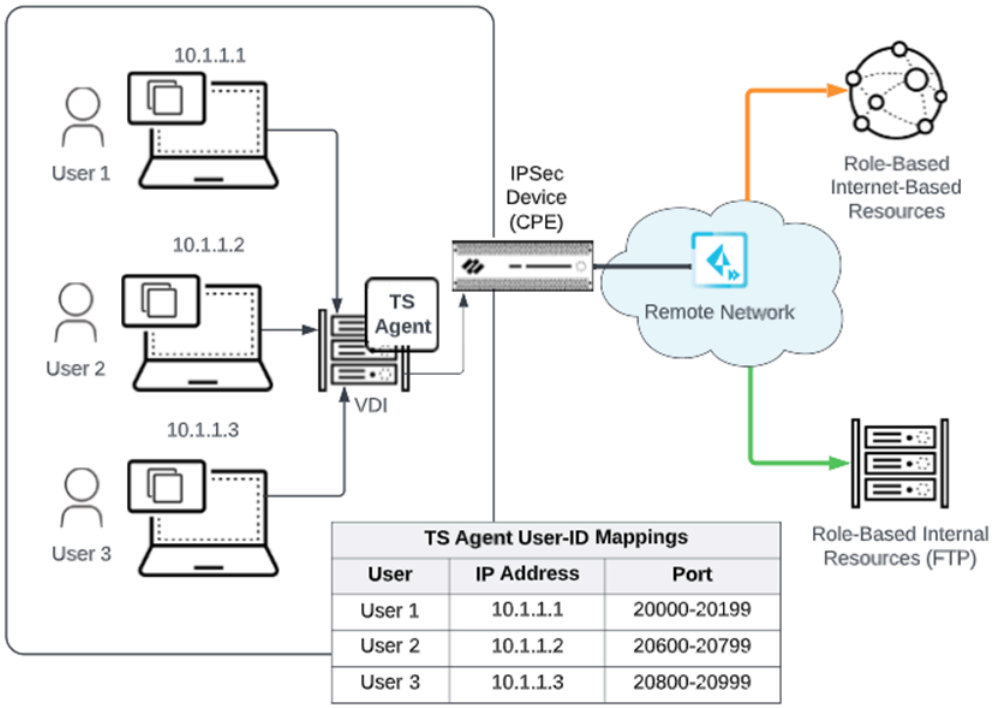
TS 代理是一种 User-ID 软件，安装该软件是为了解决在用户共享 IP 地址的情况下难以识别用户名到 IP 地址映射相关的问题。安装 TS 代理后，所有登录用户都会受到监控，并且每个用户都会被分配一组特定的端口。当 Prisma Access 从 VDI 接收此 VDI 网络流量时，它会根据用户的源端口标识用户。此部署为您提供了基于云的解决方案，允许管理员为 VDI 最终用户创建安全策略规则，以控制他们对互联网和内部站点的访问。

©2025 Palo Alto Networks, Inc.

如果您的网络有默认路由，您可以接入一个或多个远程网络并实施 TS 代理，以轻松简单地保护您组织中的用户和资源。

在此部署中：

- 可以在 TS 代理上指定端口范围来识别基于 Windows 的终端服务器上的特定用户。TS 代理向 Prisma Access 通知分配的端口范围，这样 Prisma Access 就可以根据用户和用户组执行策略。
- 远程网络加强了基于 FTP 和基于互联网的资源的安全和访问控制。



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

无法重新分发从 *TS* 代理收集的用户映射信息。

要在云托管 Prisma Access 中使用 TS 代理和 Prisma Access 远程网络集成 VDI，请完成以下步骤。

STEP 1 | 在 VDI 服务器上安装并配置 Palo Alto Networks TS 代理。

要映射所有用户，必须在用户登录的所有终端服务器上安装 TS 代理。

1. 在 VDI Windows 服务器上，安装并配置 Palo Alto Networks 终端服务器 (TS) 代理。
2. 定义 TS 代理分配给最终用户的端口范围。

   根据兼容性一览表验证 *TS* 代理支持的规模数量。

3. （可选）如果有多个 VDI 服务器，请在每个 VDI 服务器上配置一个 TS 代理。

STEP 2 | 接入远程网络并将其连接到云托管 Prisma Access 中的 VDI 分支站点（如果还没有这样做）。

©2025 Palo Alto Networks, Inc.

STEP 3 | 配置分支机构的 IPSec 设备 (CPE) 上的选项，以允许远程网络与 VDI 通信。

- 为 IPsec 隧道配置与您在 Prisma Access 中配置的参数相匹配的 IPsec 和 IKE 加密参数。
- 使用 **Service IP**（服务 **IP**）地址（**Manage**（管理） > **Remote Networks**（远程网络） > **Service IP**（服务 **IP**））作为远程网络 IPsec 隧道的 Prisma Access 端。
- 在 IPSec 设备上配置路由以允许 VDI 到远程网络隧道的流量。
- 在 IPSec 设备上配置路由，以允许远程网络流量通过隧道到达 TS 代理。
- 如果需要，可在 IPSec 设备上配置安全策略，允许流量通过隧道。

STEP 4 | 配置 TS 代理以允许在远程网络中进行用户映射。

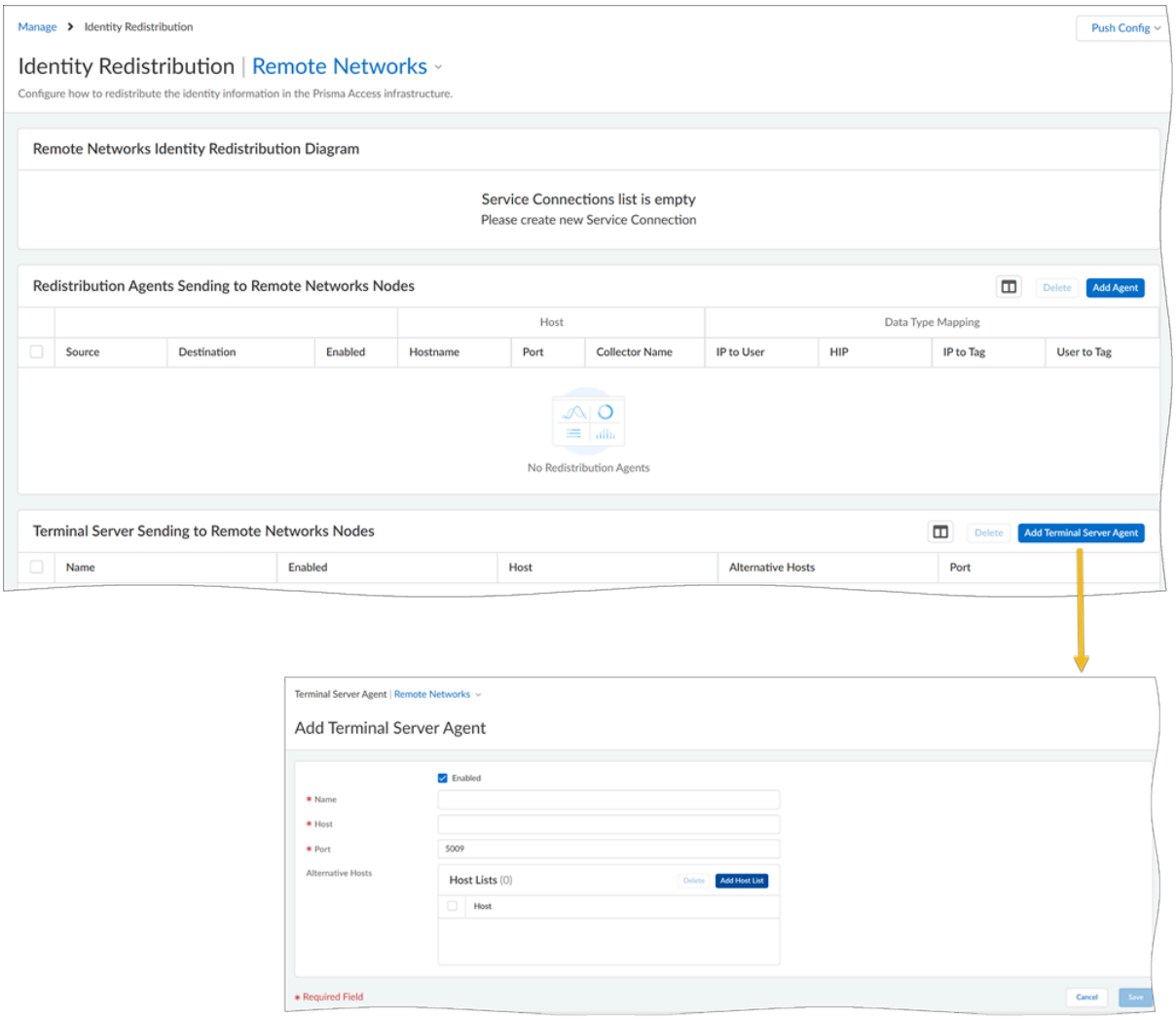
转到 **Manage**（管理） > **Configuration**（配置） > **NGFW** 和 **Prisma Access** > **Identity Services**（身份服务） > **Identity Redistribution**（身份重新分发），将 **Configuration**

 ©2025 Palo Alto Networks, Inc.

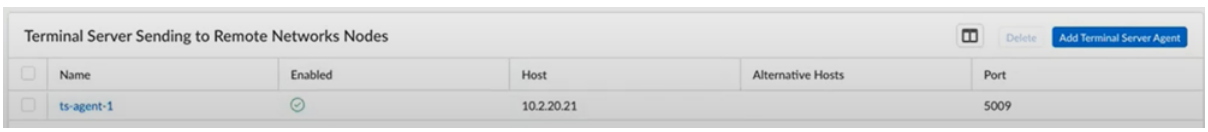
Scope（配置范围）设置为 **Remote Networks**（远程网络），然后选择 **Add Terminal Server Agent**（添加终端服务器代理）。

- 确保代理状态为 **Enabled**（已启用）。
- 输入 TS 代理的 **Name**（名称）。
- 输入安装终端服务代理的 Windows **Host**（主机）的 IP 地址。
- 输入代理监听用户映射请求的 **Port**（端口）号。

  默认情况下，该端口设置为 5009。
- **Save**（保存）更改。



在以下示例中，代理配置的主机地址为 10.2.2 0.21，端口为 5009。

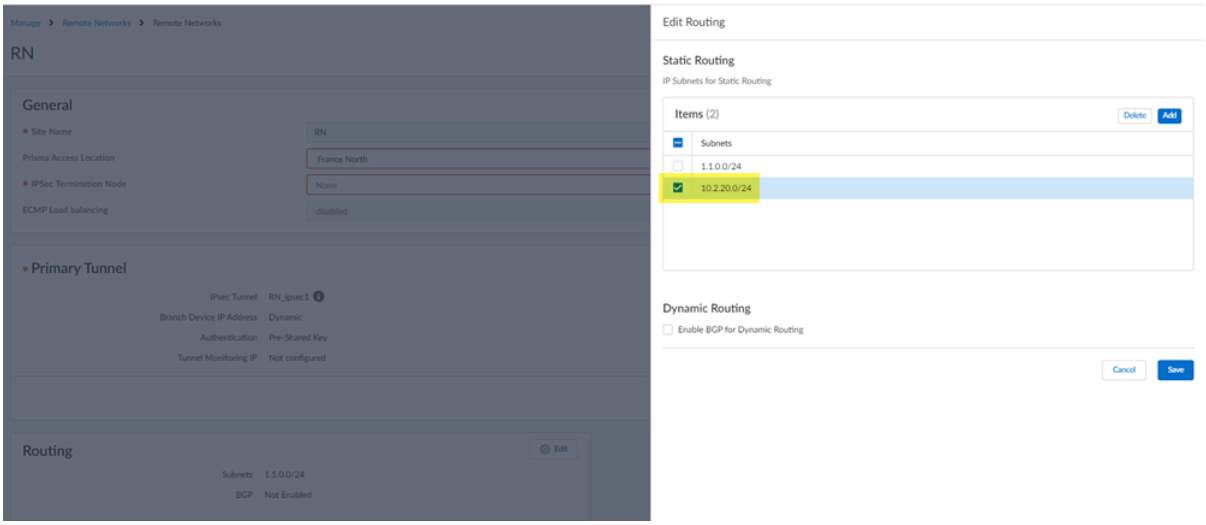


©2025 Palo Alto Networks, Inc.

STEP 5 | 允许在 VDI 和 Prisma Access 远程网络之间路由。

1. 前往**Manage**（管理） > **Service Setup**（服务设置） > **Remote Networks**（远程网络） > 远程网络名称 > **Routing**（路由），然后选择 **Add**（添加）以添加一个指向 VDI 子网的路由。

   添加此子网将允许 TS 代理与远程网络通信。在以下屏幕截图示例中，VDI 子网是 10.2.20.0/24。



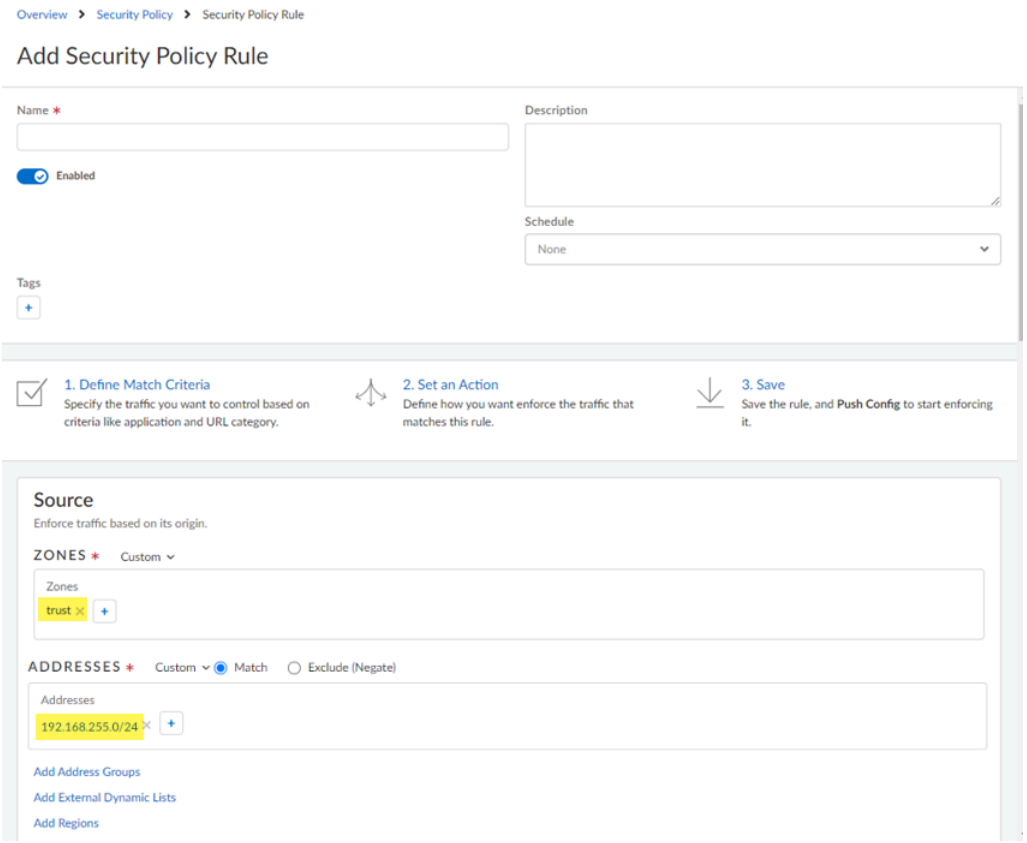
2. 前往 **Manage**（管理） > **Configuration**（配置） > **Security Services**（安全服务） > **Security Policy**（安全策略），将范围设置为 **Remote Networks**（远程网络），并添加一条安全策略规则（**Add Rule**（添加规则）），以允许 VDI 子网与远程网络之间的流量。

   从 VDI 连接到 Prisma Access 的远程网络用户会被分配一个来自Prisma Access基础设施子网的 IP 地址，并且您必须允许在基础设施子网和 VDI 子网之间进行路由。

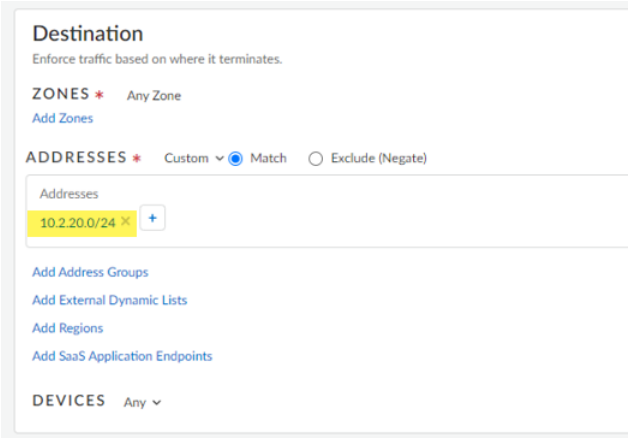
   - 确保该规则已设置为 **Enabled**（已启用）。
   - **Source**（源）—设置以下参数：
     - **Zones**（区）—设置为 **Trust**（信任）。
     - **Addresses**（地址）—为基础设施子网创建一个地址对象（**Manage**（管理） > **Shared**（共享） > **Infrastructure Settings**（基础设施设置） > **Infrastructure Subnet**（基础设施子网）），并在此处添加该地址对象。

     与输入实际的基础设施子网相比，更可取的方法是使用地址对象，因为如果子网发生更改，您可以修改该地址对象，并且这一更改会应用到所有使用了该地址对象的配置中。

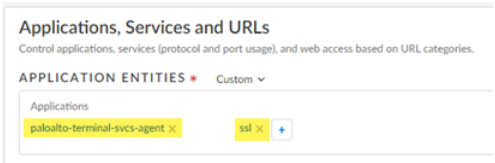
 ©2025 Palo Alto Networks, Inc.



- **Destination**（目标）—将运行 TS 代理的 VDI 主机添加到 **Addresses**（地址）中。如果已在多个 VDI 主机上配置了 TS 代理，则在此处添加所有这些主机。



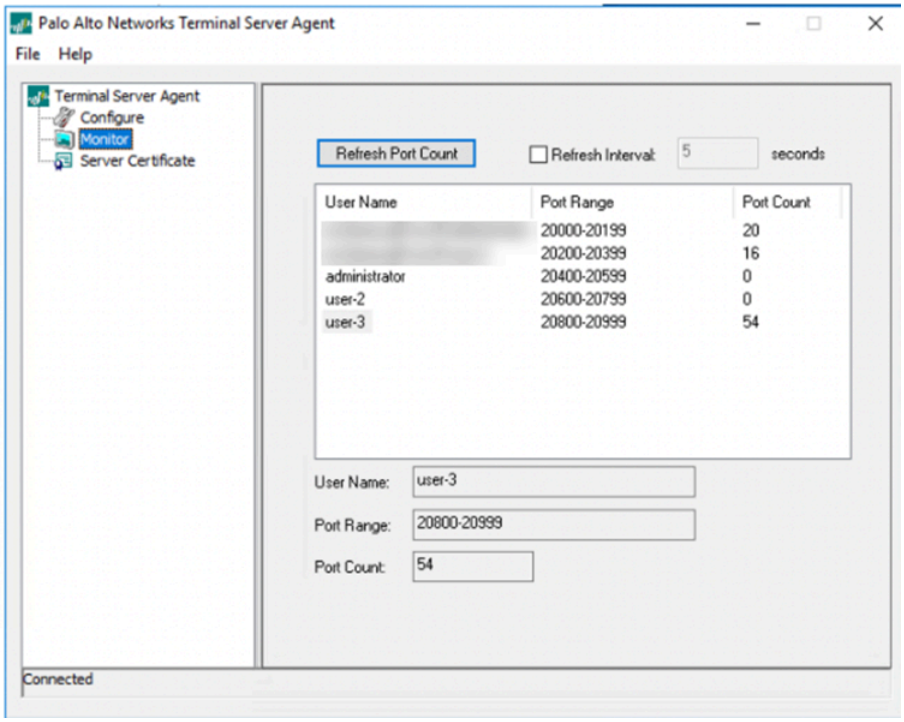
- **Applications, Services and URLs**（应用程序、服务和 **URL**）—将 **paloalto-terminal-svcs-agent** 添加到 **Application Entities**（应用程序实体）中。



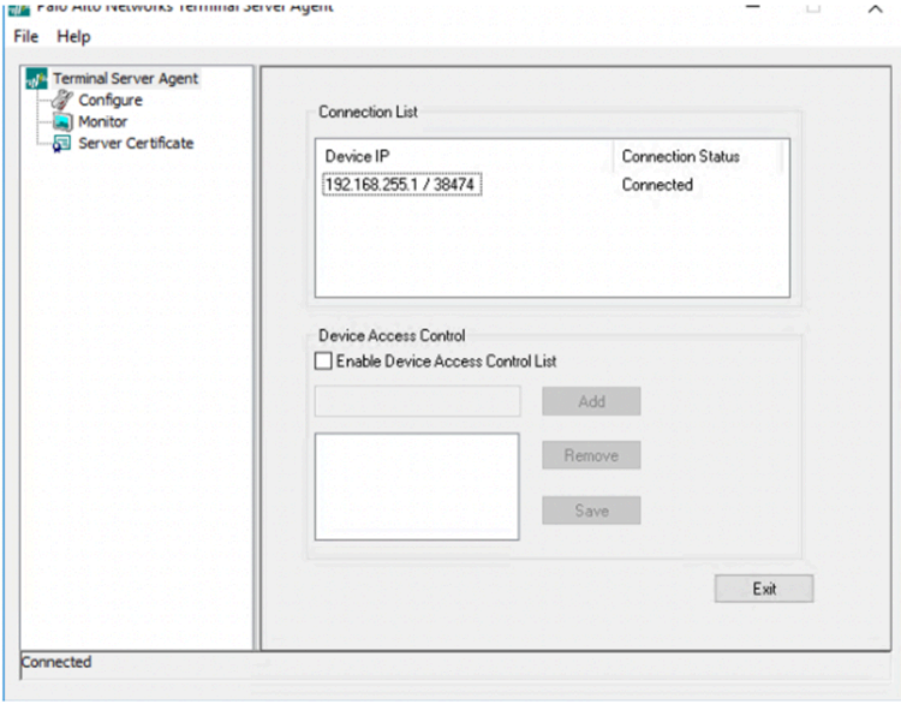
 ©2025 Palo Alto Networks, Inc.

STEP 6 | 验证实施是否正确运行。

1. 在 TS 代理中，监控代理的状态并验证 TS 代理是否反映了正确的用户名到端口映射。

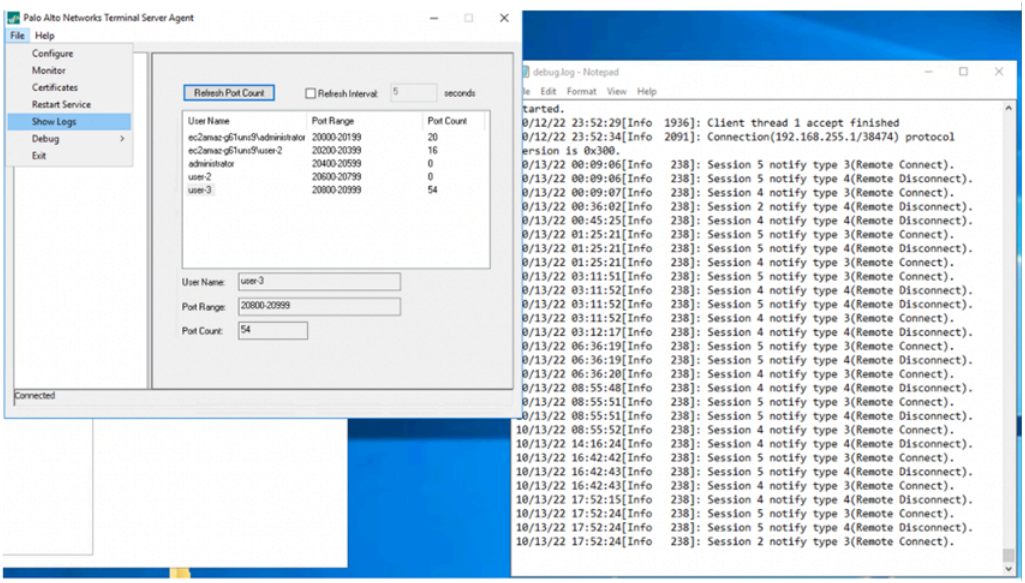


2. 确认远程网络的 IP 地址已连接到 TS 代理。

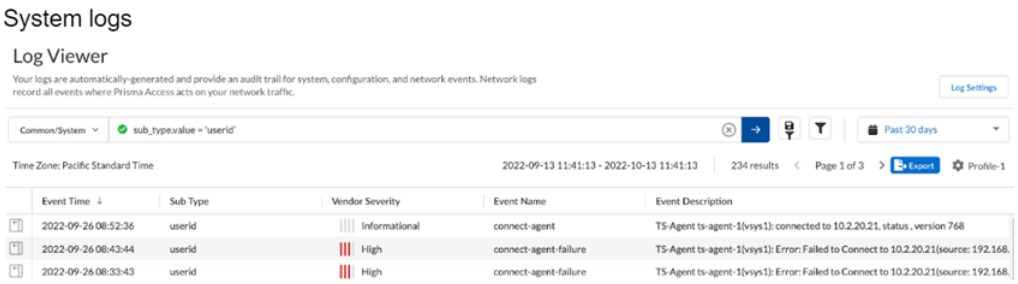


3. 转到 **File**（文件） > **Show Logs**（显示日志） 并查看 TS 代理的日志消息。

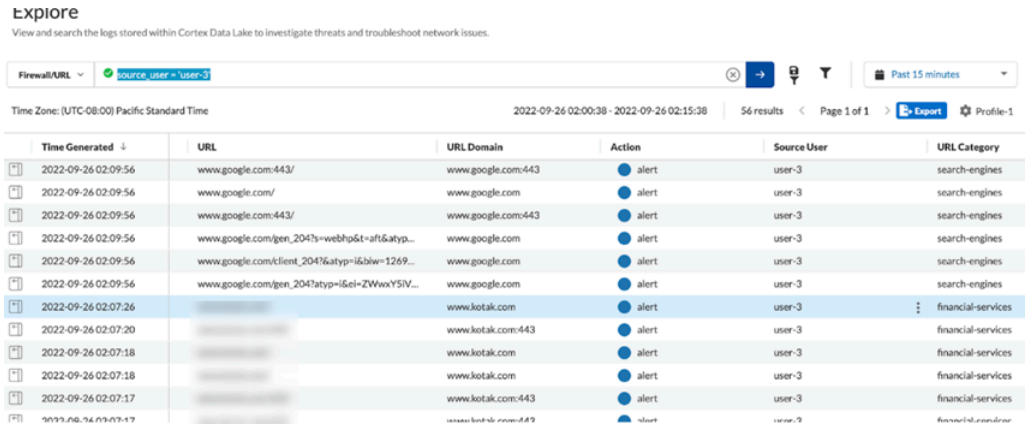
©2025 Palo Alto Networks, Inc.



4. 在 Prisma Access (Managed by Strata Cloud Manager) 中，转到 **Activity**（活动） > **Log Viewer**（日志查看器） > **Common/System**（通用/系统），并验证远程网络是否能够连接到 TS 代理。



5. 前往 **Activity**（活动） > **Log Viewer**（日志查看器） > **Firewall/URL**（防火墙/网址），并验证远程网络是否能够实施基于身份的策略。



 ©2025 Palo Alto Networks, Inc.

Prisma Access 监控和可见性

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证 ❑ 访问 Autonomous DEM 需要 ADEM Observability 许可证。

Prisma Access 提供以下功能，以深入了解您的安全活动并监控您的部署。通过日志、远程网络、服务连接、移动用户和您的许可实体的警报通知，这些功能可以提供对网络和用户流量的可见性，并通过交互式指示板提供对应用程序、威胁、用户，以及您网络中工作的安全订阅的数据的全面视图。您还可以在 Strata Cloud Manager 中监控 Prisma Access。

- Prisma Access日志

  您的日志是自动生成的，并为系统、配置和网络事件提供审计跟踪。网络日志记录 Prisma Access 对您的网络流量进行操作的所有事件。例如，当 Prisma Access 基于安全规则阻止流量、基于身份验证规则授予用户访问权限或基于QoS规则调整流量时，会记录条目。您可以在 Strata Cloud Manager 和 Panorama 管理界面中查看 Prisma Access 日志。
- Prisma Access 活动指示板和报告

  活动让您全面了解网络中发生的事情，从日志数据到关键发现，您可以利用这些信息来更新政策并弥补企业安全和用户生产力的差距。
- 在 Strata Cloud Manager 中监控 Prisma Access
- 使用 Strata Cloud Manager 的监控和工作流部分，全面了解您的网络流量以及您正在管理的产品和订阅。
- Prisma Access 和自主 DEM

  Autonomous DEM 为您的安全访问服务边缘 (Strata Cloud Manager) 中的所有用户流量提供本地、端到端的可见性和洞察力。Autonomous DEM 功能已本机集成到 GlobalProtect 应用程序和 Prisma Access 中，因此不需要您部署任何其他设备或代理。您可以快速隔离数字体验问题的来源，并简化修复过程。
- Strata Cloud Manager 命令中心

  命令是您网络上物联网设备、用户、主机和流量的交互式可视化摘要。利用云交付的安全和 ADEM 订阅中的数据，命令中心可显示有关威胁、用户体验和网络数据安全性的重要信息。

  通过命令中心，您能够与数据交互，查看网络上的事件之间的关系，以便发现异常情况，寻找增强网络安全的方法。

Prisma Access日志

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

日志是自动生成并打上时间戳的文件，可为 Prisma Access 监控的系统事件或网络流量事件提供审核跟踪。日志条目包含构件，这些构件即与记录事件关联的属性、活动或行为，例如应用程序类型或攻击者 IP 地址。每个日志类型都记录了一个单独事件类型的信息。例如，Prisma Access 可能会生成一个威胁日志，以记录与间谍软件、漏洞或病毒特征匹配的流量。Prisma Access (Managed by Strata Cloud Manager) 提供网络日志（如流量、威胁、URL、文件、HIP匹配）、端点日志和常见日志（系统和配置）。您可以查看每个日志条目的详细信息，对于威胁日志，您可以查看威胁详细信息，并查看是否存在任何威胁覆盖。

- Strata Cloud Manager
- Panorama

Prisma Access 日志 (Strata Cloud Manager)

如果您正在使用 **Strata Cloud Manager**，则转到 **Incidents & Alerts**（事件与警报） > **Log Viewer**（日志查看器）。

Prisma Access (Managed by Strata Cloud Manager) 提供网络日志（流量、威胁、URL、文件、HIP 匹配）和常见日志（系统和配置）。

您可以查看每个日志条目的详细信息，对于威胁日志，您可以查看威胁详细信息并查看是否存在任何威胁覆盖。了解更多信息。

Prisma Access 日志 (Panorama)

您还可以在 Prisma Access (Managed by Panorama) 界面中查看 Prisma Access 日志。Prisma Access 基础结构将所有日志转发到 Strata Logging Service。Prisma Access使用云服务插件从 Strata Logging Service 检索日志结果，并提供远程网络和移动用户流量日志的聚合视图。无论您使用哪种管理界面来管理 Prisma Access（Panorama 或是 Strata Cloud Manager），都可以在 Prisma Access (Managed by Strata Cloud Manager) 中的 **Activity**（活动） > **Logs**（日志） > **Log Viewer**（日志查看器）下查看日志。

除了来自 Prisma Access 云服务基础设施的日志外，您还可以直接从管理 Prisma Access 的 Panorama 设备查看日志。要查看日志，请转到 **Monitor**（监控） > **Logs**（日志）。了解更多信息。

©2025 Palo Alto Networks, Inc.

外部日志和其他数据

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

您可能已经习惯了从 **Activity**（活动） > **Logs**（日志）中查看 Prisma Access 日志（这些日志存储在 Strata Logging Service 中）并且与之交互。但您可能还不知道，当您拥有 Cortex XDR Pro 按每 TB 许可的数据湖时，Prisma Access 还支持从各种外部第三方来源提取日志和其他数据。设置完成后，您可以使用中心内的 Strata Logging Service 应用程序来查看日志并设置日志转发。支持的供应商包括：

• 激活 Windows 事件收集器	• Corelight Zeek	• PAN IoT Security
• Amazon S3	• ElasticSearch Filebeat	• PingFederate
• Apache Kafka	• Forcepoint DLP	• PingOne for Enterprise
• AWS	• Fortinet Fortigate	• Prisma Cloud
• AWS CloudTrail 和 Amazon Cloudwatch	• Google Cloud Platform	• Prisma Cloud Compute
• Azure Event Hub	• Google Kubernetes Engine	• Proofpoint Targeted Attack Protection
• Azure 网络观察程序	• Google Workspace	• ServiceNow CMDB
• BeyondTrust Privilege Management Cloud	• Microsoft Azure	• 使用 Elasticsearch Filebeat 的 Windows DHCP
• Check Point FW1/VPN1	• Microsoft Office 365	• Workday
• Cisco ASA	• Okta	• Zscaler Cloud Firewall

可以将从第三方来源接收的日志用作唯一的数据源，也可以将这些日志与 Palo Alto Networks Prisma Access 日志和其他数据源结合使用。

借助 Palo Alto Networks，通过收集、集成和规范化来自所有数据源（网络、端点和云）的数据，减轻您的运营负担并从根本上简化您的 SOC 运营。统一查看企业内应用程序的使用状况、流量模式、面临的威胁以及各类事件，进而获得行之有效的见解。

©2025 Palo Alto Networks, Inc.

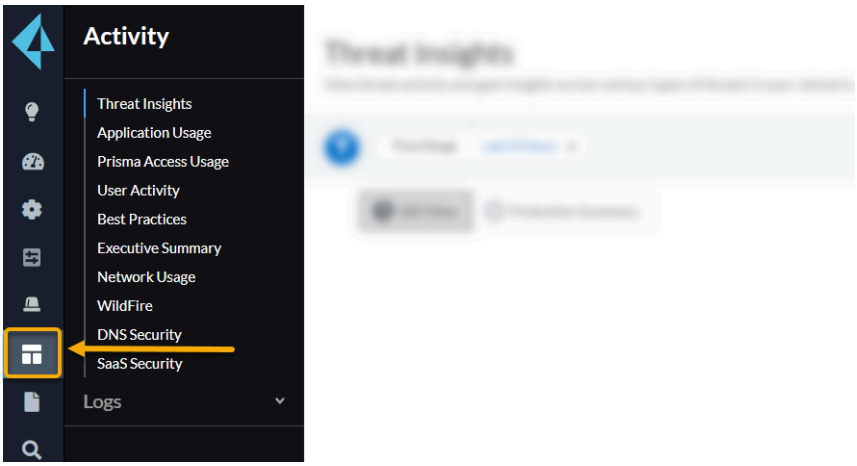
Prisma Access 活动指示板和报告

哪里可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Panorama Managed Prisma Access	❑ Prisma Access 许可证 ❑ 查看活动指示板和报告的许可证及其他要求

活动可识别重要调查结果，您可以使用这些调查结果来了解策略更新并缩小企业安全和用户工作效率之间的差距。活动为您提供：

- 交互式指示板，用于探索在网络中运行的应用程序、威胁、用户和安全订阅的数据。
- 您可以离线共享并安排定期更新的报告。
- 日志查看器为系统、配置和网络事件提供审计跟踪。您可以从指示板跳转到日志查看器，以获取更多上下文并深入研究数据。
- 搜索安全工件可帮助您搜索文件哈希、URL、域或 IP 地址（IPv4 或 IPv6）等工件，以便仅与该工件的数据进行交互。搜索结果包括工件的历史记录、工件的威胁情报以及工件的第三方分析结果。

Prisma Access (Managed by Strata Cloud Manager) 和 Panorama Managed Prisma Access 用户可以在 Prisma Access (Managed by Strata Cloud Manager) 应用程序中使用 **Activity**（活动）。要开始使用，请启动Prisma Access (Managed by Strata Cloud Manager)并单击左侧导航窗格中的 **Activity**（活动）选项卡。



“见解”功能正在通过 Prisma SASE FedRAMP 高级认证。“活动”功能正在通过 Prisma SASE FedRAMP 高级认证。

- 活动入门

©2025 Palo Alto Networks, Inc.

在 Strata Cloud Manager 中查看和监控 Prisma Access

哪里可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证 ❑ 这是一个 Prisma Access Insights 功能。

Palo Alto Networks 推出的 Strata Cloud Manager Command Center 是一个 AI 驱动的网络安全平台。借助 Strata Cloud Manager 和 Strata Cloud Manager Command Center，您可以从单个简化的用户界面轻松管理 Palo Alto Networks 网络安全基础设施。

可以使用命令中心中的 Activity Insights（活动洞察）以及命令中心的 Monitor（监控）和 Workflows（工作流）部分，全面了解您的网络流量情况，以及您所管理的产品和订阅信息。

- 查看和监控应用程序—转到 **Activity Insights**（活动洞察） > **Applications**（应用程序）以获取有关您正在使用的应用程序的信息。
- 查看和监控应用程序加速—应用程序加速功能可解决应用程序性能不佳的原因，并实时采取措施加以缓解，从而提升 Prisma Access GlobalProtect 和远程网络用户的体验。转到 **Activity Insights**（活动洞察） > **Applications**（应用程序）以查看有关所有加速应用程序的详细信息。
- 查看移动用户—**All Users**（所有用户）显示了连接到 Palo Alto Networks 安全解决方案（其中包括新一代防火墙 (NGFW) 和 Prisma Access）的所有用户的概览。您可以轻松确定用户与 NGFW 或 Prisma Access 的连接状态，无论是在分支站点、服务连接还是远程位置。转到 **Activity Insights**（活动洞察） > **Insights**（洞察） > **Users**（用户） 以查看有关您的 Prisma Access **Agent Users**（代理用户）、**Agentless Proxy Users**（无客户端代理用户）、**Office Users**（办公室用户） 以及 **Other Users**（其他用户）的信息。
- 查看和监控分支站点—转到 **Monitor**（监控） > **Branch Sites**（分支站点） > **Prisma Access**，以查看您的远程网络的运行状况和连接情况，以及部署在不同 Prisma Access 位置的所有远程网络的使用情况。您将看到实时连接状态和带宽消耗详情以及其他部署详细信息。移动用户、分支机构和零售店连接到远程网络。.您还可以查看远程网络和移动用户中配置的隧道的运行状况。
- 查看和监控数据中心—转到 **Monitor**（监控） > **Data Centers**（数据中心） > **Service Connections**（服务连接），以查看聚合的服务连接数据以及有关各个服务连接的信息。

  转到 **Monitor**（监控） > **Data Centers**（数据中心） > **ZTNA Connectors**（**ZTNA** 连接器），以查看 ZTNA 连接器组以及各个 ZTNA 连接器的运行状况和状态。
- 转到 **Monitor**（监控） > **Data Centers**（数据中心） > **ZTNA Access Objects**（**ZTNA** 访问访问对象），以洞察您的 ZTNA 连接器访问对象的相关情况。
- 查看和监控网络服务—转到 **Monitor**（监控） > **Network Services**（网络服务） > **GlobalProtect Authentication**（**GlobalProtect** 身份验证），以查看影响您访问应用程序的用户体验的常见网络服务的性能。网络服务包括报告 GlobalProtect 身份验证成功和失败的次数，作为衡量移动用户能够连接到 Prisma Access 的指标。转到 **Monitor**（监控） > **Network Services**（网络服务） > **DNS**，以查看在您指定的时间范围内转发到服务器的 DNS 代理请求和响应。

 ©2025 Palo Alto Networks, Inc.

- 查看和监控订阅使用情况—选择 **Monitor**（监控） > **Subscription Usage**（订阅使用情况），以查看有关您的 **Prisma Access Base Subscriptions**（**Prisma Access** 基础订阅）的详细信息，包括到目前为止您已使用的许可证数量。
- 查看和监控 **Prisma Access** 位置）—前往 **Monitor**（监控） > **Prisma Access Locations**（**Prisma Access** 位置），以查看您的远程网络和移动用户的所有 Prisma Access 位置的运行状况概览。您可以选择一个时间范围，以查看该时间段内的 Prisma Access 位置状态和 Strata Logging Service 连接情况，查看列出所有 Prisma Access 位置的表格，并可按名称选择单个 Prisma Access 位置以查看其详细信息。
- 查看 **Prisma Access** 升级情况—选择 **Workflows**（工作流） > **Software Upgrades**（软件升级） > **Prisma Access**（**Prisma Access**），以查看有关 Prisma Access 升级过程的信息。
- 查看和监控第三方设备 **ID**—转到 **Monitor**（监控） > **Devices**（设备） > **IoT**（物联网），以深入了解您的物联网设备，例如在过去 30 分钟内连接的物联网设备数量、在所选时间范围内连接的所有物联网设备，以及所有已连接物联网设备的详细信息。
- 查看和监控远程浏览器隔离—选择 **Monitor**（监控） > **Users**（用户），通过查看诸如活跃的 RBI 用户数量、趋势、连接状态、RBI 位置状态、流量测量数据和许可证使用情况等指标，可以深入了解您的 RBI 部署情况。

在 Strata Cloud Manager 中使用 Prisma Access Monitoring 入门

哪里可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证 ❑ 这是 Prisma Access Insights 提供的一项功能。

使用 Prisma Access，您可以在 Strata Cloud Manager Command Center 中持续监视 Prisma Access 环境。多个指示板为您提供不同部署、警报和 Prisma Access 基础设施的专注视图。当事件或状态需要您注意时，Prisma Access 会向您发送警报通知，以便您快速定位可以解决的问题。还可以让您了解 Prisma Access 团队正在进行的修复。使用 Autonomous DEM 许可证，您可以通过选择或设置时间范围来筛选您想要查看的数据，并可在“Monitor（监控）”页面中查看基准信息。

时间范围选择筛选器

Time Range（时间范围）选择筛选器出现在您希望按时间范围筛选信息的指示板顶部。

时间已进行本地化设置，因此您能够依据所在地区的当地时间执行筛选操作。数据每分钟获取一次，但大多数直方图中显示的数据点会根据所选的 **Time Range**（时间范围）而有所不同。

为了方便您操作，Prisma Access 允许您从几个预定义的时间范围中选择时间范围，您可以自行配置日期和时间范围：

- 最近 **15** 分钟

  每 3 分钟 1 个数据点，总共 5 个数据点。
- 过去 **1** 小时

  每 3 分钟 1 个数据点，总共 20 个数据点。

 ©2025 Palo Alto Networks, Inc.

- 过去 **3** 小时

  每 3 分钟 1 个数据点，总共 60 个数据点。
- 过去 **24** 小时

  每 5 分钟 1 个数据点，总共 288 个数据点。
- 过去 **7** 天

  每 30 分钟 1 个数据点，总共 336 个数据点。
- 过去 **30** 天

  每 3 小时 1 个数据点，总共 180 个数据点。
- 自定义

  除了筛选器中可用的预填充时间范围选项外，还可以设置自定义时间间隔（例如，日期和时间示例从 6 月 1 日下午 5:00 开始，到 6 月 2 日下午 4:00 结束）。

  要设置开始时间，首先在日历中选择日期，然后在 **Start**（开始）下选择时间。选择 **Apply**（应用）以应用开始时间，然后设置结束时间，方法是在日历中选择结束日期，在 **End**（结束）下面选择时间。

  设置了自定义时间范围后，该范围将被保存并应用于“Insights（洞察）”中的所有小部件。这些小部件会使用该时间范围过滤器来显示数据，而非实时数据。

  可以从预先填充的 **Time Range**（时间范围）选项中选择自定义时间间隔：

  - 最近 **15** 分钟

    每 3 分钟 1 个数据点，总共 5 个数据点。
  - 过去 **1** 小时

    每 3 分钟 1 个数据点，总共 20 个数据点。
  - 过去 **3** 小时

    每 3 分钟 1 个数据点，总共 60 个数据点。
  - 过去 **24** 小时

    每 5 分钟 1 个数据点，总共 288 个数据点。
  - 最近 **48** 小时

    每 30 分钟 1 个数据点，总共 96 个数据点。
  - 过去 **7** 天

    每 30 分钟 1 个数据点，总共 336 个数据点。
  - 过去 **30** 天

    每 3 小时钟 1 个数据点，总共 240 个数据点。

小部件中的基线

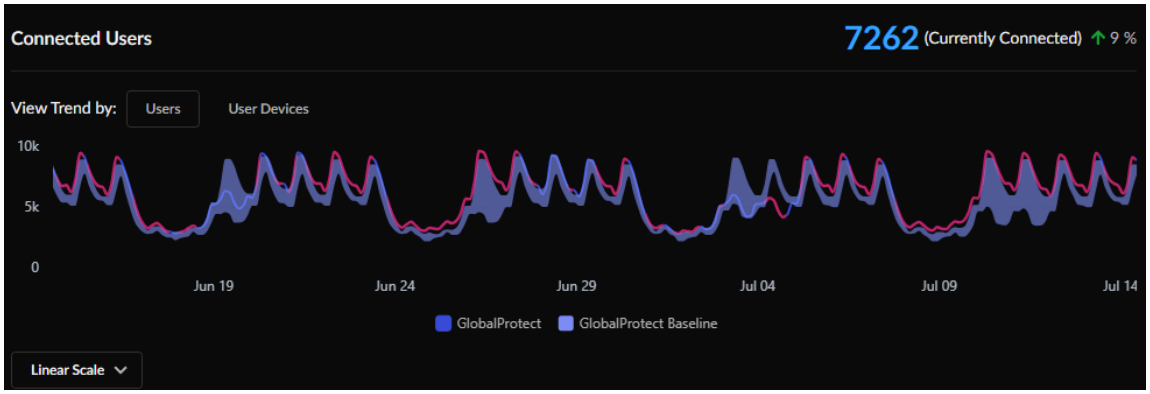
如果您购买了 AI-Powered ADEM 许可证，您将在以下监视页面的趋势小部件上看到基线数据带：用户、分支机构、数据中心和网络服务。这些小部件会在趋势线背后，以背景形式呈现基线。您可以一目了然地查看您的数据是否超出了基线的上限或下限。

 ©2025 Palo Alto Networks, Inc.

基线数据以 1 小时区间进行计算，并且会考虑特定隧道、站点、Prisma Access 位置或 GlobalProtect 用户数量在过去 28 天内 1 小时区间的数据情况。例如，从星期二下午 1:00 到下午 2:00 的基线是根据前四个星期二下午 1:00 到下午 2:00 的时间范围计算的。下限是收集的历史数据的第 10 个百分位数，上限是其第 90 个百分位数。这使您能够查看带宽、用户数量、身份验证数量以及 DNS 代理请求和响应的趋势。由于基线数据取自过去 28 天的历史数据，因此新接入的租户需要运行并积累丰富数据达 28 天，才能正确计算出基线。如果您的数据少于 28 天，您可能会看到一些差异。

如果小部件中的趋势线值偏离基线的上限或下限，该期间的趋势线在网页界面中以红色显示。

以下示例显示了“Users（用户）”页面上 **Connected User**（连接用户）小部件的 GlobalProtect 基线。



查看和监控应用程序

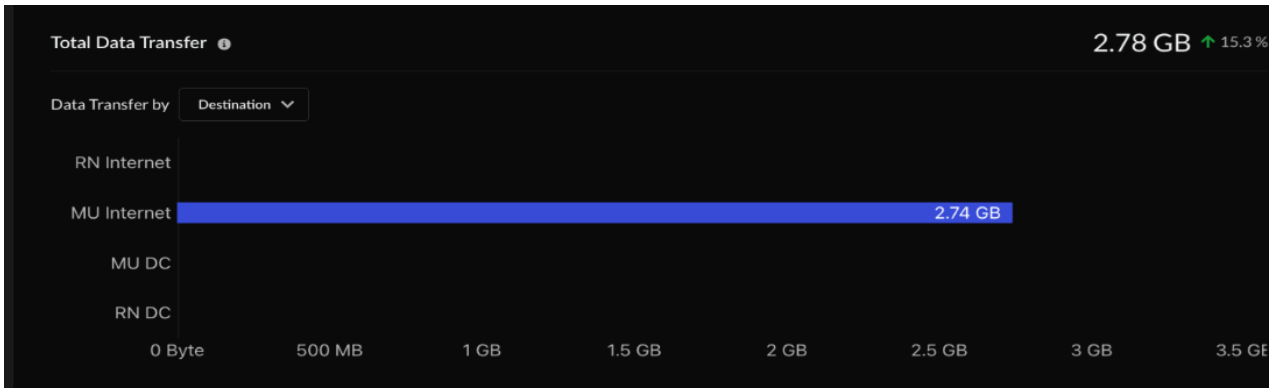
哪里可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证 ❑ 这是一个 Prisma Access Insights 功能。

使用 Strata Cloud Manager Command Center 监控您网络中的 Prisma Access 应用程序、使用该应用程序的用户及其潜在的安全影响。 > 前往 Insights Applications 以获取 Prisma Access 应用程序的可见性，以及有关威胁、用户、数据传输、风险评分和应用程序用户体验的信息。

总数据传输

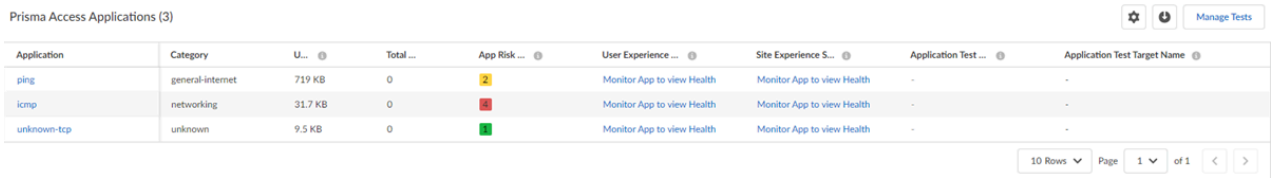
总数据传输显示您在所选时间范围内通过 Prisma Access 防火墙的总数据传输。使用添加过滤器下拉菜单进行其他过滤选项。在这个例子中，您可以看到按应用类别的数据传输，这显示了最热门的应用程序及其总数据传输量。您还可以按目的地查看总传输数据。

©2025 Palo Alto Networks, Inc.



Prisma Access 应用程序

使用此小部件查看正在监控的应用程序，以及在其上运行的合成测试。该表还显示了它们的体验分数，这些分数可以让您了解每个应用程序的运行状况。单击 **Manage Tests**（管理测试）按钮，在“应用程序测试”表中查看为所有应用程序设置的所有综合测试。



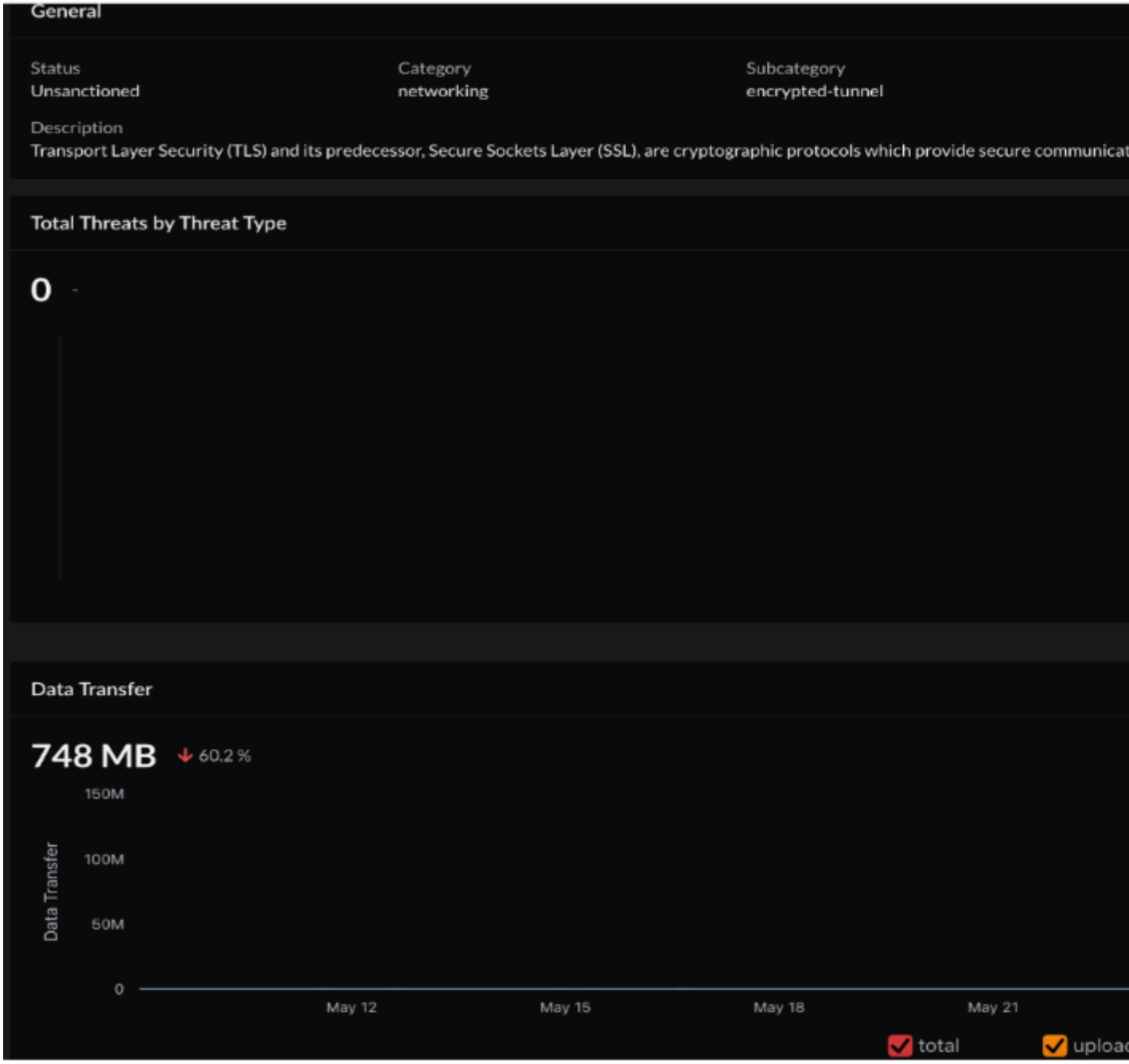
列	说明
应用程序	被监控应用程序的应用 ID。
类别	应用程序类型。
使用情况	检测到特定应用程序的 Prisma Access 基础设施中的总流量。
威胁总数	应用程序经历的威胁总数。
应用程序风险评分	此特定应用程序的威胁数据。1是最低风险，5是最高风险。
用户体验	应用体验分数收集自 Autonomous DEM。它是针对所有监控此应用程序的用户进行汇总的。
站点体验分数	此特定分支网站的应用体验评分。
应用程序测试名称	用户为此应用程序设置的测试集名称。
应用程序测试目标名称	从各个端点针对合成测试的FQDN的IP地址。

©2025 Palo Alto Networks, Inc.

应用程序详情

选择任何应用程序以查看其一般详细信息，例如状态、类别、子类别、端口、技术和风险评分。

- 当前应用程序的总威胁按威胁类型分类。
- 总用户数 — 在指定时间范围内访问此应用程序的用户总数。
- 数据传输—查看为此应用程序上传或下载的数据。



 ©2025 Palo Alto Networks, Inc.

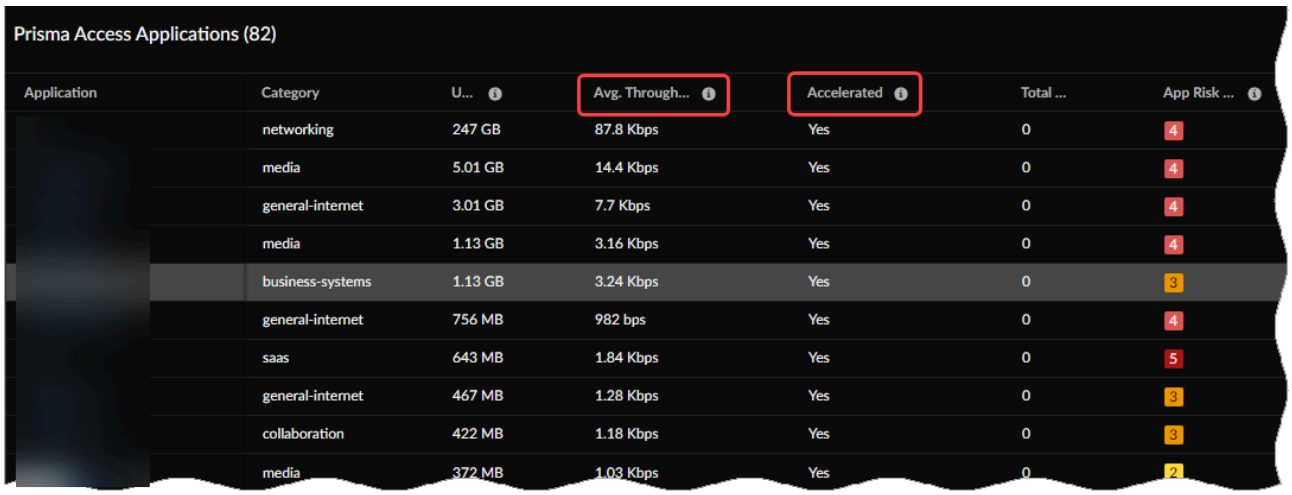
查看和监控应用加速

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证

App Acceleration解决了应用程序性能低下的原因，并实时采取措施缓解这些问题，从而改善Prisma Access GlobalProtect和远程网络用户的用户体验。

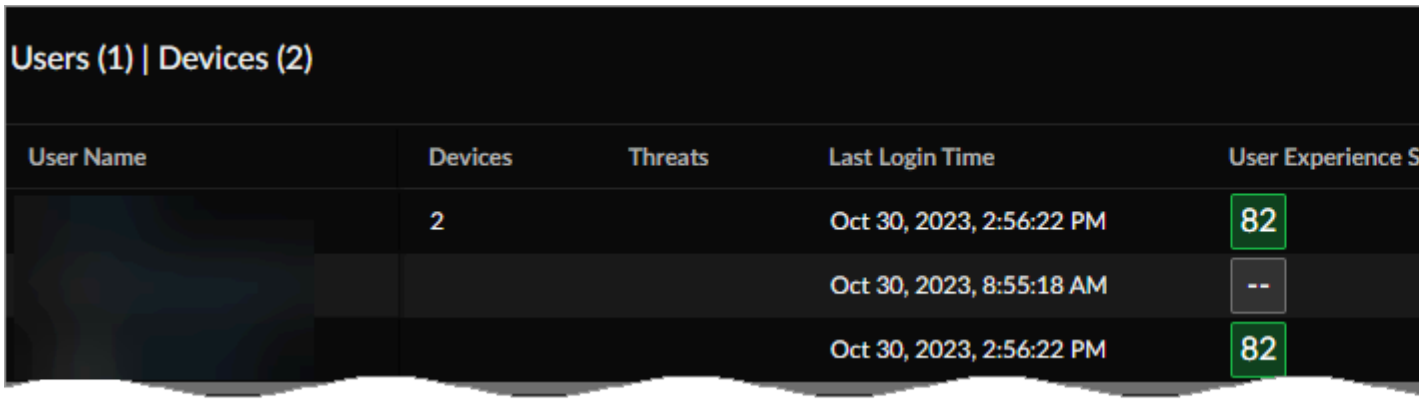
当您的用户访问应用程序时，他们可能会遇到由于吞吐量下降而导致的应用程序性能下降，这可能是由无线连接降级、网络拥塞和其他因素造成的。这些网络问题可能会对员工体验产生不利影响，并降低他们的生产力。App Acceleration能够安全地了解设备功能、网络功能和应用环境，以最大限度地提高吞吐量，并实时调整以应对不断变化的网络条件。

在Strata Cloud Manager命令中心中，转至Insights Applications以查看有关在您的环境中已加速的应用程序的详细信息。 > Prisma Access 应用程序表包括平均（平均）整个列，只有当您的用户流量加速时才能看到;加速列，显示您的部分或全部应用程序流量已加速。



> 转到洞察用户以查看有关您环境中的App Acceleration用户的信息。在环境中启用了应用加速的用户具有|“设备”表，该表显示“流量加速”列。此列表示部分或全部用户的应用程序流量已加速。

©2025 Palo Alto Networks, Inc.



AI驱动的Autonomous DEM（ADEM）与App Acceleration集成，并为您提供加速的应用程序数量和整体性能提升等指标。转到SASE Health Experience，在加速应用程序和并行应用程序选项卡中查看ADEM性能指标。 >

查看移动用户

在何处可以使用？	需要提供什么？
• Prisma Access（由 Strata Cloud Manager 管理）	• Prisma Access 许可证 • AI 驱动的 ADEM 许可证

Activity Insights：用户，您可以查看所有连接到 Palo Alto Networks 的 Prisma Access 安全解决方案的用户和主机的概览。您可以轻松确定用户或主机与 Prisma Access 的连接状态，无论是在分支站点、服务连接还是远程位置。查看

- 当前连接到 Palo Alto Networks 安全解决方案的独特用户总数以及连接到 Prisma Access 的用户总数。
- 在某个时间范围内连接的用户数量，按通过 Prisma Access 连接的用户进行细分。
- 通过 Prisma Access 连接的基于代理的用户。
- 连接到 Prisma Access 的基于代理或基于浏览器的显式代理用户。
- 通过 Prisma Access 浏览器连接的用户。
- 访问 Prisma Access 的未管理设备用户的列表。
- 从分支机构位置连接到 Prisma Access 的用户列表。
- 通过特定的服务连接连接数据中心的用户列表。

查看和监视移动用户的 IPv6

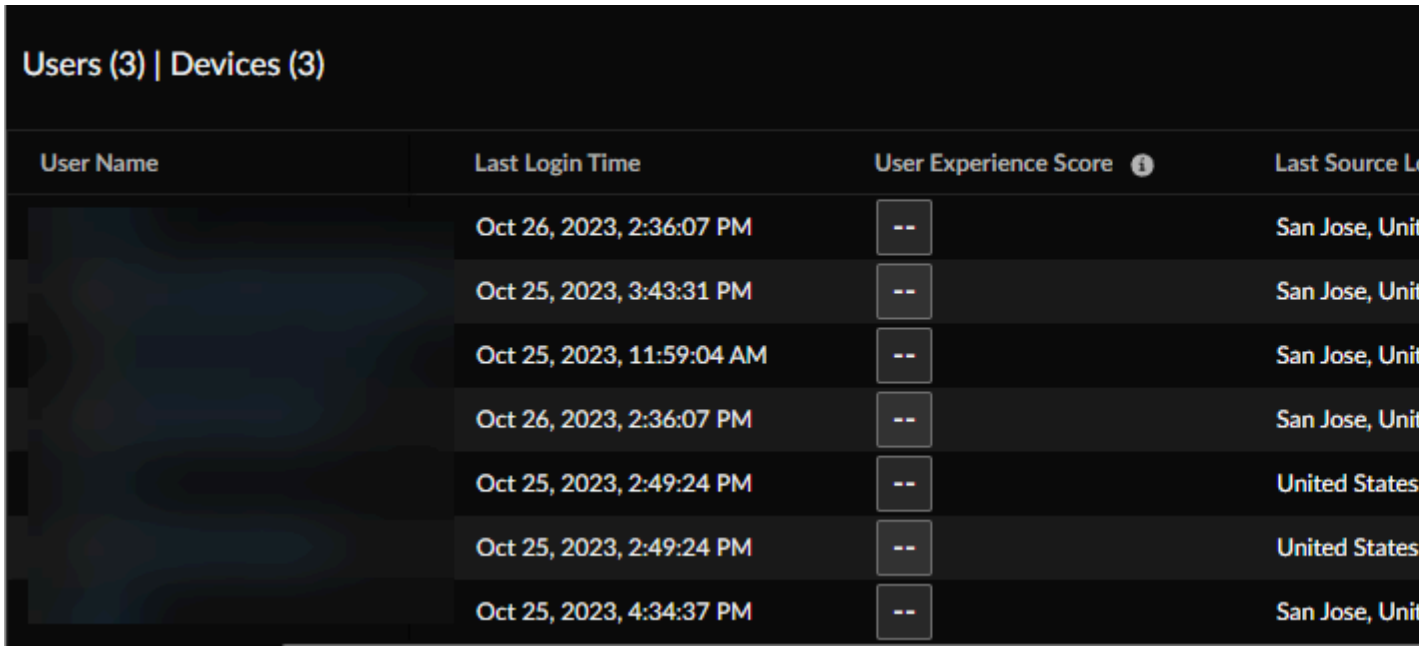
在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.0 创新 ❑ Prisma Access 许可证

 ©2025 Palo Alto Networks, Inc.

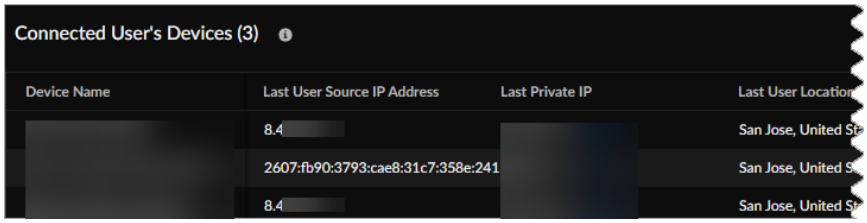
在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	

如果在 用户 - GlobalProtect 部署中使用 IPv6 网络，您可以将 Prisma Access 配置为在移动用户网络中使用 IPv6 地址。您还需要在 Prisma Access 基础架构中启用 IPv6 网络，然后才能使用 IPv6 寻址。

对于 GlobalProtect 部署中的 IPv6，用户 | 设备表在“源 IP 地址”列中显示 IPv4 或 IPv6 地址。

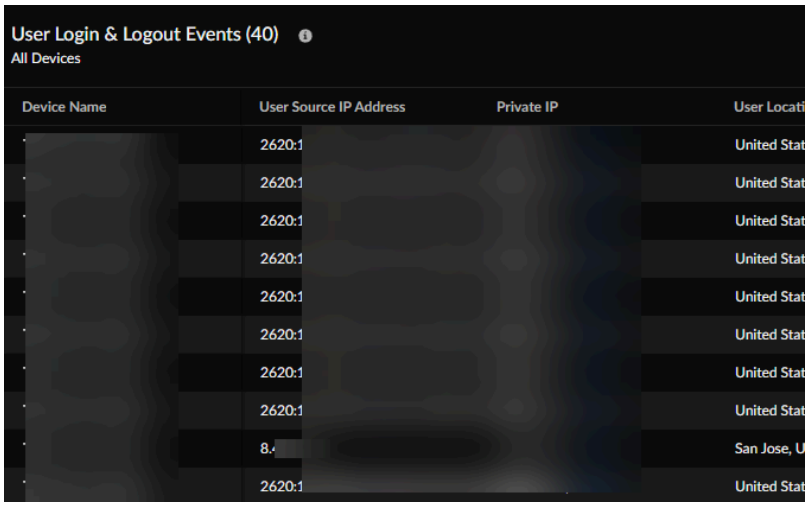


选择任何已连接的用户来查看有关其设备趋势的信息。“已连接用户的设备”表显示有关用户设备的数据，包括“最后一个用户源 IP 地址”和“最后一个专用 IP”，两者都可以包含单个设备条目的 IPv4 和 IPv6 地址。



您可以在用户登录和注销事件表中查看 IPv6 地址信息。“用户源 IP 地址”和“专用 IP 地址”列显示 IPv4 或 IPv6 地址。

©2025 Palo Alto Networks, Inc.

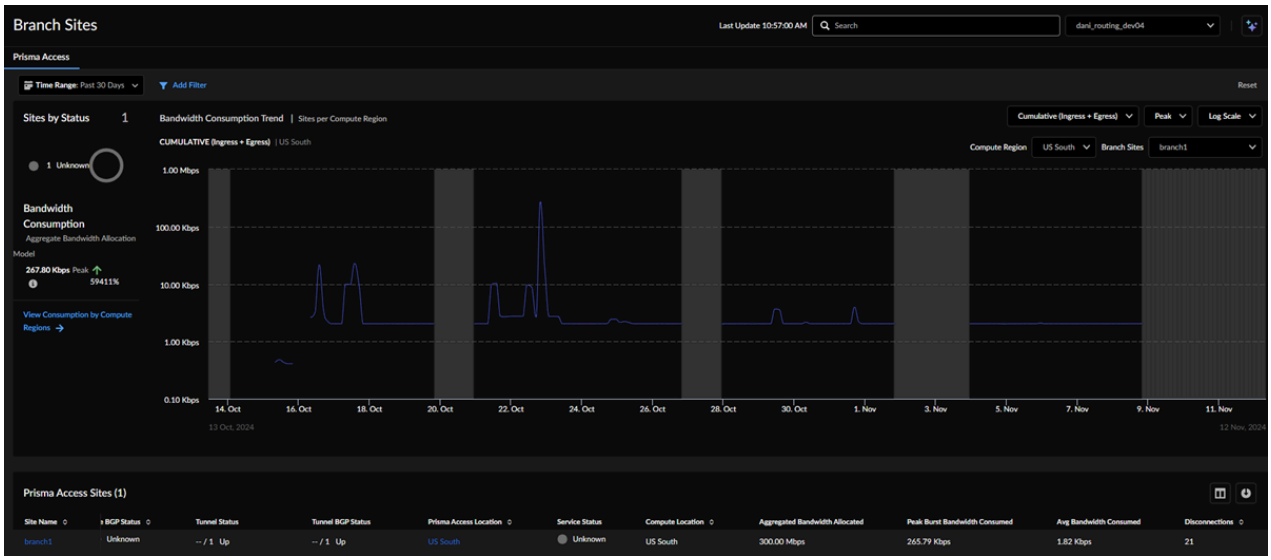


查看和监控分支站点

哪里可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证 ❑ adem-aiops-value

选择 **Monitor**（监控） > **Branch Sites**（分支站点） > **Prisma Access**，看远程网络的运行状况和连接情况，以及部署在 Prisma Access 位置的所有远程网络的使用情况。它向您显示实时连接状态和带宽消耗详情以及其他部署详细信息。您还可以查看在远程网络中配置的隧道的运行状况。

查看 Prisma Access 远程网络以获取有关如何规划远程网络、分配远程网络带宽和入驻远程网络的信息。 > > 要查看您的分支站点，请转到监视分支站点 Prisma Access。



 ©2025 Palo Alto Networks, Inc.

按状态划分的网站

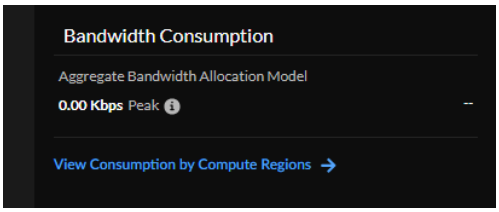
Sites by Status（按状态）查看远程网络站点。您可以查看在选定时间范围内有多少网站处于正常、关闭、非活动或不可用状态，以及有多少网站发出警告。



带宽消耗

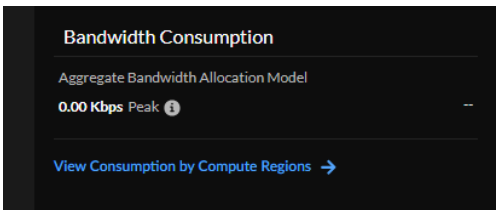
带宽消耗显示在所有租户的计算区域中，聚合带宽分配模型下，计算区域消耗的最高峰带宽。一个站点在所有站点中消耗的最高峰带宽显示在每个站点的带宽分配模型中。所选时间过滤持续时间的峰值被计算出来。

选择按计算区域查看消费，以查看所有计算区域及其配置的IPSec终止节点的消费值和趋势图。



按计算区域查看消耗量

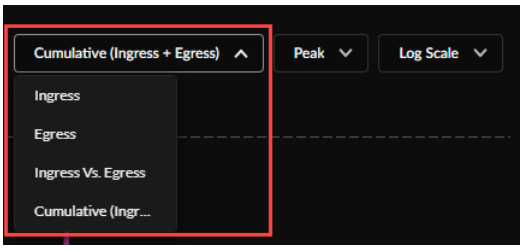
导航到 **Monitor**（监视） > **Branch Sites**（分支站点） > **Prisma Access**。在使用聚合带宽分配模型时，在带宽消耗小部件中选择按计算区域查看消耗，以查看您区域的带宽消耗和趋势。



计算区域页面显示您选择的时间范围内的带宽消耗数据。您可以查看一张表，其中包含您计算区域的平均带宽、中位带宽和峰值带宽。

带宽消耗趋势按计算区域图表显示有关您的计算区域的数据。筛选数据以提炼您想要查看的信息。

- 从下拉菜单中选择 **Cumulative (Ingress + Egress)**（累计（传入 + 传出））、**Ingress**（传入）、**Egress**（传出）或 **Ingress vs.Egress**（传入与传出）。



©2025 Palo Alto Networks, Inc.

- 查看所选时间范围内的峰值、中位数或平均带宽消耗趋势。默认设置为 **Peak**（峰值）带宽消耗。



- 对数刻度或线性刻度。
- 计算区域—选择一个或多个区域以查看。

IPSec终止节点利用率图表允许您查看在特定计算区域配置的IPSec终止节点的带宽消耗。筛选数据以提炼您想要查看的信息：

- 选择您要查看数据的计算区域。
- 选择您想要查看的计算区域的特定站点。
- 选择节点聚合或按站点细分，以查看在所选IPSec终止节点终止的站点的带宽消耗趋势。
- 查看峰值、平均值或中位数。

©2025 Palo Alto Networks, Inc.

- 查看 **Log Scale**（对数刻度）或 **Linear Scale**（线性刻度）。



带宽消耗趋势

在主分支站点页面，您可以查看在使用聚合带宽分配模型时，按计算区域划分的带宽消耗趋势站点，或在使用每站点带宽分配模型时，按分支站点划分的带宽消耗趋势。对于聚合带宽分配模型，您可以选择一个计算区域，然后选择该计算区域中带宽消耗趋势引起您兴趣的网站。过滤数据以提炼您想要查看的信息，您可以将鼠标悬停在图表上以查看当时网站的带宽消耗。

- 默认视图显示累积（流入 + 流出）带宽消耗。其他选项包括 **Ingress**（传入）、**Egress**（传出）或 **Ingress vs.Egress**（传入与传出）。
- 查看所选时间范围内的峰值、中位数或平均带宽消耗趋势。默认设置为 **Peak**（峰值）带宽消耗。
- 对数刻度或线性刻度。
- 计算区域—查看计算区域及其终止在该区域的站点的细分，当租户使用聚合带宽分配模型时。对于每个计算区域，选择在计算区域内终止的网站，以查看它们的带宽消耗趋势。

分支站点—选择至少 1 个站点和最多 10 个站点，以查看它们在所选时间范围内的趋势线。

©2025 Palo Alto Networks, Inc.



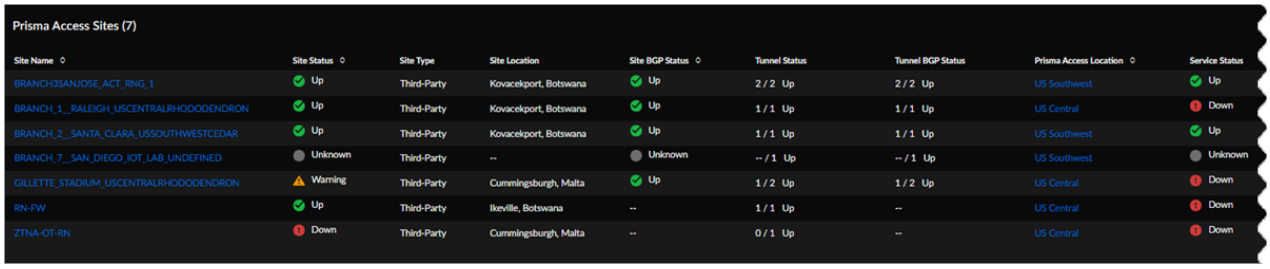
Prisma Access 站点

Prisma Access 站点表列除您的远程 Prisma Access 站点和信息。

- 站点名称—Prisma Access 站点的唯一名称。
- 网站状态—正常、故障、警告或未知。
- 站点类型—第三方。
- 站点位置—Prisma Access 站点位置。
- 站点BGP状态 — 站点BGP状态是正常、故障还是未知。
- 隧道状态—网站隧道的数量以及这些隧道中有多少处正常运行。
- 隧道 BGP 状态—每个隧道的 BGP 状态。
- Prisma Access 位置—此 Prisma Access 站点的位置。选择一个位置以查看其 Prisma Access 位置的详细信息。
- 服务状态—此字段指示与站点连接的实例或防火墙的状态。状态可以是上升、下降或未知。
- 计算位置—所有 Prisma Access 位置都根据优化的性能和延迟映射到安全处理计算位置或区域。至少两个（通常是多个）地理位置彼此靠近的 Prisma Access 地点被分组为单个计算地点。

©2025 Palo Alto Networks, Inc.

- 分配的聚合带宽 — 在所选时间范围内为该站点分配的聚合带宽。此列仅在您使用聚合带宽模型时出现。
- 峰值突发带宽消耗 — 在所选时间范围内，通过结合该站点的入口和传出值获得的累积峰值。
- 平均带宽消耗 — 在选定时间范围内，通过结合该站点的入口和传出值获得的累积平均值。
- 断开连接 — 在选定的时间范围内，该站点发生了多少次断开连接。
- 断开连接持续时间 — 在所选时间范围内，网站断开连接的总时间（以秒为单位）。



高性能分支站点可见性

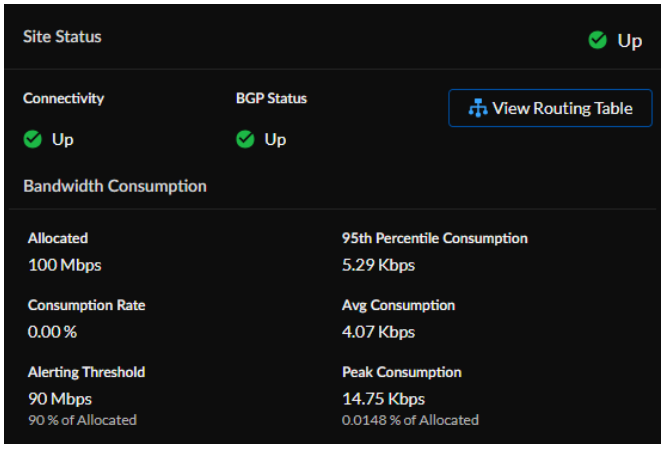
高性能分支（RN-HP）具有与传统分支不同的属性，二者将在您的租户中共存。Prisma Access中的高性能分支站点具有以下优点：

- 该架构通过将网络处理功能与安全处理功能分开来解决容量效率问题。一款具有大数据包处理能力的ION设备终止多个分支连接，容量高达5Gbps，并将安全处理分配给SPN。
- 您可以使用单个 IP 或 FQDN 将区域中的多个分支终止到单个网络处理节点 (NPN)。
- 您不再需要监控和管理分支站点到IPSec终止节点的终止。适合的SPN进行分支流量检查，而NPN执行负载均衡。
- 通过能够为冗余指定不同的区域，您可以实现真正的高可用性。

您可以在您的环境中查看高性能和遗留分支。 > > 在 Strata Cloud Manager 中，转到监控分支站点 Prisma Access，然后从 Prisma Access 站点表中选择一个分支站点。

Prisma Access 站点详情

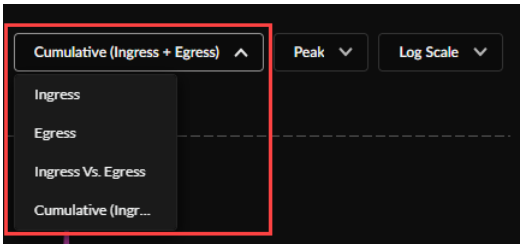
选择任何 Prisma Access 站点名称以查看其站点状态，在这里您可以查看其连接性和 BGP 状态（正常、关闭、非活动或不可用）。查看所选时间间隔的带宽 **Peak Consumption**（峰值消耗）。



您可以在带宽消耗趋势图中查看累积（流入 + 流出）信息。

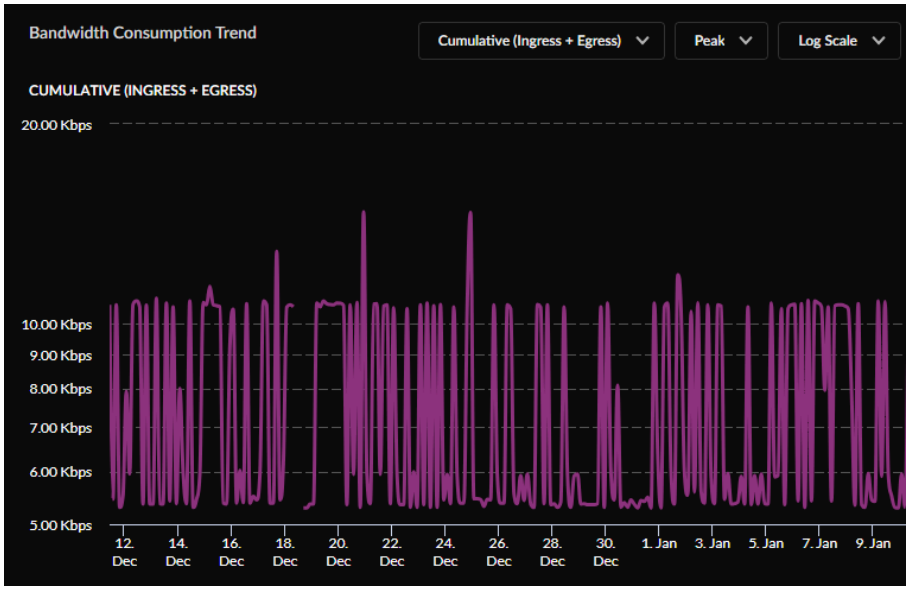
 ©2025 Palo Alto Networks, Inc.

- 使用下拉菜单查看按入口、传出、入口对比的带宽消耗图表。**Egress**（传入与传出）或累积（传入 + 传出）查看带宽消耗图表。



- 按 **Peak**（峰值）（默认值）、**Average**（平均值）或 **Median**（中值）查看分支站点的带宽消耗趋势图表指标。





路由表可见性

为了帮助您解决可达性挑战，我们提供对每个远程网络站点路由表的可见性。您可以对目标 IP 地址执行路由表搜索，以确定是否有可用的路由到达所需的目的地。通过这些信息，您可以调查其他潜在的故障原因。这项知识使您能够将精力集中在解决可能影响可达性的问题上。

选择查看路由表以查看该分支的路由表，其中包含来自Prisma Access的可用目的地的IP路由。

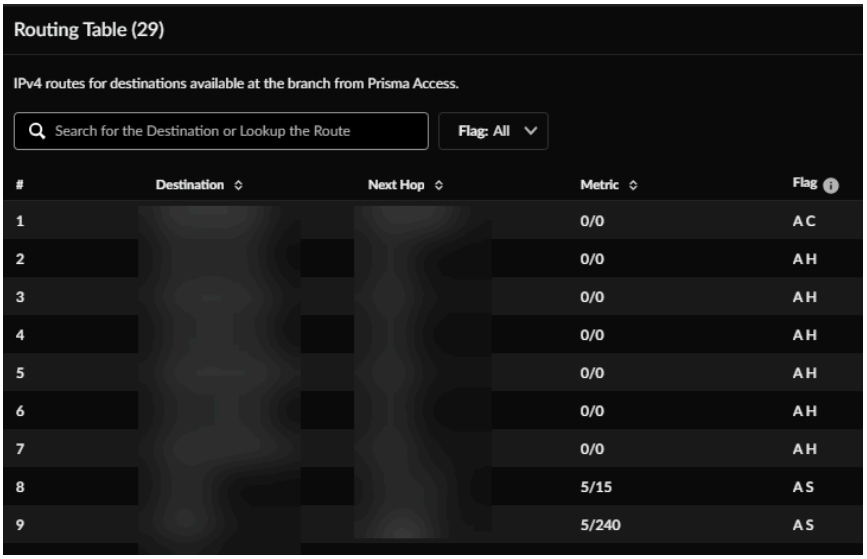
- 使用搜索栏选择目的地或查找路线。
- 使用下拉菜单按标志进行过滤。

路由表显示：

- **#** — 路由编号。
- 目标—可达网络的IP地址和子网。

 ©2025 Palo Alto Networks, Inc.

- **Next Hop**（下一个跃点）— 连接至目标网络的下一个跃点上的网关的 IP 地址。如果下一个跃点为 0.0.0.0，即表示默认路由。
- 度量—由路由协议确定的路由的度量。
- 标志—此路线的信息如下：
- • **A B** — 活动状态，并且从 BGP 获得。
  - A C—活跃并连接。目标 — 网络。
  - A H—活跃并已连接。目标 — 仅主机。
  - **A R** — 活动，并且从 RIP 获得。
  - **O1** — OSPF 外部 type-1。
  - **O2** — OSPF 外部 type-2。
  - **Oi**—OSPF 服务区间。
  - **Oo** — OSPF 服务区间。
  - **S** — 非活动和静态。
  - **A S** — 活动和静态。



隧道

查看此站点的隧道和隧道数据。

- 隧道名称 — 隧道的唯一名称。
- **Prisma Access** 位置—此远程网络的 **Prisma Access** 位置。
- 隧道状态—正常、关闭、初始化或不可用。
- 隧道BGP状态—正常、关闭或未知。
- 隧道监控—如果您已启用隧道监控，则此列显示其状态是正常还是故障。如果您尚未启用它，则此列显示未配置。
- 平均吞吐量 — 在选定时间范围内，考虑到入口、传出、入口与传出的平均带宽。您选择的传出或累积（入口 + 传出）值。

 ©2025 Palo Alto Networks, Inc.

- 峰值吞吐量—在选定时间范围内，考虑到入口、传出、入口与传出的隧道的峰值带宽。Egress（传入与传出）或累积（传入 + 传出）查看带宽消耗图表。
- 源 IP 地址—源 IP 地址。
- 目的地端点地址—用于 Prisma Access 确定隧道是否正常的 IP 或 FQDN 地址。
- 断开连接—在选定时间范围内的断开连接次数。
- 断开连接持续时间 — 在选定时间范围内，隧道断开连接的时间（以秒为单位）。

选择一个隧道名称以查看其隧道状态、带宽消耗趋势和其他隧道详细信息。

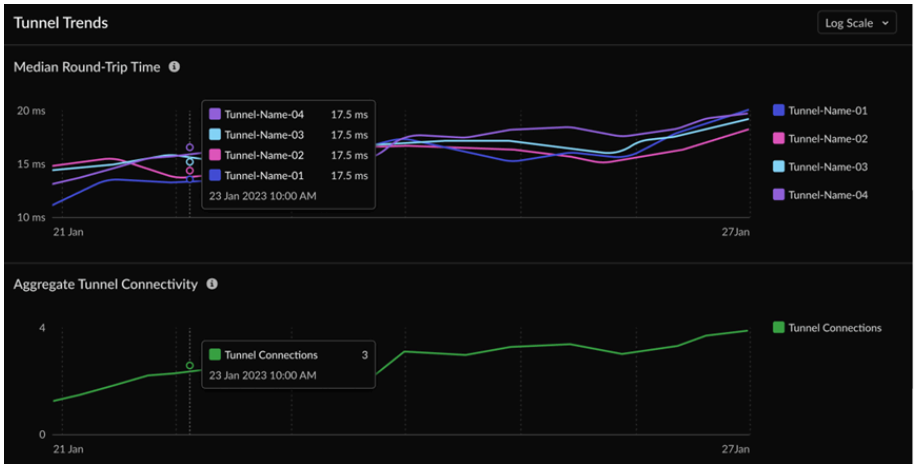


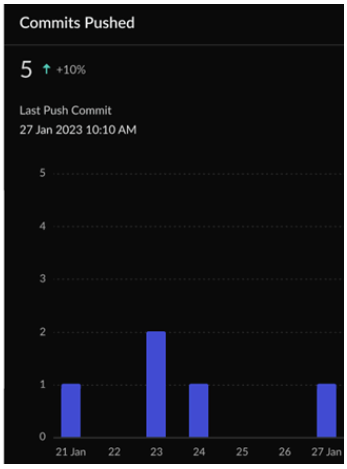
隧道趋势

启用隧道监控后，您可以选择多个隧道并查看它们的中位往返时间。如果您不指定一组隧道，默认情况下，将为观察到的 RTT 最高的 10 个隧道计算中位数 RTT。

聚合隧道连接性显示所选时间范围内连接隧道的总数。将鼠标悬停在任一图表上以查看特定时间的连接数量。

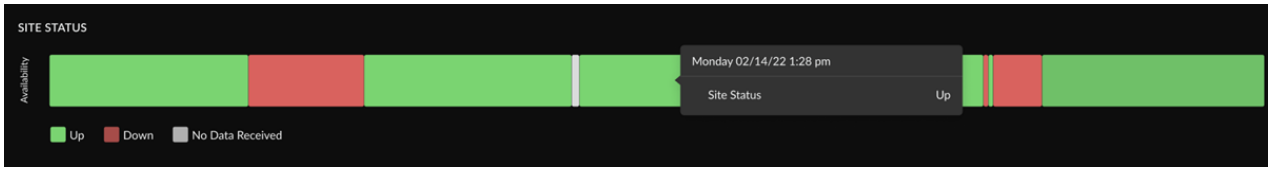
提交推送显示在选定的时间范围内推送了多少次提交，以及最后一次推送提交发生的时间。





站点状态

网站状态显示在所选时间范围内的网站可用性。绿色表示该网站在此期间正常运行，红色表示该网站宕机，灰色表示在显示的时间内没有可用数据。



©2025 Palo Alto Networks, Inc.

查看和监视数据中心

哪里可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

服务连接

服务连接（也称为企业访问节点（简称 CAN））允许移动用户和远程网络用户访问专用应用程序和资源，并允许移动用户和远程网络相互通信。Palo Alto Networks 建议在您的 Prisma Access 部署中始终创建服务连接。所有服务连接都允许访问您总部或数据中心的资源，并允许远程网络和移动用户相互通信。

您收到的服务连接数量取决于您的 Prisma Access 许可证。有关服务连接及其配置的详细信息，请参阅 Prisma Access 服务连接。

在 Strata Cloud Manager 中，选择 **Monitor**（监视） > **Data Centers**（数据中心） > **Service Connections**（服务连接），以便查看您的服务连接。

ZTNA 连接器

零信任网络访问 (ZTNA) 连接器允许您将 Prisma Access 连接到您组织的私有应用程序。ZTNA 连接器为移动用户和分支机构位置的用户提供通过自动安全隧道访问您的私有应用程序的能力。ZTNA 连接器自动设置隧道，因此您无需手动设置 IPSec 隧道和路由到数据中心或总部位置、公共云位置以及您的私有应用程序所在的合作伙伴网络。

在 Strata Cloud Manager 中，选择 **Monitor**（监视） > **Data Centers**（数据中心） > **ZTNA Connectors**（**ZTNA** 连接器），以便查看您的 ZTNA 连接器。

查看和监视服务连接

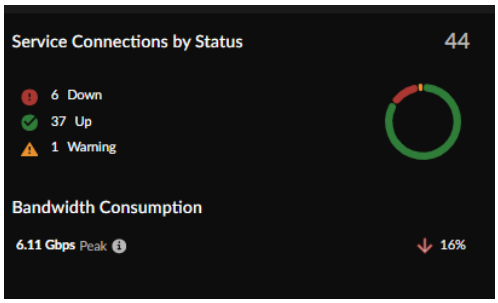
哪里可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

查看聚合的服务连接数据以及有关单个服务连接的信息。服务连接可实现移动用户和远程网络。除了提供对公司资源的访问，服务连接还允许您的移动用户到达分支机构。您可以在 Strata Cloud Manager 中查看您的服务连接，以查看服务连接状态、带宽消耗趋势、隧道数据和趋势以及有关整体服务连接健康状况的信息。要开始，请选择 **Monitor**（监控） > **Data Centers**（数据中心） > **Service Connections**（服务连接）。

按状态划分的服务连接

您可以查看所有服务连接的运行状况。颜色编码的图表显示了处于开启、关闭或需要注意的服务连接的分布情况。您可以查看过去 30 天内服务连接消耗的带宽概要。

©2025 Palo Alto Networks, Inc.



带宽消耗显示每个站点带宽分配模型中某个站点在所有站点中消耗的最高峰值带宽。所选时间过滤持续时间的峰值被计算出来。

带宽消耗趋势

查看每个服务连接的带宽消耗趋势。趋势显示每个服务连接的带宽消耗以及它们的平均和峰值利用率。

- 默认视图显示 累计（传入 + 传出）带宽消耗。其他选项包括 **Ingress**（传入）、**Egress**（传出）或 **Ingress vs.Egress**（传出）。
- 查看所选时间范围内的峰值、中位数或平均带宽消耗趋势。默认设置为峰值带宽消耗。
- 对数刻度或线性刻度。
- 选择 1 到 10 个服务连接以在选定时间范围内在图表上查看它们的趋势线。将鼠标悬停在图表上即可查看有关您选择的每个服务连接的信息。



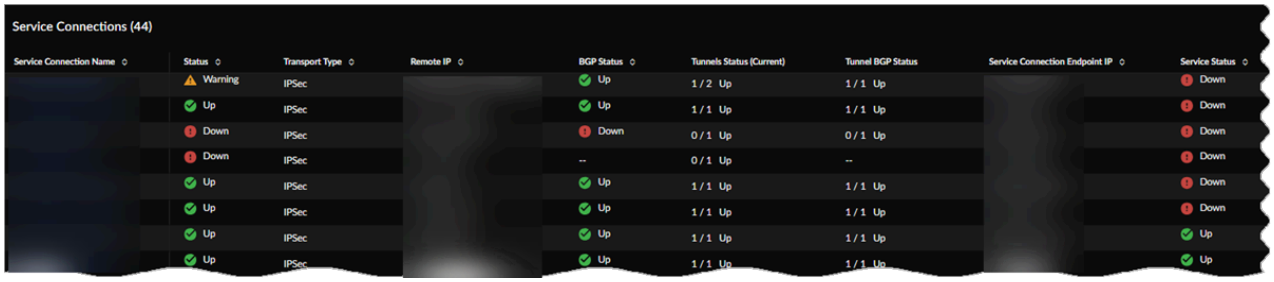
服务连接表

Service Connections（服务连接）表显示有关服务连接的数据，例如状态、远程 IP 地址、BGP 状态、当前隧道状态和其他数据。选择服务连接名称以获取有关该服务连接的详细信息。

- 服务连接名称 — 服务连接的唯一名称。
- 状态 — 启动、关闭、警告或未知。
- 传输类型 — IPSec。
- 远程 **IP** — 远程 IP 地址。
- **BGP** 状态 — 站点 BGP 状态是 **Up**（启动）、**Down**（关闭）或 **Unknown**（未知）。
- 隧道状态（当前） — 站点的隧道数量以及其中有多少隧道已启动。

 ©2025 Palo Alto Networks, Inc.

- 隧道 BGP 状态—每个隧道的 BGP 状态。
- 服务连接端点 **IP** — 服务连接的端点 IP 地址。
- 服务状态—此字段指示与站点连接的实例或防火墙的状态。状态可以是上升、下降或未知。
- **Prisma Access** 位置 — 服务连接的 Prisma Access 位置。
- 平均带宽消耗 — 平均带宽消耗 (Kbps)。
- 峰值带宽消耗 — 峰值带宽消耗 (Kbps)。

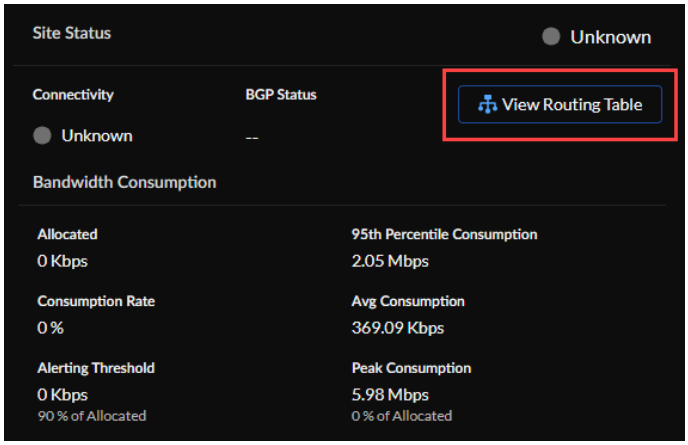


服务连接详细信息

选择要查看详细信息的任何 **Service Connection Name**（服务连接名称）。查看服务连接状态、过去 30 天内消耗的带宽。带宽消耗趋势图显示选定时间范围内每个服务连接的带宽消耗情况。

站点状态

选择任何服务连接名称以查看其 站点状态，您可以在其中看到其连接性和**BGP** 状态（启动、关闭、不活动或不可用）。查看所选时间间隔的带宽 **Peak Consumption**（峰值消耗）。



路由表可见性

为了帮助您解决可达性挑战，我们在每个服务连接处提供路由表的可见性。您可以对目标 IP 地址执行路由表搜索，以确定是否有可用的路由到达所需的目的地。有了这些信息，您可以从 Prisma Access 基础设施获得指导，以调查其他潜在的故障原因。这些知识使您能够集中精力解决任何影响可达性的问题。

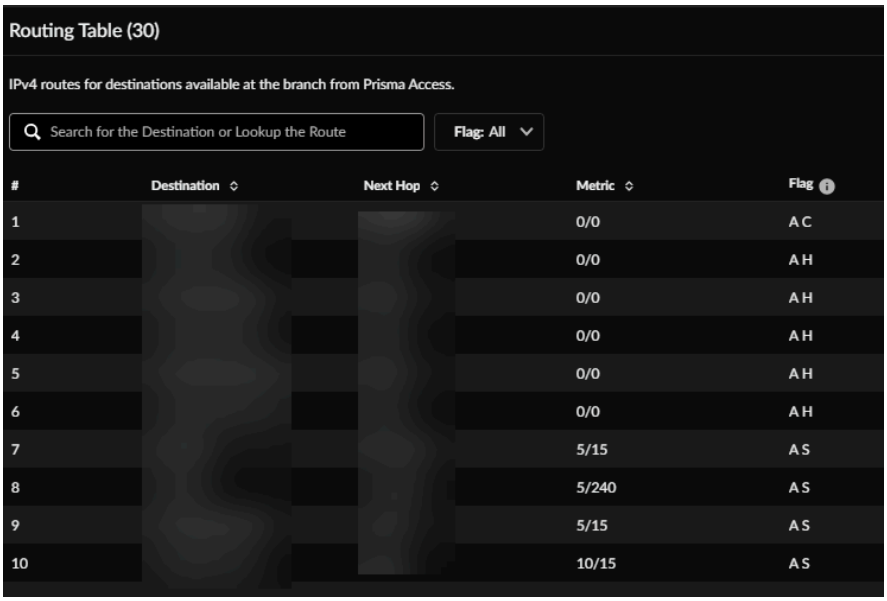
选择查看路由表以查看该分支的路由表，其中包含来自Prisma Access的可用目的地的IP路由。

- 使用搜索栏选择目的地或查找路线。
- 使用下拉菜单按标志进行过滤。

路由表显示：

 ©2025 Palo Alto Networks, Inc.

- **#** — 路由编号
- 目标 — 可达网络的 IP 地址和子网。
- **Next Hop**（下一个跃点）— 连接至目标网络的下一个跃点上的网关的 IP 地址。如果下一个跃点为 0.0.0.0，即表示默认路由。
- 度量—由路由协议确定的路由的度量。
- 标志—此路线的信息如下：
- • **A B** — 活动状态，并且从 BGP 获得。
  - A C—活跃并连接。目标 — 网络。
  - A H—活跃并已连接。目标 — 仅主机。
  - **A R** — 活动，并且从 RIP 获得。
  - **O1** — OSPF 外部 type-1。
  - **O2** — OSPF 外部 type-2。
  - **Oi**—OSPF 服务区间。
  - **Oo** — OSPF 服务区间。
  - **S** — 非活动和静态。
  - **A S** — 活动和静态。

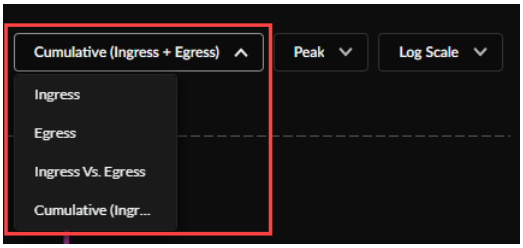


带宽消耗趋势

带宽消耗趋势默认显示累积（传入 + 传出）信息。

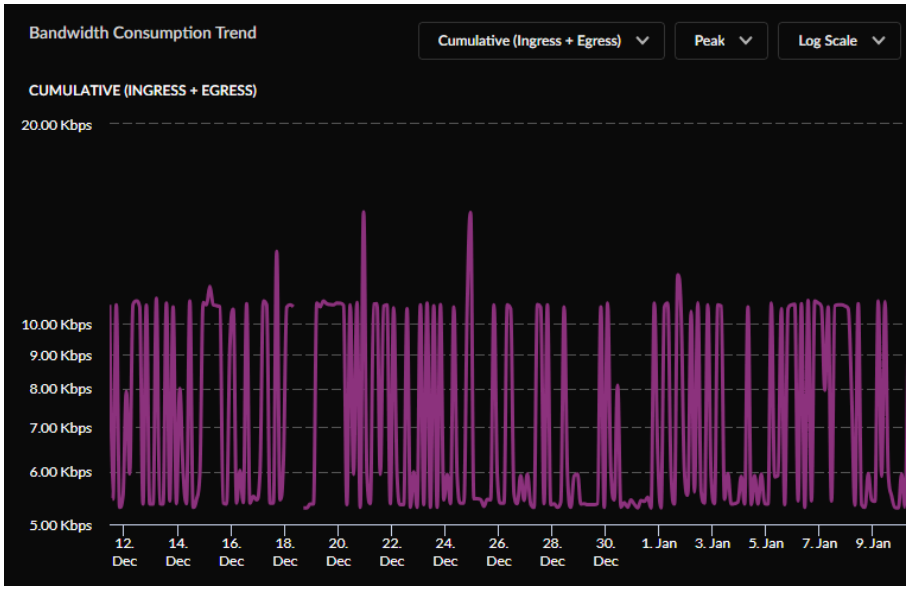
 ©2025 Palo Alto Networks, Inc.

- 使用下拉菜单查看按入口、传出、入口对比的带宽消耗图表。**Egress**（传入与传出）或累积（传入 + 传出）查看带宽消耗图表。



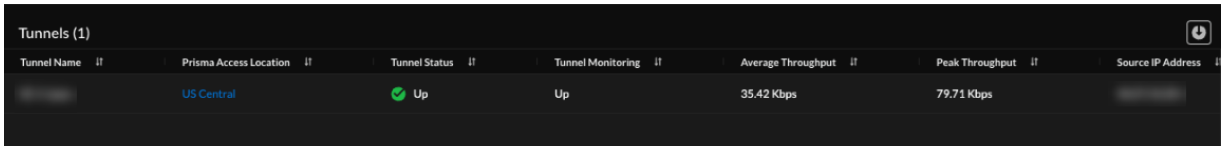
- 按 **Peak**（峰值）（默认值）、**Average**（平均值）或 **Median**（中值）查看分支站点的带宽消耗趋势图表指标。





隧道

查看此服务连接有多少个隧道，并查看每个隧道的详细信息。要下载隧道数据，请选择下载图标。



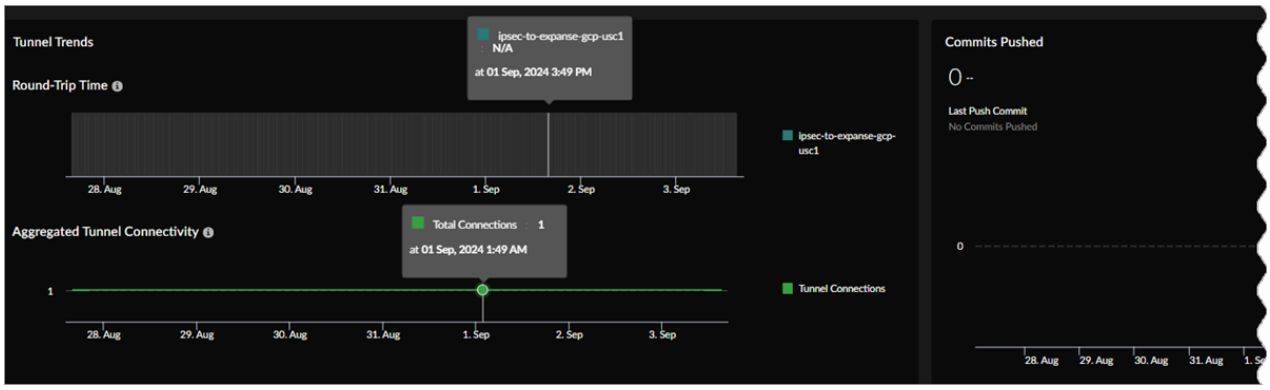
隧道趋势

您可以选择多个隧道并查看它们的平均往返时间。如果您未指定隧道集，则会计算观察到的 RTT 最高的 10 个隧道的中位 RTT。

聚合隧道连接性显示所选时间范围内连接隧道的总数。将鼠标悬停在任一图表上以查看特定时间的连接数量。

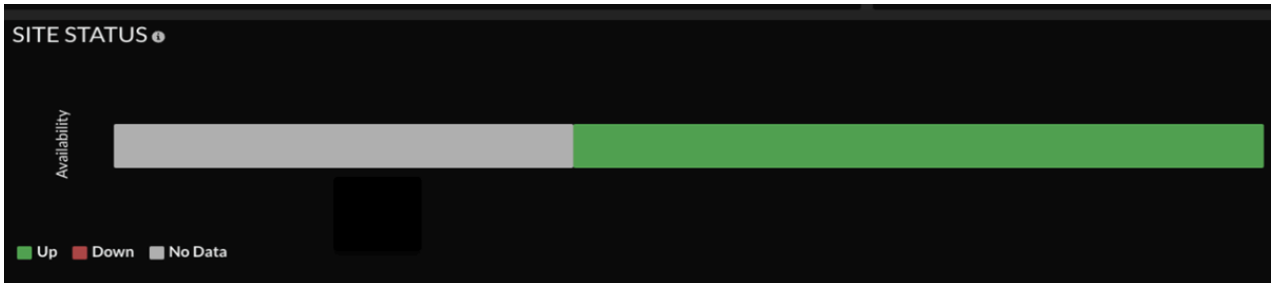
已推送的提交显示在选定的时间范围 内推送了多少次提交以及最后一次推送提交发生的时间。

 ©2025 Palo Alto Networks, Inc.



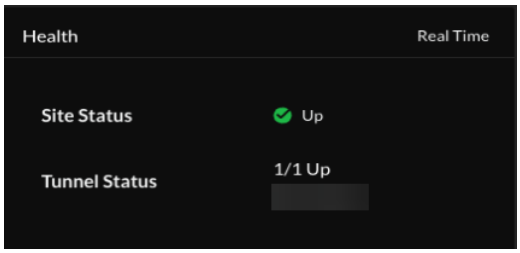
站点状态

网站状态显示在所选时间范围内的网站可用性。绿色表示该网站在此期间处于运行状态，红色表示该网站处于关闭状态，灰色表示在显示的时间内没有可用数据。



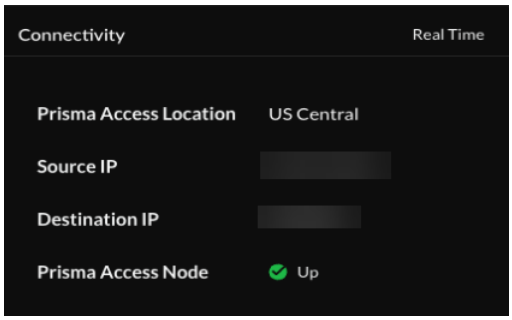
运行状况

运行状况显示站点状态，并显示站点中每个隧道的名称和状态。



连性

连接 显示 Prisma Access 网站所连接的位置、其源 IP 和目标 IP，以及 Prisma Access 节点状态。



消耗

消耗 显示带宽消耗详情。

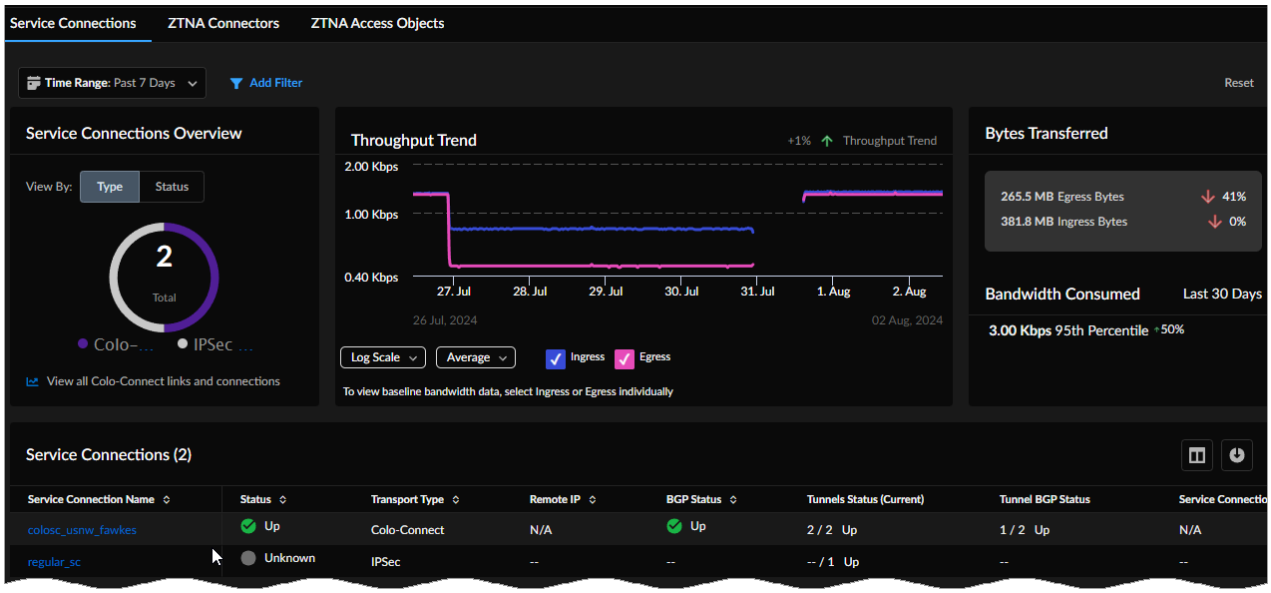
 ©2025 Palo Alto Networks, Inc.

查看和监视 Colo-Connect

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	Prisma Access 许可证

Prisma Access Colo-Connect 利用云原生 GCP 互连技术为您的专用应用程序提供高带宽服务连接。Colo-Connect与现有的基于IPSec隧道的服务连接共存，因此如果您需要为不需要高带宽吞吐量的小型数据中心提供私有应用访问，您也可以使用与这些数据中心的服务连接。通过查看 Colo-Connect 链接数量和状态、吞吐量趋势以及单个隧道、连接和链接的详细信息，获得对您的 Colo-Connect 部署的可见性。通过查看有关 Colo-Connect 服务连接的数据，您可以全面了解部署的运行状况和连接性。

转到 **Monitor**（监视） > **Data Centers**（数据中心） > **Service Connections**（服务连接），查看和监视通过云互连与混合云和本地数据中心之间的专用连接。



服务连接概述

服务连接概述显示按传输类型的服务连接数量。

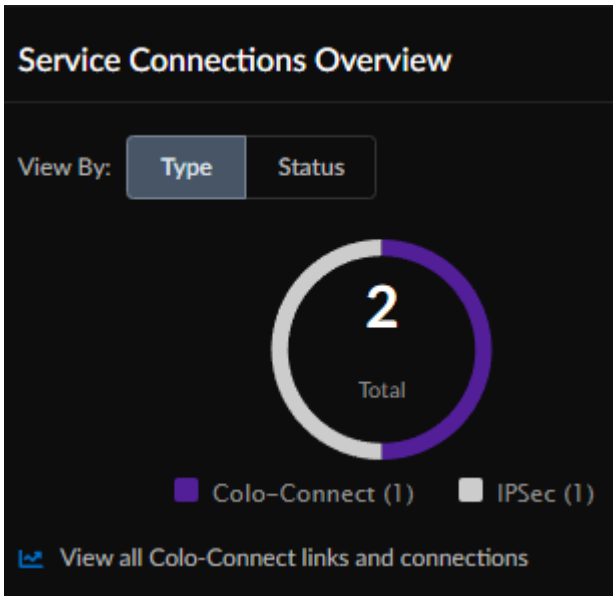
您可以按类型或可用状态查看连接运输的聚合。

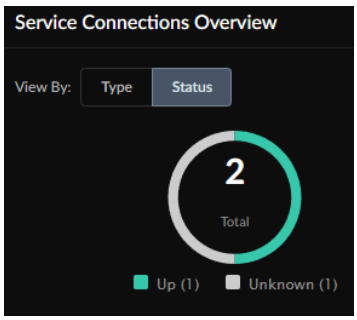
- **IPSec**
- **Colo-Connect**

您可以通过状态查看隧道运输类型：向上，向下，降级或未知。

选择查看所有 Colo-Connect 链接和连接，以查看 Colo-Connect 详细信息页面。

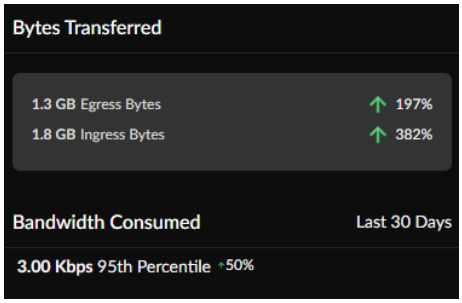
©2025 Palo Alto Networks, Inc.





服务连接概述：传输的字节和消耗的带宽

字节传输显示了所消耗的入口和传出字节的汇总，以及您之前选择的时间范围内的消耗差异。带宽消耗显示过去30天中消耗带宽的第95个百分位数。



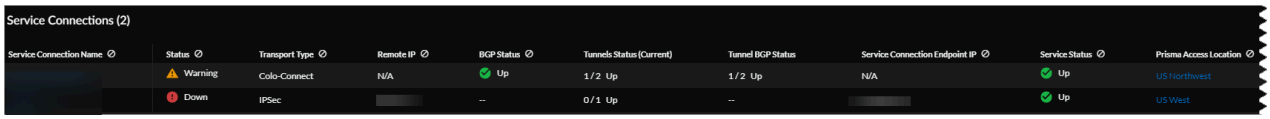
服务连接

服务连接表显示每个指示的服务连接的以下详细信息：

- 服务连接名称—Colo-Connect或IPSec服务连接的名称。选择一个服务连接名称以进入其详细信息页面。
- 状态—正常、故障、降级或未知。
- 运输类型—Colo-Connect或IPSec。
- 远程IP—目标IP。
- BGP状态—正常、关闭，或警告（如果某些BGP隧道正常而某些关闭）。

 ©2025 Palo Alto Networks, Inc.

- 隧道状态（当前）—当前隧道状态。
- 隧道 BGP 状态—按 BGP 状态（正常、关闭或警告）分类的隧道数量。
- 服务连接端点 IP — Prisma Access 节点 IP 地址。
- 服务状态—服务状态由活动服务连接或数据中心集群或集群的状态（正常、故障或警告）决定。
- Prisma Access 位置—选择一个 Prisma Access 位置。
- 平均带宽消耗 — 在所选时间范围内，网站的平均带宽消耗。
- 峰值带宽消耗—在所选时间范围内，网站的峰值带宽消耗。



服务连接详细信息

从主页上的服务连接表中，选择一个传输类型为 Colo-Connect 的服务连接，以进入其详细信息页面。



服务连接状态，*Colo-Connect* 和并发会话

- 查看服务连接的访问位置和 GRE 隧道状态（正常、故障或警告）。
- 查看 Colo-Connect 链接和连接的总数。
- 并发会话显示当前会话的数量以及过去30天内的总会话数量。

吞吐量趋势

吞吐量趋势显示在所选时间范围内此服务连接消耗的入口和传出吞吐量流量。

传输的字节和消耗的带宽

字节传输显示了此服务连接消耗的入口和传出字节的汇总，以及与先前选择的时间范围的消耗差异。带宽消耗显示服务连接在过去30天内消耗的带宽的第95个百分位数。

GRE 隧道

查看此服务连接中隧道的详细信息：

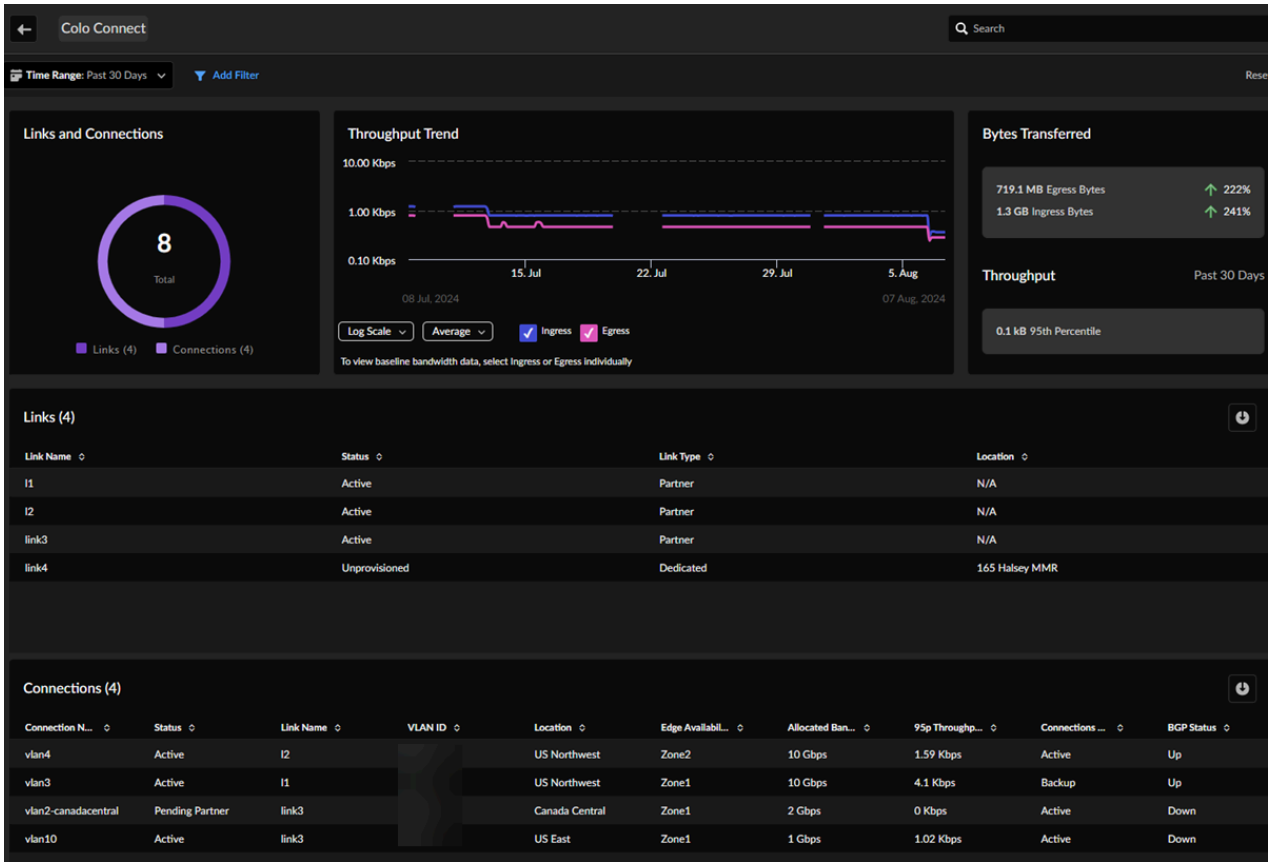
- 隧道名称 — 唯一的隧道名称。

 ©2025 Palo Alto Networks, Inc.

- 隧道状态—正常、关闭或未知。
- 连接名称—连接的唯一名称。
- 隧道状态—连接状态（活动或备份）。
- 远程 **IP** — 目标 IP 地址。
- 源IP—本地设备的IP地址。
- 95%的吞吐量 — 过去30天内消耗带宽的第95个百分位。
- 峰值吞吐量—在所选时间范围内的峰值吞吐量。
- BGP状态—正常、关闭、降级或未知。
- BGP本地IP—BGP本地IP。
- 断开连接 — 这个隧道发生了多少次断开连接。
- 断开连接持续时间 — 断开连接持续了多长时间。
- 入口字节 - 在所选时间范围内消耗了多少入口字节。
- 出站字节 — 在所选时间范围内消耗了多少出站字节。
- 入口数据包计数—入口数据包计数。
- 出站数据包计数 — 出站数据包的计数。

Colo Connect 详细信息

从主服务连接页面，选择从服务连接概述小部件查看所有Colo-Connect链接和连接，以打开Colo-Connect详细信息页面。此页面上的小部件显示您的当前详细信息（当前定义为过去 20 分钟）。



 ©2025 Palo Alto Networks, Inc.

链接和连接

圆形图表显示当前 Colo-Connect 链接和连接的总数。

链接

该表显示了您当前 Colo-Connect 链接的详细信息。

- 链接名称 — 独特的 Colo-Connect 链接名称。
- 状态 — 活动或维护。
- 链接类型 — 合作伙伴或专用.
- 地点 — Prisma Access 地点。

连接

查看有关您当前 Colo-Connect 链接的详细信息。将鼠标悬停在连接上以查看所示状态的信息。

- 连接名称 — 唯一的 Colo-Connect 连接名称。
- 状态 — 活跃，待定合作伙伴，失效。
- 链接名称 — 连接的链接名称。
- **VLAN ID** — 连接的 VLAN ID。
- 地点 — Prisma Access 地点。
- 边缘可用区 — Zone1 或 Zone2。
- 分配带宽— 1 Gbps、2 Gbps、5 Gbps、10 Gbps 或 20 Gbps。
- **95%** 吞吐量 — 消耗带宽的第 95 百分位。
- 连接状态 — 活动或备份。
- **BGP** 状态 — 正常或异常。

查看和监视 ZTNA 连接器

哪里可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证 ❑ 这是一个 Prisma Access Insights 功能。

零信任网络接入 (ZTNA) 连接器简化了所有应用程序的私有应用程序访问。您环境中的 ZTNA 连接器虚拟机会自动在您的专用应用程序和 Prisma Access 之间形成隧道。查看所有已配置的 ZTNA 连接器的摘要，包括与连接器关联的**Application Targets**（应用程序目标）、其平均带宽和中位带宽以及 **Status**（状态）（启动、部分启动或关闭）。 > > Strata Cloud Manager选择中的监控数据中心ZTNA连接器以查看ZTNA连接器和连接器组的性能。

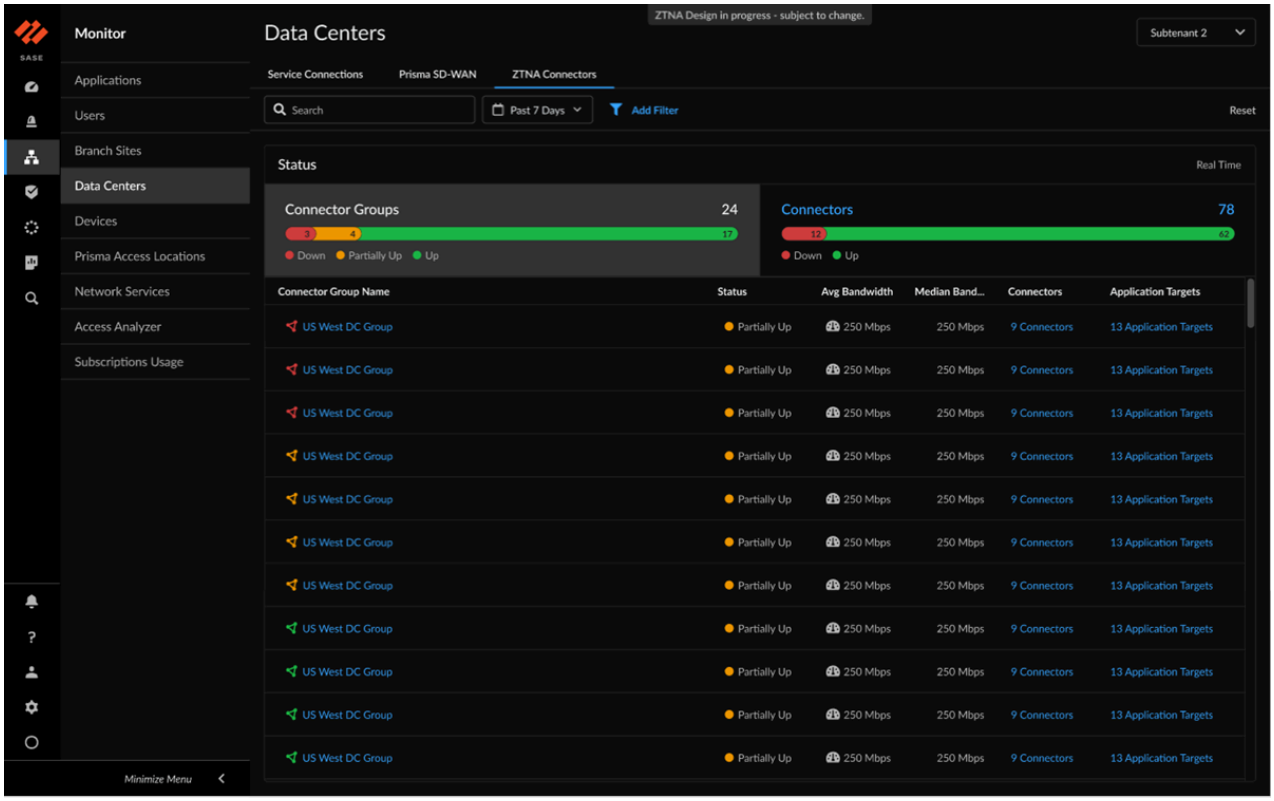
ZTNA连接器组状态

每个组中的连接器确定连接器组的状态。

- 如果连接器组中的所有连接器都已启动，则状态为“启动”（绿色）。

 ©2025 Palo Alto Networks, Inc.

- 如果所有连接器都已关闭，则状态为“关闭”（红色）。
- 如果某些连接器已打开，而某些连接器已关闭，则状态为部分打开（橙色）。
- 禁用的连接器显示为灰色。



ZTNA 连接器状态

查看所有已配置连接器的摘要，包括与连接器关联的应用程序目标和状态。

选择任意连接器名称以查看有关关联连接器组和与每个连接器关联的应用程序目标的详细信息。

查看和监控 ZTNA 连接器访问对象

哪里可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

通过查看由 FQDN、IP 子网和通配符添加的应用程序数量、每个访问对象的连接状态以及与每个访问对象关联的 连接器组 和 连接器 等数据，了解通过 ZTNA 连接器访问对象添加的私有应用程序。通过查看此信息，您可以全面了解部署的运行状况和连接性。

数据中心 中的私有应用程序通过您的连接器虚拟机 (VM) 连接到 Prisma Access。您可以根据这些访问对象（FQDN、FQDN 通配符或 IP 子网）添加应用程序。

- **FQDN**—Prisma Access 将您加入 ZTNA Connector 的应用程序的 FQDN 解析为应用程序 IP 地址块中的 IP 地址。

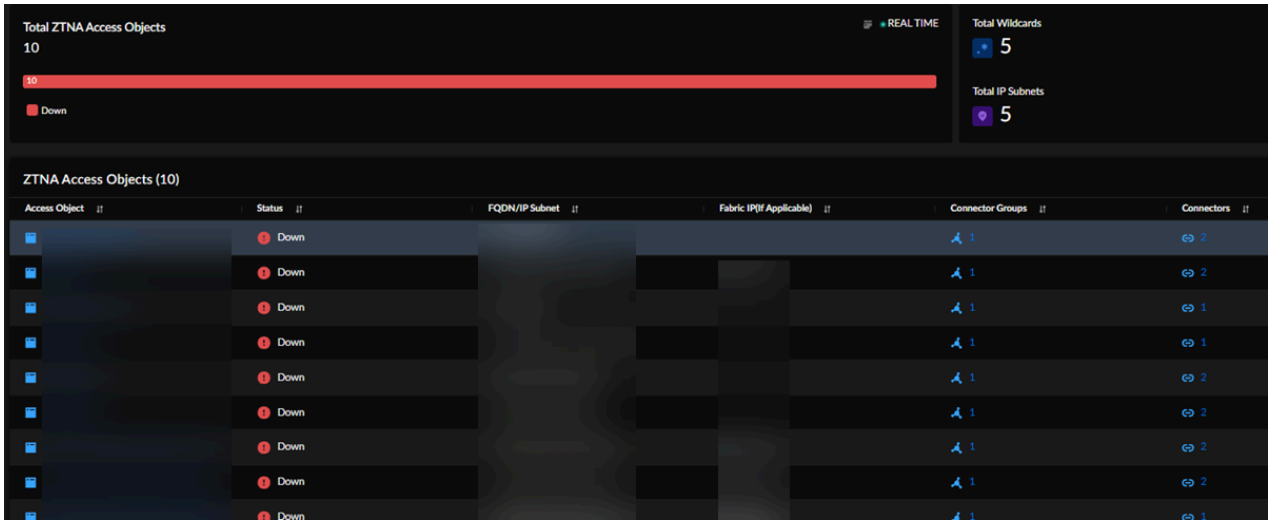
 ©2025 Palo Alto Networks, Inc.

- 通配符— 对于基于通配符的应用程序，创建一个基于 FQDN 的连接器组，然后指定应用程序目标要使用的通配符（例如，*.example.com）。当用户访问与通配符匹配的站点时，这些应用程序将自动加入，以便您的移动用户和远程网络用户从 ZTNA 连接器进行访问。
- **IP** 子网— 创建基于 IP 子网的连接器组，然后输入用于应用目标的 IP 子网。

在 Strata Cloud Manager中，转到 监控 > 数据中心 > **ZTNA** 访问对象 以查看您的 ZTNA 连接器访问对象。

所有访问对象

查看 总 **ZTNA** 访问对象 以实时查看有关所有 ZTNA 连接器访问对象（FQDN、通配符和 IP 子网）的信息。总 **ZTNA** 访问对象 和 **ZTNA** 访问对象 表中的数字应该匹配，代表 FQDN 应用程序、子网应用程序和发现的通配符应用程序的数量。



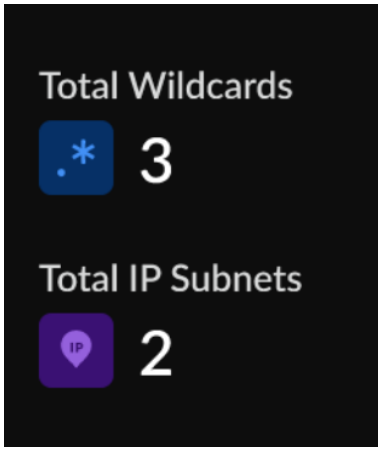
- 按状态查看您环境中的 总 **ZTNA** 访问对象 图表，这意味着访问对象的自动安全隧道处于启动、部分启动、关闭或禁用状态。如果状态为 down，则与此访问对象关联的连接器将无法访问您的应用程序。
  - 向上— 所有隧道均已向上。
  - 部分正常运行— 一些隧道已正常运行，其他隧道已关闭或被禁用。
  - 关闭— 所有隧道均已关闭。
  - 已禁用— 所有隧道均已禁用。

  在 “总 **ZTNA** 访问对象 ”小部件中选择一个状态颜色方块，以便在 **ZTNA** 访问对象 表中按状态对访问对象进行排序。

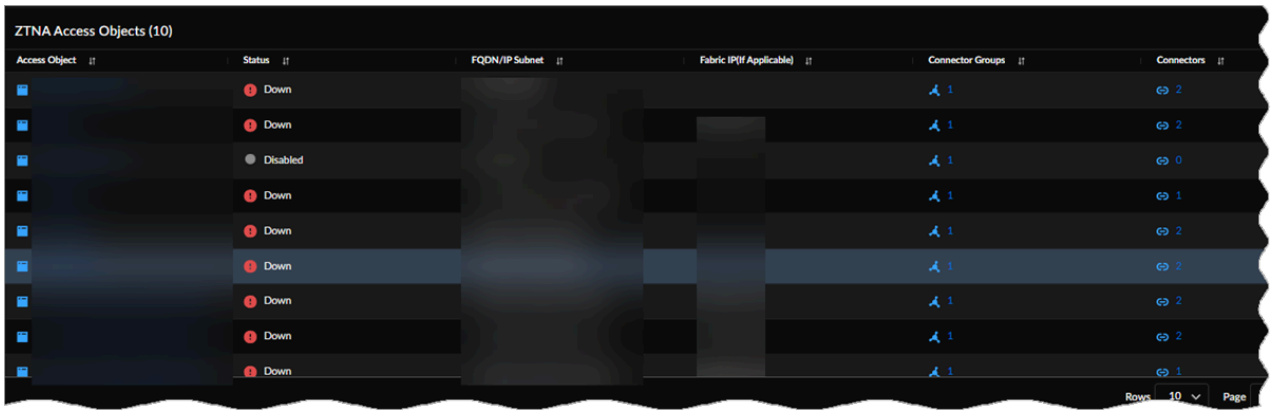


 ©2025 Palo Alto Networks, Inc.

- 总通配符和总 **IP** 子网 总结了您已加入的 IP 子网和通配符规则的数量。这是您创建的通配符规则的数量，它与创建这些规则后发现的应用程序数量总数不同。



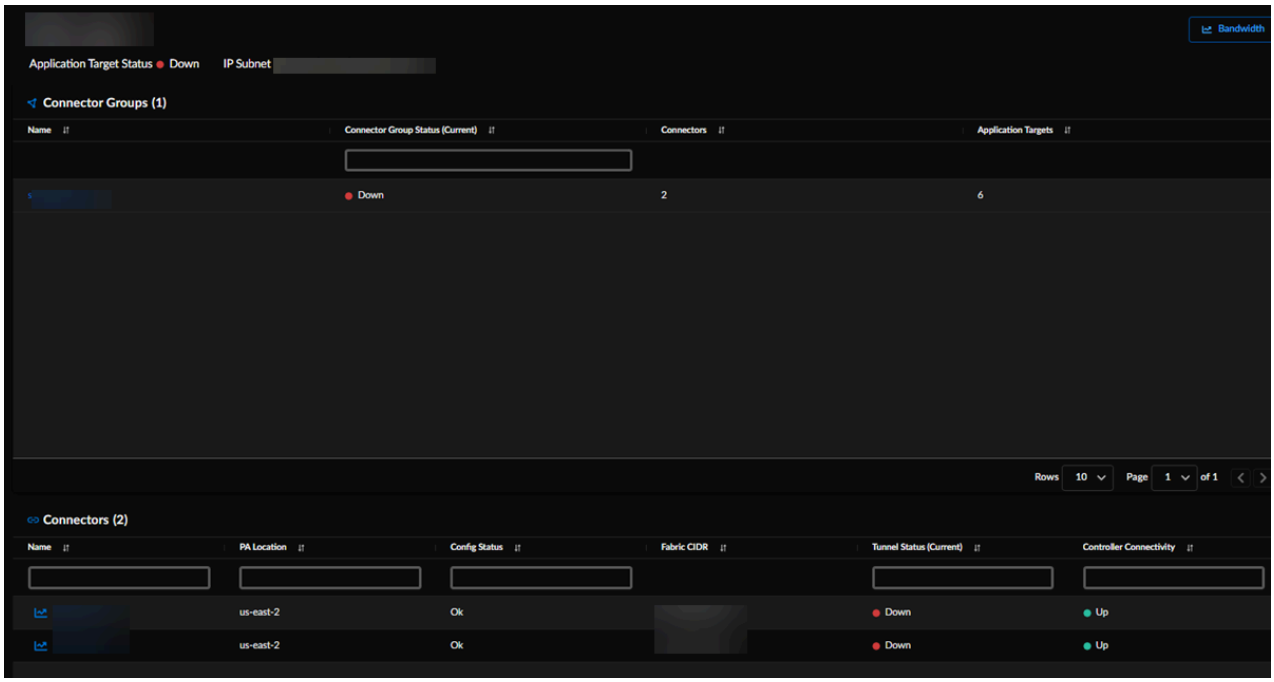
- **ZTNA** 访问对象 提供有关所有访问对象的信息。
  - 访问对象— 选择特定的访问对象以查看其详细信息。
  - 状态— 访问对象的自动安全隧道处于启动、部分启动、关闭或禁用状态。
  - **FQDN/IP** 子网— 用于添加此访问对象的 FQDN 或 IP 子网。
  - 结构 **IP**（如果适用）— 与此访问对象关联的结构 IP。
  - 连接器组— 连接器组是连接器和应用程序的逻辑分组。查看与访问对象关联的连接器组。
  - 连接器 — 连接器代表在数据中心运行并连接到 Prisma Access 的虚拟机。查看与访问对象关联的连接器。



选择任何 访问对象 来查看其详细信息。

- 连接器组— 查看有多少个连接器组与此访问对象关联。选择一个连接器组以查看有关其 服务连接的信息。
- 连接器组状态（当前）— 启动、部分启动、关闭或禁用。
- 连接器 — 此连接器组中的连接器数量。
- 应用程序目标 — 此连接器组中的应用程序目标的数量。
- 带宽— 选择 带宽 按钮可以查看此访问对象的带宽信息。

 ©2025 Palo Alto Networks, Inc.



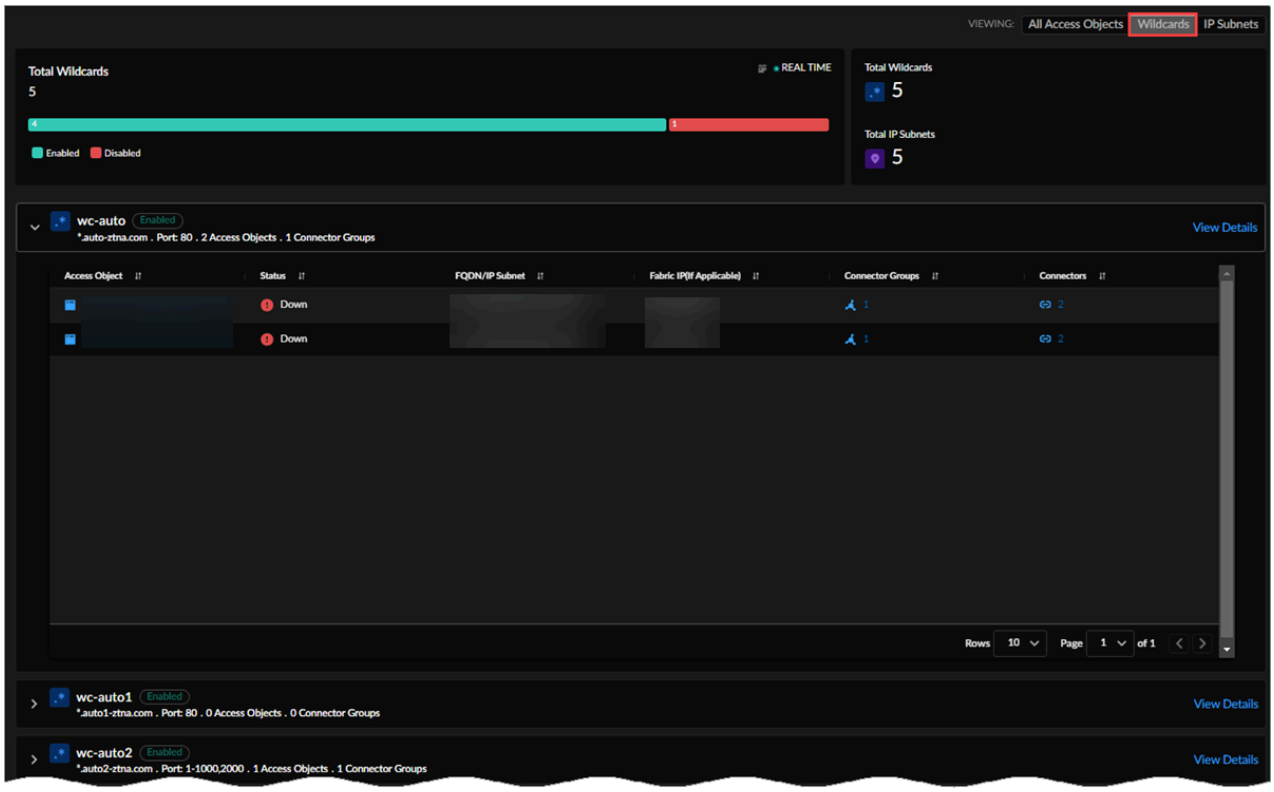
选择任意访问对象的 连接器 来查看其详细信息。

- **PA**（**Prisma Access**）位置 — 与每个连接器相关的 Prisma Access 位置。
- 配置状态 — 连接器的配置状态为正常或错误。如果状态为错误，则表示 ZTNA 连接器尚未完成入职。
- **Fabric CIDR**— 与此连接器关联的 Fabric CIDR。
- 隧道状态（当前） — 此连接器的自动安全隧道状态。
- 控制器连接— 启动、部分启动、关闭或禁用。

通配符

选择 通配符 来查看您的通配符访问对象。按状态查看 通配符总数 以及 通配符 总数和 **IP** 子网总数。

 ©2025 Palo Alto Networks, Inc.



选择通配符旁边的箭头，或者选择 **View Details**（查看详细信息），以获取有关组成此通配符的访问对象的信息。

- 访问对象— 选择特定的访问对象以查看其详细信息。
- 状态— 访问对象的自动安全隧道处于启动、部分启动、关闭或禁用状态。
- **FQDN/IP** 子网— 用于添加此访问对象的 FQDN 或 IP 子网。
- 结构 **IP**（如果适用）— 与此访问对象关联的结构 IP。
- 连接器组— 连接器组是连接器和应用程序的逻辑分组。查看与访问对象关联的连接器组。
- 连接器 — 连接器代表在数据中心运行并连接到 Prisma Access 的虚拟机。查看与访问对象关联的连接器。



选择任何 访问对象 来查看其详细信息。

- 连接器组— 查看有多少个连接器组与此访问对象关联。选择一个连接器组以查看有关其 服务连接的信息。
- 连接器组状态（当前）— 启动、部分启动、关闭或禁用。
- 连接器 — 此连接器组中的连接器数量。
- 应用程序目标 — 此连接器组中的应用程序目标的数量。
- 带宽— 选择 带宽 按钮可以查看此访问对象的带宽信息。

 ©2025 Palo Alto Networks, Inc.

选择 “连接器组” 或 “连接器”可查看与通配符中的访问对象关联的唯一连接器组或连接器。

IP 子网

选择“**IP** 子网” 可查看 IP 子网访问对象的总数。一个 IP 子网访问对象由几个不同的应用程序组成。

按状态（启动、部分启动、关闭或禁用）查看环境中的 总 **IP** 子网 。

IP 子网 **ZTNA** 访问对象 提供有关所有访问对象的信息。

- • 访问对象— 选择特定的访问对象以查看其详细信息。
  - 状态— 启动、部分启动、关闭或禁用。
  - **IP** 子网— 用于添加此访问对象的 IP 子网。
  - 连接器组— 连接器组是连接器和应用程序的逻辑分组。查看与访问对象关联的连接器组。
  - 连接器— 连接器代表数据中心中运行的虚拟机，它们连接到 Prisma Access。查看与访问对象关联的连接器。



选择任何 访问对象 来查看其详细信息。

- 连接器组— 查看有多少个连接器组与此访问对象关联。选择一个连接器组以查看有关其 服务连接的信息。
- 连接器组状态（当前）— 启动、部分启动、关闭或禁用。
- 连接器 — 此连接器组中的连接器数量。
- 应用程序目标 — 此连接器组中的应用程序目标的数量。
- 带宽— 选择 带宽 按钮可以查看此访问对象的带宽信息。

选择 连接器组 或 连接器 来查看与 IP 子网中的访问对象关联的唯一连接器组或连接器。

查看和监控网络服务

哪里可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证 ❑ 这是一个 Prisma Access Insights 功能。

©2025 Palo Alto Networks, Inc.

您可以查看影响访问应用程序的用户体验的常见网络服务的性能。网络服务包括报告 GlobalProtect 身份验证成功和失败的次数，作为移动用户能够连接到 Prisma Access 并显示您指定的时间范围内转发到服务器的 DNS 代理请求和响应。

GlobalProtect 身份验证

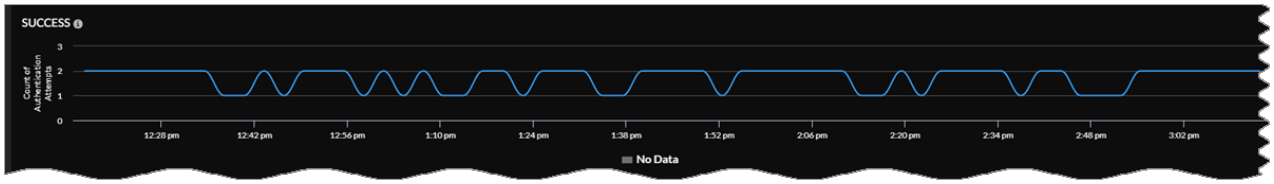
在 Strata Cloud Manager 中转至监控 > 网络服务 > **GlobalProtect** 身份验证，以便查看影响您环境的 GlobalProtect 身份验证成功和失败。

- 设置时间范围过滤器以查看该时间范围的网络服务数据。
- 指定一个 **Prisma Access** 位置，以查看其在所选时间范围内的身份验证成功、总失败和超时失败。

数据表示在给定时间内有多少移动用户尝试向 GlobalProtect 门户进行身份验证，然后该门户将移动用户的凭据发送到内部活动目录 (AD) 服务器进行验证，从而得出身份验证成功或失败的结论。如果您发现大量的身份验证失败，则可以将这些失败与网络事件关联起来，该事件表明某个位置出现问题或本地身份验证服务器出现故障。这些图表中的数据为解决网络问题的网络管理员提供了故障排除见解。您可以在 GlobalProtect 门户和网关上查看移动用户的身份验证成功或失败趋势的数量，使用这些数据了解一段时间内身份验证成功或失败的模式，并建立 Prisma Access 部署中正常或异常的数量范围。例如，异常计数可能表明现有用户无法连接到 Prisma Access，因为 GlobalProtect 门户存在可用性问题或身份验证服务器速度慢。或者，异常计数可能代表大量用户同时加入客户网络。

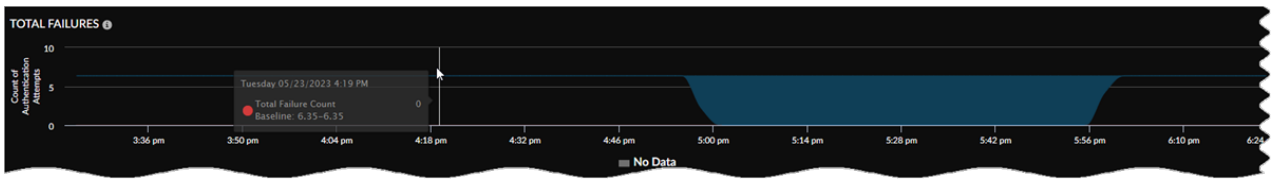
GlobalProtect 身份验证成功

查看有关身份验证成功的具体信息对不同位置的 GlobalProtect 至关重要。将光标悬停在图形中的任意点上，可查看特定时间显示的不同 Prisma Access 位置站点成功身份验证的用户计数的详细信息。



GlobalProtect 身份验证失败总数

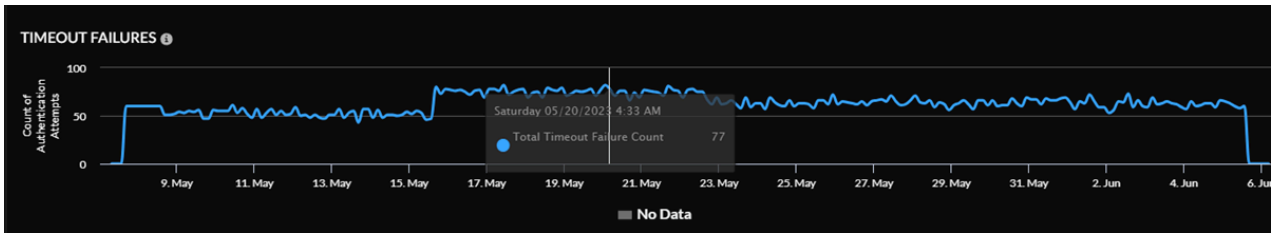
查看有关身份验证失败的具体信息对不同位置的 GlobalProtect 至关重要。将光标悬停在图形中的任意点上，可查看特定时间显示的不同 Prisma Access 位置站点(如美国东部和加拿大东部)身份验证失败的用户计数的详细信息。



GlobalProtect 身份验证超时失败

查看有关身份验证失败的具体信息对不同位置的 GlobalProtect 至关重要。将光标悬停在图形中的任意点上，可查看特定时间显示的不同 Prisma Access 位置站点(如美国东部和加拿大东部)身份验证失败的用户计数的详细信息。

 ©2025 Palo Alto Networks, Inc.



DNS

在 Strata Cloud Manager 中转至监控 > 网络服务 > **GlobalProtect** 身份验证，以便查看您指定的时间范围内转发到服务器的 DNS 代理请求和响应。

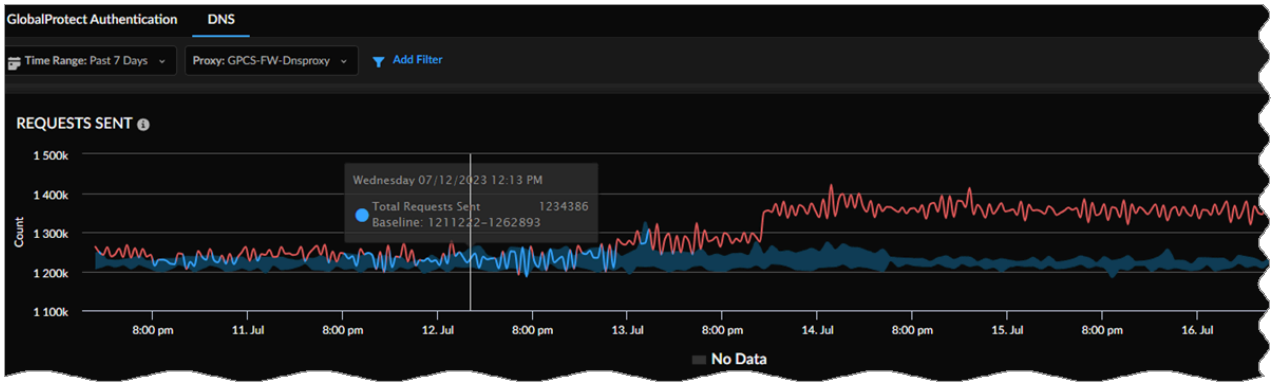
您可以使用的过滤器有：

- 时间范围
- **DNS** 代理名称

DNS 代理筛选器值与过去 30 天相关，并在加载时自动选择（也就是说，如果没有显式代理数据，则没有显式代理筛选器）。将鼠标悬停在图表上可查看有关在特定时间内发送到 DNS 代理服务器的所有 **Requests Sent**（已发送请求），以及从 DNS 代理服务器接收的所有 **Requests Received**（已接收请求）的详细信息。

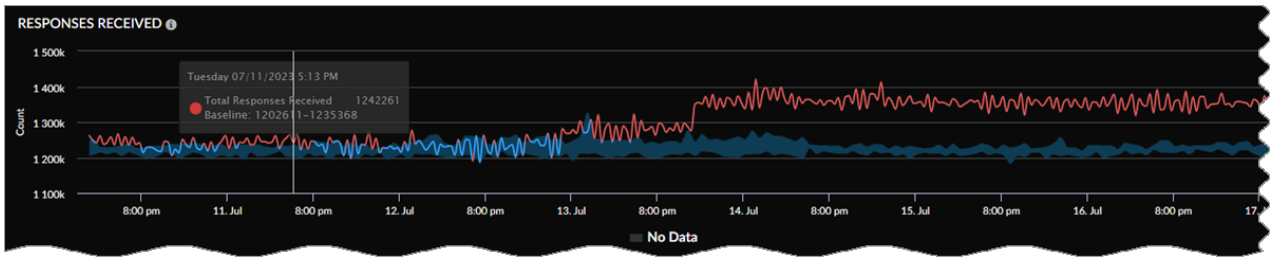
请求已发送

查看您指定的时间范围内转发到服务器的网络请求和查询。将光标悬停在图表中的任意点上，即可查看有关当时发送到 DNS 代理服务器的请求的信息。如果您选择了要过滤的代理名称，您将看到该代理的数据。



收到的响应

查看指定时间范围内各个租户收到的总响应数。将光标悬停在图表中的任意点上即可查看有关当时收到的响应的信息。如果您选择了要过滤的代理名称，您将看到该代理的数据。



 ©2025 Palo Alto Networks, Inc.

查看和监视网络服务：GlobalProtect 身份验证

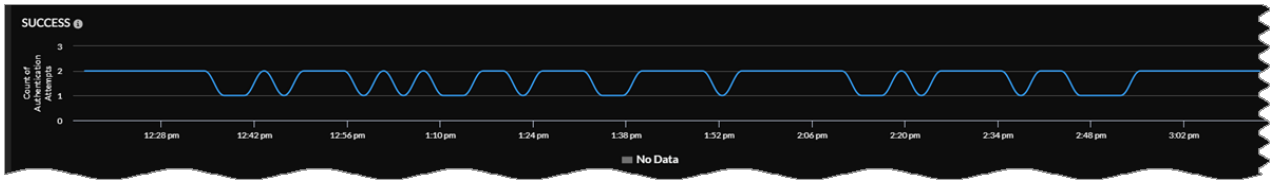
哪里可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证 ❑ 这是一个 Prisma Access Insights 功能。

网络服务包括报告 GlobalProtect 身份验证成功和失败的次数，作为衡量移动用户能够连接到 Prisma Access 的指标。要开始，请在 Strata Cloud Manager 中选择 **Monitor**（监控） > **Network Services**（网络服务） > **GlobalProtect Authentication**（**GlobalProtect** 身份验证）。

- 设置时间范围过滤器以查看该时间范围的网络服务数据。
- 指定一个 **Prisma Access** 位置，以查看其在所选时间范围内的身份验证成功、总失败和超时失败。

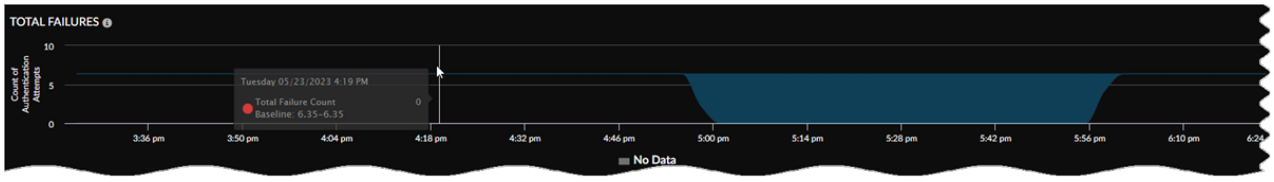
GlobalProtect 身份验证成功

查看有关身份验证成功的具体信息对不同位置的 GlobalProtect 至关重要。将光标悬停在图形中的任意点上，可查看特定时间显示的不同 Prisma Access 位置站点成功身份验证的用户计数的详细信息。



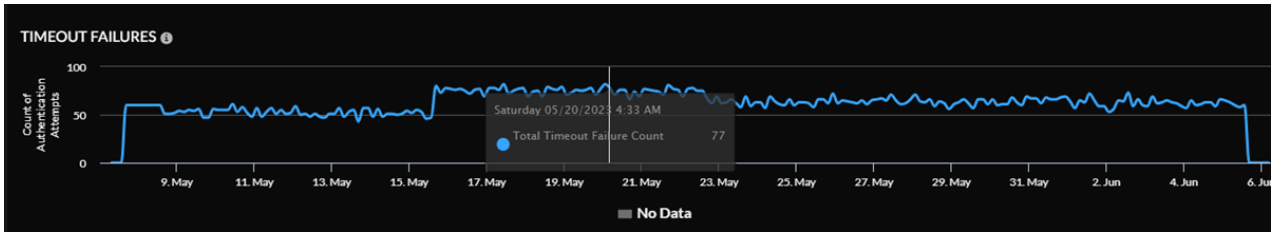
GlobalProtect 身份验证失败总数

查看有关身份验证失败的具体信息对不同位置的 GlobalProtect 至关重要。将光标悬停在图形中的任意点上，可查看特定时间显示的不同 Prisma Access 位置站点(如美国东部和加拿大东部)身份验证失败的用户计数的详细信息。



GlobalProtect 身份验证超时失败

查看有关身份验证失败的具体信息对不同位置的 GlobalProtect 至关重要。将光标悬停在图形中的任意点上，可查看特定时间显示的不同 Prisma Access 位置站点(如美国东部和加拿大东部)身份验证失败的用户计数的详细信息。



 ©2025 Palo Alto Networks, Inc.

查看和监视网络服务：DNS

哪里可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证 ❑ 这是一个 Prisma Access Insights 功能。

网络服务：**DNS** 显示在指定的时间范围内转发到服务器的 DNS 代理请求和响应。

您可以使用的筛选器：

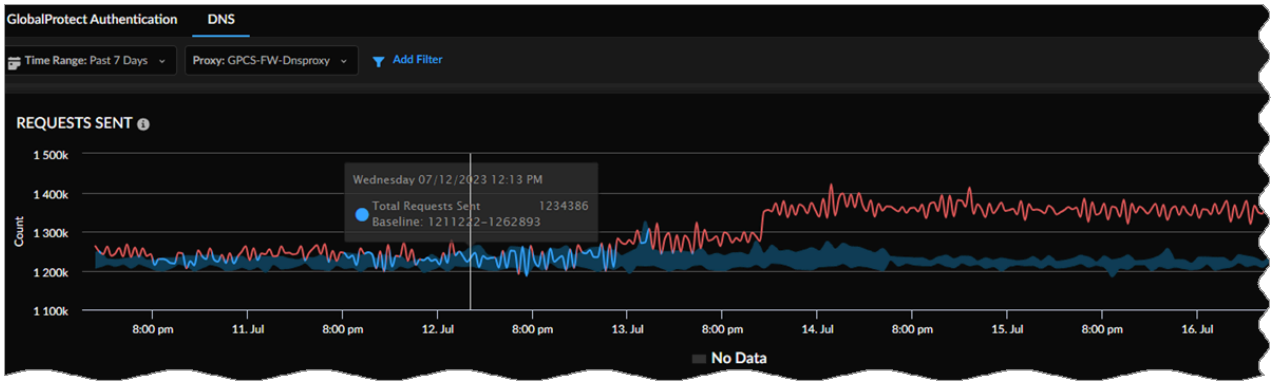
- 时间范围
- **DNS** 代理名称

DNS 代理筛选器值与过去 30 天相关，并在加载时自动选择（也就是说，如果没有显式代理数据，则没有显式代理筛选器）。

将鼠标悬停在图表上可查看有关在特定时间内发送到 DNS 代理服务器的所有 **Requests Sent**（已发送请求），以及从 DNS 代理服务器接收的所有 **Requests Received**（已接收请求）的详细信息。

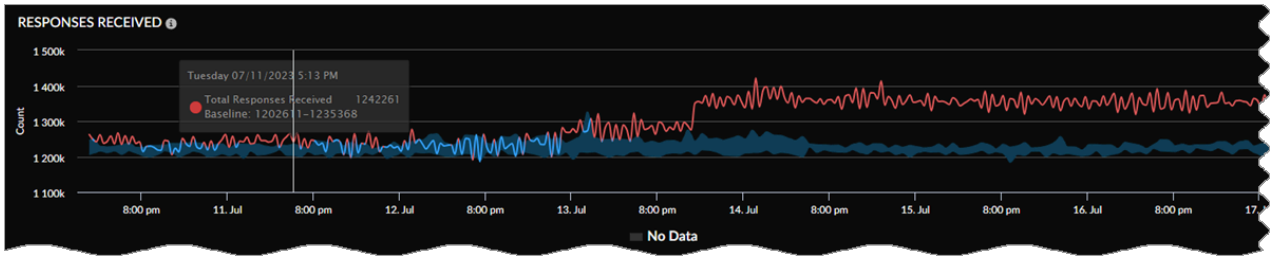
已发送请求

查看在指定的时间范围内转发到服务器的网络请求和查询。将光标悬停在图表中的任意点上，以查看有关当时发送到 DNS 代理服务器的请求的信息。如果您选择了要过滤的代理名称，则会看到该代理的数据。



收到的响应

查看在指定的时间范围内跨租户收到的响应总数。将光标悬停在图表中的任意点上，可以查看有关当时收到的响应的信息。如果您选择了要过滤的代理名称，则会看到该代理的数据。

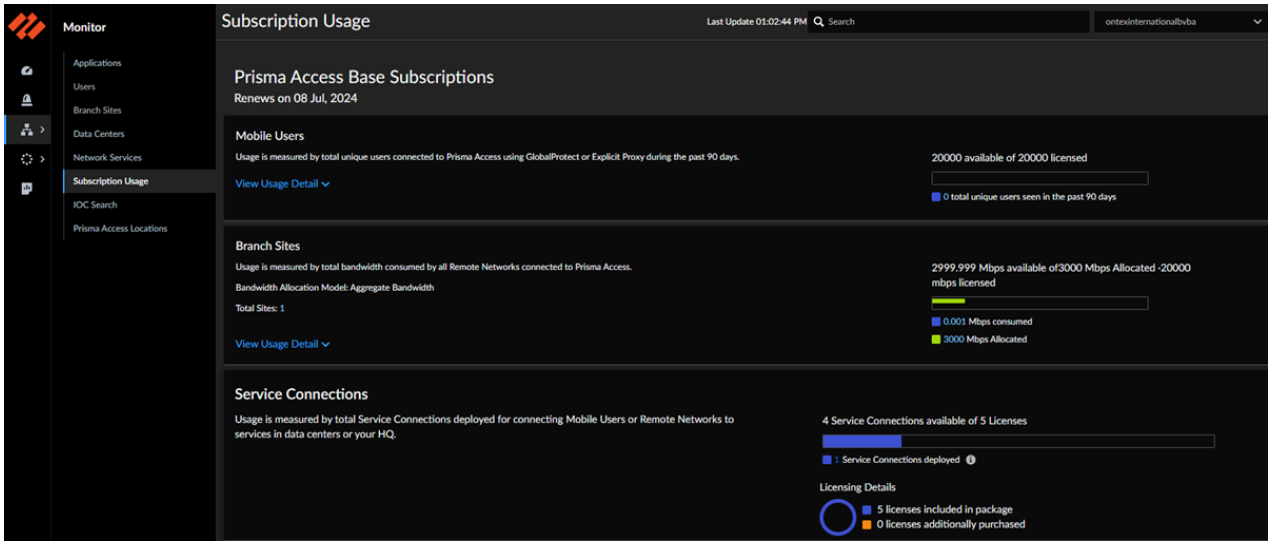


©2025 Palo Alto Networks, Inc.

查看订阅使用情况

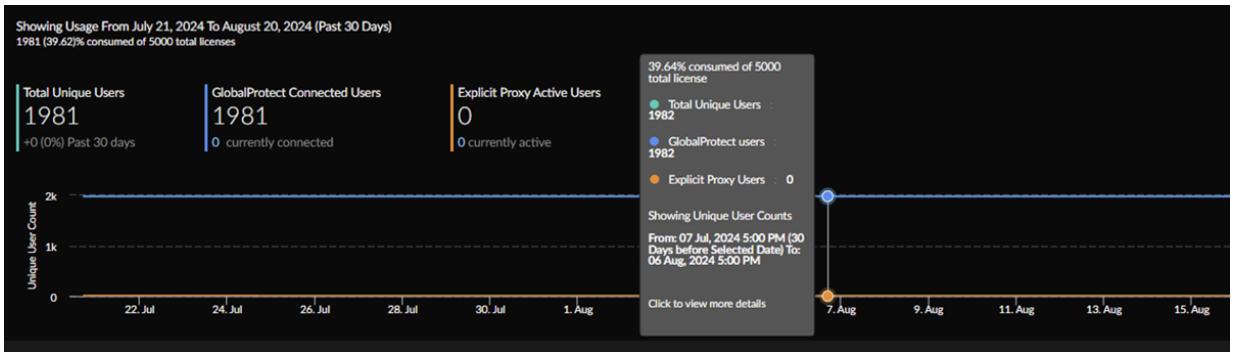
哪里可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

选择 监控 > 订阅使用情况 以查看您的 **Prisma Access** 基本订阅，包括迄今为止您已使用的许可证数量。



- **Mobile Users**（移动用户）— 查看到目前为止您已使用多少唯一 **Mobile Users**（移动用户）许可证。该小部件显示过去 30 天内连接到 Prisma Access 的唯一移动用户使用的许可证总数，因为许可证的使用基于过去 30 天的 Prisma Access 登录数据。在过去 30 天内至少登录过 Prisma Access 一次的用户将贡献一个移动用户许可证的使用。

  选择 查看使用情况详情 可查看过去 30 天内许可证使用情况的详情。您可以查看过去 30 天内的唯一用户总数、GlobalProtect 连接的用户总数以及显式代理活跃用户总数。将鼠标悬停在图表上可以查看当时消耗的许可证。

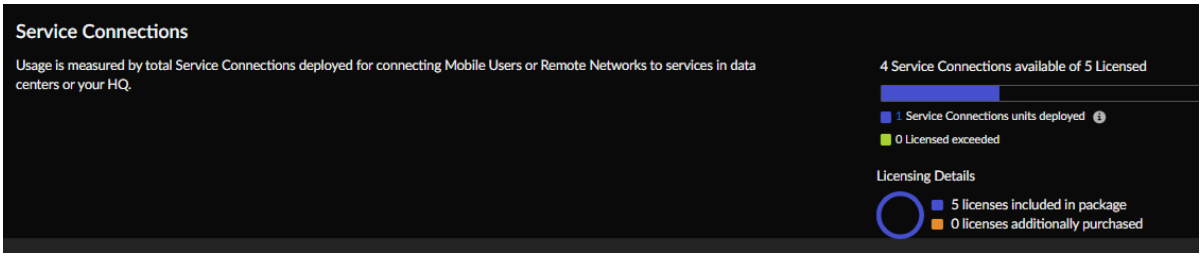


 ©2025 Palo Alto Networks, Inc.

- **Branch Sites**（分支站点）— 查看连接到 Prisma Access 的所有远程网络消耗的总带宽使用量。查看您分配了多少带宽以及您使用了多少带宽（以 Mbps 为单位）。您可以通过连接到 Prisma Access 的所有远程网络所消耗的总带宽来查看使用情况。

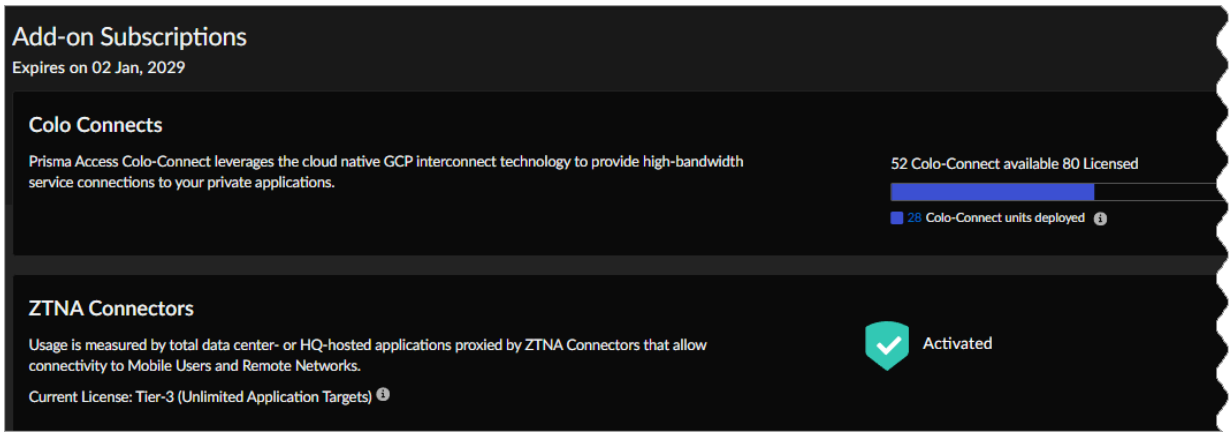
  选择 “查看使用情况详情”以根据带宽分配模型查看计算区域或分支站点的许可带宽消耗。在每种情况下，都会针对用于许可证计算的 30 天中的每一天指示出每日峰值带宽消耗值。您可以通过选择计算区域或分支站点来过滤图形视图。图表中每个计算区域或每个站点绘制了三条线，表示每日峰值消耗值、分配给计算区域或站点的带宽以及从每日峰值获得的第 95 个百分位数值。

- **Service Connections**（服务连接）— 查看到目前为止您已使用多少 **Service Connections**（服务连接）许可证。

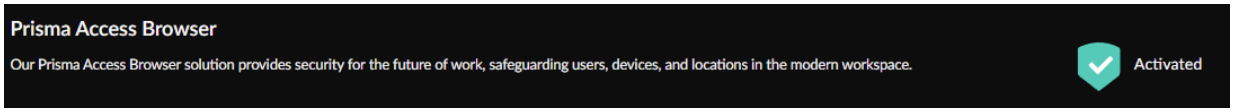


请参阅此页面的 **Add-On Subscriptions**（附加组件订阅）部分，查看您已购买的附加许可证。您可以看到购买的许可证总数以及迄今为止未使用的许可证数量。下面的图片描述了您可以购买的一些附加许可证。

- **Colo-Connects** — Prisma Access Colo-Connect 利用云原生 GCP 技术为您的私有应用程序提供高带宽服务连接。



- **Prisma Access** 浏览器—Prisma Access 安全企业浏览器（Prisma Access 浏览器）是唯一通过本机集成的企业浏览器保护托管和非托管设备的解决方案，该浏览器将保护扩展到非托管设备。Prisma Access Browser 通过在浏览器中设置安全措施来保护业务应用程序和数据。您的 Prisma Access 浏览器订阅将显示在 附加订阅 或 **Prisma Access** 基本订阅中。
  - **Prisma Access** 基础订阅 — 租户拥有 Prisma Access Browser 独立许可证。
  - 附加订阅— 当您为所有移动用户购买了 Prisma Access Browser 许可证时，Prisma Access Browser 订阅即被 激活。



 ©2025 Palo Alto Networks, Inc.

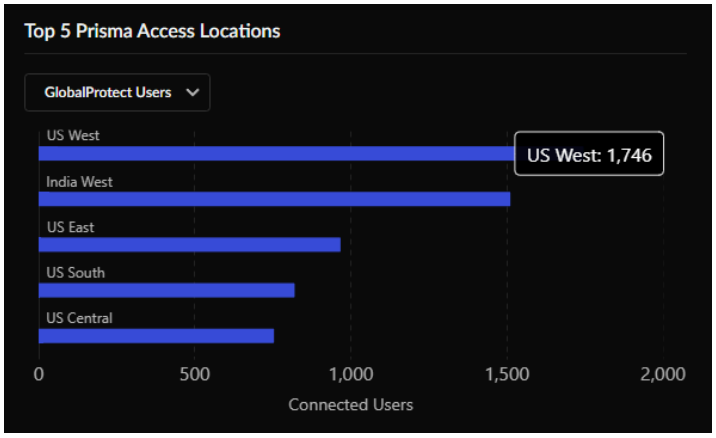
查看和监控 Prisma 访问位置

哪里可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证 ❑ 这是一个 Prisma Access Insights 功能。

选择 **Monitor**（监控） > **Prisma Access** 地点，以便查看您的远程网络和移动用户的所有 Prisma Access 地点的运行状态概览。

排名前 5 位的 Prisma Access 地点

该条形图根据所选时间范围内消耗的总带宽，显示前 5 个 Prisma Access 位置的远程网络、服务连接、GlobalProtect 移动用户或显式代理移动用户（从下拉菜单中选择）的数据。将鼠标悬停在任意栏上即可查看该特定位置有多少用户。

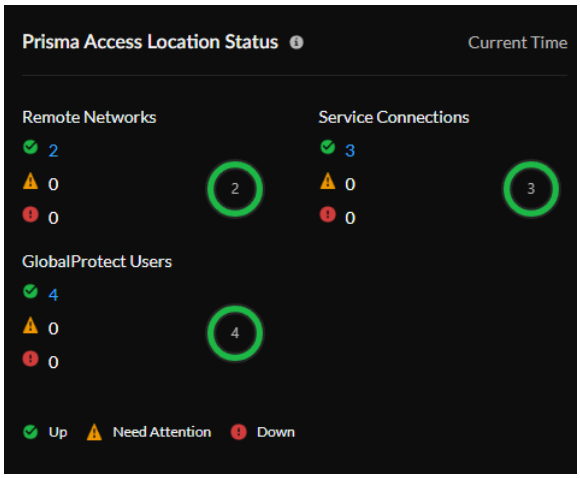


Prisma Access 位置状态

根据您的许可证，此小部件显示已连接的远程网络站点、服务连接站点、唯一的 GlobalProtect 用户以及登录到 Prisma Access 的唯一的显式代理用户的数量。小部件的颜色代码基于有多少远程网络、服务连接、GlobalProtect 用户和显式代理用户处于以下状态：

- 已连接（绿色）— 全部 Prisma Access 位置已连接。
- 已断开连接（红色）— 全部 Prisma Access 位置已断开连接。
- 部分连接（橙色）— 一个或多个 Prisma Access 位置已断开连接。

©2025 Palo Alto Networks, Inc.

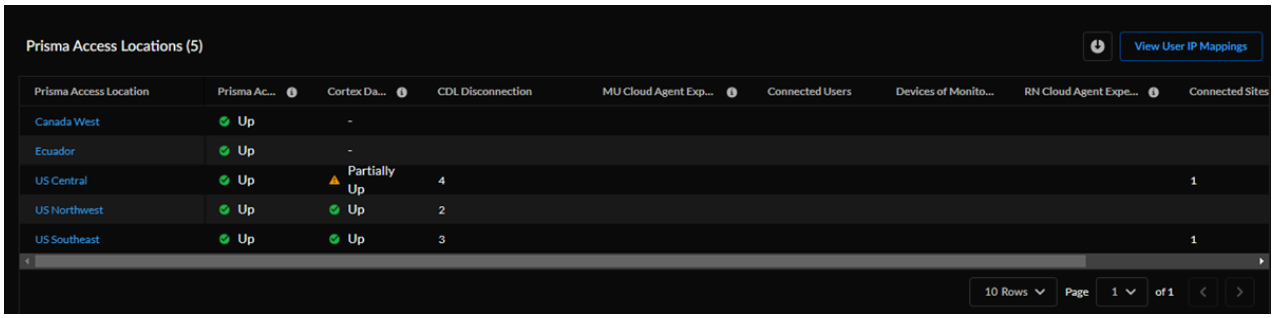


Strata Logging Service 连接性

Strata Logging Service 连接性小部件可让您查看在 Prisma Access 许可证激活期间选择的Strata Logging Service区域的所有 Prisma Access 实例的Strata Logging Service连接的运行状况。它可以帮助您确定防火墙是否已与 Strata Logging Service断开连接，并且您将无法再获取防火墙日志。每个租户只能连接到选择的任何区域中的一个 Strata Logging Service。Prisma Access 每 5 分钟轮询一次Strata Logging Service数据库，以检查各节点（移动用户、远程网络和服务连接）与 Strata Logging Service 数据库之间的连接性。

Prisma Access 位置状态

实时查看 **Prisma Access** 位置状态。在特定位置内，如果用户从多台主机登录，则该用户被视为单个用户，但如果任何用户从两个不同的 Prisma Access 位置登录，并在时间段内从一个位置断开连接并从另一个位置登录，该用户将被视为两个用户。选择一个位置以查看详细信息，例如消耗的带宽、状态、Strata Logging Service连接以及用户 ID 和组映射。



查看和监控第三方设备 ID

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	☐ Prisma Access 许可证

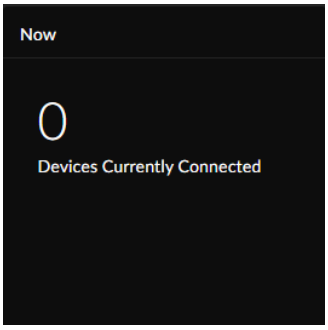
 ©2025 Palo Alto Networks, Inc.

您可以将 Cloud Identity Engine 与 Prisma Access 结合使用，应用来自第三方 IoT 检测源的信息，以简化识别和弥补网络中设备的安全漏洞的任务。有关设置和配置的详细信息，请参阅 Prisma Access 中的配置第三方设备 ID。

转到 监控 > 设备物 > 联网 以了解您的物联网设备，例如过去 30 分钟内连接的物联网设备数量、选定时间范围内连接的所有物联网设备以及所有连接的物联网设备的详细信息。

当前连接的设备

查看过去 30 分钟内连接的设备数量（如果有）。现在 始终仅显示最近 30 分钟内 当前连接的设备。

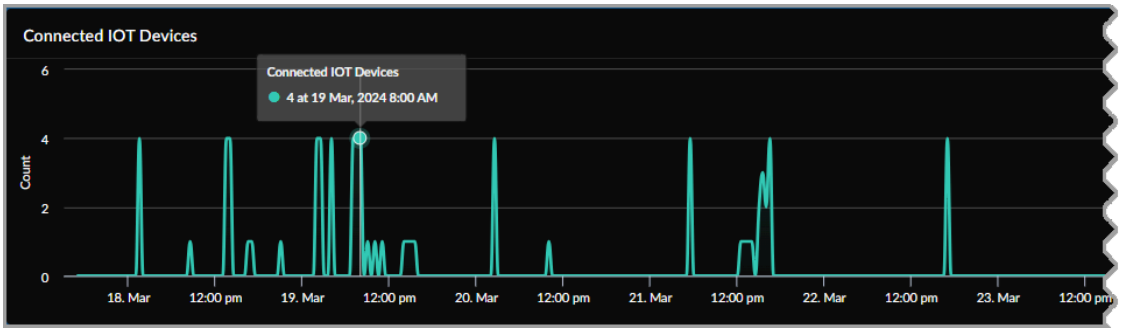


联网 IoT 设备

已连接的物联网设备 显示按 时间范围过滤的连接设备数量。通过从 添加过滤器 下拉菜单中选择其他过滤选项来定制显示的数据。

- 类别 — 此设备所属的类别。
- **Mac** 地址— 设备的 MAC 地址。
- 配置文件 — 设备配置文件。
- 供应商 — 设备供应商。
- 源 **IP**— 设备的 IP 地址。
- **Prisma Access** 位置— 设备的 Prisma Access 位置。
- 分支站点— 设备所在的分支站点。

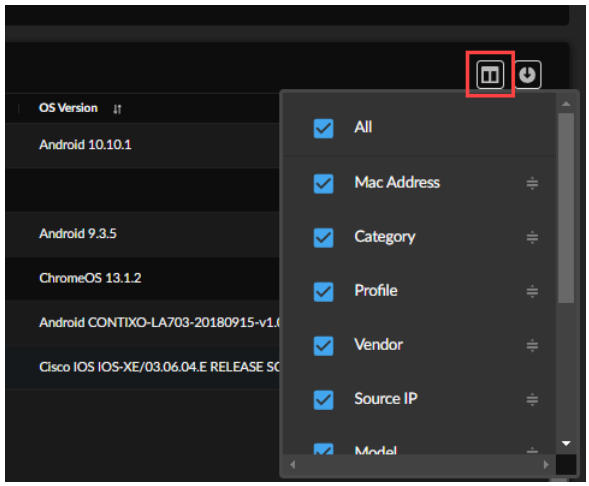
将鼠标悬停在图表中的某个点上可以查看特定时间的用户数量。了解特定时间段内的用户趋势可以帮助您监控使用情况并调查任何异常模式。



 ©2025 Palo Alto Networks, Inc.

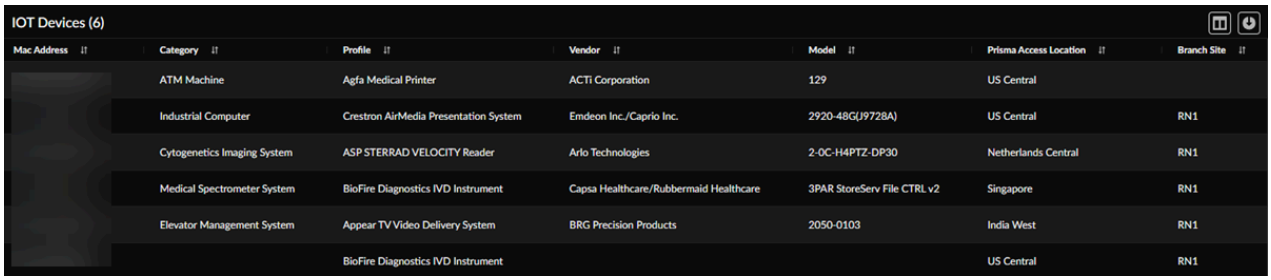
IoT 设备

查看选定 时间范围内连接的物联网设备数量。使用列下拉菜单来选择或取消选择表中显示的列。



- **Mac** 地址— 设备的 MAC 地址。
- 类别 — 此设备所属的类别。
- 配置文件 — 设备配置文件。
- 供应商 — 设备供应商。
- 源 **IP** — 设备的 IP 地址。
- 型号— 设备型号。
- 操作系统版本— 操作系统版本。
- 操作系统系列 — 设备所属的操作系统系列。
- **Prisma Access** 位置— 使用的 Prisma Access 位置。
- 分支站点— 设备所在的分支站点。

下面的物联网设备表显示了自定义的列选择。要显示表中的所有列，请在下拉菜单中选择所有选项。



查看和监控远程浏览器隔离

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 5.0 创新

©2025 Palo Alto Networks, Inc.

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	

您可以使用 Strata Cloud Manager 全面了解您的网络流量，并使用 Strata Cloud Manager 的监控和工作流部分实现远程浏览器隔离 (RBI)。通过查看活动 RBI 用户数量、趋势、连接状态、RBI 位置状态、流量测量和许可证消耗等指标，了解您的 RBI 部署。通过查看有关用户的数据，您可以全面了解部署的运行状况和连接性。

RBI 将用户的互联网浏览活动重定向到由 RBI 提供商托管的隔离环境。隔离环境中会为用户显示该网站，用户可以查看所需的资源，而无需直接从他们的设备和网络访问未知或有危险的网站。Prisma Access 可轻松与 RBI 提供商集成，实现此类浏览器重定向。

 ©2025 Palo Alto Networks, Inc.

Prisma Access 和自主 DEM

哪里可以使用？	需要提供什么？
• Strata Cloud Manager Managed Prisma Access • Panorama Managed Prisma Access	❑ Prisma Access 许可证 ❑ Autonomous DEM 许可证

开始使用 Prisma Access 中的自主 DEM，持续监控 SASE 环境中所有用户、应用程序和远程站点的数字体验。只要您拥有相应的许可证，就可以为连接到 Prisma Access 的 GlobalProtect 移动用户启用自主 DEM。

- 速查表：Prisma Access 的 ADEM
- 开始使用自主 DEM
- 使用自主 DEM 监控用户流量和应用程序

©2025 Palo Alto Networks, Inc.

©2025 Palo Alto Networks, Inc.

Prisma Access 基于用户的策略

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • Cloud Identity Engine	• Prisma Access 许可证

Prisma Access 要求您配置 IP 地址到用户名的映射，以便对移动用户和远程网络位置的用户一致地强制实施基于用户的策略。此外，如果您希望根据组成员资格强制实施策略，则需要配置用户名到用户组的映射。

要在 Panorama 中创建和配置策略时从下拉列表中选择组，还可以配置 Panorama 以获取从用户名到用户组映射中检索的用户组列表。

以下各节提供了在 Prisma Access 中配置和实施 User-ID 以及使用 Cloud Identity Engine 获取 IP 地址到用户名和用户名到用户组映射的概述和执行步骤。

为 Prisma Access 配置基于用户的策略

- Strata Cloud Manager
- Panorama

©2025 Palo Alto Networks, Inc.

Prisma Access 基于用户的策略 (Strata Cloud Manager)

将 Cloud Identity Engine 与 Prisma Access 集成后，您必须确认 Prisma Access 已连接到 Cloud Identity Engine，并且 Cloud Identity Engine 将会与 Prisma Access 共享目录信息。

检查您是否可以在 Prisma Access 中看到您的目录。

转到 **Manage**（管理） > **Configuration**（配置） > **NGFW** 和 **Prisma Access** > **Identity Services**（身份服务） > **Cloud Identity Engine**。

验证您是否可以将用户和组添加到策略规则。

选择 **Manage**（管理） > **Configuration**（配置） > **NGFW** 和 **Prisma Access** > **Security Services**（安全服务） > **Decryption**（解密）。

在安全或解密策略规则中，检查 **Users**（用户）下拉列表是否显示您的 Active Directory 用户和组条目。现在，您可以开始将这些用户和组添加到安全和解密策略规则中。

确认 Cloud Identity Engine 成功连接后，您可以开始运行用户活动报告，以更好地了解用户群的行为。

©2025 Palo Alto Networks, Inc.

Prisma Access 基于用户的策略 (Panorama)

本节提供为 Prisma Access 配置 User-ID 所需执行的步骤。

STEP 1 | 为移动用户和远程网络位置的用户配置 IP 地址到用户名的映射。

- 对于移动用户—GlobalProtect 部署，Prisma Access 中的 GlobalProtect 代理会自动执行 User-ID 映射。
- 对于远程网络中的用户，为远程网络部署配置 User-ID，以将 IP 地址映射到用户 ID。

STEP 2 | 为移动用户和远程网络位置的用户配置用户名到用户组的映射。

对于移动用户—GlobalProtect、显式代理和远程网络部署，为 Cloud Identity Engine 配置目录同步组件，以从 Active Directory (AD) 检索用户和组信息；然后，在移动用户—GlobalProtect 或远程网络部署中配置 **Group Mapping Settings**（组映射设置）。

或者，您可以使用 LDAP 服务器配置文件为移动用户和远程网络用户启用用户名到用户组的映射。



我们建议在 *LDAP* 服务器配置文件中使用组包含列表，这样您就可以指定要检索的组，而不是检索所有组信息。

STEP 3 | 通过完成以下操作之一，允许 Panorama 在安全策略中使用用户名到用户组映射：

- 为 Cloud Identity Engine 配置目录同步组件，以从 Active Directory (AD) 检索用户和组信息；然后，在移动用户—GlobalProtect、移动用户—显式代理或远程网络部署中配置 **Group Mapping Settings**（组映射设置）。
- 通过为组指定完整的专有名称 (DN) 配置基于组的策略。

STEP 4 | 将 HIP 信息重新分发到 Panorama。

©2025 Palo Alto Networks, Inc.

将 Cloud Identity Engine 与 Prisma Access 集成

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证

- Strata Cloud Manager
- Panorama

将 Cloud Identity Engine 与 Prisma Access (Strata Cloud Manager) 集成

Cloud Identity Engine（目录同步）为 Prisma Access 提供对 Active Directory 信息的只读访问权限，以便您可以轻松设置和管理用户和组的安全和解密策略。

Cloud Identity Engine 可与本地 Active Directory 和 Azure Active Directory 配合使用。

要使用 Prisma Access 设置 Cloud Identity Engine，首先，请转到中心以激活 Cloud Identity Engine，并将其添加到 Prisma Access。然后转到 Prisma Access 以验证 Prisma Access 能够访问目录数据。

 ©2025 Palo Alto Networks, Inc.



STEP 1 | 激活 Cloud Identity Engine

Cloud Identity Engine 可以与中心上任何受支持的应用程序共享 Active Directory 信息。它是免费的，不需要授权代码即可开始使用。Cloud Identity Engine 设置包括激活中心上的 Cloud Identity Engine 应用程序，配置 Cloud Identity Engine 代理以收集 Active Directory 映射，以及配置 Cloud Identity 和代理之间的相互身份验证。

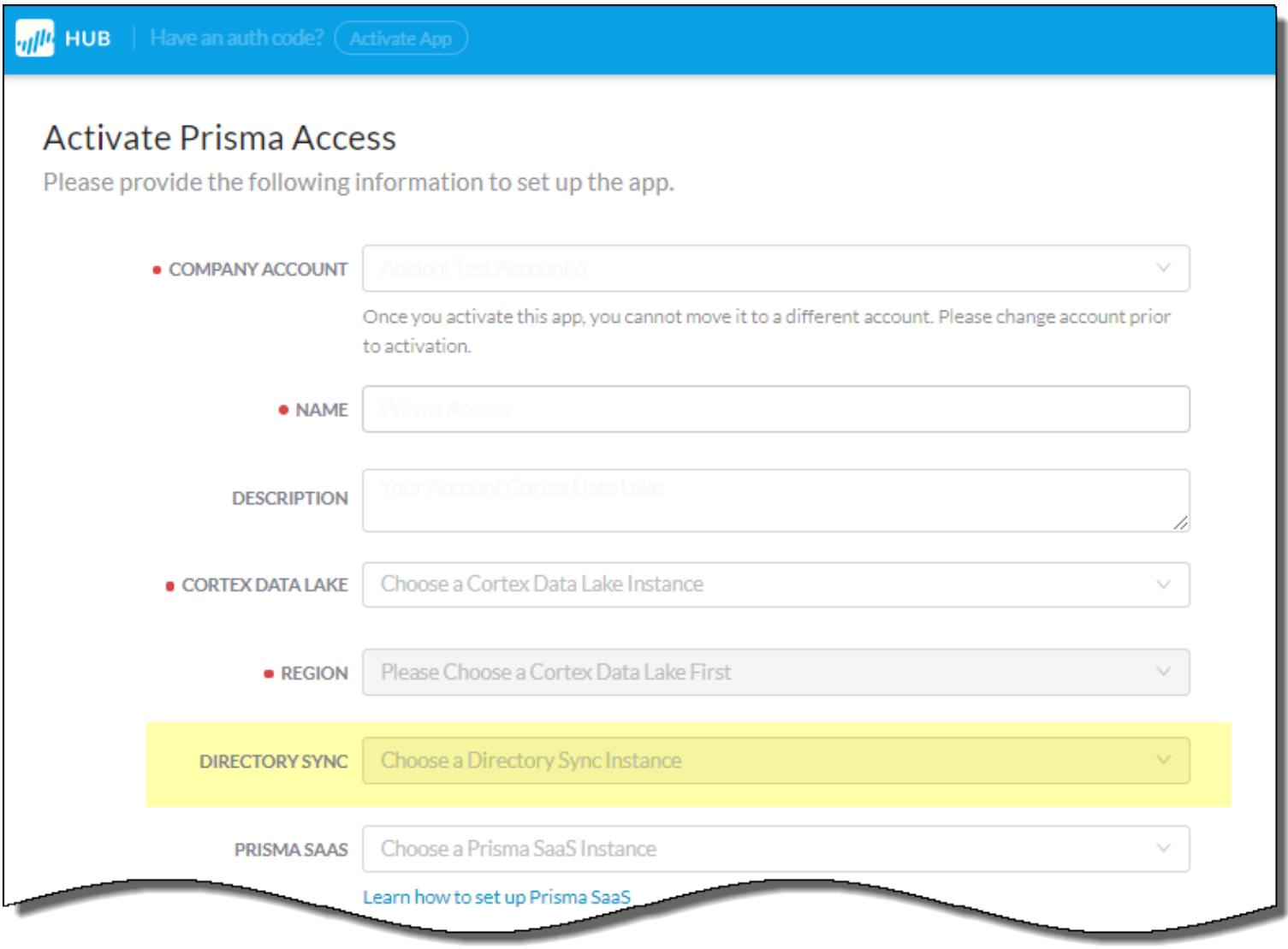
确保在部署 Prisma Access 和 Strata Logging Service 的同一区域中部署 Cloud Identity Engine 实例。

 ©2025 Palo Alto Networks, Inc.

STEP 2 | 为 Prisma Access 启用 Cloud Identity Engine。

您可以在首次激活 Prisma Access 时或之后的任何时间将 Prisma Access 与 Cloud Identity Engine 关联：

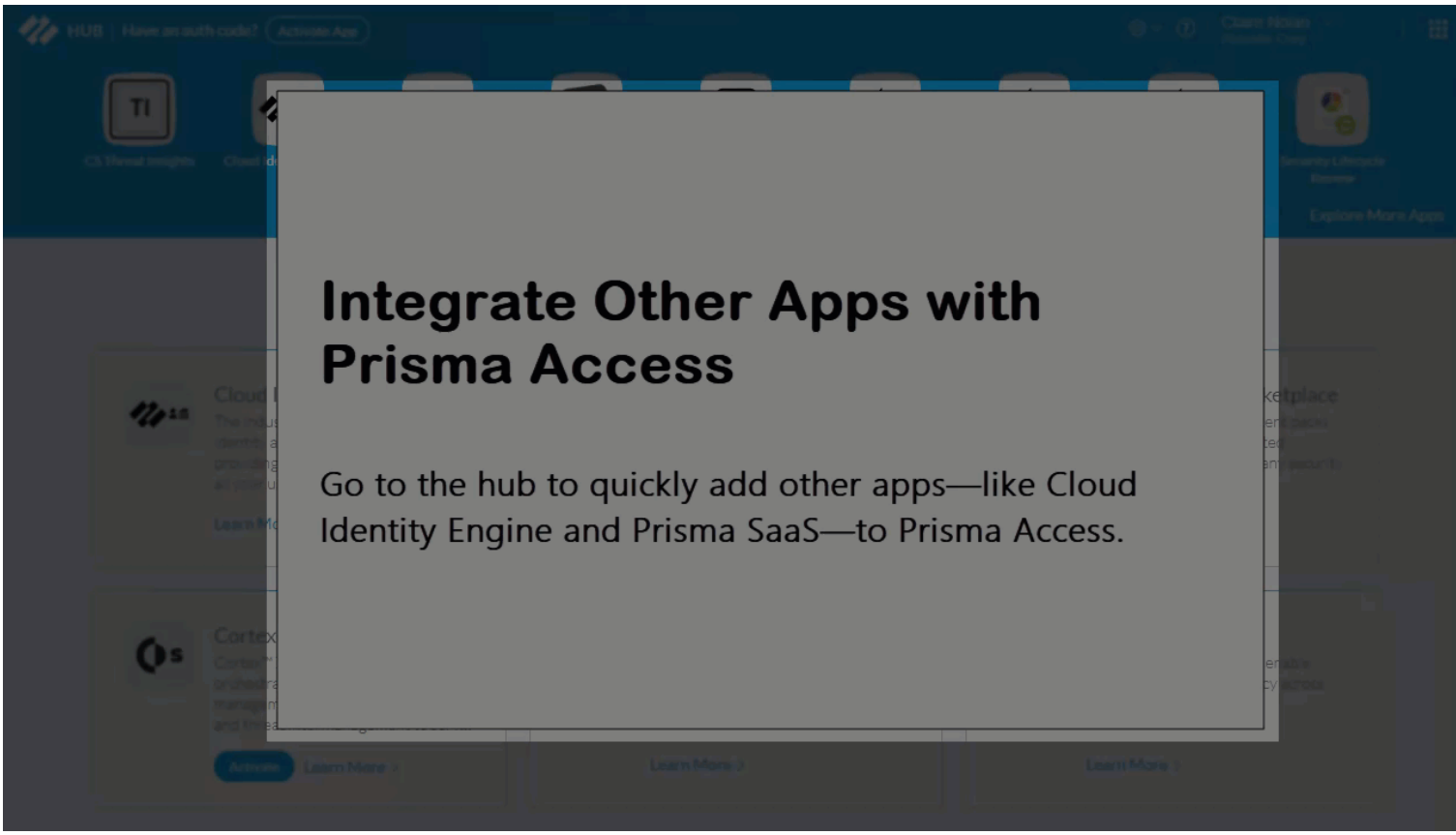
- 激活 **Prisma Access** 时：首次激活 Cloud Managed Prisma Access 时，您可以选择 Prisma Access 要使用的 Cloud Identity Engine 实例。请确保选择与 Prisma Access 部署在同一区域的实例。



- 激活 **Prisma Access** 后：要为现有 Prisma Access 实例启用 Cloud Identity Engine，请登录到中心。从中心设置选项卡（请参阅顶部菜单栏上的齿轮）中，选择 **Manage Apps**（管理

 ©2025 Palo Alto Networks, Inc.

应用程序）。找到要更新的 Prisma Access 实例，然后选择 Prisma Access 要使用的 Cloud Identity Engine 实例。



STEP 3 | 确认 Prisma Access 已连接到 Cloud Identity Engine。

将 Cloud Identity Engine 与 Prisma Access (Panorama) 集成

Prisma Access 从您组织的云目录或 Active Directory (AD) 检索用户和组信息，以实施基于用户和基于组的策略。（可选） Prisma Access 从某些云目录供应商（如 Azure Active Directory）检索基于用户行为的风险信号，以强制执行自动安全操作。可以使用 Cloud Identity Engine 简化用户和组信息的检索。

除了简化用户和组信息的检索之外，将 Cloud Identity Engine 与 Prisma Access 进行集成还可以释放您的云目录或 AD 的带宽并减轻其负载。

通过完成以下步骤，可使用 Cloud Identity Engine 检索适用于移动用户和/或远程网络的 Prisma Access 的用户和组信息。

Cloud Identity Engine 与 Prisma Access 的集成在实施方面存在以下限制：

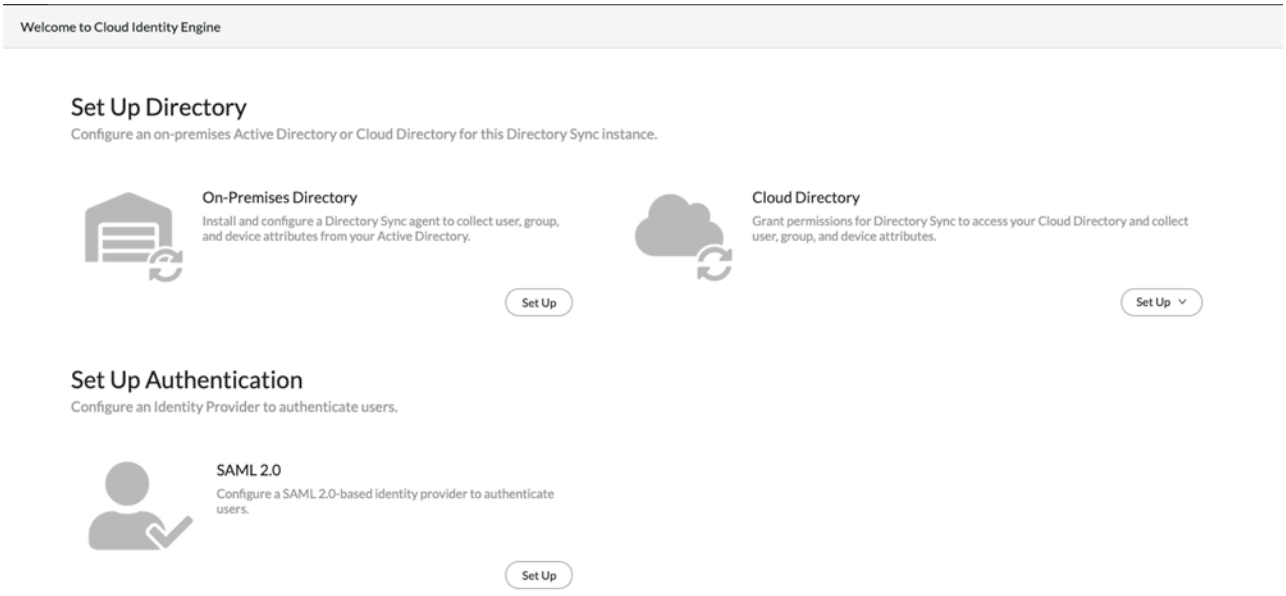
 ©2025 Palo Alto Networks, Inc.

- 确保您用于 Cloud Identity Engine 的组不包含以下任何特殊字符，因为 Prisma Access 不支持在组中使用以下特殊字符，否则提交操作将失败：
  - "（双引号）
  - '（撇号）
  - <（小于号）
  - >（大于号）
  - &（与号）
- 如果将 Cloud Identity Engine 与 Prisma Access 关联，则用户名必须使用 NetBIOS 格式（该格式包含域）。指定用户名时，可以采用电子邮件格式 (*username*@*domain*)、**NetBIOS \sAMAccountName** 格式或用户主体名称 (UPN) 格式 (*username*@*domain*.com)。
- 以 **distinguishedName** 格式输入组名称（例如，**CN=Users,CN=Builtin,DC=Example,DC=com**）。
- Cloud Identity Engine 不会应用您在组包含列表（**Device**（设备） > **User Identification**（用户标识） > **Group Mapping Settings**（组映射设置） > **Group Include List**（组包含列表））中指定的任何设置；而是从您的整个配置中检索用户和组信息，包括所有设备组和模板中使用的组。

STEP 1 | 为 Prisma Access 创建一个 Cloud Identity Engine 实例，然后记下实例名称。

激活 Cloud Identity Engine 后，它会创建一个实例。在后面的步骤中将 Cloud Identity Engine 与 Prisma Access 关联时，将使用该实例名称。（可选）如果需要为 Prisma Access 创建单独实例，请创建该实例并记下实例名称。

STEP 2 | 配置 Cloud Identity Engine 以检索您的目录数据。



STEP 3 | （仅使用本地活动目录的部署）如果使用 Active Directory，请安装并配置 Cloud Identity Agent 以与您的本地 AD 进行通信，并配置 Cloud Identity Agent 与代理之间的相互身份验证。

 ©2025 Palo Alto Networks, Inc.

STEP 4 | 在 Prisma Access 中启用 Cloud Identity Engine。

1. 在管理 Prisma Access 的 Panorama 上，选择从用户名到用户组映射的设置选项卡。
   - 对于“移动用户—GlobalProtect”部署，选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Mobile Users—GlobalProtect**（移动用户—**GlobalProtect**），选择齿轮图标以编辑设置，然后选择 **Group Mapping Settings**（组映射设置）。
   - 对于“移动用户—显式代理”部署，选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Mobile Users—Explicit Proxy**（移动用户—显式代理），选择齿轮图标以编辑设置，然后选择 **Group Mapping Settings**（组映射设置）。
   - 对于远程网络部署，选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Remote Networks**（远程网络），选择齿轮图标来编辑设置，然后选择 **Group Mapping Settings**（组映射设置）。
2. 选择 **Enable Directory Sync Integration**（启用目录同步集成）以启用 Cloud Identity Engine 与 Prisma Access 的集成。
3. 输入以下信息：
   - 输入 **Primary Username**（主用户名）。此为必填字段。

     Primary Username（主用户名）属性控制日志和报告中使用的格式。如果主用户名属性为 **userPrincipalName** (UPN)，则所有日志和报告条目都会以该格式显示源用户。许多部署使用 UPN、**sAMAccountName** 或 **mail** 格式。如果您的组织使用其他属性，您可以在此处指定，以确保整个组织的日志记录和报告的一致性。

     如果将 Azure AD 或 Okta Directory 配置为 Cloud Identity Engine 中的身份提供商 (IdP)，请将 **Primary Username**（主用户名） 指定为 **userPrincipalName**。Prisma Access 支持与 Azure AD 和 Okta Directory 一起使用的 userPrincipalName (UPN) 属性。
   - （可选）输入 **E-Mail**（电子邮件）属性（例如 **mail**）。
   - （可选）如果您对用户使用备用名称属性，请输入这些属性。最多可以输入三个备用用户名（**Alternate User Name 1**（备用用户名 **1**）、**Alternate User Name 2**（备用用户名 **2**）和 **Alternate User Name 3**（备用用户名 **3**））。
4. 完成后单击 **OK**（确定）。

STEP 5 | 提交并推送您的更改（依次选择 **Commit**（提交） > **Commit and Push**（提交并推送））。

 ©2025 Palo Alto Networks, Inc.

检索 Prisma Access 的 User-ID 组映射

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama) • Cloud Identity Engine	• Prisma Access 许可证

在 Prisma Access 中配置 User-ID 映射后，您需要能够检索移动用户和远程网络用户的当前 username-to-user 组信息。在 Cloud Identity Engine 中配置组映射以执行 username-to-user 组映射时，这些用户组在安全策略规则中不可选。您可以将新一代防火墙配置为主设备，或者将 Cloud Identity Engine 配置为主设备来填充群组，以便可在安全策略规则下拉列表中将其选中。

- 云身份引擎
- 主设备
- 长格式专有名称条目

云身份引擎

除了使用 Cloud Identity Engine 检索用户和组信息之外，您还可以使用 Cloud Identity Engine 在安全策略规则中填充用户组名称。通过这种集成，无需为此目的配置内部部署或 VM 系列新一代防火墙作为主设备；但是，仍然支持主设备。

您还可以使用 Cloud Identity Engine 在 Panorama 管理的多租户部署中填充组名，而使用主设备时则无法做到这一点。

要使 Cloud Identity Engine 能够在安全策略规则中填充组名，请完成以下步骤。

STEP 1 | 在 Cloud Identity Engine 中，激活 Cloud Identity Engine 并添加 本地 或基于云的目录（如果您尚未这样做）。

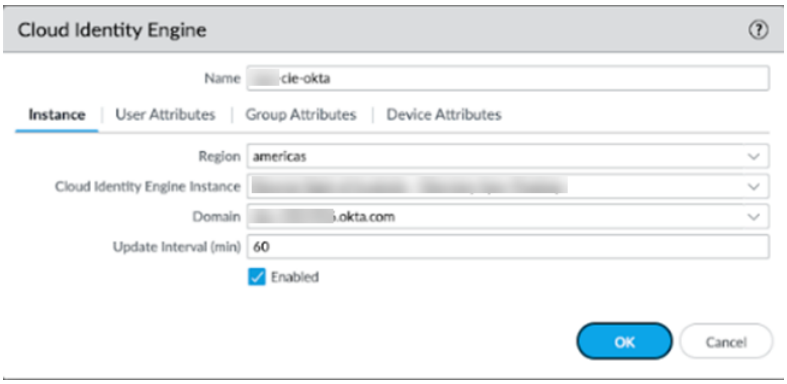
©2025 Palo Alto Networks, Inc.

STEP 2 | 将 Cloud Identity Engine 配置为映射源。

1. 从管理 Prisma Access 的 Panorama，选择 **Panorama** > **User Identification**（用户身份）> **Cloud Identity Engine**，然后 **Add**（添加）配置文件。
2. 对于 **Instance**（实例），指定以下参数：
   - **Region**（区域）— 为您的租户选择区域端点。

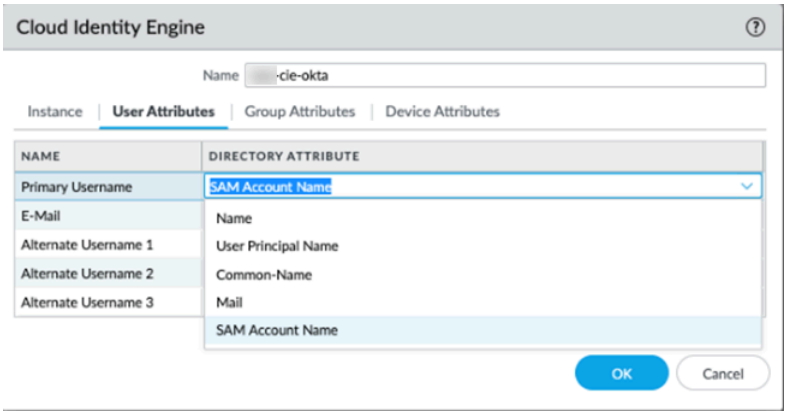
     您选择的区域必须与激活云身份引擎租户时选择的区域匹配。

   - **Cloud Identity Engine Instance**（**Cloud Identity Engine** 实例）— 选择要与配置文件关联的 Cloud Identity Engine 实例。
   - **Domain**（域）— 选择包含要使用目录的域。
   - **Update Interval (min)**（更新间隔（分钟））— 输入您希望 Panorama 在从 Cloud Identity Engine 应用程序到 Panorama 的更新之间等待的分钟数（也称为刷新间隔）。默认值是 60 分钟，范围是 5-1440。
3. 验证配置文件是否 **Enabled**（已启用）。



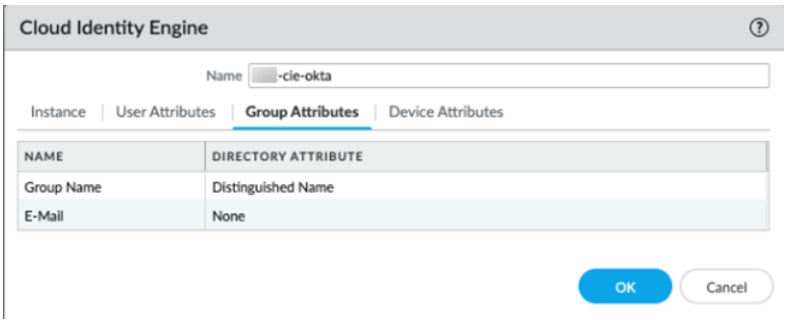
4. 对于 **User Attributes**（用户属性），选择 **Primary Username**（主用户名）的格式。您可以选择为电子邮件和备用用户名选择格式。如果用户使用多种用户名格式登录，则您最多可以配置三种备用用户名格式。

   当您在安全策略规则中查看用户时，用户名将以您在此处选择的主用户名格式显示。

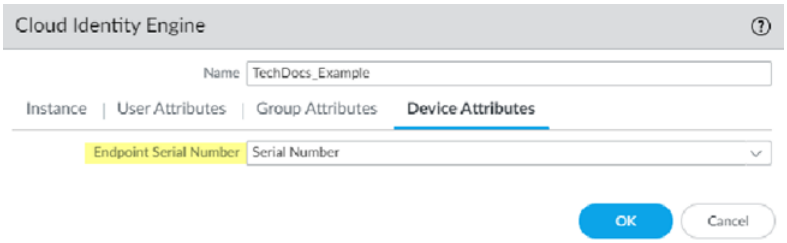


5. 对于 **Group Attributes**（组属性），选择 **Group Name**（组名称）的格式。

 ©2025 Palo Alto Networks, Inc.



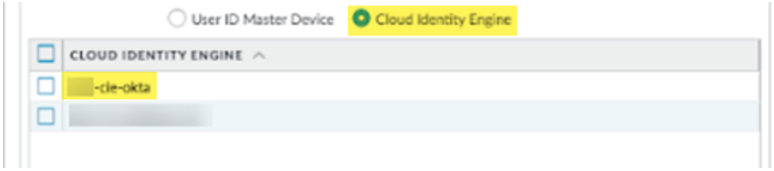
6. 将设备属性保留为无。



7. 单击确定，然后提交并推送您的更改。

STEP 3 | 将您的个人资料附加到您的 Prisma Access 配置。

1. 转到您要添加的部署的设置。
   - 对于移动用户 — GlobalProtect 部署，选择 **Panorama** > 云服务 > 配置 > 移动用户 — **GlobalProtect**，然后单击齿轮以编辑设置。
   - 对于移动用户 — 显式代理部署，选择 **Panorama** > 云服务 > 配置 > 移动用户 — 显式代理，然后单击齿轮以编辑设置。
   - 对于移动用户 - 远程网络部署，选择 **Panorama** > 云服务 > 配置 > 移动用户 - 远程网络，然后单击齿轮以编辑设置。
2. 选择 **Cloud Identity Engine**（云身份引擎）。
3. 选择您创建的 Cloud Identity Engine 配置文件。



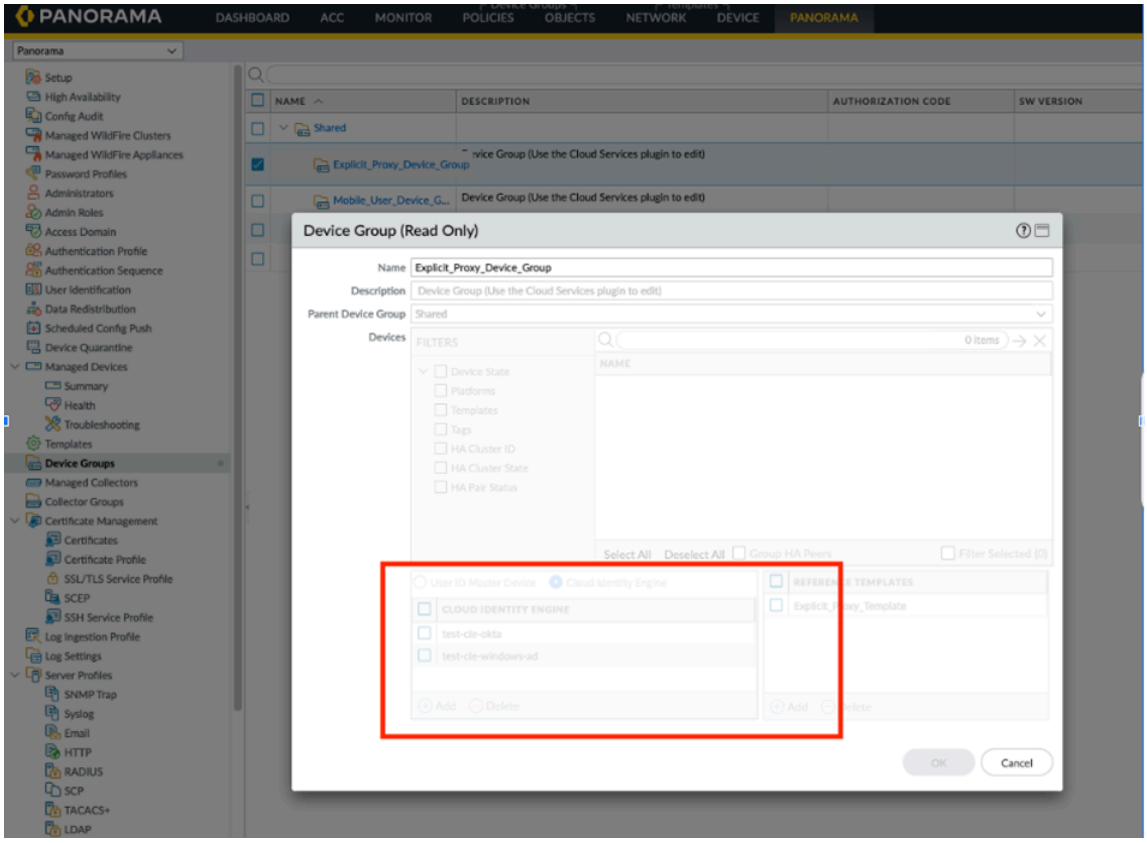
STEP 4 | 选择 **Commit**（提交） > **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

©2025 Palo Alto Networks, Inc.

STEP 5 | 验证 Prisma Access 是否具有来自云身份引擎的映射信息。

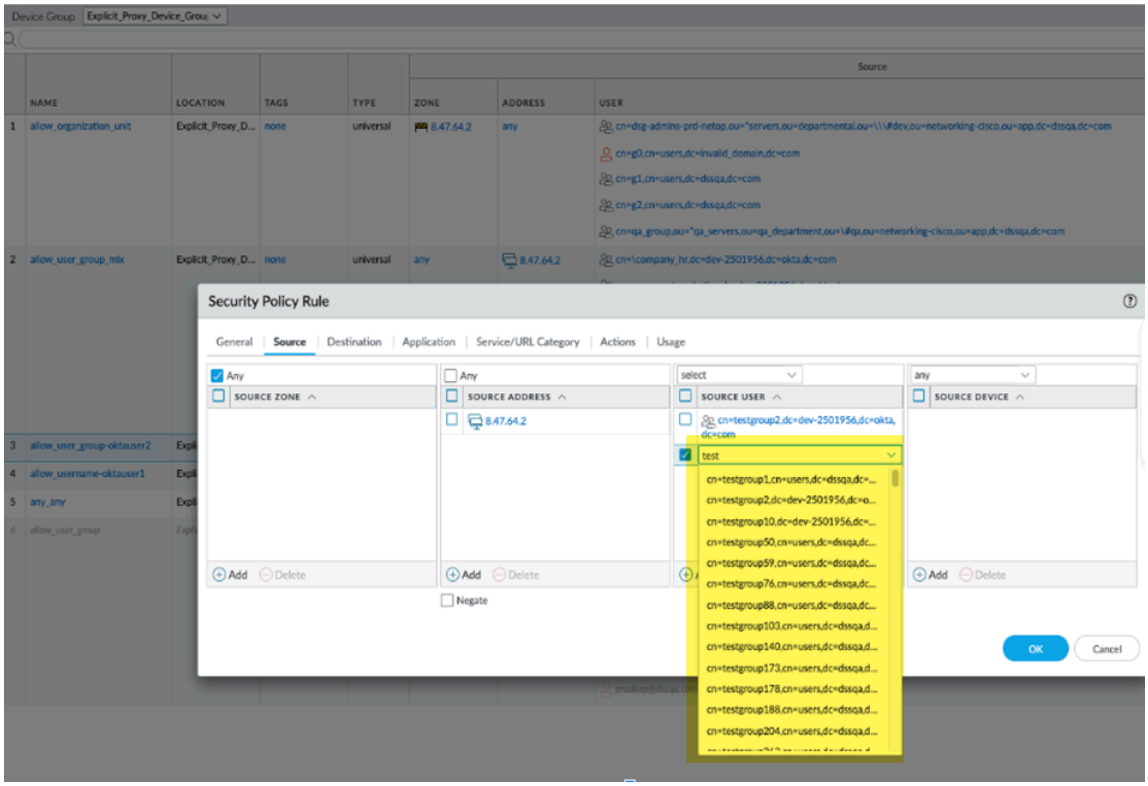
1. 选择 **Panorama** > 设备组 > ***<template-name>***，其中 *<template-name>* 是您正在配置的部署的模板，并验证 Cloud Identity Engine 配置文件是否附加到设备组。

   以下示例显示设备组已成功附加到 Explicit_Proxy_Device_Group。



2. 选择对象 > 安全 > 预规则，添加安全策略规则，并验证组是否填充在用户区域中。

©2025 Palo Alto Networks, Inc.



主设备

虽然在 Cloud Identity Engine 中配置组映射会执行用户名到用户组的映射，但这些用户名和用户组不会填充到安全策略中。要简化基于用户和组的策略的创建或修改，您可以使用主设备将组名称添加到安全策略规则的下拉列表中。您需要将防火墙指定为每个设备组的主设备。添加主设备后，设备组将继承在主设备上定义的所有策略;因此，它应该是要用于该设备组的独立专用设备。

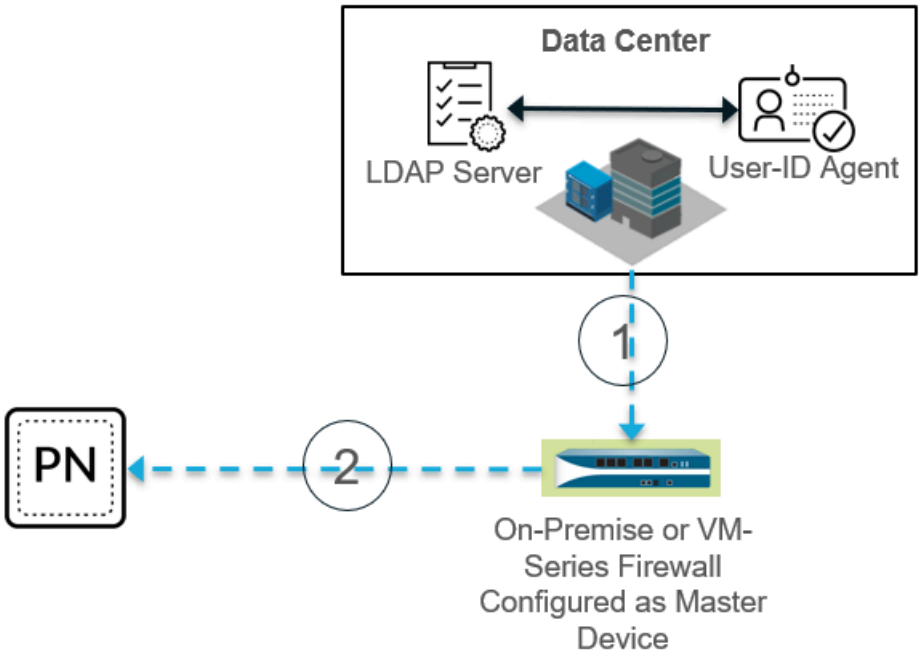
要允许在安全策略的下拉列表中选择组名称，Palo Alto Networks建议您为每个设备组指定一个 **Master Device**（主设备）。您可以将本地防火墙或 VM 系列防火墙配置为主设备。

下图显示了管理员已将本地设备配置为**Master Device**（主设备）的 User-ID 部署。图中的标注显示了该过程。

1. 管理员已配置为主设备的新一代本地或 VM 系列防火墙从数据中心的 LDAP 服务器和 User-ID 代理检索最新的用户名到用户组映射。
2. Panorama 从主设备获取用户名到用户组的映射。

   Panorama 仅在安全策略的下拉列表中填充组名时使用此映射，从而简化了基于组的策略创建。

©2025 Palo Alto Networks, Inc.



将本地或 VM 系列防火墙配置为主设备

使用以下过程将本地或 VM 系列防火墙配置为主设备。

每个设备组只能使用一个主设备;如果需要为不同的设备组配置主设备，则需要为每个设备组创建单独的主设备。

STEP 1 | 确保要用作主设备的设备由管理 Prisma Access 的同一 Panorama 管理。

您可以在 **Panorama** > **Managed Devices**（托管设备）下查看您的托管设备。

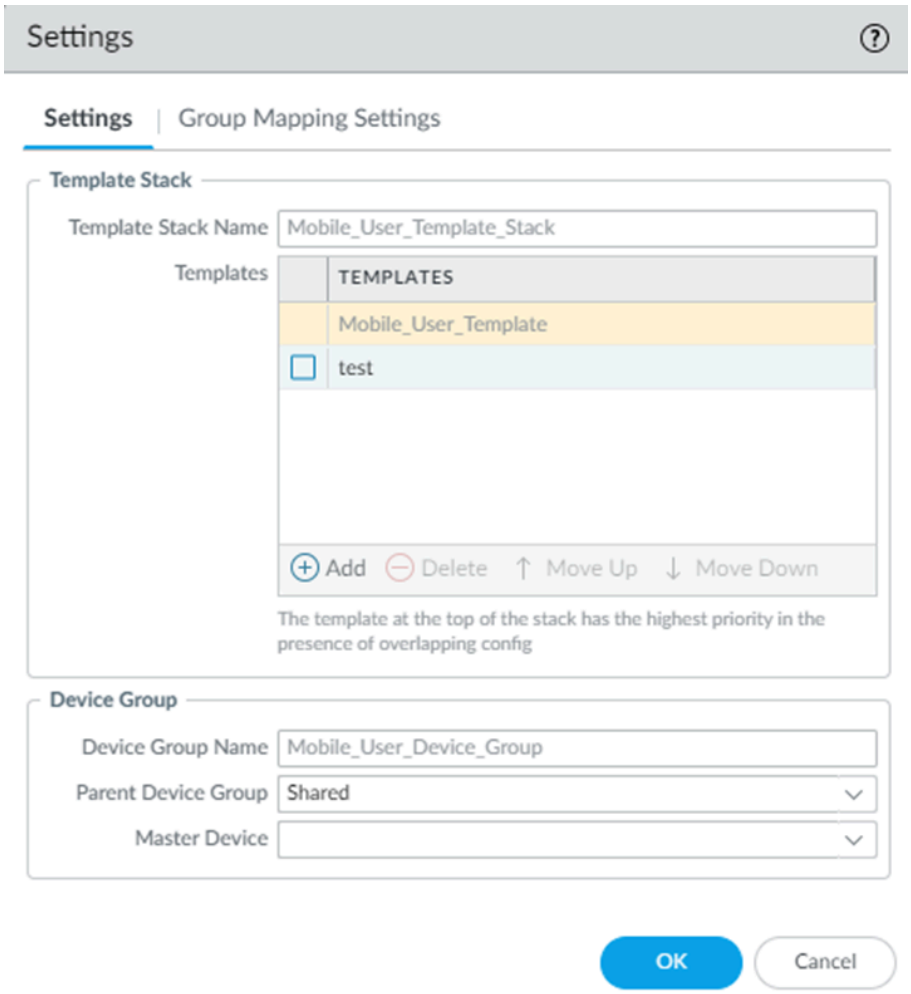
STEP 2 | 将主设备添加到 Prisma Access 移动用户或远程网络部署。

- 对于“移动用户—GlobalProtect”部署，选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Mobile Users—GlobalProtect**（移动用户—**GlobalProtect**），单

 ©2025 Palo Alto Networks, Inc.

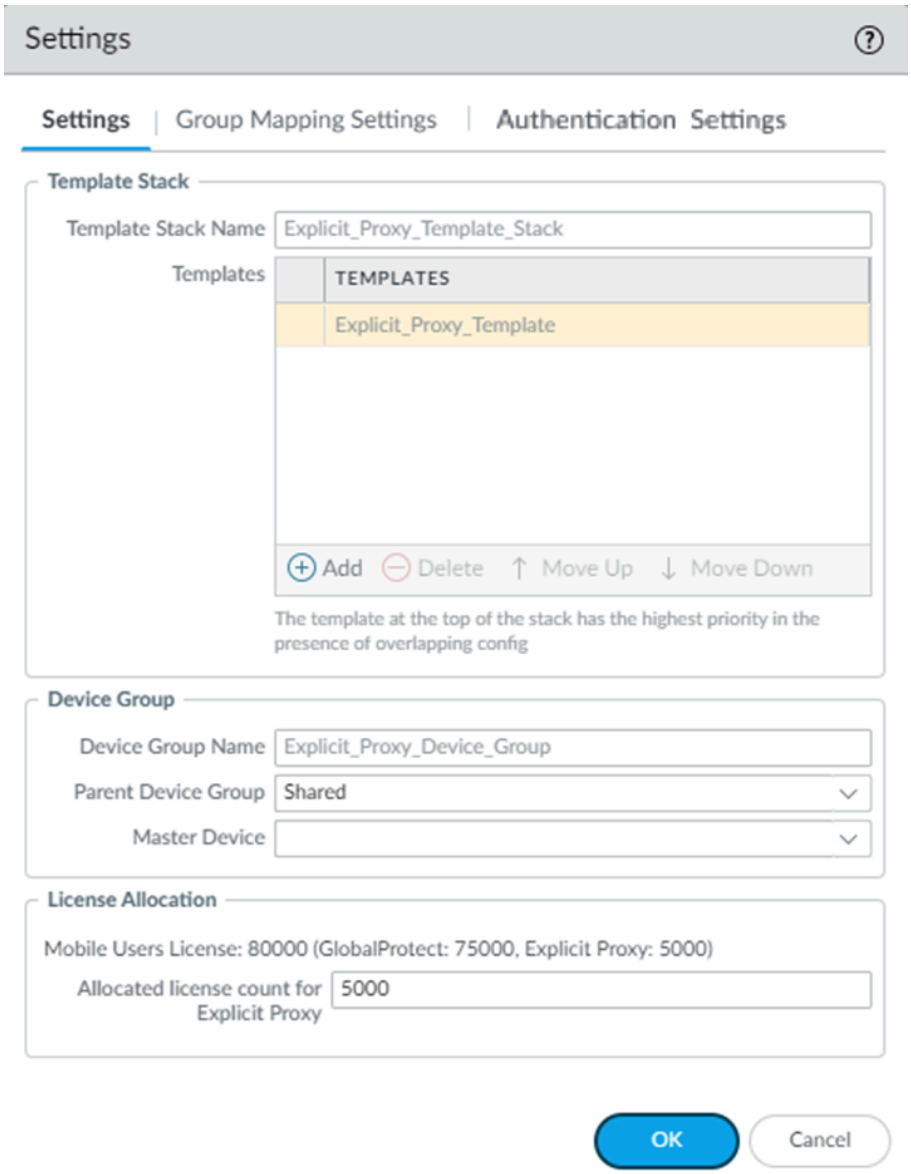
击 **Settings**（设置）的齿轮图标，然后选择要指定为 **Master Device**（主设备）的本地防火墙。

如果使用默认的 ***Device Group Name***（设备组名称）（本例中为 ***Mobile_User_Device_Group***）和 ***Parent Device Group***（父设备组）（本例中为 ***Shared***），则下拉选项中会显示与其他设备组不关联的所有设备。如果已将主设备与另一个设备组关联，请选择与该设备组关联的 ***Parent Device Group***（父设备组），并将其显示在下拉列表中。



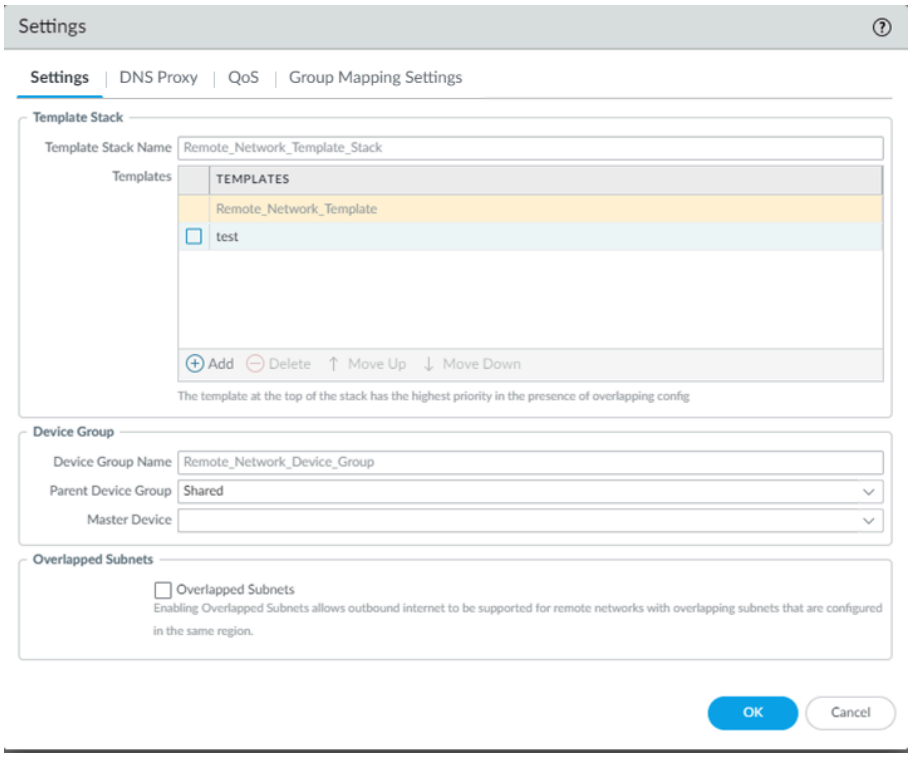
- 对于“移动用户—显式代理”部署，请选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Mobile Users—Explicit Proxy**（移动用户—显式代理），选择 **Settings**（设置）的齿轮图标，然后选择创建的 **Master Device**（主设备）。

©2025 Palo Alto Networks, Inc.



- 对于设备组具有远程网络连接的远程网络部署，请选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Remote Networks**（远程网络），单击 **Settings**（设置）的齿轮图标，然后选择创建的 **Master Device**（主设备）。

©2025 Palo Alto Networks, Inc.



Prisma Access 自动填充仅与主设备关联的设备组的用户名到用户组映射。对于本示例，自动填充仅发生在 ***Remote_Network_Device_Group*** 设备组中，不会填充到任何其他设备组。

STEP 3 | 单击 **OK**（确定）。

长格式专有名称条目

如果尚未将新一代防火墙配置为主设备，也未配置云身份引擎以在安全策略规则中填充用户和用户组信息，则可以在 Panorama 中使用长格式专有名称 (DN) 条目。Prisma Access 会使用这些 DN 条目来评估您在 Panorama 中配置的基于用户 ID 的策略。

例如，假设有一位名为 **Bob Alice** 的用户，在 IT 部门工作，工位在一楼。如果策略要应用于一楼的所有 IT 员工，则匹配安全策略可能包含 `cn=first_floor, ou=it_staff, dc=dev, dc=example, dc=com`；如果策略仅要应用于 Bob Alice，则匹配安全策略可能包含 `cn=Bob Alice, ou=it_staff, dc=dev, dc=example, dc=com`。

 ©2025 Palo Alto Networks, Inc.

身份重新分发

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证

为确保您始终如一地实施安全策略，Prisma Access 会在整个 Prisma Access 环境中共享 GlobalProtect 在本地发现的身份数据。Prisma Access 还可以与远程网络站点或服务连接站点（总部和数据中心）的本地设备共享身份数据。

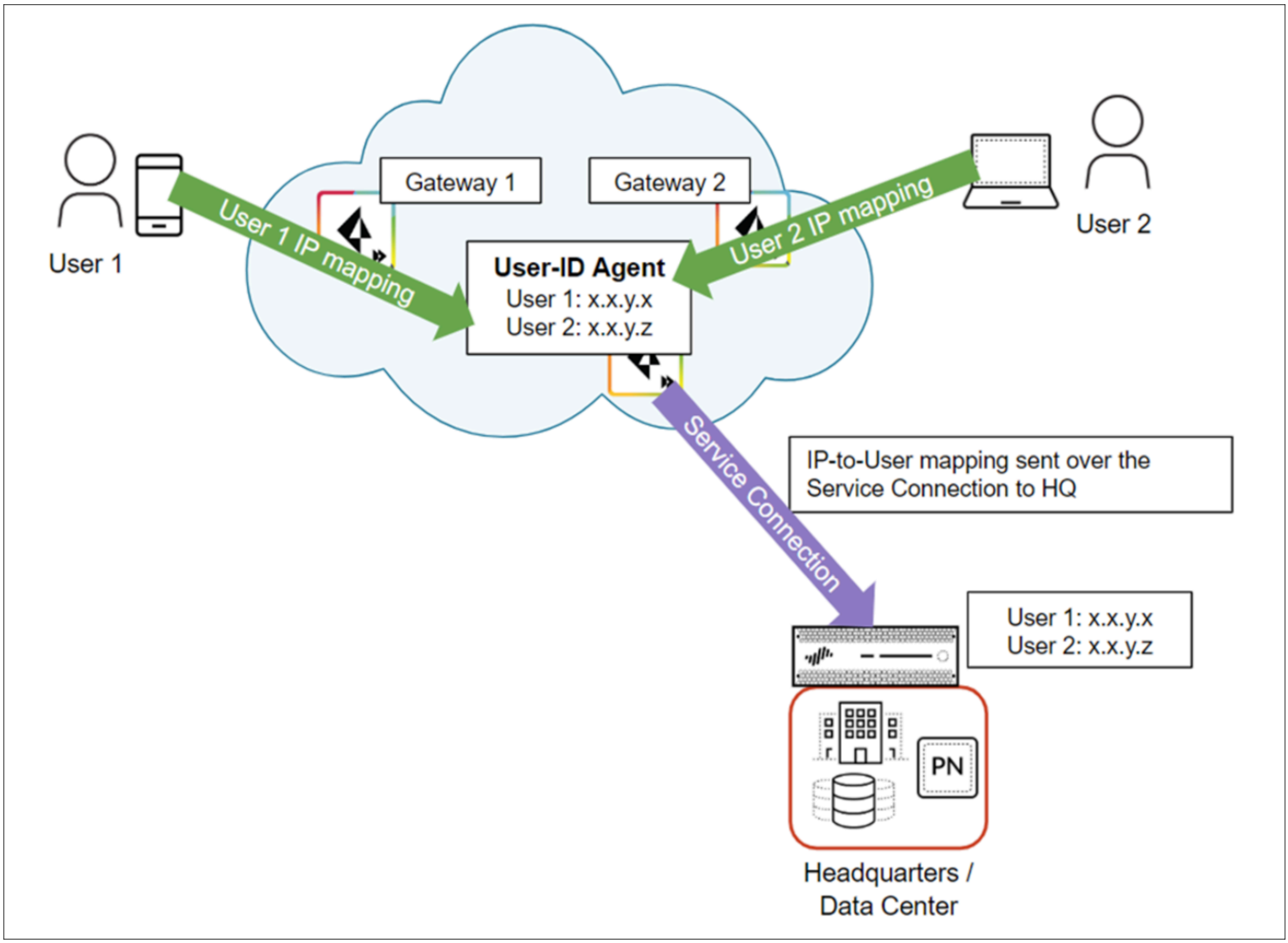
要让移动用户访问远程网络位置或总部/数据中心的资源，该资源由具有用户策略的设备提供保护，则必须将来自 Prisma Access 移动用户和远程网络用户的身份数据重新分配到该本地设备。

当用户连接到 Prisma Access 时， Prisma Access 会收集用户的身份数据并存储。

以下示例展示了两名移动用户，他们在 Prisma Access 中已有 IP 地址到用户名的映射关系。随后， Prisma Access 通过服务连接将此映射关系重新分发至用于保护总部/数据中心安全的本地设备。

Prisma Access (Managed by Strata Cloud Manager) 自动允许服务连接充当身份重新分发代理（也称为 User-ID 代理）。

©2025 Palo Alto Networks, Inc.



- Strata Cloud Manager
- Panorama

身份重新分配 (Strata Cloud Manager)

这样您就可以一致地执行安全策略，Prisma Access 共享 GlobalProtect 在整个 Prisma Access 环境中本地发现的身份数据。Prisma Access 还可以与远程网络站点或服务连接站点（总部和数据中心）的本地设备共享身份数据。

对于 Prisma Access (Managed by Strata Cloud Manager)，在默认情况下，我们启用了一些身份数据重新分发，对于剩余部分，我们简化了启用重新分发的配置（只需选中一个复选框即可选择要共享的数据）。

在“身份分发”指示板中，您可以查看身份数据的共享方式和管理数据重新分发（**Manage**（管理） > **Configuration**（配置） > **NGFW** 和 **Prisma Access** > **Identity Services**（身份服务））。

您可以重新分发的身份数据包括：

- HIP 数据

©2025 Palo Alto Networks, Inc.

- IP 地址到标签的映射
- IP 地址到用户的映射
- 用户到标签的映射
- 隔离的设备

开始进行身份重新分配：

- 设置身份重新分配
- 识别和隔离受影响的设备

设置身份重新分配

设置身份重新分配

确认服务连接设置。

如果您尚未为总部或数据中心设置服务连接，请先配置服务连接。Prisma Access 需要服务连接才能在您的环境中共享身份数据；Prisma Access 会自动将服务连接作为重新分发代理。当您看到新创建的服务连接站点已被分配 User-ID 代理地址（Prisma Access 会自动执行此操作，只需几分钟）时，该站点就已经准备就绪，可用作重新分发代理。



User-ID 重新分发管理 — 有时，对于规模特别大的 *Prisma Access* 部署，*User-ID* 重新分发需要进行精细控制。*User-ID* 重新分发管理允许您通过删除 ***User ID***（用户 ***ID***）列中的复选标记来手动禁用某些服务连接的默认标识重新分发行为，然后选择要用于标识重新分发的特定服务连接。对于大多数配置，无需执行此操作。请联系 *Palo Alto Networks* 支持部门以激活此功能。

转到 **Manage**（管理） > **Configuration**（配置） > **NGFW** 和 **Prisma Access** > **Identity Services**（身份服务） > **Identity Redistribution**（身份重新分发），将范围设置为 **Service Connections**（服务连接），以验证服务连接 User-ID 代理详细信息。

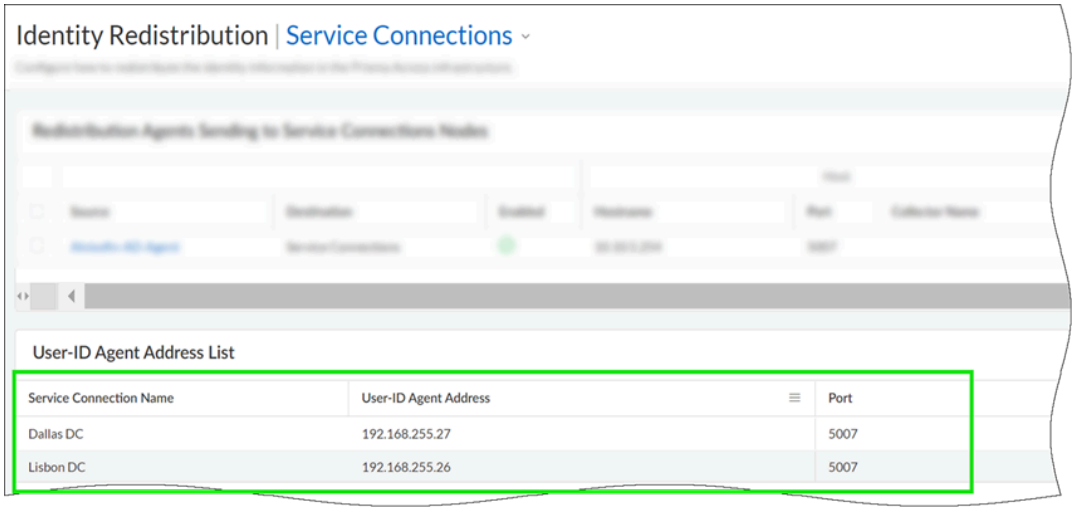
©2025 Palo Alto Networks, Inc.

将身份数据从 Prisma Access 发送到 本地设备

配置 Prisma Access 以将身份数据分发到本地设备只需要服务连接的 User-ID 代理信息。

转到 **Manage**（管理） > **Configuration**（配置） > **NGFW** 和 **Prisma Access** > **Identity Services**（身份服务） > **Identity Redistribution**（身份重新分发），将配置范围设置为 **Service Connections**（服务连接），以获取服务连接 User-ID 代理详细信息。

在 Panorama 或 Palo Alto Networks NGFW 上，使用这些详细信息来将 Prisma Access 配置为数据重新分发代理。



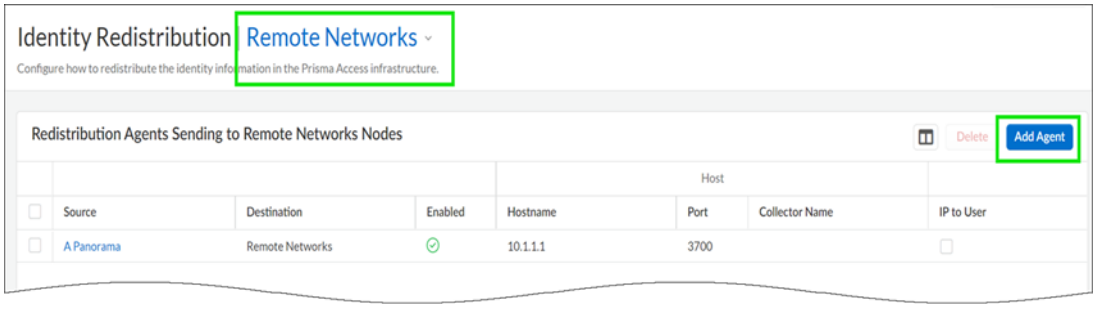
 ©2025 Palo Alto Networks, Inc.

将身份数据从本地设备发送到 Prisma Access

将本地设备作为重新分发代理添加到 Prisma Access；您添加的设备将能够向 Prisma Access 分发身份数据。

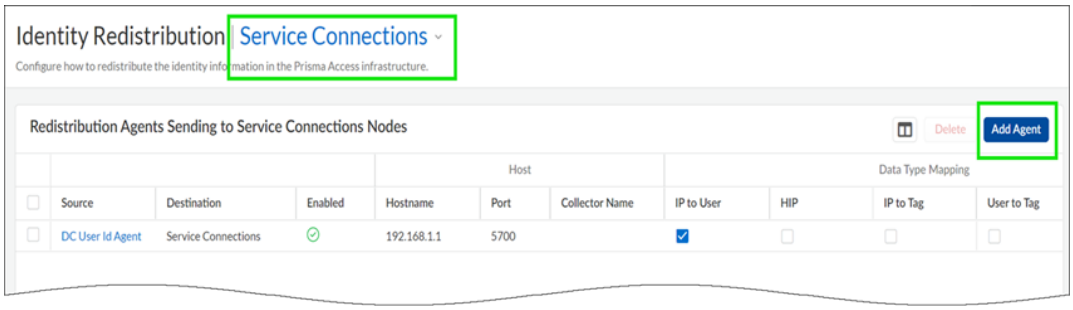
- 从远程网络站点的设备上：

  转到 **Identity Redistribution**（身份重新分配）指示板，将配置范围设置为 **Remote Networks**（远程网络），然后 **Add Agent**（添加代理）。除了指定主机详细信息外，还要选择设备与 Prisma Access 共享的数据类型。可选设置包括设备的名称和预共享密钥。



- 从服务连接站点的设备上：

  转到 **Identity Redistribution**（身份重新分配）指示板，将配置范围设置为 **Service Connections**（服务连接），然后 **Add Agent**（添加代理）。除了指定主机详细信息外，还要选择设备与 Prisma Access 共享的数据类型。可选设置包括设备的名称和预共享密钥。



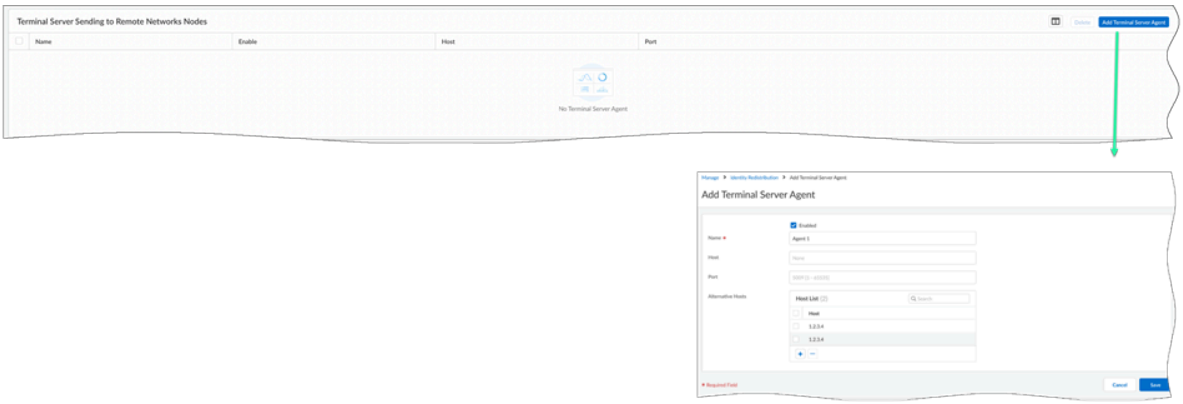
 ©2025 Palo Alto Networks, Inc.

为用户映射配置终端服务器代理。

终端服务器 (TS) 代理为每个用户分配一个端口范围，以便识别基于 Windows 的终端服务器上的特定用户。TS 代理通知 Prisma Access 分配的端口范围，这样，Prisma Access 就可以根据用户和用户组执行策略。

在 **Identity Redistribution**（身份重新分配）指示板上，将范围设置为 **Remote Networks**（远程网络），并在 **Terminal Server Sending to Remote Networks Nodes**（发送到远程网络节点的终端服务器）下 **Add Terminal Server Agent**（添加终端服务器代理）。

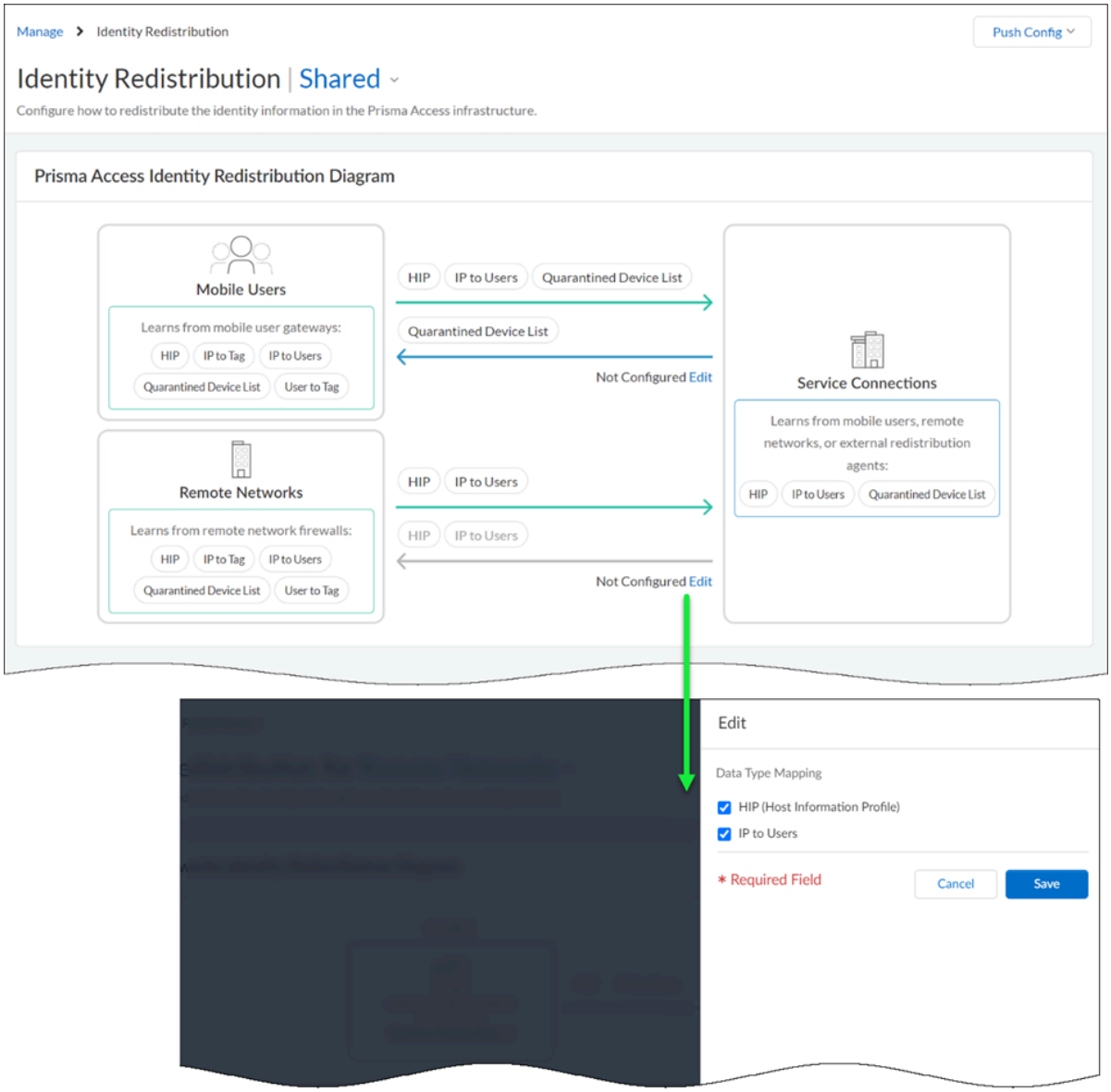
- 默认情况下，该配置为 **Enabled**（已启用）。
- 输入 TS 代理的 **Name**（名称）。
- 输入安装 TS 代理的 Windows **Host**（主机）的 IP 地址。
- 输入代理监听用户映射请求的 **Port**（端口）号。默认情况下，该端口设置为 5009。
- **Save**（保存）更改。



 ©2025 Palo Alto Networks, Inc.

在 Prisma Access 环境中分发身份数据。

在 **Identity Redistribution**（身份重新分发）指示板上，**Edit**（编辑）图表以指定要从每个来源收集并在 Prisma Access 上共享的身份数据。



要激活更改，请将配置推送到 Prisma Access。

身份重新分配 (Panorama)

配置 User-ID 后，您可以从 Prisma Access 将 IP 地址到用户名的映射重新分发到所有新一代防火墙（用于保护对网络资源的访问），从而一致地为所有移动用户和远程网络位置的用户执行基于用户的策略。使用以下方法之一将 IP 地址到用户名的映射从本地新一代防火墙重新分发到移动用户和远程网络中的用户，反之亦然：

- 将 User-ID 信息从 Prisma Access 重新分发到本地防火墙

©2025 Palo Alto Networks, Inc.

- 将 User-ID 信息从本地防火墙重新分发到 Prisma Access

将 User-ID 信息从 Prisma Access 重新分发到本地防火墙

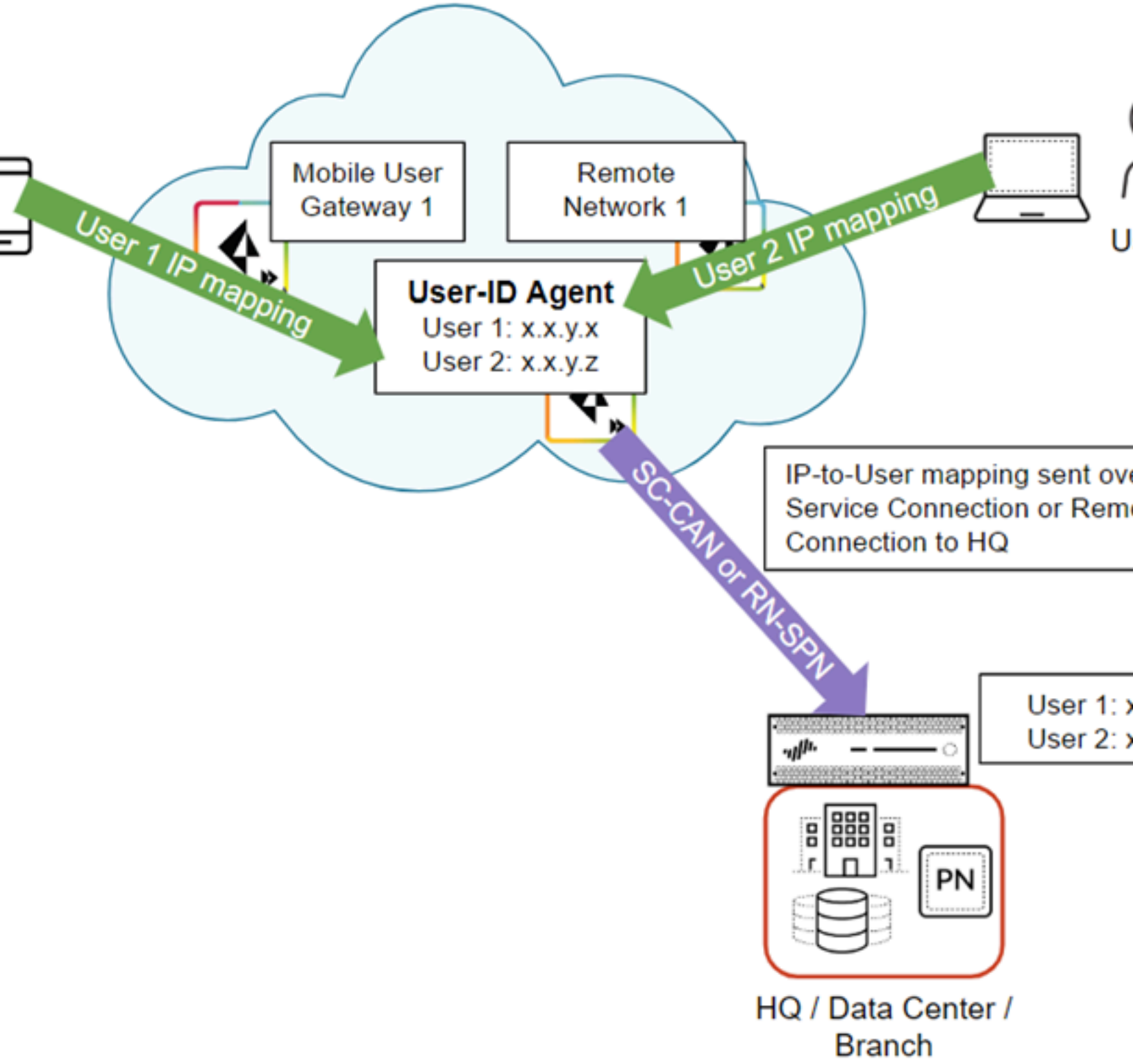
将 **User-ID** 信息从 **Prisma Access** 重新分发到本地防火墙。

如果移动用户需要访问远程网络位置或总部/数据中心的资源，并且该资源由具有基于用户的策略的本地新一代防火墙保护，则必须从 Prisma Access 移动用户和远程网络中的用户连接到本地防火墙。当用户连接到 Prisma Access 时，它会收集并存储此用户到 IP 地址映射。

下图展示了在 Prisma Access 中有现有 IP 地址到用户名映射的两个移动用户。然后，通过服务连接 (SC-CAN) 或远程网络连接 (RN-SPN)，Prisma Access 将此映射重新分发到保护总部/数据中心的本地防火墙。

Prisma Access 将服务连接或远程网络连接用作 *IPSec* 隧道，作为通往第 *3* 层网络的底层路径。对于专用地址的目标，您可以通过 *IPSec* 可信隧道使用任何路由路径来重新分发此映射。

 ©2025 Palo Alto Networks, Inc.



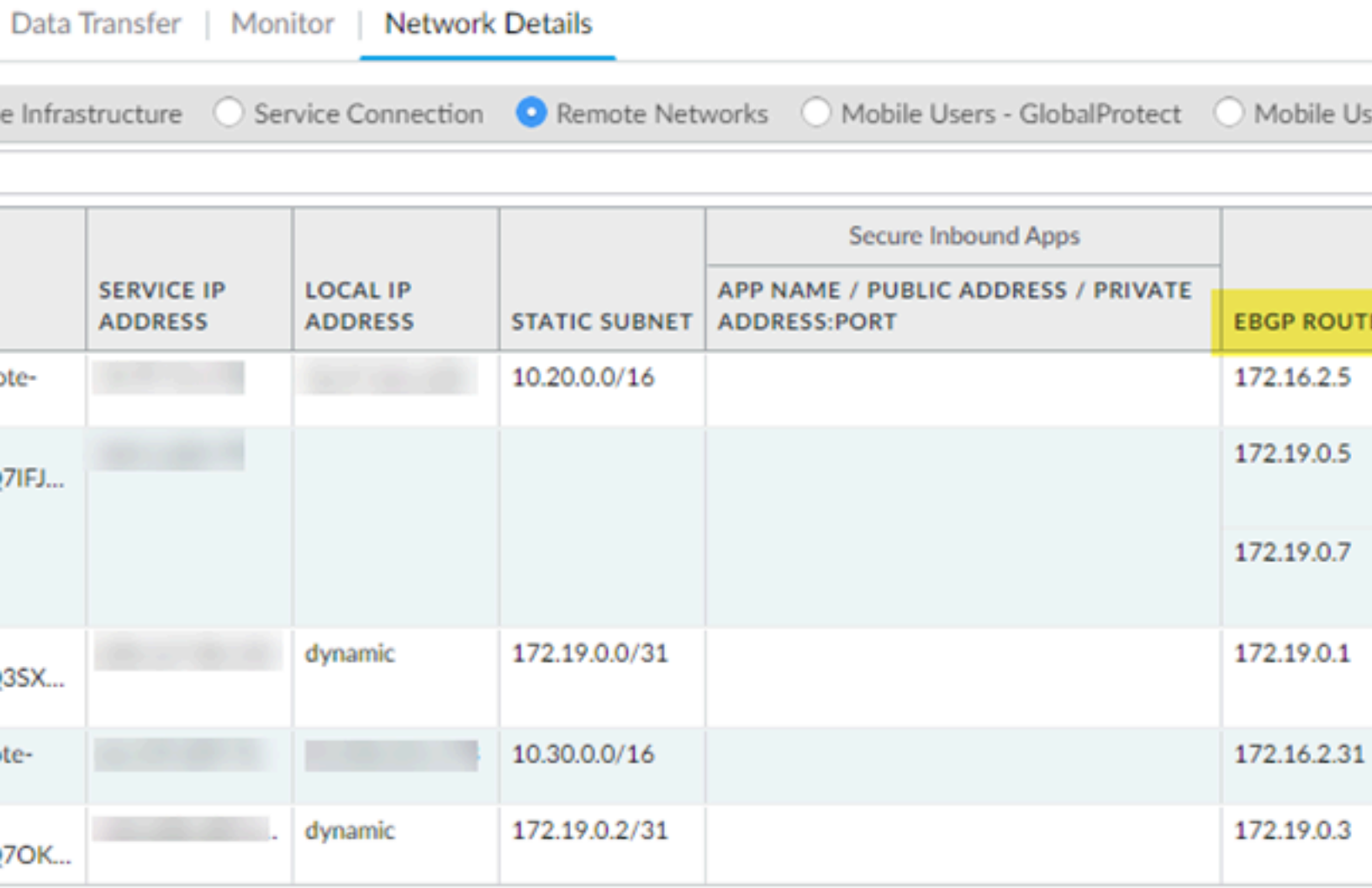
要从 Prisma Access 重新分发 User-ID 映射到本地防火墙，请完成以下步骤。

 ©2025 Palo Alto Networks, Inc.

确保不要在将用户身份重新分发到本地防火墙（*SC-CAN* 或 *RN-SPN*）的任何连接上应用任何 *SSL* 解密，包括重新分发路径中的任何防火墙。或者，您也可以对重新分发流量应用排除解密。

STEP 1 | 记下配置数据重新分发代理时要使用的 IP 地址。

- 对于远程网络连接，请找到 **EBGP Router**（**EBGP** 路由器）地址（**Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息） > **Remote Networks**（远程网络） > **EBGP Router**（**EBGP** 路由器））。



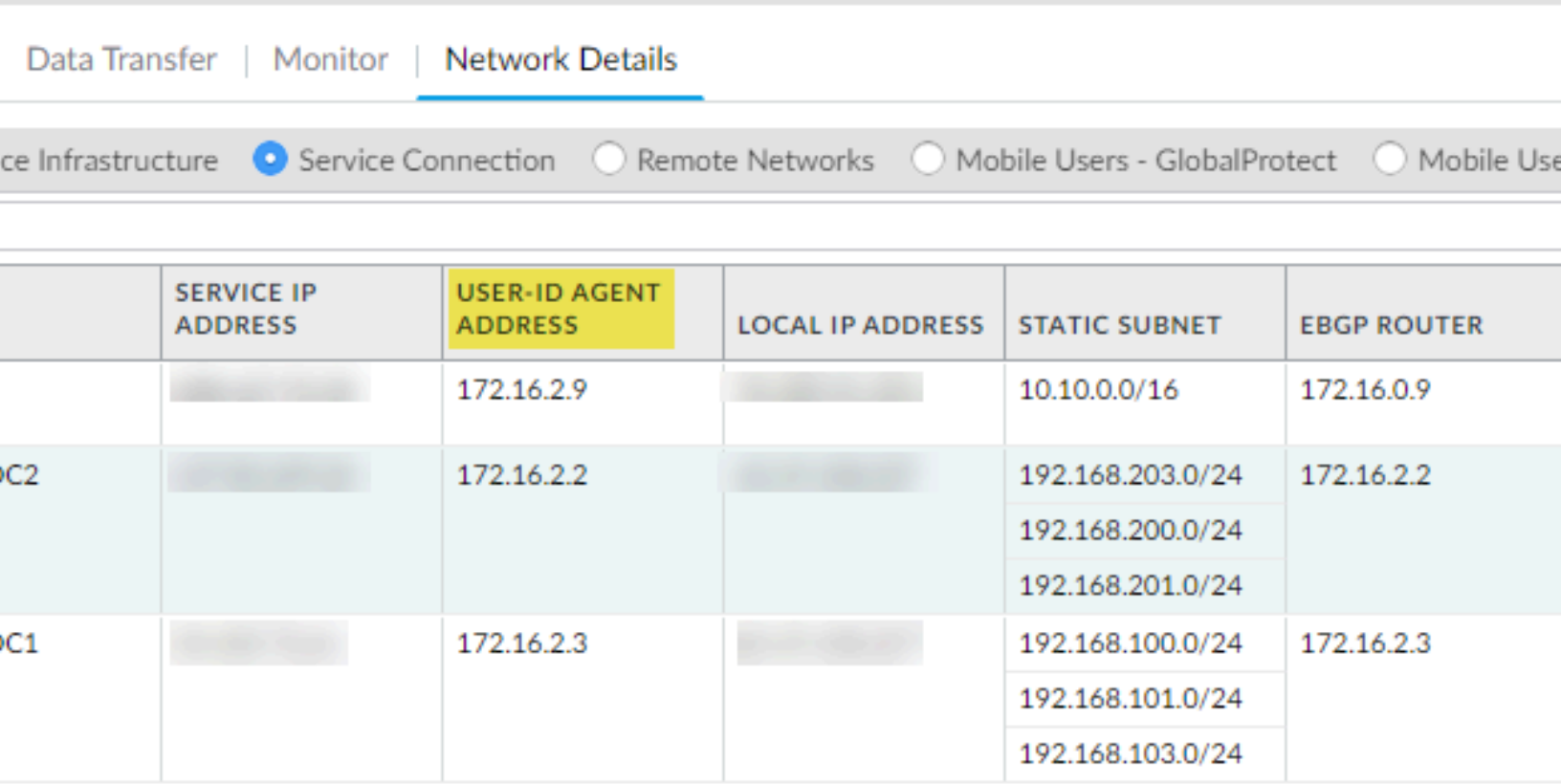
- 对于服务连接，请找到 **User-ID Agent Address**（**User-ID** 代理地址）（**Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息） > **Service Connection**（服务连接） > **User-ID Agent Address**（**User-ID** 代理地址））。

  如果您尚未为总部或数据中心设置服务连接，请先配置服务连接。Prisma Access 使用服务连接在您的环境中共享身份数据；Prisma Access 自动启用服务连接以用作重新分发代理。

 ©2025 Palo Alto Networks, Inc.

当您看到新创建的服务连接站点已被分配 User-ID 代理地址时，即可将其用作重新分发代理（Prisma Access 会自动执行此操作，只需要几分钟）。

User-ID 重新分发管理 — 有时，对于规模特别大的 *Prisma Access* 部署，需要重新分发 *User-ID* 以进行精细控制。*User-ID* 重新分发管理允许您通过删除 ***User ID***（用户 ***ID***）列中的复选标记来手动禁用某些服务连接的默认标识重新分发行为，然后选择要用于标识重新分发的特定服务连接。对于大多数配置，无需执行此操作。请联系 *Palo Alto Networks* 支持部门以激活此功能。

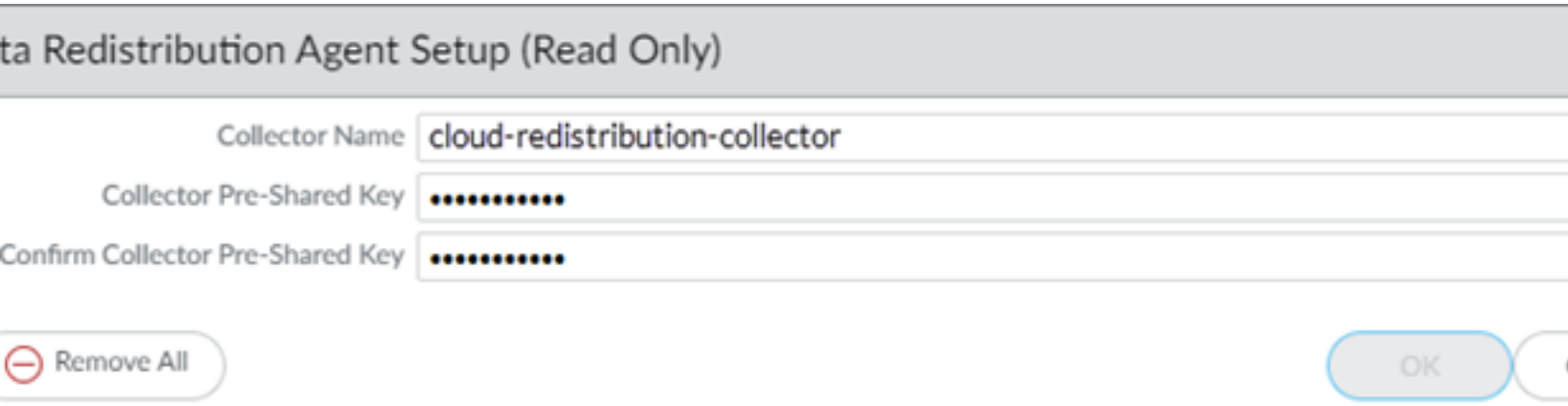


 ©2025 Palo Alto Networks, Inc.

STEP 2 | 配置 Prisma Access 以作为重新分发用户映射信息的 User-ID 代理。

1. 在管理 Prisma Access 的 Panorama 中，选择 **Device**（设备） > **Data Redistribution**（重新分发数据） > **Collector Settings**（收集器设置）。

   要在服务连接上配置收集器，请选择 **Service_Conn_Template**；要在远程网络连接上配置收集器，请选择 **Remote_Network_Template**。
2. 要编辑设置，请单击齿轮图标。
3. 提供 **Collector Name**（收集器名称）和 **Collector Pre-Shared Key**（收集器预共享密钥），以便将 Prisma Access 识别为 User-ID 代理。
4. 单击 **OK**（确定）保存更改。

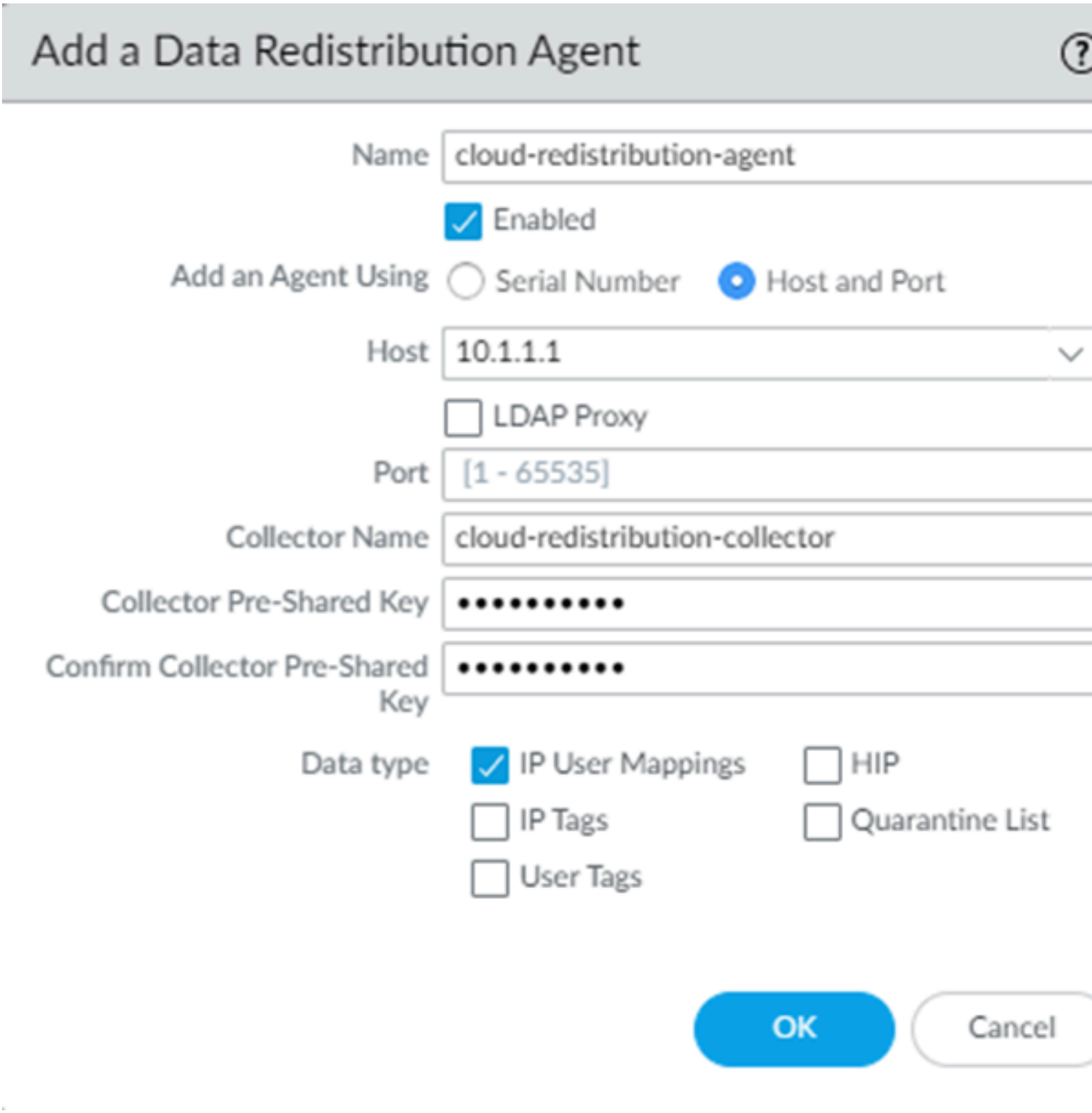


 ©2025 Palo Alto Networks, Inc.

STEP 3 | 配置本地防火墙以从 Prisma Access 收集 User-ID 映射。

1. 从本地防火墙中，选择 **Device**（设备） > **Data Redistribution**（重新分发数据） > **Agents**（代理）。
2. **Add**（添加） User-ID 代理并为其 **Name**（命名）。
3. 选择 **Host and Port**（主机和端口）。
4. 在 Prisma Access 的 **Host**（主机）字段中，输入 **User-ID Agent Address**（**User-ID** 代理地址）（对于服务连接）或 **EBGP Router Address**（**EBGP** 路由器地址）（对于远程网络连接）。
5. 对于在此过程的前面创建的 Prisma Access 收集器，请输入 **Collector Name**（收集器名称）和 **Collector Pre-Shared Key**（收集器预共享密钥）。
6. 选择 **IP User Mappings**（**IP** 用户映射）。
7. 单击 **OK**（确定）。
8. 对要重新分发映射的每个服务连接或远程网络连接重复这些步骤。

 ©2025 Palo Alto Networks, Inc.



将 User-ID 信息从本地防火墙重新分发到 Prisma Access

将 **User-ID** 信息从本地防火墙重新分发到 **Prisma Access**

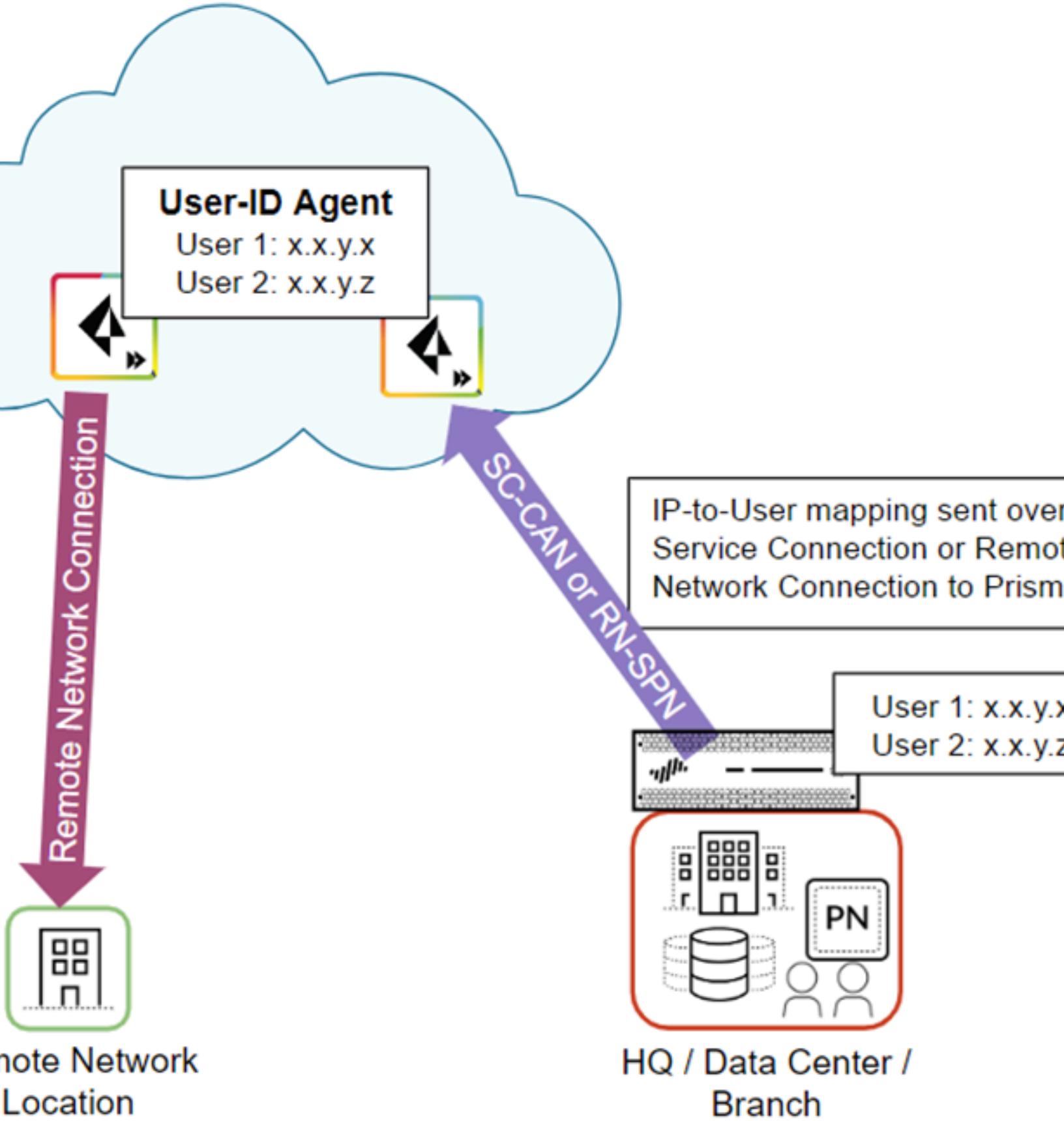
 ©2025 Palo Alto Networks, Inc.

如果用户位于由具有基于用户策略的本地新一代防火墙保护的分支机构或总部，并且他们需要访问您使用 Prisma Access 保护的另一个分支机构中的资源，则必须从本地防火墙重新分发 IP 地址到用户名的映射到 Prisma Access

下图展示了一个具有本地新一代防火墙以及现有的 IP 地址到用户名映射的总部/数据中心。Prisma Access 通过服务连接 (SC-CAN) 或远程网络连接 (RN-SPN) 连接到防火墙，本地防火墙将映射重新分发到 Prisma Access

下图显示了一个用于重新分发映射的 Prisma Access 服务连接或远程网络连接。对于专用地址的目标，您可以通过 IPSec 可信隧道使用任何路由路径来重新分发此映射。

 ©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.

要将 User-ID 映射从本地防火墙重新分发到 Prisma Access，请完成以下步骤。

STEP 1 | 将本地防火墙配置为 重新分发 User-ID 信息到 Prisma Access

1. 从本地防火墙中，选择 **Device**（设备） > **Data Redistribution**（重新分发数据） > **Collector Settings**（收集器设置）。
2. 要编辑设置，请单击齿轮图标。
3. 提供 **Collector Name**（收集器名称）以及 **Collector Pre-Shared Key**（收集器预共享密钥），以便将本地防火墙标识为 User-ID 代理。
4. 单击 **OK**（确定）保存更改。

STEP 2 | 配置 Prisma Access，以便从本地防火墙收集 User-ID 映射。

1. 从管理 Prisma Access 的 Panorama 中，选择 **Device**（设备） > **Data Redistribution**（重新分发数据） > **Agents**（代理）。

   确保在页面顶部的 **Templates**（模板） 下拉列表中已选择 **Service_Conn_Template**（对于服务连接）或 **Remote_Network_Template**（对于远程网络连接）。
2. **Add**（添加） User-ID 代理并为其 **Name**（命名）。
3. 选择 **Host and Port**（主机和端口）。
4. 在 **Host**（主机）字段中输入防火墙用于发送用户映射的 MGT 接口或服务路由的 IP 地址。

   对于 MGT 接口，可以输入主机名（而非 IP 地址）。
5. 使用在步骤 1 中为本地防火墙使用的收集器的值，输入 **Collector Name**（收集器名称）和 **Collector Pre-Shared Key**（收集器预共享密钥）。
6. 选择 **IP User Mappings**（**IP** 用户映射）。
7. 单击 **OK**（确定）。

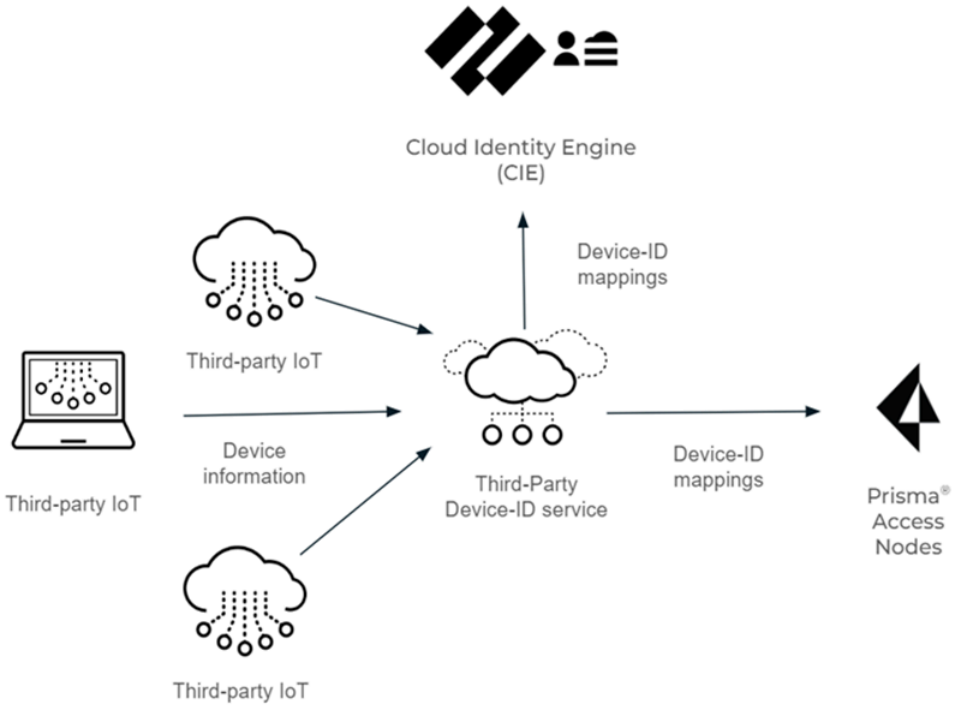
 ©2025 Palo Alto Networks, Inc.

在 Prisma Access 中配置第三方 Device-ID

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) 如果您想在 Prisma Access 环境中使用此功能，请与客户团队联系以了解更多信息。	❑ 已启用 Cloud Identity Engine 功能的 Prisma Access 许可证

您可以将 Cloud Identity Engine 与 Prisma Access 结合使用，以应用来自第三方 IoT 检测源的信息，从而简化识别和缩小网络中设备的安全差距的任务。使用 API 在 Cloud Identity Engine 中设置第三方 Device-ID 后，您可以在 Prisma Access 中设置设备对象和安全策略规则，以通过 Cloud Identity Engine 获取和使用来自第三方 IoT 可见性解决方案的信息，从而实现设备可见性和控制。

在下图中，第三方 Device-ID 服务从第三方 IoT 解决方案接收设备信息，然后将其作为 IP 地址到设备的映射传输到 Cloud Identity Engine 和 Prisma Access 安全处理节点 (SPN)。



- Strata Cloud Manager
- Panorama

©2025 Palo Alto Networks, Inc.

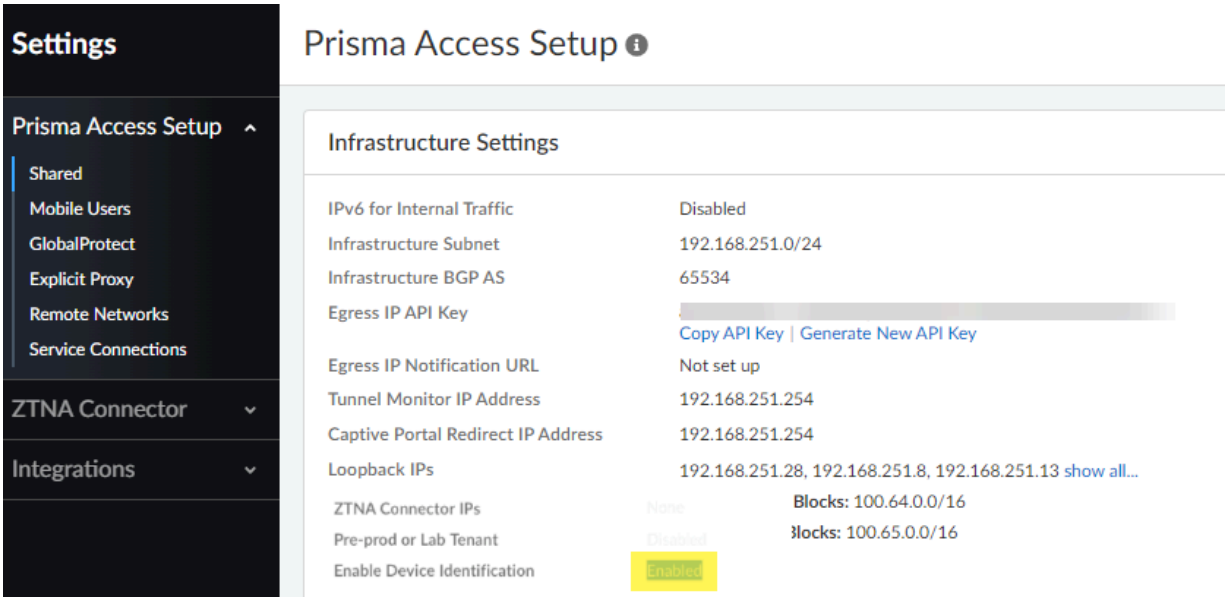
在 Prisma Access 中配置第三方 Device-ID (Strata Cloud Manager)

要配置第三方 Device-ID，请完成以下任务。

STEP 1 | 在 Cloud Identity Engine 中激活第三方 Device-ID。

此过程包括上传签名证书以及将证书与 API 一起使用，以便与第三方 IoT 供应商进行通信并从第三方 IoT 供应商那里下载 Device-ID 信息。

STEP 2 | 要在 Prisma Access 中激活第三方 Device-ID，请转到 **Settings**（设置） > **Prisma Access** 设置 > **Shared**（共享），或转到 **Workflows**（工作流） > **Prisma Access** 设置 > **Prisma Access**，并将 **Enable Device Identification**（启用设备标识）设置为 **Enabled**（已启用）。



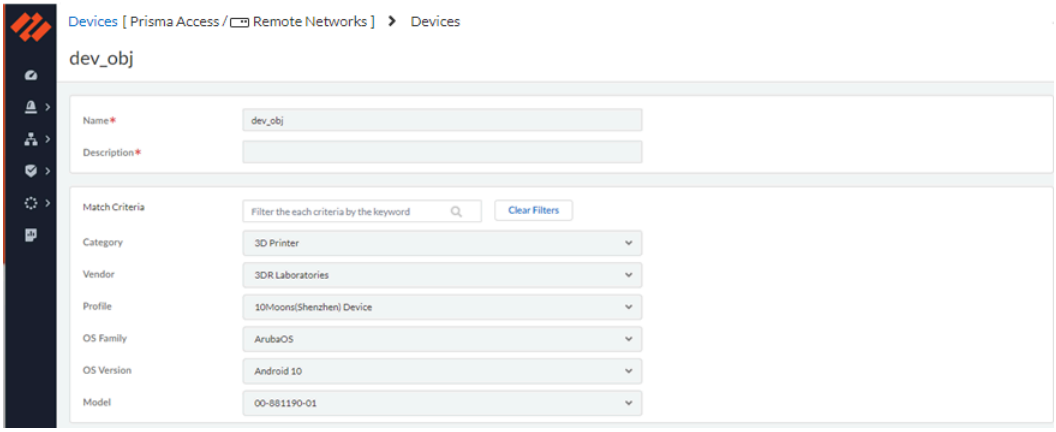
STEP 3 | 配置设备对象并输入设备属性。**Manage**（管理） > **Configuration**（配置） > **NGFW** 和 **Prisma Access**，将配置范围设置为 **Remote Networks**（远程网络），选择 **Objects**（对象）

 ©2025 Palo Alto Networks, Inc.

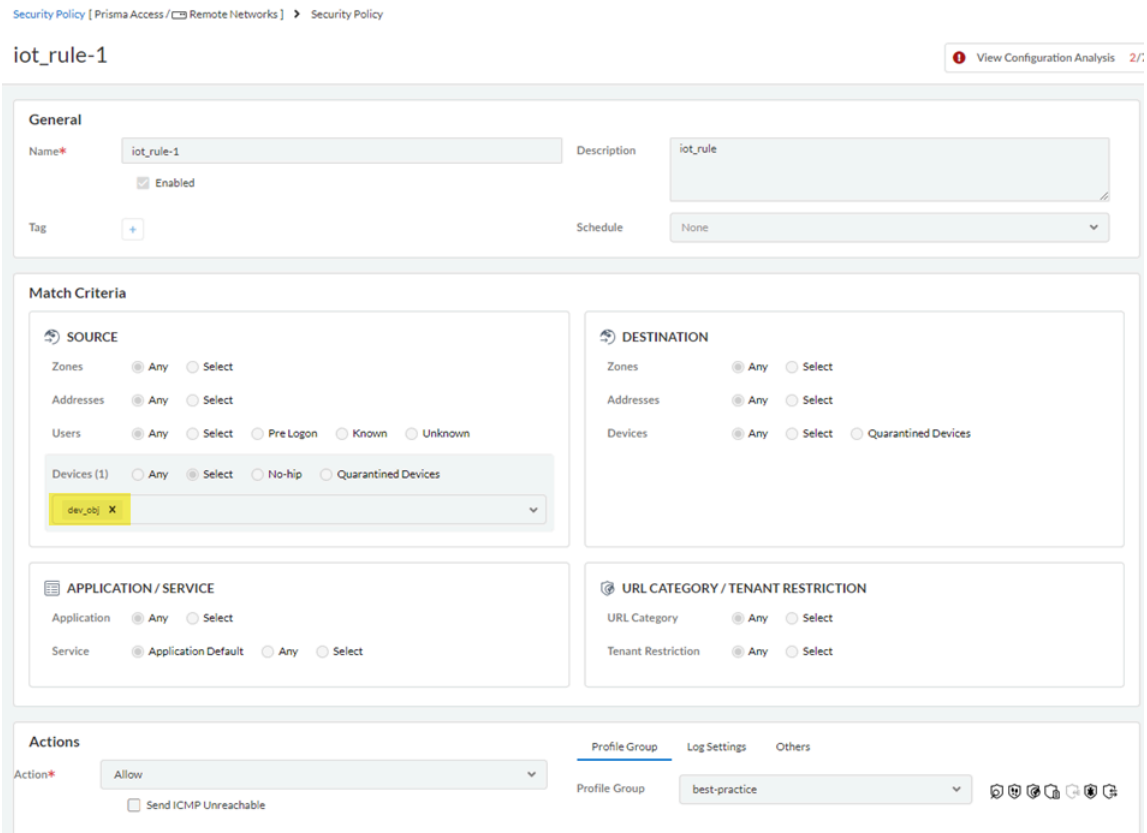
> **Devices**（设备），然后单击 **Add Devices**（添加设备）。确保您位于“远程网络”设备组中。

1. 添加与第三方对象的属性相匹配的设备对象。

   Cloud Identity Engine **Mappings**（映射）区域显示第三方设备的属性；您可以使用从该区域检索到的任何属性。



STEP 4 | 转到 **Manage**（管理） > **Configuration**（配置） > **NGFW** 和 **Prisma Access**，将配置范围设置为 **Remote Networks**（远程网络），选择 **Security Services**（安全服务） > **Security Policy**（安全策略），然后 **Add**（添加）安全策略，以添加您在 **Devices**（设备）区域中创建的设备对象。

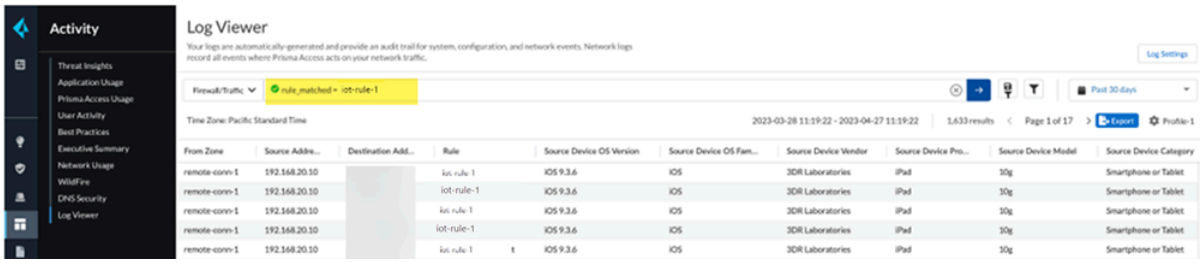


 ©2025 Palo Alto Networks, Inc.

STEP 5 | **Push Config**（推送配置）以保存对 Prisma Access 配置进行的更改，确保在推送范围内选择 **Remote Networks**（远程网络）。

STEP 6 | 要验证 Prisma Access 是否接收 Device-ID 日志，请转到 **Incidents & Alerts**（事件和警报）> **Log Viewer**（日志查看器），选择 **Firewall/Traffic**（防火墙/流量），并通过输入 `rule_matched = rulename` 搜索您创建的规则下的流量，其中 *rulename* 代表您为第三方 IoT 设备创建的安全策略规则。

Device-ID 到 IP 地址的映射显示在日志中。



在 Prisma Access 中配置第三方 Device-ID (Panorama)

要配置第三方 Device-ID，请完成以下任务。

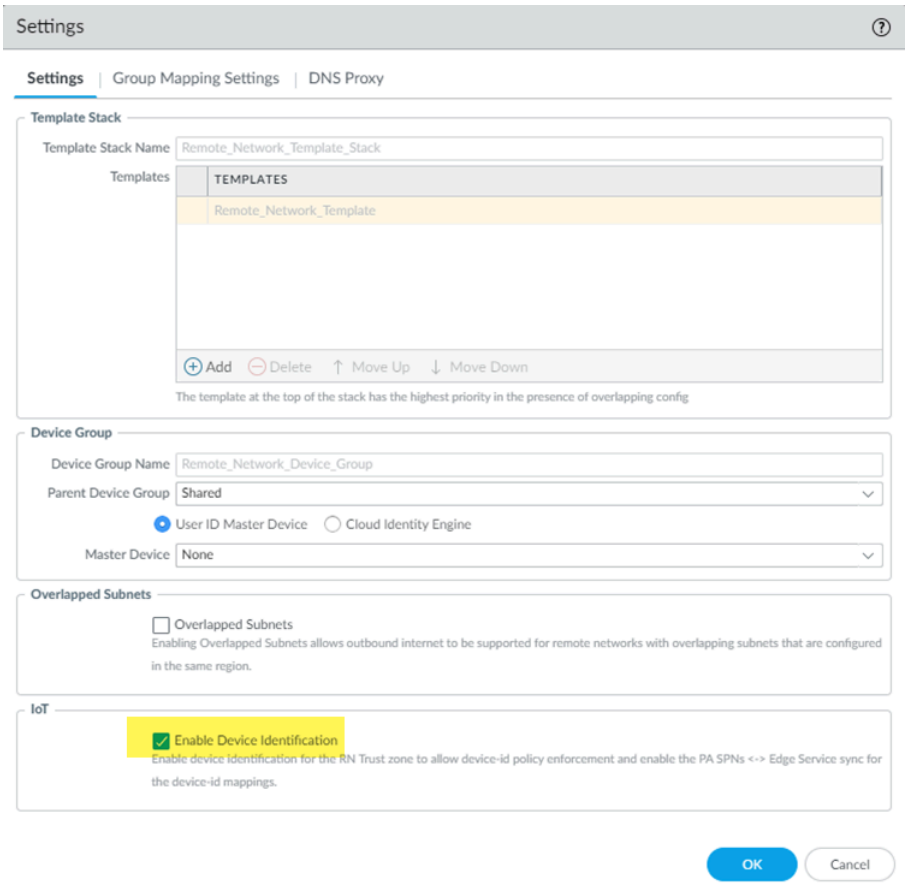
STEP 1 | 在 Cloud Identity Engine 中激活第三方 Device-ID。

此过程包括上传签名证书以及将证书与 API 一起使用，以便与第三方 IoT 供应商进行通信并从第三方 IoT 供应商那里下载 Device-ID 信息。

STEP 2 | 要在 Prisma Access 中激活第三方 Device-ID，请转到 **Panorama** > **Cloud Services**（云服务）> **Configuration**（配置）> **Remote Networks**（远程网络）> **Settings**（设置），单

 ©2025 Palo Alto Networks, Inc.

击齿轮图标以编辑 **Settings**（设置），然后选择 **Enable Device Identification**（启用设备标识）。



©2025 Palo Alto Networks, Inc.

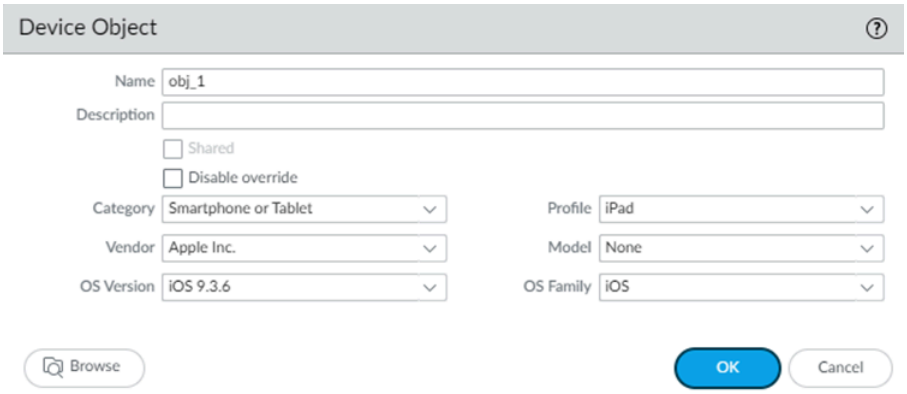
STEP 3 | 配置设备对象并输入设备属性。

1. 转到 **Objects**（对象） > **Devices**（设备），**Add**（添加）与所有设备 ID 属性匹配的设备对象。

   确保您位于 **Remote_Network_Device_Group** 或 **Shared**（共享）设备组中。

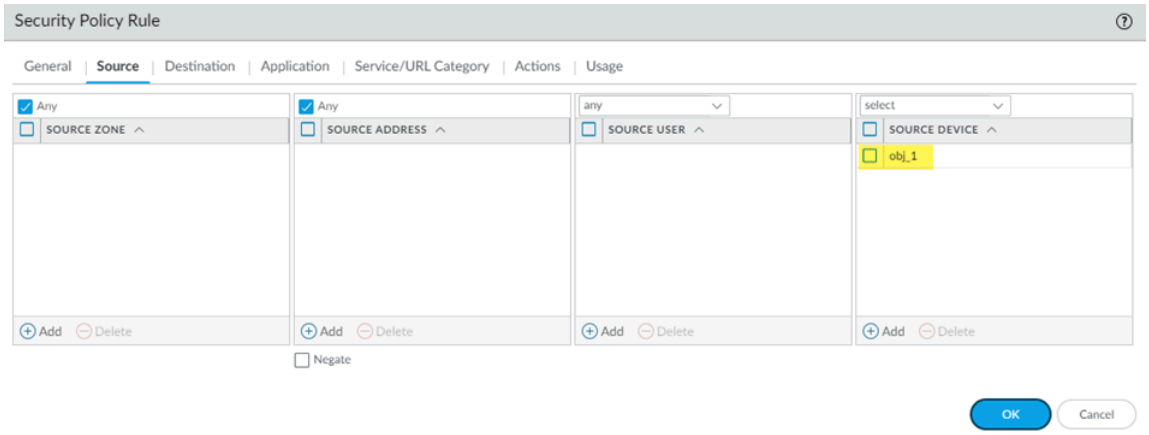
2. **Add**（添加）与第三方对象的属性相匹配的设备对象。

   Cloud Identity Engine ***Mappings***（映射）区域显示第三方设备的属性；您可以使用从该区域检索到的任何属性。



STEP 4 | 转到 **Policies**（策略） > **Security**（安全） > **Pre Rules**（预规则），**Add**（添加）安全策略，将您在 **Devices**（设备）区域中创建的设备对象添加为 **Source Device**（源设备）。

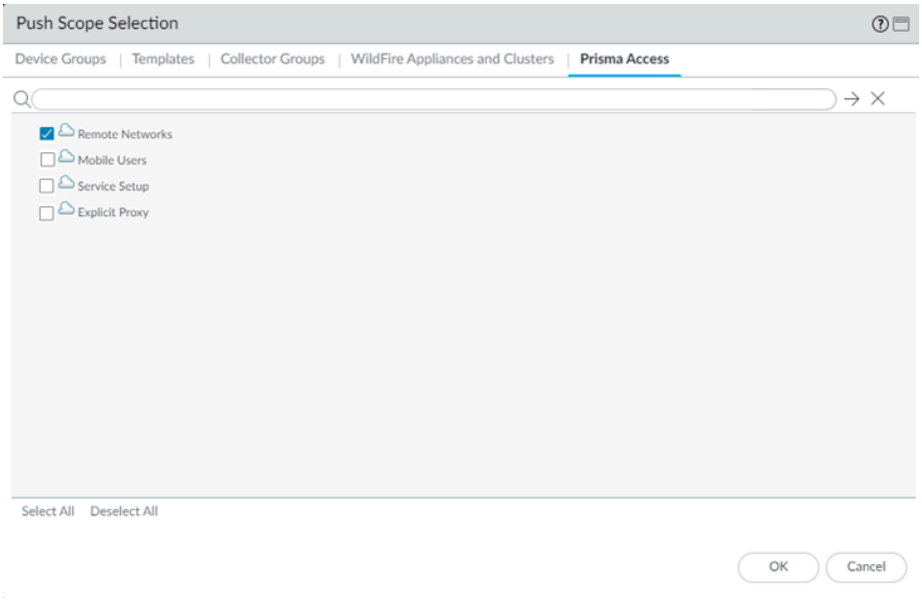
确保您位于 **Remote_Network_Device_Group** 或 **Shared**（共享）设备组中。



 ©2025 Palo Alto Networks, Inc.

STEP 5 | 提交并推送您的更改，确保在 **Push Scope**（推送范围）中选择 **Remote Networks**（远程网络）。

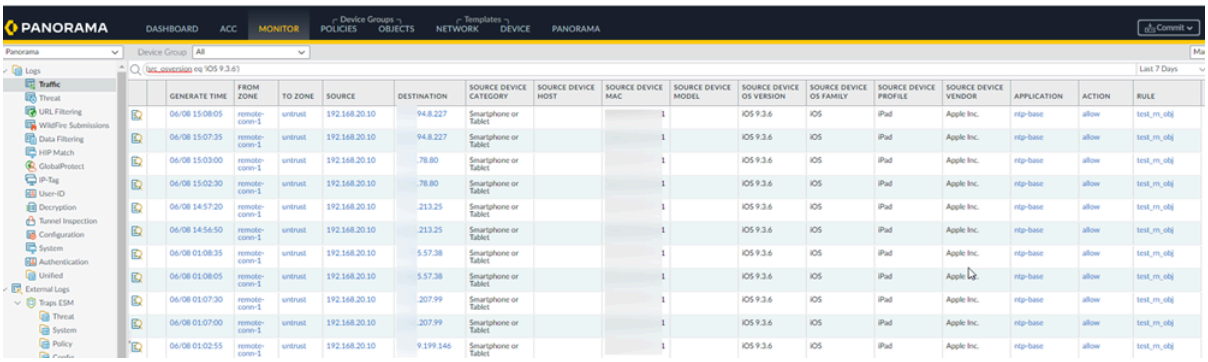
1. 单击 **Commit**（提交） > **Commit and Push**（提交并推送）。
2. **Edit Selections**（编辑选择），在 **Prisma Access** 选项卡中，确保在 **Push Scope**（推送范围）中选择 **Remote Networks**（远程网络），然后单击 **OK**（确定）。



3. 单击 **Commit and Push**（提交并推送）。

STEP 6 | 要验证 Prisma Access 是否接收 Device-ID 日志，请转到 **Monitor**（监控） > **Logs**（日志），并通过输入 `rule_matched = rulename` 为您创建的规则下的流量搜索 **Traffic**（流量）日志，其中 *rulename* 代表您为第三方 IoT 设备创建的安全策略规则。

Device-ID 到 IP 地址的映射显示在日志中。



 ©2025 Palo Alto Networks, Inc.

第三方 Device-ID API

通过 Cloud Identity Engine 用户界面载入第三方 Device-ID 服务后，您可以使用这些 API 来管理在网络中检测到并存储在第三方 Device-ID 服务中的判决或 IP 地址到设备映射。这些映射将告知 Prisma Access，哪些属性属于具有特定 IP 地址的设备，以便您可以定义针对具有特定属性的设备的安全策略。

这些 API 不会直接访问存储在您的 Cloud Identity Engine 租户中的数据。相反，API 与第三方 Device-ID 服务中的 IP 地址到设备的映射进行交互，而该服务会将这些映射与 Cloud Identity Engine 共享。

第三方 Device-ID API 使用证书、API 密钥和 API 请求的基本 URL。要验证第三方 Device-ID API 请求，您必须使用在 Cloud Identity Engine 用户界面上获得的签名证书和 API 令牌。

当您拥有证书和 API 密钥时，可以对第三方 Device-ID 服务发出请求。在每个请求中提供包含其公钥的证书、API 密钥和基本 URL。示例：

```
curl --cert onida1.crt --key onida.key "https://device-identity-
broker-beta.service-edge.panservicetest.com/:443/api/v1/token/
{apiKey}/verdicts"
```

- 更新判定
- 删除所有判定
- 查询判定
- 按 IP 地址查询判定结果
- 查询判定统计信息

更新判定

添加、修改或删除 IP 地址到设备的映射。

摘要

URI	`/api/v1/token/{apiKey}/verdicts:update`
HTTP 方法	POST

说明

第三方 Device-ID 从网络中的第三方 IoT 检测源提取数据，并创建，Prisma Access 可用于执行特定于设备的安全策略规则的 IP 地址到设备映射。使用此 API 添加新映射、修改现有映射或删除映射。

您可以使用 `update` 字段添加或修改映射，并使用 `delete` 字段删除映射。

如果映射已经存在，则 `update` 将使用请求正文中指定的属性覆盖现有设备属性。如果映射不存在，则更新会创建新的映射。

©2025 Palo Alto Networks, Inc.

此 API 不支持部分更新。如果要更新映射的特定属性，则还必须为不想更新的属性重新输入先前的值。将属性留空将擦除现有值。

一次最多可以更新或删除 10,000 个映射。该请求是原子的：成功的响应意味着系统处理了所有内容，失败的响应意味着系统没有处理任何内容。

字段

字段	说明
update	JSON 对象，提供您要更新或创建的 IP 地址到设备映射的属性。必须填充 IP 和至少一个其他属性。
delete	一个 JSON 对象，用于指定要删除的映射的 IP 地址。

例如：

```
{ "update": [ { "ip": "string", "serialNo": "string", "mac":
 "string", "category": "string", "vendor": "string", "model":
 "string", "os": "string", "osFamily": "string", "hostname":
 "string", "profile": "string", } ], "delete": [ { ip: "string" } ] }
```

成功响应

成功后，HTTP 响应代码为 200。此外，响应还包含一个带有以下字段的 JSON 对象：

字段	说明
更新时间	一个 Unix 时间戳，表示请求成功的时间。

例如：

```
{ "updateTime": unix-timestamp }
```

错误响应

出现错误时，HTTP 响应代码为以下代码之一：

响应码	说明
400	无效请求。请求不完整或格式不正确。在重试之前修复请求。
401	未经授权的令牌。尝试重新生成您的 API 令牌。如果这不起作用，请联系支持人员。

 ©2025 Palo Alto Networks, Inc.

响应码	说明
409	冲突。无法处理该请求，因为还有另一个正在进行的更新或删除任务。在其他任务完成后再试一次。
429	请求过多。无法处理该请求，因为系统在特定时间段内发出了太多请求。每秒不要超过一个请求。等着再试一次。

此外，响应正文包含以下字段：

字段	说明
code	错误代码。
message	错误消息

update Object

包含 更新 IP 地址到设备映射所需的信息。该 JSON 对象具有以下字段：

字段	说明
ip	设备的 IP 地址。
updateTime	表示映射上次更新发生时间的 Unix 时间戳。
类别	设备类型。示例：打印机
供应商	设备供应商。示例：夏普公司
model	设备模型。示例：MX-6070N
os	设备操作系统。示例：ThreadX 5
osFamily	设备操作系统所属的系列。示例：ThreadX RTOS
profile	设备配置文件。示例：夏普打印机

删除所有判定

从第三方 Device-ID 服务中删除所有 IP 地址到设备的映射。

摘要

URI	/api/v1/token/{apiKey}/verdicts:all

 ©2025 Palo Alto Networks, Inc.

HTTP 方法	DELETE

说明

请求第三方 Device-ID 服务删除第三方 Device-ID 服务中的所有 IP 地址到设备的映射。成功响应意味着服务已删除所有映射。错误响应意味着服务无法删除任何映射。

成功响应

成功后，HTTP 响应代码为 200。响应主体为空。

错误响应

发生错误时，HTTP 响应代码为以下之一：

响应码	说明
401	令牌未授权。尝试重新生成您的 API 令牌。如果仍然无效，请联系支持人员。
409	冲突。系统无法处理该请求，因为还有另一个正在进行的更新或删除作业。待另一项工作完成后再试。
429	请求过多。系统无法处理该请求，因为系统在特定时间段内的请求过多。每秒的请求数不得超过一个。等待并重试。

此外，响应主体还包含以下字段：

字段	说明
code	错误代码。
message	SSO 错误消息。

查询判定

检索第三方设备 ID 服务中的 IP 地址到设备的映射。

摘要

URI	/api/v1/token/{apiKey}/verdicts? bookmark={STRING}&pageLen={INTEGER}
HTTP 方法	入

©2025 Palo Alto Networks, Inc.

说明

返回所有映射或子集。

要返回所有映射，请发送一次请求（不带任何参数）。记录响应中的 `nextBookmark` 值。使用附加到 URI 的 `bookmark` 的值发送另一个请求。调用程序将重复查询，直到响应中的 `count` 为空，这表明它已返回所有映射。

要返回映射子集，请使用 `pageLen` 指定要检索的映射数量，最多 10000。

参数

此 API 接受以下参数：

参数	说明
bookmark	（可选）在第一个请求后使用以返回所有映射。
pageLen	（可选）要检索的映射数。范围为 1-10000。如果未指定，则默认值为 10000。

成功响应

成功时，HTTP 响应代码为 200。此外，响应还包含一个具有以下字段的 JSON 对象：

字段	说明
nextBookmark	您在 bookmark 参数中使用的值将执行重复查询，直到返回所有映射。
count	表示响应中返回的映射数量的整数。
判定结果	包含在请求中指定的映射的对象。

例如：

```
{ "nextBookmark":CkcKVxdWVuY2USAggEEjFqCHN, "count":1,
 "verdicts" : [ { "ip":"10.10.10.10", "updateTime":1623974506,
 "mac":"0a:d4:5f:e9:96:10", "category":"Smartphone or Tablet",
 "vendor":"Apple Inc.", "model": "iPad2", "os": "iOS 9.3.6",
 "osFamily": "iOS", "profile": "iPad" } ] } }
```

错误响应

发生错误时，HTTP 响应代码为以下之一：

响应码	说明

©2025 Palo Alto Networks, Inc.

400	请求无效。该请求不完整或格式有误。 您应该先更正请求，然后重试。
401	令牌未授权。
429	请求过多。无法处理请求，因为在指定时间段内发出的请求数量过多。每秒最多 等待并重试。

此外，响应主体还包含以下字段：

字段	说明
code	错误代码。
message	错误消息。

判定结果

成功查询 IP 地址到设备映射时返回的对象。该对象包含以下信息：

字段	说明
ip	设备的 IP 地址。
更新时间	表示映射上次更新发生时间的 Unix 时间戳。
类别	设备类型。示例：打印机
供应商	设备供应商。示例：夏普公司
model	设备模型。示例：MX-6070N
os	设备操作系统。示例：ThreadX 5
操作系统系列	设备操作系统所属的系列。示例：ThreadX RTOS
profile	设备配置文件。示例：夏普打印机

按 IP 地址查询判定结果

根据 IP 地址检索 IP 地址到设备的映射。

©2025 Palo Alto Networks, Inc.

摘要

URI	/api/v1/token/{apiKey}/verdicts?ip={STRING}
HTTP 方法	GET

说明

使用 IP 地址返回相应的设备映射。您可以通过提供附加到 URI 的最多 10 个 IP 地址（以逗号分隔）列表来检索多个映射。

如果服务找不到与 IP 地址关联的映射，则不会返回该 IP 地址的映射。

成功响应

如果成功，HTTP 响应代码为 200。此外，响应还包含一个具有以下字段的 JSON 对象：

字段	说明
count	表示响应中返回的映射数量的整数。
verdicts	包含在请求中指定的映射的对象。

例如：

```
{ "count":1, "verdicts" : [ { "ip":"10.10.10.10",
 "updateTime":1623974506, "mac":"0a:d4:5f:e9:96:10",
 "category":"Smartphone or Tablet", "vendor":"Apple Inc.",
 "model": "iPad2", "os": "iOS 9.3.6", "osFamily": "iOS", "profile":
 "iPad" } ] } }
```

错误响应

发生错误时，HTTP 响应代码为以下之一：

响应码	说明
400	请求无效。该请求不完整或格式有误。 请修复请求，然后重试。
401	令牌未授权。
429	请求过多。系统无法处理该请求，因为系统在指定时间段内发出了太多请求。每秒超过一个。请等待并重试。

此外，响应主体还包含以下字段：

©2025 Palo Alto Networks, Inc.

字段	说明
code	错误代码。
message	错误消息。

查询判定统计信息

检索有关第三方 Device-ID 服务的统计信息。

摘要

URI	/api/v1/token/{apiKey}/verdicts:statistics
HTTP 方法	GET

成功响应

成功时，HTTP 响应代码为 200。此外，响应还包含一个具有以下字段的 JSON 对象：

字段	说明
判定结果	包含有关租户中 IP 地址到设备映射的统计信息的对象。包含以下字段： • totalCount - 租户中 IP 地址到设备映射的总数。 • totalUpdate - 自创建以来更新的 IP 地址到设备映射的数量。 • totalDelete - 自创建租户以来删除的 IP 地址到设备映射的数量。
requestRcvd	包含租户收到每个类型请求的次数的对象： • update - 收到的 更新判定 请求的数量。 • deleteAll - 收到的 删除所有判定 请求的数量。 • query - 收到的 查询判定 和 按 IP 地址查询判定结果 请求的数量。 • Statistics - 收到的 查询判定统计信息 请求的数量。

例如：

```
{ "verdicts: { "totalCount":1, "totalUpdate":0, "totalDelete":0, },
 "requestRcvd": { "update":1, "deleteAll":0, "query":0,
 "statistics":1 } }
```

错误响应

发生错误时，HTTP 响应代码为以下之一：

©2025 Palo Alto Networks, Inc.

响应码	说明
401	令牌未授权。
429	请求过多。无法处理请求，因为在指定时间段内发出的请求数量过多。每秒最多 等待并重试。

此外，响应主体还包含以下字段：

字段	说明
code	错误代码。
message	错误消息。

©2025 Palo Alto Networks, Inc.

Prisma Access 多租户

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama) • 有关在 Prisma Access (Managed by Strata Cloud Manager) 中管理多个租户的信息，请参阅 Prisma SASE。	❑ Prisma Access 许可证

本节仅提供有关在 Prisma Access (Panorama) 中管理多个租户的信息。有关在 Prisma Access (Managed by Strata Cloud Manager) 中管理多个租户的信息，请参阅 Prisma SASE。

为了允许您创建和管理多个 Prisma Access 实例，Prisma Access 提供了多租户功能，使您可以在单个 Panorama 设备（或高可用性（HA）模式下的 2 个设备）上创建最多 200 个实例（租户），每个租户都有自己单独的模板和模板堆栈、设备组和访问域。

现有或将来的非多租户部署不受多租户影响，并将继续正常运行。我们的建议是，仅当组织需要在 Prisma Access 中管理多个租户时才启用多租户。

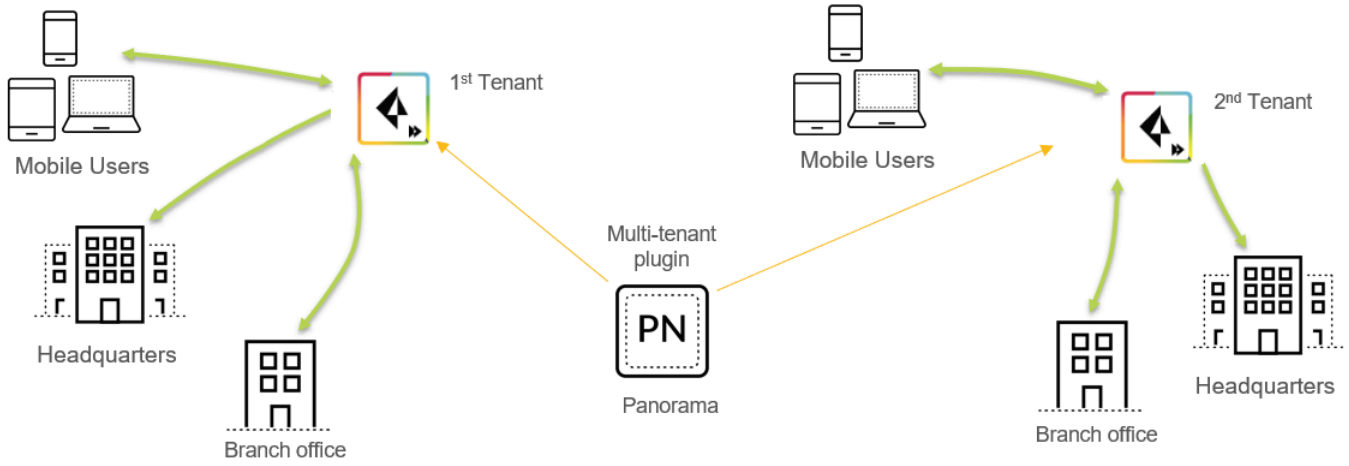
本节仅提供为远程网络、移动用户或远程网络和移动用户部署的组合配置租户时执行的任务。要配置 Clean Pipe 服务，请参阅Prisma Access for Clean Pipe。

多租户配置概述

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama) • 有关在 Prisma Access (Managed by Strata Cloud Manager) 中管理多个租户的信息，请参阅 Prisma SASE。	❑ Prisma Access 许可证

通过启用多租户，您可以在单个 Panorama 设备上托管多个 Prisma Access 实例。每个实例都称为一个租户。

Prisma Access 租户获得自己的专用 Prisma Access 实例，并且不在租户之间共享。



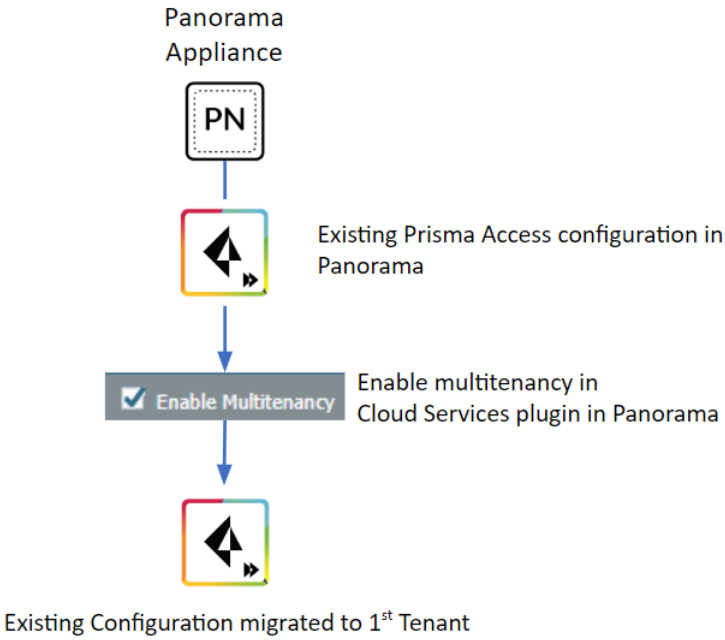
使用以下工作流配置在单个 Panorama 设备中管理多个租户的功能：

©2025 Palo Alto Networks, Inc.

STEP 1 | 启用多租户。如果您有现有的 Prisma Access 实例，则启用多租户会自动将现有的 Prisma Access 配置迁移到第一个租户。

为第一个（迁移的）租户提供名称并指定访问域。Prisma Access 迁移与现有配置相关联的模板、模板堆栈和设备组，并将其与您创建的访问域相关联。

迁移初始配置后，Panorama 中的管理用户将成为能够创建和管理所有 Prisma Access 租户的超级用户。



STEP 2 | 然后，将租户添加到 Prisma Access。

要部署多个租户，请确保您满足以下许可证最低要求：

要确定您从 *Panorama* 获得的 *Prisma Access* 许可证类型，请选择 ***Panorama*** > ***Licenses***（许可证）。

- 如果您拥有商业版、商业增强版、零信任网络访问 **(ZTNA)** 安全互联网网关 **(SIG)** 或 企业版许可证，请将以下最低要求作为参考准则：

  适用于网络的 **Prisma Access** 和适用于用户的 **Prisma Access**：

  如果您有 **Local**（本地）版本，则每个租户需要最低数量为 200 个单位，并且所有租户都为本地。

  如果您拥有**Worldwide**（全球）版本，则需要至少 1,000 个单位才能创建 **Worldwide**（全球）租户。如果您为一个租户分配 200 到 999 个单位，Prisma Access 会创建一个

 ©2025 Palo Alto Networks, Inc.

Local（本地） 租户；如果您为一个租户分配 1000 个或更多单位，那么 Prisma Access 会创建一个 **Worldwide**（全球） 租户。

对于适用于远程网络的 Prisma Access，单位对应带宽（以 Mbps 为单位）；对于适用于用户的 Prisma Access 来说，则对应移动用户的数量。

- 如果您的许可证类型以 **GlobalProtect** 云服务起步，请使用以下最低标准作为指导：

  适用于网络的 **Prisma Access**—您必须为每个租户在许可证中至少提供 200 Mbps 的带宽。

  适用于用户的 **Prisma Access**—对于每个租户，许可证中必须至少有 200 个可用的移动用户。

  在这两种类型的 Prisma Access 配置中，您可以添加任一种类型的附加许可（高于上述最小值）。您可以在接入后增加或减少任何租户的带宽或移动用户分配，前提是您保持每个租户所需的最低分配，并且不超过总许可容量。

您可以仅为远程网络、仅为移动用户或同时为两者设置多租户配置。在您启用多租户时，您需要根据每个租户分配许可证。

如果您拥有远程网络和移动用户的许可证，则可以仅为移动用户或仅为远程网络设置一个单独租户。例如，如果您的 Prisma Access 部署具有适用于移动用户和远程网络的 **Worldwide**（全球）版本许可证，则您可以仅为移动用户设置租户，前提是您为租户指定最少 1000 个移动用户。

对于在第一个租户之后创建的每个租户，Prisma Access 将自动为每个租户创建模板、模板堆栈和设备组，并将它们与您创建的访问域相关联。Prisma Access 创建此环境以允许您使用基于租户的设备组和模板的管理角色创建租户级别的管理用户，然后基于该角色创建管理用

 ©2025 Palo Alto Networks, Inc.

户。通过这种方式，您可以创建对单个租户具有访问权限的管理用户，而不允许该用户访问由 Panorama 设备管理的其他租户。

Prisma Access 使用以下命名约定创建模板堆栈、模板和设备组：

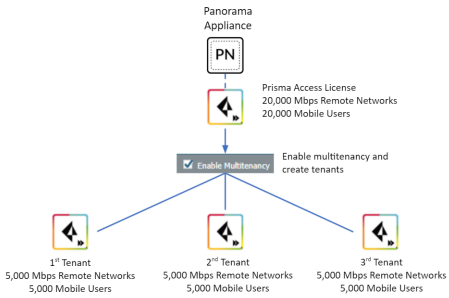
- 名称为 **sc-stk-***tenant* 的服务连接模板堆栈，其中 *tenant* 是租户的名称。
- 一个名为 **sc-tpl-***tenant* 的服务连接模板。
- 一个名为 **sc-dg-***tenant* 的服务连接设备组。
- 一个名为 **mu-stk-***tenant* 的移动用户模板堆栈。
- 一个名为 **mu-tpl-***tenant* 的移动用户模板。
- 一个名为 **mu-dg-***tenant* 的移动用户设备组。
- 一个名为 **rn-stk-***tenant* 的远程网络模板堆栈。
- 一个名为 **rn-tpl-***tenant* 的远程网络模板。
- 一个名为 **rn-dg-***tenant* 的远程网络设备组。
- 一个名为 **ep-stk-***tenant* 的显式代理模板堆栈。
- 一个名为 **ep-tpl-***tenant* 的显式代理模板。
- 一个名为 **ep-dg-***tenant* 的显式代理设备组。
- 一个名为 **cp-stk-***tenant* 的 Clean Pipe 模板堆栈。
- 一个名为 **cp-tpl-***tenant* 的 Clean Pipe 模板。
- 一个名为 **cp-dg-***tenant* 的 Clean Pipe 设备组。

为所有 Prisma Access 类型创建模板堆栈、模板和设备组，甚至包括您可能未获得许可的访问类型。例如，如果您为远程网络购买了许可证，Prisma Access 会自动为远程网络、移动用户和 Clean Pipe 创建模板堆栈、模板和设备组。

如果添加自定义模板，则自定义模板不能优先于 Prisma Access 创建的模板。

您可以根据与 Panorama 中的云服务插件关联的许可证，为每个租户分配远程网络和移动用户许可证资源。

下图展示了一个 Prisma Access 部署示例，其使用的许可证具备一个 20,000 Mbps 的远程网络带宽池以及 20,000 名移动用户。管理员为现有配置分配了 5,000Mbps 的远程网络带宽和 5,000 个移动用户。在管理员启用多租户后，许可证分配与所有其他配置一起迁移到第一个租户。然后，管理员创建了其他租户，每个租户具有用于远程网络的 5,000 Mbps 带宽池，并且每个租户具有 5,000 个移动用户。Prisma Access 从总体许可证分配中分配许可证资源。完成此配置后，许可证中可用的远程网络带宽为5000 Mbps，移动用户为 5000 个。



 ©2025 Palo Alto Networks, Inc.

规划您的多租户部署

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama) • 有关在 Prisma Access (Managed by Strata Cloud Manager) 中管理多个租户的信息，请参阅 Prisma SASE。	• Prisma Access 许可证

在启用多租户之前，迁移第一个租户并创建其他租户，请确保您已通过完成以下任务获得所有所需的信息和资源：

- 如果您要将现有的单租户部署迁移到多租户部署，请注意 Prisma Access 的下列功能不受支持。有关不支持功能的列表，请参阅 Palo Alto Networks兼容性一览表。
- 如果还没有 Prisma Access 配置，请启用多租户并添加租户。然后，在创建租户后配置租户。如需更多信息，请参阅 创建全新的多租户部署。
- 请注意您对远程网络和移动用户的许可证分配。

  打开许可证（**Panorama** > **Licenses**（许可证））并找到远程网络的 Prisma Access **Total Mbps**（总带宽）（远程网络带宽池）和移动用户的 **User Limit**（用户限制）（许可用户总数）。

  创建租户时，您需要从该许可证分配中为远程网络和移动用户分配资源。如果您耗尽了远程网络或移动用户所需的最低许可带宽，您将无法创建更多的租户。

  您还应该记录您现有配置的带宽和移动用户分配情况。在将配置迁移到第一个租户后，请检查这些值以验证第一个租户是否正确迁移。
- 列出您将用于识别每个租户的名称。

  在创建租户名称时，避免使用类似于 *Tenant-1*、*Tenant-2*、*Tenant-3* 的名称。系统日志在日志输出中会为租户名称预留少量字符，如果租户名称相似，您可能难以将租户与日志关联起来。我们建议为租户使用一个独特且简短的名称（例如，*Acme* 或 *Hooli*）。
- 列出您将为每个租户创建并分配的管理用户名单，并记录可同时登录的管理用户的最大数量。

  当管理用户执行诸如配置更改和提交操作等常规多租户操作时，我们建议最多同时有 12 名管理用户登录到 Panorama。

  能够管理多个租户的管理用户可以通过一次提交操作同时配置最多 200 个租户。
- 请确保您拥有足够的许可证资源来启用多个租户。

  每个租户的最低许可证分配标准是，每个远程网络 200 Mbps 带宽，或者支持 200 个移动用户。您也可以仅为远程网络或移动用户创建租户，并且可以在同一台 Panorama 设备上以不同配置来配置租户。例如，只要每个租户满足最低许可证分配要求，并且相关许可证已激活并关联到您配置租户的 Panorama 设备，您就可以创建仅包含远程网络的租户、仅包含移动用户的租户，或者同时包含移动用户和远程网络的租户。

©2025 Palo Alto Networks, Inc.

- 在多租户模式下配置租户时，要为服务连接和远程网络连接的每个 IPsec 隧道和 IKE 网关创建唯一的名称，并尽量使用不会与其他租户重复的名称。虽然这对功能没有影响，但如果其他租户正在使用同名的 IPsec 隧道或 IKE 网关，您将无法删除该 IPsec 隧道或 IKE 网关。

  这条注意事项适用于所有对象，包括 QoS 配置文件（在多租户部署中，如果某个对象被其他租户引用，您将无法删除具有重复名称的对象）。
- 单租户用户无法查看系统日志；只有超级用户可以。然您可以按租户对日志进行排序。
- 当移动用户登录到单一 Prisma Access 租户时，该用户消耗一个许可证单位。如果用户在单个多租户部署环境下登录多个租户，那么该用户每登录一个租户就会消耗一个许可证单元。例如，如果一个用户同时登录了五个租户，那么该用户总共会消耗五个移动用户许可证单元。
- 使用多租户功能并以租户级管理用户身份登录时，打开 Panorama 任务管理器（在 Panorama Web 界面底部单击 **Task**（任务））将显示所有租户的所有任务，包括超级用户（管理员）级别执行的任何任务。
- 某些 Prisma Access 功能不支持在多租户环境下使用。有关详细信息，请参阅 Palo Alto Networks 兼容性一览表中的 多租户不支持的功能。
- 如果您备份了 Panorama 配置，而后将其恢复到先前保存的配置，若您按以下顺序执行以下操作，Panorama 将无法恢复到您保存的配置：

  1. 备份 Panorama 配置
  2. 删除租户。
  3. 恢复配置。

  如果您删除了租户，则无法使用在删除租户之前保存的任何先前备份。不过，您可以使用在删除租户之后进行的任何备份。

©2025 Palo Alto Networks, Inc.

创建全新的多租户部署

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama) • 有关在 Prisma Access (Managed by Strata Cloud Manager) 中管理多个租户的信息，请参阅 Prisma SASE。	❑ Prisma Access 许可证

如果您想创建多租户部署但还没有现有 Prisma Access 配置，请 **Enable Multitenancy**（启用多租户）并添加租户；然后，在创建租户后对其进行配置。

如果您有现有的单租户部署并希望迁移到多租户部署，请使用工作流启用多租户并迁移第一个租户。

当您在没有现有配置的情况下创建第一个租户时，请确保遵循以下差异和准则：

- 由于没有要迁移的配置，Prisma Access 会为每个租户创建模板、模板堆栈和设备组，并将它们关联到您在创建租户期间创建的访问域。有关 Prisma Access 使用的命名约定，请参阅多租户配置概述。
- 或者，在创建租户级访问域后，您可以通过将管理员与访问域关联，创建管理用户以允许管理单个租户。
- 如果您有任何现有模板或设备组（例如，由 Panorama 管理的本地设备的模板也应供 Prisma Access 使用），请确保在创建和配置访问域时将这些设备组和模板域添加到 **Access Domain**（访问域）。如果没有将设备组和模板添加到访问域，则在云服务插件中配置 Prisma Access 组件时无法查看或选择它们。

©2025 Palo Alto Networks, Inc.

启用多租户并迁移第一个租户

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama) • 有关在 Prisma Access (Managed by Strata Cloud Manager) 中管理多个租户的信息，请参阅 Prisma SASE。	❑ Prisma Access 许可证

使用以下工作流程来启用多租户并将您现有的配置迁移到您创建的第一个租户。如果还没有任何配置，可以启用多租户并添加您的租户；然后配置这些租户。

启用多租户时，Prisma Access 将迁移您配置的以下组件：

- 所有服务连接和远程网络隧道接入信息，包括隧道配置。
- 现有移动用户接入信息。
- Strata Logging Service 信息
- 现有的自主 DEM (ADEM) 配置
- 用于服务连接、远程网络以及移动用户的模板、模板堆栈和设备组。

您需要指定用户数量（用于移动用户部署）、带宽（用于远程网络部署）以及要为每个部署分配的自主 DEM (ADEM)（如果您已购买 ADEM 许可证）。

由于这些设备组的改变，您创建了一个访问域并添加了迁移的设备组、模板和模板堆栈，如以下工作流程中所示。

如果您还没有 *Prisma Access* 配置，并且正在创建全新的多租户部署，请不要使用此工作流程；相反，请完成 向 Prisma Access 添加租户 中的步骤以创建第一个租户。

STEP 1 | 确定您要分配给此部署的许可单位数量。

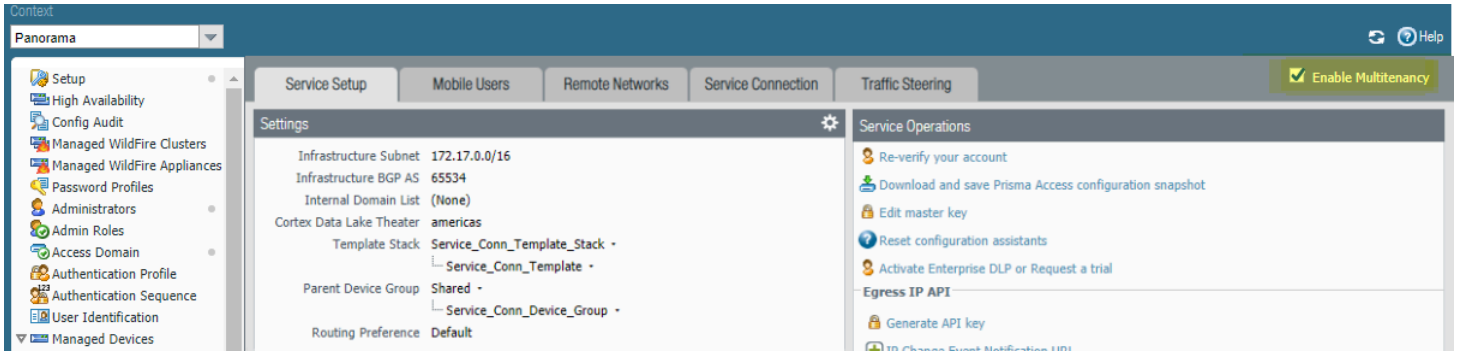
在 Prisma Access 将您的配置迁移到第一个租户时，您需要指定：

- 为租户的远程用户部署分配的 **Bandwidth**（带宽）（如果适用）。
- 为租户的移动用户部署分配的 **Users**（用户）（如果适用）。
- 为移动用户和远程网络分配的 ADEM 单元数量（如果适用）。

STEP 2 | 选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置）。

©2025 Palo Alto Networks, Inc.

STEP 3 | 选择 **Enable Multitenancy**（启用多租户）（位于页面右上角）。



启用多租户后，Panorama 将显示一条通知，告知您现有的 Prisma Access 配置已移至第一个租户。

在您启用多租户后，您的部署将永久更改为多租户部署，无法恢复到单租户模式。

STEP 4 | 点击 **OK**（确定）以将现有配置迁移到第一个租户。

此时将显示 **Tenants**（租户）页面，窗口中央显示饼图。

- 如果您拥有远程网络或移动用户许可证，则将显示可用的许可远程网络带宽和移动用户数量。
- （仅限远程网络和移动用户部署）如果您购买了自主 DEM 许可证，则将显示可用于 ADEM 的可用单位数量。
- 如果您已实施了 Clean Pipe 部署，则会显示租户的带宽。

STEP 5 | 选择要用于租户的部署类型。

- 对于远程网络部署和移动用户部署，或者要为租户配置这两种部署类型，请选择 **Remote Networks/Mobile Users**（远程网络/移动用户）。
- 要进行 Clean Pipe 部署，请选择 **Clean Pipe**。

  本节介绍如何为远程网络和/或移动用户部署类型配置租户。要配置 Clean Pipe 服务，请参阅Prisma Access for Clean Pipe。

©2025 Palo Alto Networks, Inc.

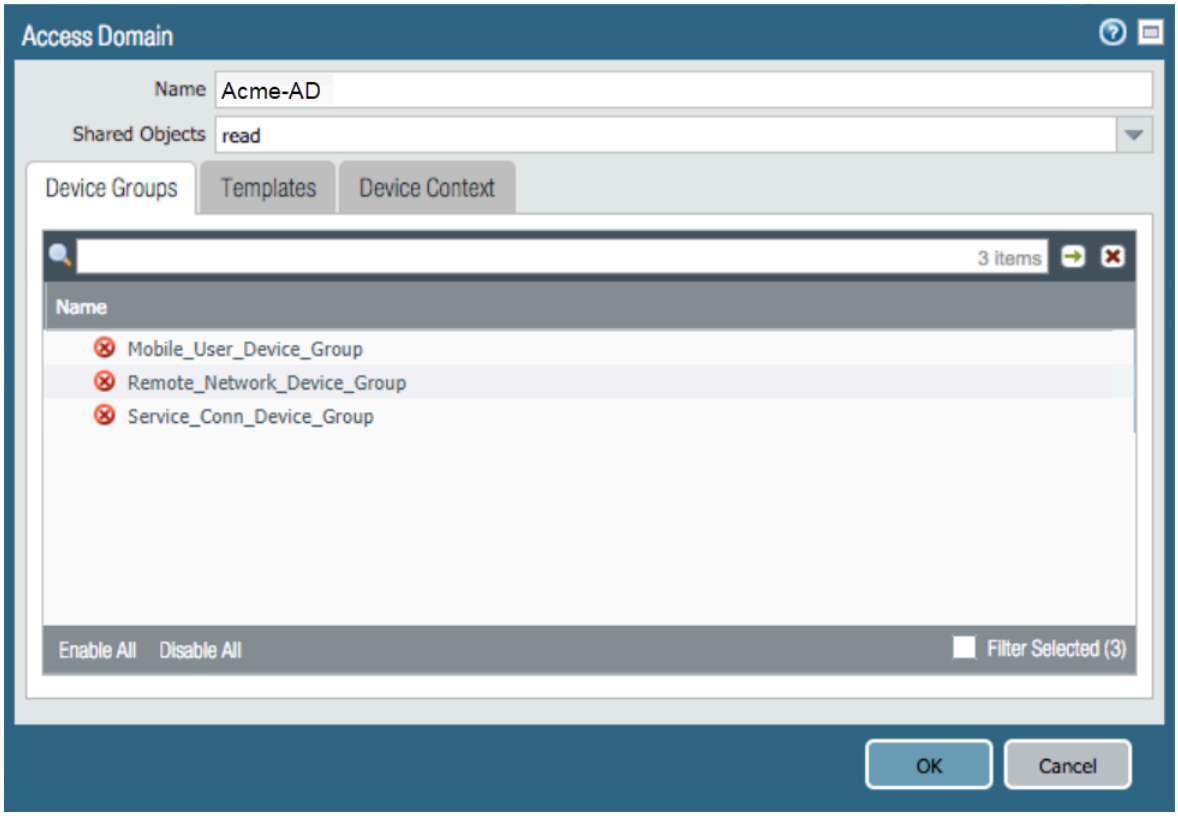
STEP 6 | 将现有配置迁移到第一个租户。

第一个迁移的子租户名称会根据您正在迁移的租户自动填充，且无法编辑。

1. 单击向下箭头，选择 **New Access Domain**（新建访问域）来创建新的访问域。
2. 在 **Name**（名称）中，输入访问域的名称，然后单击 **OK**（确定）。

   Prisma Access 会将 **Mobile_User_Device_Group**、**Remote_Network_Device_Group** 和 **Service_Conn_Device_Group** 设备组添加到新的访问域。

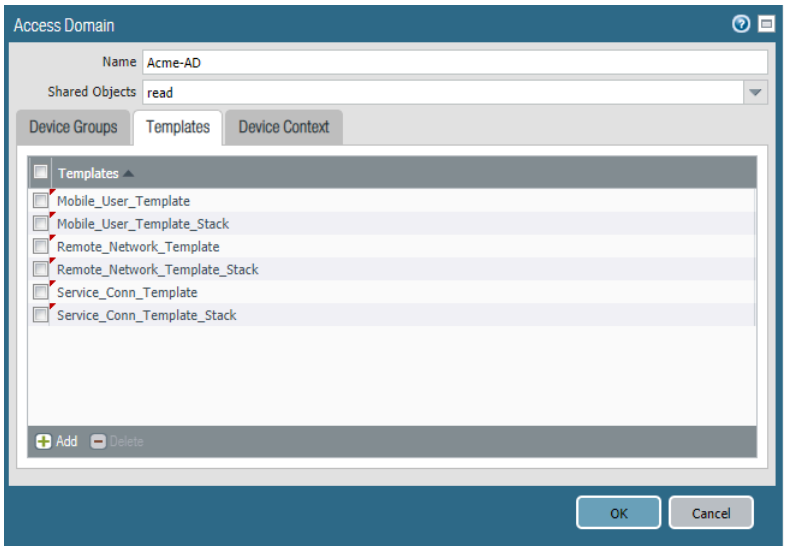
   请勿将默认的设备组和模板关联到除第一个迁移的子租户之外的其他子租户。



3. （可选）单击 **Templates**（模板）以确认 Prisma Access 已添加以下模板和模板堆栈：
   - **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**

     这些是标准 Prisma Access 部署的默认模板堆栈和模板；如果您添加了其他模板，请确保 Prisma Access 已添加这些模板。

©2025 Palo Alto Networks, Inc.

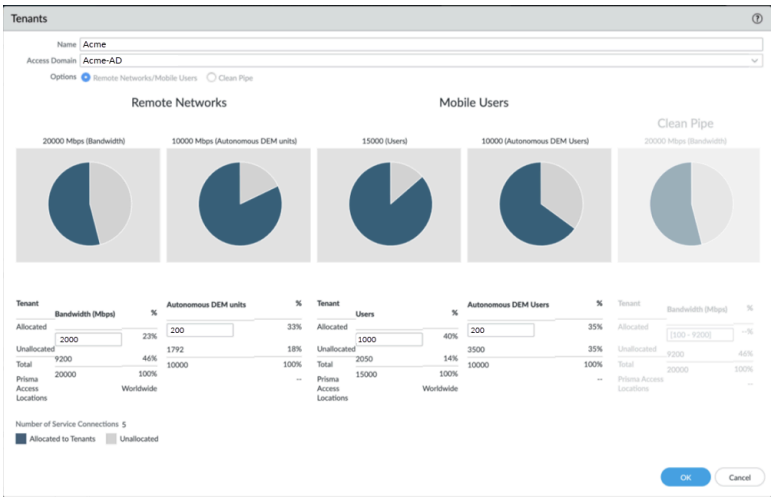


4. （可选）如果您有与此配置相关的其他模板，请选择这些模板。
5. 单击 **OK**（确定）以关闭 **Access Domain**（访问域）页面并回到 **Tenants**（租户）页面。

STEP 7 | 在远程网络的 **Bandwidth (Mbps)**（带宽 **(Mbps)**）字段中、移动用户的 **Users**（用户）字段中输入值，在 **Autonomous DEM Users**（自主 **DEM** 用户）中输入要为每个部署类型分配的用户数。

为租户分配 ADEM 单元时，请遵循以下准则：

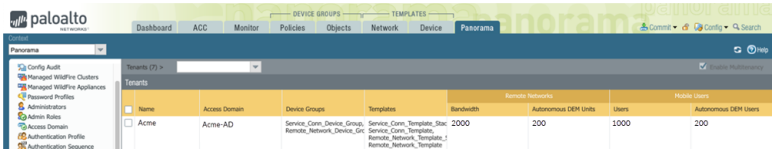
- 为移动用户和远程网络分配的 ADEM 单元数只能等于或小于基本许可证。
- 可分配的最小单元数为 200。
- 为租户分配 ADEM 单元后，可以编辑或删除这些单元。
- 如果没有为部署类型（移动用户或远程网络）购买 ADEM 许可证，则该选项将显示为灰色。



 ©2025 Palo Alto Networks, Inc.

STEP 8 | 单击 **OK**（确定）。

Panorama > **Cloud Services**（云服务） > **Configuration**（配置）页面显示了第一个成功迁移的租户，**Tenants**（租户）区域上方将增加一个 **Tenants**（租户）下拉菜单。



STEP 9 | 确保所有模板和设备组都已填充到租户中。

1. 从下拉列表中选择租户。
2. 转到 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置）。
3. 选择 **Service Setup**（服务设置）。
4. 单击齿轮以编辑 **Settings**（设置）。
5. 确保设置中填充了正确的模板堆栈、模板和设备组（Service_Conn_Template_Stack、Service_Conn_Template 和 Service_Conn_Device_Group）。
6. 转到您已有配置的其他选项卡（例如，**Mobile Users** — **GlobalProtect**（移动用户 — **GlobalProtect**）、**Mobile Users**—**Explicit Proxy**（移动用户 — 显式代理）、**Remote Networks**（远程网络）或 **Service Connection**（服务连接）），单击齿轮以编辑 **Settings**（设置），并确保设置中填充了正确的模板堆栈、模板和设备组。

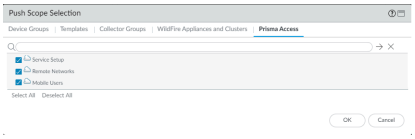
STEP 10 | 在本地将更改提交到 Panorama（**Commit**（提交） > **Commit to Panorama**（将更改提交到 **Panorama**）。

STEP 11 | 选择 **Commit**（提交） > **Commit to Panorama**（提交到 **Panorama**）以在管理 Prisma Access 的 Panorama 上本地保存您的更改。

如果不执行本地提交，则当您提交和推送更改时，Prisma Access 组件不会显示在推送范围内。

STEP 12 | 提交并推送您的更改，使其在 Prisma Access 中处于活动状态。

1. 选择 **Commit**（提交） > **Commit and Push**（提交并推送）和推送范围中的 **Edit Selections**（编辑选择）。
2. 选择 **Prisma Access**，然后选择您创建的租户，然后依次选择 **Service Setup**（服务设置）、**Remote Networks**（远程网络）和 **Mobile Users**（移动用户）。

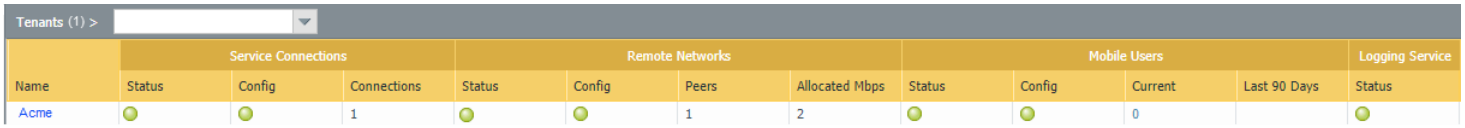


3. 单击 **OK**（确定）保存对推送范围所作的更改。
4. **Commit**（提交）并 **Push**（推送）您的更改。

 ©2025 Palo Alto Networks, Inc.

STEP 13 | 选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态）。

状态页面显示所有租户的状态。因为您只创建了一个租户，因此只会显示该租户。如果您从下拉菜单中选择该租户，则将显示该租户的详细状态。



从下拉菜单中选择一个租户后，将回到该租户的状态页面。

STEP 14 | 继续向 Prisma Access 中添加更多租户。

©2025 Palo Alto Networks, Inc.

向 Prisma Access 添加租户

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama) • 有关在 Prisma Access (Managed by Strata Cloud Manager) 中管理多个租户的信息，请参阅 Prisma SASE。	❑ Prisma Access 许可证

作为第一个租户迁移现有信息后，您可以创建并配置其他租户。对于第一个租户之后创建的每个租户，Prisma Access 都会创建一个单独的访问域，该域具有自己的一组模板堆栈和模板以及自己的域组。

使用此工作流将更多租户添加到 Prisma Access。

如果您要创建全新的多租户部署，请使用此工作流添加第一个租户以及其他租户。如需更多信息，请参阅 创建全新的多租户部署。

STEP 1 | 以超级用户身份登录到 Panorama。

STEP 2 | 添加并配置租户。

1. 选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置），然后 **Add**（添加）新租户。

   确保选择 **Remote Networks/Mobile Users**（远程网络/移动用户）；要创建和配置 Clean Pipe 部署，请参阅Prisma Access for Clean Pipe。
2. 为该租户指定描述性 **Name**（名称）。
3. **Add**（添加）新的 **Access Domain**（访问域），输入描述性 **Name**（名称），然后单击 **OK**（确定）返回 **Tenants**（租户）窗口。

   单击 **OK**（确定）后，Prisma Access 会自动创建模板、模板堆栈和设备组，并将它们关联到您创建的访问域。

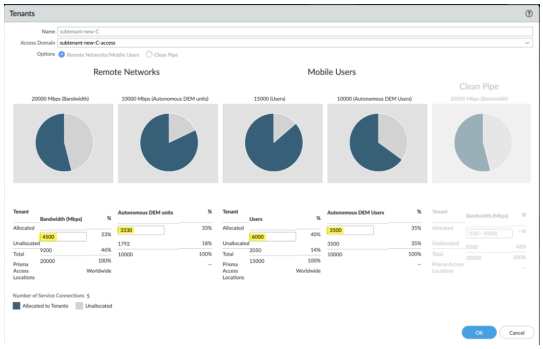
STEP 3 | 指定要分配给 **Remote Networks**（远程网络）的 **Bandwidth**（带宽）**(Mbps)** 量以及要分配给 **Mobile Users**（移动用户）的 **Users**（用户）数。

©2025 Palo Alto Networks, Inc.

STEP 4 | （仅限具有自主 DEM 的部署）如果您购买了自主 DEM (ADEM) 许可证，请选择要为 ADEM 分配的单元数。

为租户分配 ADEM 单元时，请遵循以下准则：

- 为移动用户和远程网络分配的 ADEM 单元数只能等于或小于基本许可证。
- 可分配的最小单元数为 200。
- 为租户分配 ADEM 单元后，可以编辑或删除这些单元。
- 如果没有为部署类型（移动用户或远程网络）购买 ADEM 许可证，则该选项将显示为灰色。

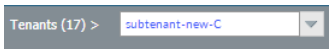


STEP 5 | 单击 **OK**（确定）以创建第一个租户。

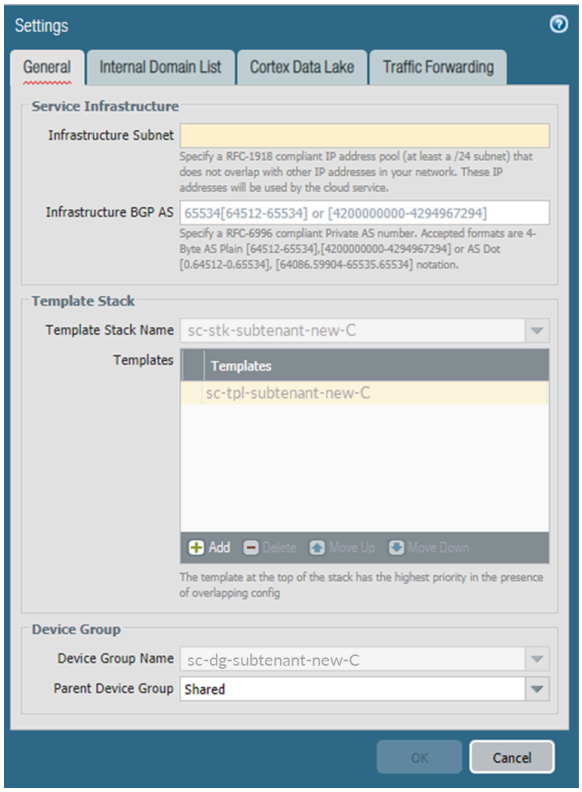
©2025 Palo Alto Networks, Inc.

STEP 6 | 确保 Prisma Access 将模板堆栈、模板和设备组服务设置应用于您刚刚创建的租户的服务连接设置。

1. 从 **Tenant**（租户）下拉列表中选择您创建的租户。



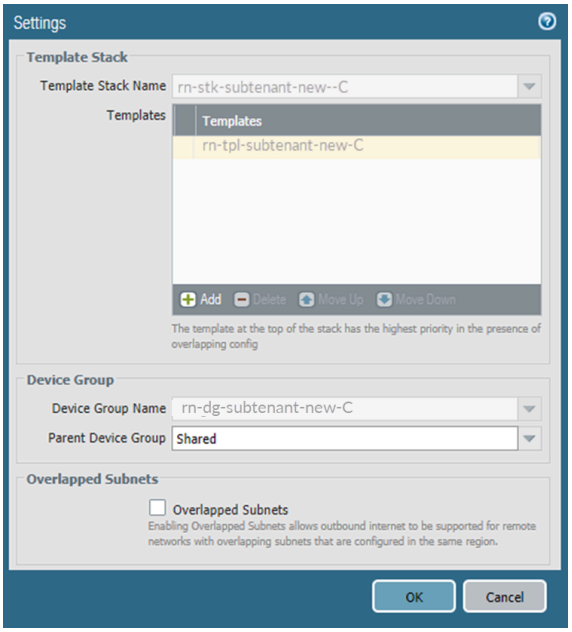
2. 选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Service Setup**（服务设置）。
3. 单击 **Settings**（设置）区域右侧的齿轮图标来编辑设置。
4. 确保 Prisma Access 将模板堆栈 (**sc-stk-*tenant***)、模板 (**sc-tpl-*tenant***) 和设备组 (**sc-dg-*tenant***) 关联到服务连接设置。
5. 确保将 **Parent Device Group**（父设备组）设置为 **Shared**（共享）， 然后单击 **OK**（确定）。



 ©2025 Palo Alto Networks, Inc.

STEP 7 | 确保 Prisma Access 将模板堆栈、模板和设备组应用于远程网络设置。

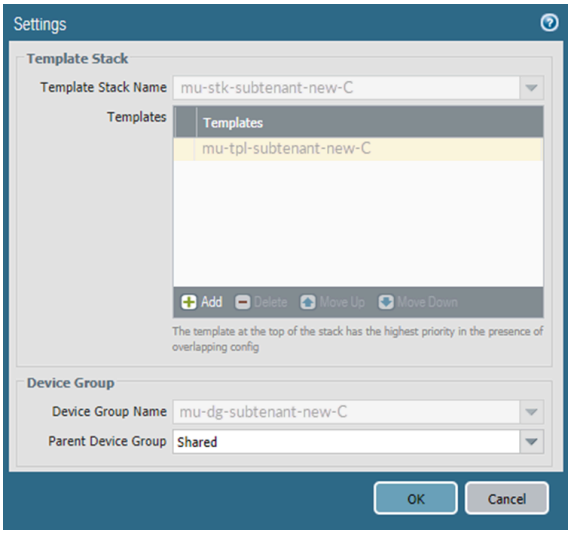
1. 选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Remote Networks**（远程网络），然后单击 **Settings**（设置）区域右侧的齿轮图标来编辑设置。
2. 确保 Prisma Access 将模板堆栈 (**rn-stk-***tenant*)、模板 (**rn-tpl-***tenant*) 和设备组 (**rn-dg-***tenant*) 关联到远程网络设置。
3. 确保将 **Parent Device Group**（父设备组）设置为 **Shared**（共享），然后单击 **OK**（确定）。



 ©2025 Palo Alto Networks, Inc.

STEP 8 | 确保 Prisma Access 将模板堆栈、模板和设备组应用于移动用户设置。

1. 选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Mobile Users**（移动用户），然后单击 **Settings**（设置）区域右侧的齿轮图标来编辑设置。
2. 确保 Prisma Access 将模板堆栈 (**mu-stk-***tenant*)、模板 (**mu-tpl-***tenant*) 和设备组 (**mu-dg-***tenant*) 关联到远程网络设置。
3. 确保将 **Parent Device Group**（父设备组）设置为 **Shared**（共享），然后单击 **OK**（确定）。



STEP 9 | 在本地将更改提交到 Panorama（**Commit**（提交） > **Commit to Panorama**（将更改提交到 **Panorama**）。

STEP 10 | （仅限移动用户部署）— 添加基础架构子网，然后提交并推送更改以使其在 Prisma Access 中处于活动状态。

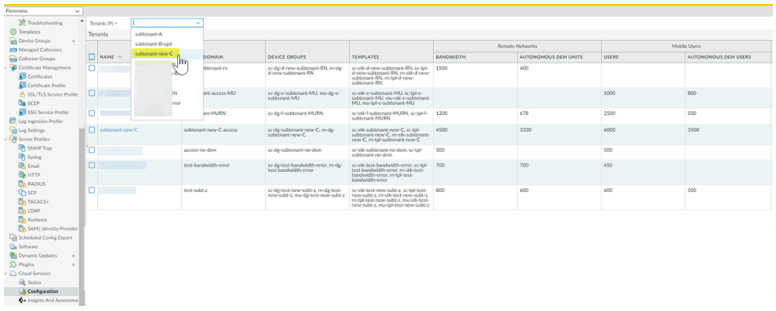
需要执行这些步骤才能使移动用户更改生效。

1. 选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Service Setup**（服务设置），单击齿轮图标以编辑设置，然后配置基础架构子网。
2. 选择 **Commit**（提交） > **Commit and Push**（提交并推送），然后在推送范围中选择 **Edit Selections**（编辑选择），请务必选择 **Mobile Users**（移动用户）。
3. 单击 **OK**（确定）保存对推送范围所作的更改。
4. **Commit**（提交）并 **Push**（推送）更改。

©2025 Palo Alto Networks, Inc.

STEP 11 | 通过选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > ***tenant-name***选择您创建的新租户，然后继续配置租户。

1. 配置服务基础架构。
2. 创建服务连接以允许访问私有应用。
3. 如果您获得了远程网络许可，请加入并配置远程网络。
4. 如果您获得了远程用户许可，请设置 Prisma Access (Managed by Panorama) 的 Global Protect。



 ©2025 Palo Alto Networks, Inc.

删除租户

完成以下步骤来删除 Prisma Access (Managed by Panorama) 部署中的租户。

在什么情况下使用此操作？	需要提供什么？
• Prisma Access (Managed by Panorama) • 有关在 Prisma Access (Managed by Strata Cloud Manager) 中管理多个租户的信息，请参阅 Prisma SASE。	❑ Prisma Access 许可证

- 虽然可以删除多租户部署中的所有租户，但不能删除添加或删除租户的管理员级别 *Prisma Access* 配置。
- 删除租户时，*Prisma Access* 会删除您已获得许可的模板和设备组集，但不会删除未获得许可的集。例如，如果您具有 *Prisma Access* 用户许可证并删除租户，则 *Prisma Access* 将删除与移动用户相关的模板堆栈、模板和设备组，但不会删除它为 *Networks* 的未授权 *Prisma Access* 创建的集。删除租户后，可以手动删除这些未使用的模板和设备组集。

STEP 1 | 从管理 Prisma Access 的 Panorama 中，选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置）。

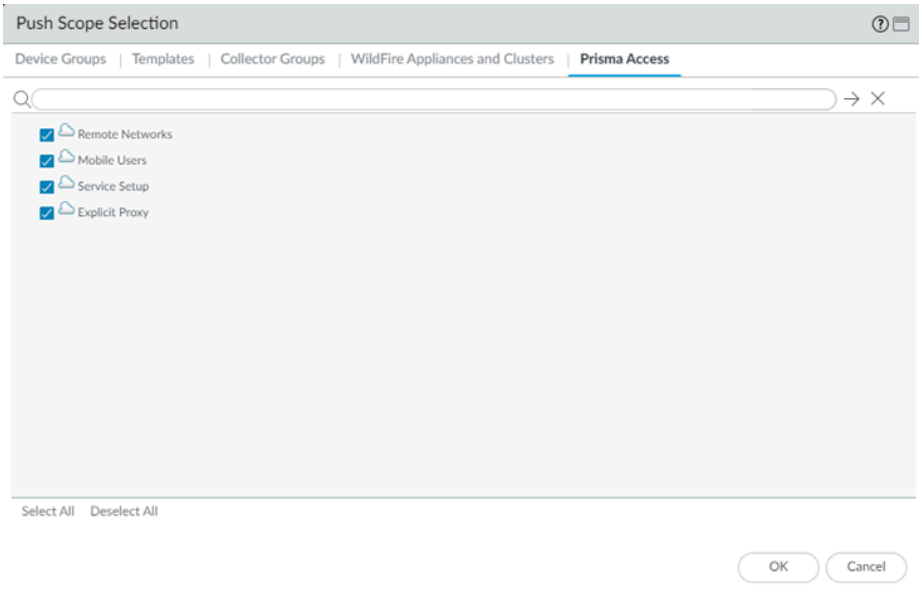
STEP 2 | 选择租户，并删除与其相关的所有配置。

最佳实践是执行此步骤作，以确保从租户中删除所有配置，包括任何服务连接、移动用户、远程网络或 Clean Pipe 配置。

©2025 Palo Alto Networks, Inc.

STEP 3 | 提交并将更改推送到 Prisma Access。

1. 选择 **Commit**（提交） > **Push to Devices**（推送到设备）。
2. 单击 **Edit Selections**（编辑选择），确保选择了已删除的所有组件（包括远程网络、移动用户、服务设置、显式代理和 Clean Pipe，具体取决于您的部署）。



3. 单击 **Push**（推送）。

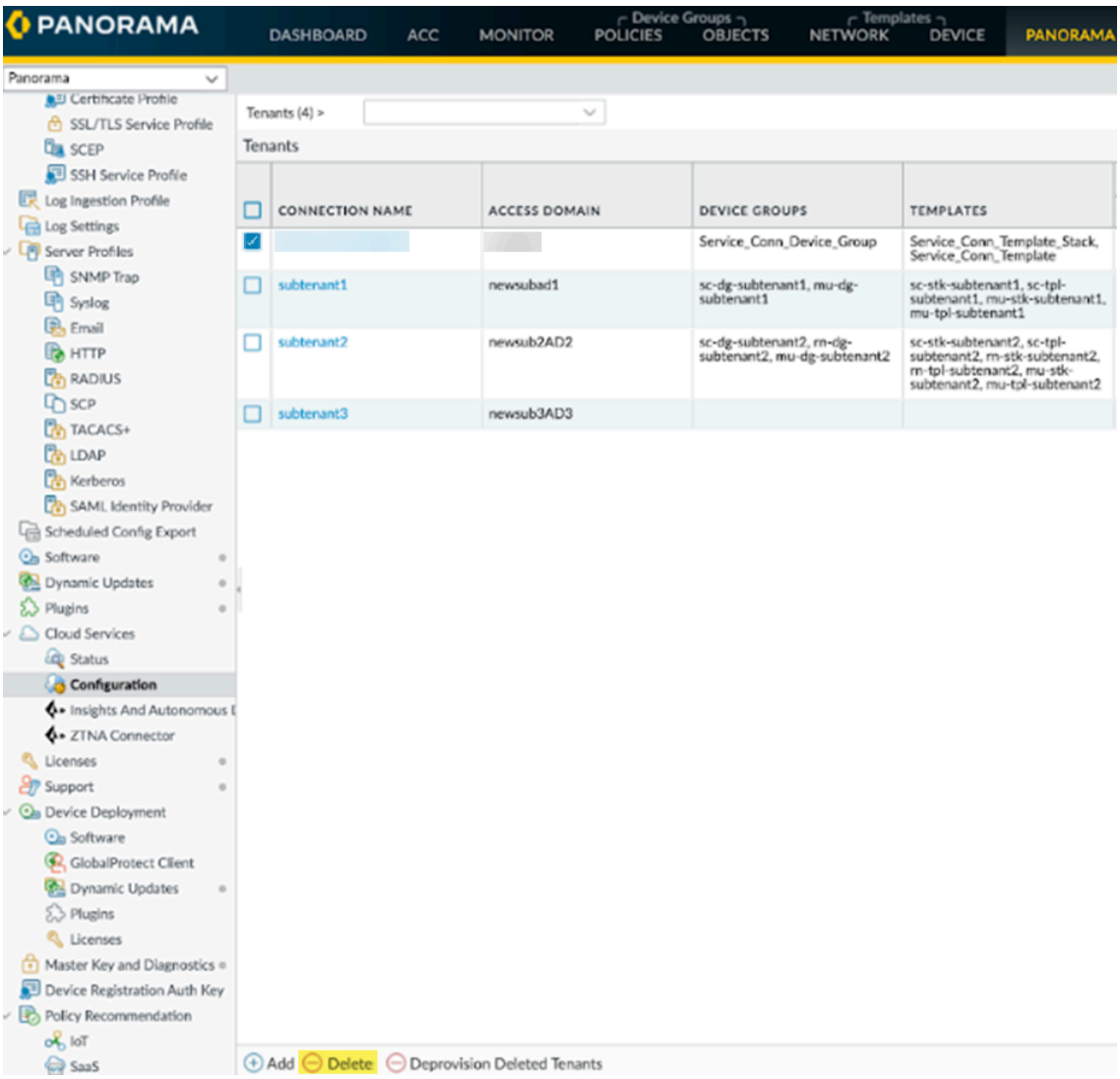
©2025 Palo Alto Networks, Inc.

STEP 4 | 选择一个或多个租户，然后单击 **Delete**（删除）以将其删除。

删除租户只是将其从 Panorama 中移除，而不会从 Prisma Access 基础设施中移除。要删除租户并将其从基础设施中移除，请在删除后执行本地提交，然后为其取消配置，如以下步骤所示。

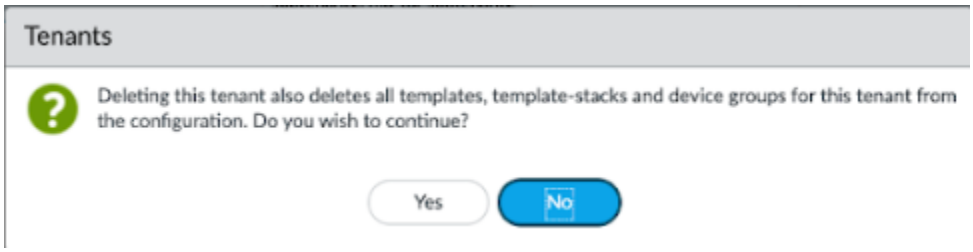
如果您删除了租户，但没有取消配置，则仍然可以通过联系 Palo Alto Networks 支持来找回。

如果您将 *Panorama* 设备设置为高可用性 *(HA)* 配置，则只能在 *HA* 对中的活动 *Panorama* 设备上执行删除和取消配置操作。



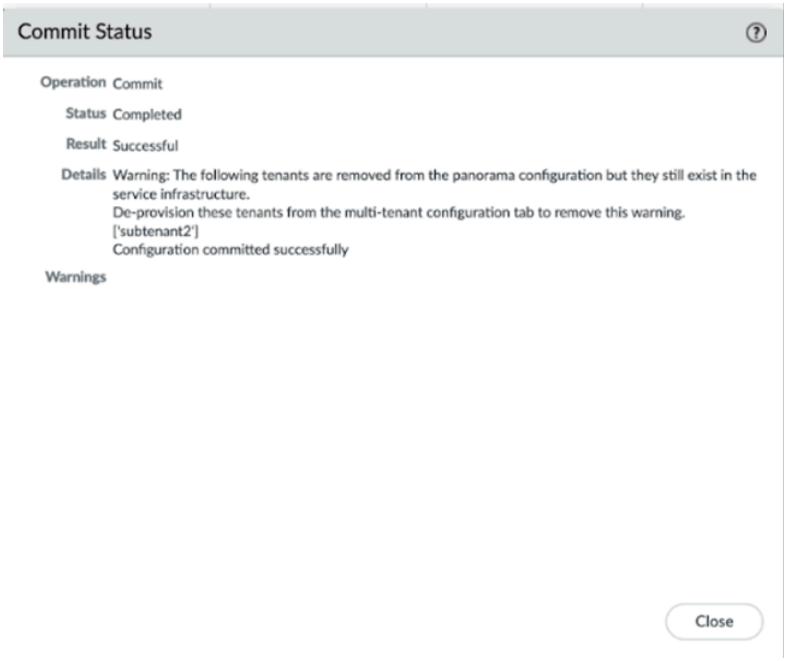
将显示一个弹出窗口，确认租户删除过程。单击 **Yes**（是）继续删除，或单击 **No**（否）取消删除。

©2025 Palo Alto Networks, Inc.



STEP 5 | 要在本地将更改提交到 Panorama，可选择 **Commit**（提交） > **Commit to Panorama**（提交到 **Panorama**），然后单击 **Commit**（提交）来提交更改。

本地提交后，会将租户标记为删除并从租户列表中移除，但不会从 Prisma Access 基础设施中移除。将会弹出一个窗口，显示已删除的租户。



 ©2025 Palo Alto Networks, Inc.

STEP 6 | （可选）要完全从 Prisma Access 基础设施中移除租户，可选择 **Deprovision Deleted Tenants**（取消配置已删除的租户）。

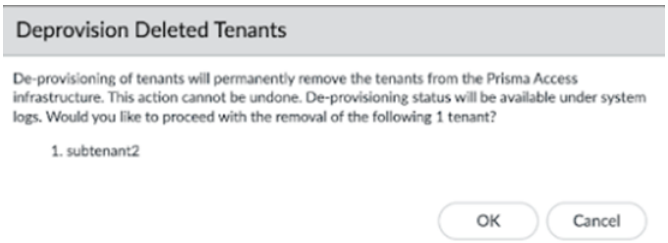
取消租户配置：

- 将其从配置和 Prisma Access 基础设施中删除，并且您无法找回。
- 收回分配给租户的许可证。



将显示一条确认消息，其中包含要取消配置的租户的名称；单击 **OK**（确定）以继续取消配置租户，或单击 **Cancel**（取消）以取消该操作。

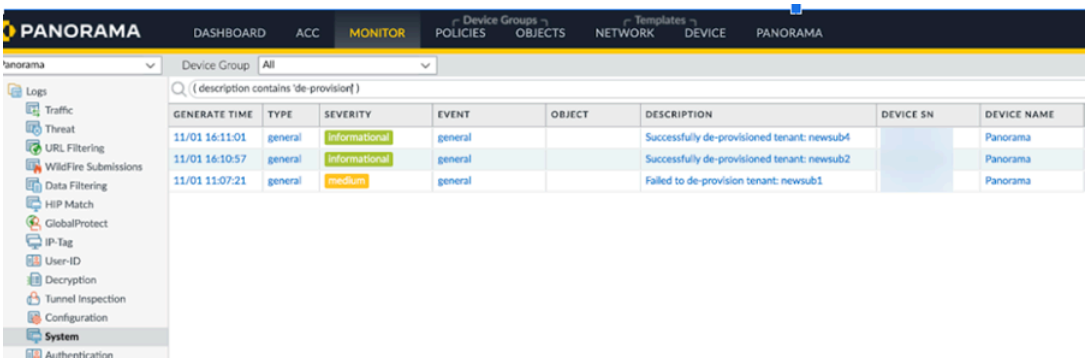
取消配置租户后，将完全删除该租户以及为其分配的所有资源，并收回分配给这些租户的许可证。无法找回租户。



如果不需要取消配置租户，则会显示以下消息。



STEP 7 | （可选）转到 **Monitor**（监控） > **Logs**（日志） > **System**（系统），检查取消配置操作的状态。日志中会显示取消配置操作和租户的名称。



 ©2025 Palo Alto Networks, Inc.

创建租户级管理用户

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama) • 有关在 Prisma Access (Managed by Strata Cloud Manager) 中管理多个租户的信息，请参阅 Prisma SASE。	❑ Prisma Access 许可证

您应该为每个租户创建一个管理用户。这样，租户级管理员可以查看并更改其租户配置，但无权访问其他租户。要为特定租户创建管理用户，请完成以下任务。有关租户级管理用户的基于角色的访问控制 (RBAC) 的更多信息，请参阅控制租户级管理用户的基于角色的访问权限。

由于 ***Monitor***（监控） ***> Logs***（日志） ***> System***（系统）选项不可用，因此管理单个租户的用户无法查看系统日志。此限制适用于具有 ***Device Group and Template***（设备组和模板）管理员角色的所有管理员。只有超级用户可以在多租户模式下查看系统日志。

©2025 Palo Alto Networks, Inc.

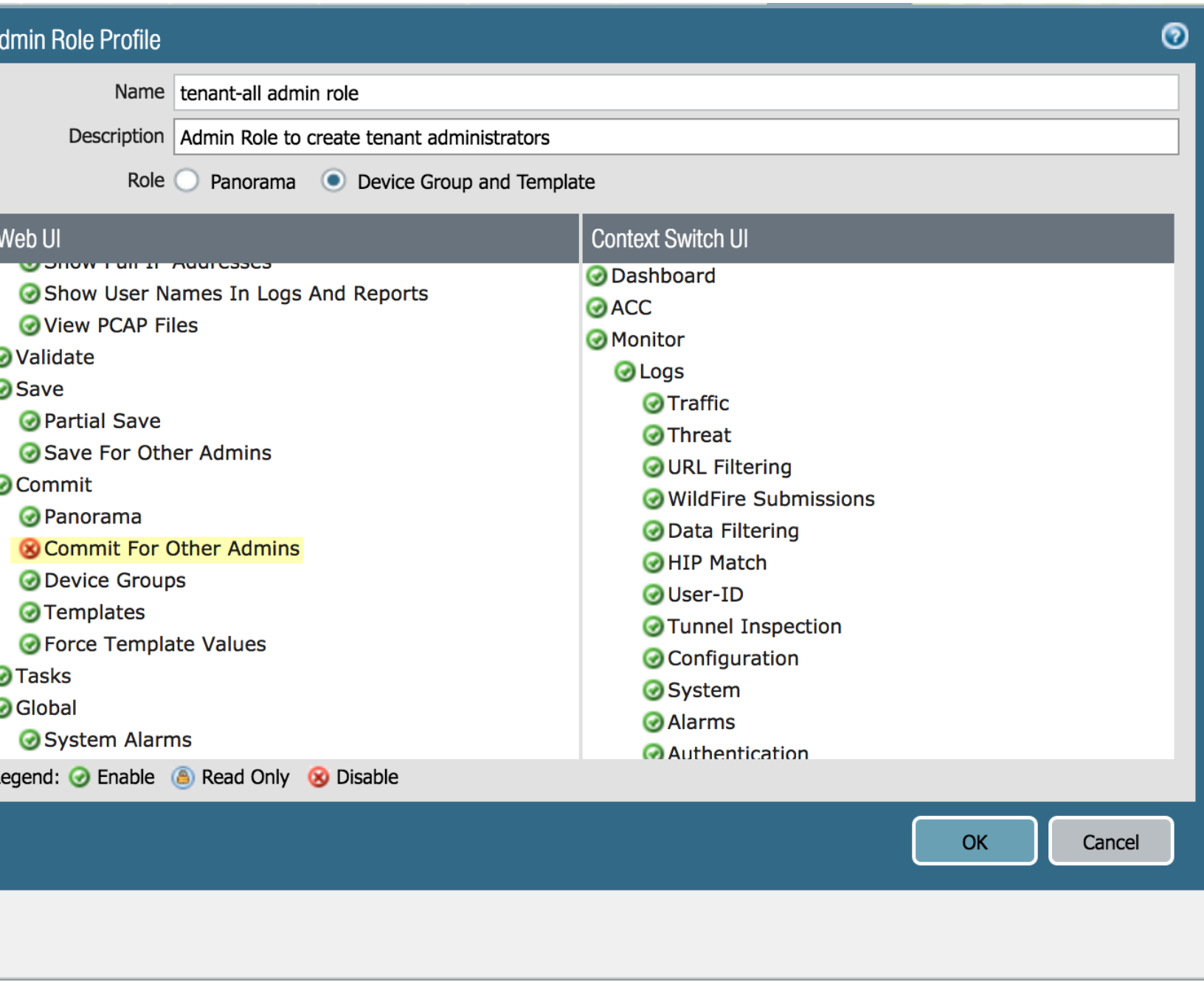
STEP 1 | 创建类型为 **Device Group and Template**（设备组和模板）的管理员角色。

1. 选择 **Panorama** > **Admin Roles**（管理员角色）。
2. **Add**（添加）**Role**（角色）为 **Device Group and Template**（设备组和模板）的管理员角色配置文件。
3. 单击 **OK**（确定）。

您可以创建单个管理员角色配置文件并在多个租户之间共享；但是，您必须为每个租户创建一个单独的管理员。

在您根据组织的需求定制管理员角色时，我们建议取消选择 ***Commit for Other Admins***（为其他管理员提交）。取消选择此选项可让租户级用户仅提交他们所做的更改，并防止他们无意中提交其他租户级管理用户所进行的尚未提交的其他更改。

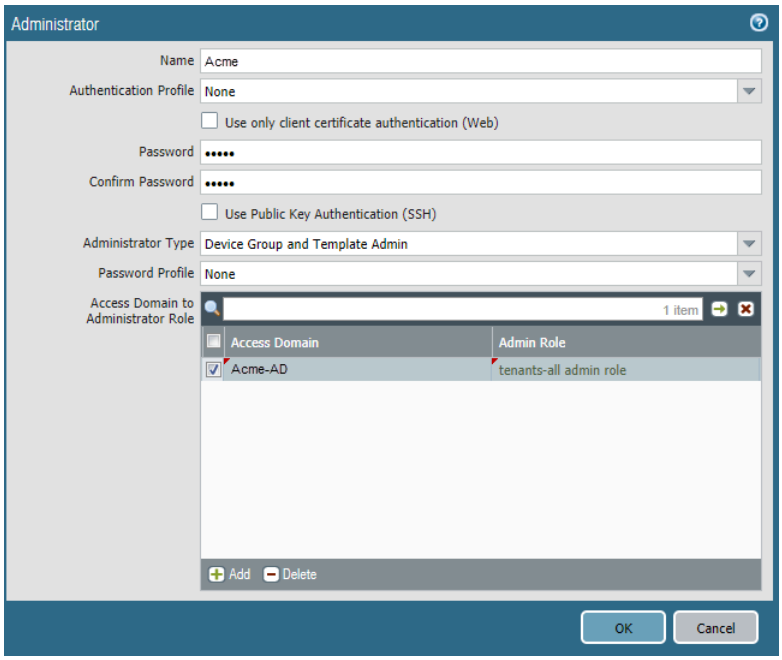
©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.

STEP 2 | 为该租户创建并配置管理员。

1. 选择 **Panorama** > **Administrators**（管理员）。
2. **Add**（添加）管理员。
3. 输入并确认新管理员的 **Password**（密码）。
4. 将 **Administrator Type**（管理员类型）指定为 **Device Group and Template Admin**（设备组和模板管理员）。
5. 指定与该租户的设备组关联的 **Access Domain**（访问域）。
6. 指定您在步骤 1 中为该租户创建的 **Admin Role**（管理员角色）。



STEP 3 | 单击 **OK**（确定）。

STEP 4 | 重复步骤 2 和 3，以根据需要添加其他用户来管理您的租户。

STEP 5 | 选择 **Commit**（提交） > **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

©2025 Palo Alto Networks, Inc.

控制租户级管理用户的基于角色的访问权限

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama) • 有关在 Prisma Access (Managed by Strata Cloud Manager) 中管理多个租户的信息，请参阅 Prisma SASE。	❑ Prisma Access 许可证

如果您管理多租户部署，则可以使用基于角色的访问控制 (RBAC) 创建租户级管理用户。

要在 Panorama 中修改租户级管理用户的 RBAC 级别访问权限，请创建租户级管理用户，使用具有 **Device Group and Template**（设备组和模板）**Role**（角色）的管理员角色配置文件，然后 **Enable**（启用）、**Disable**（禁用）或授予对 Panorama **Web UI** 区域的 **Read Only**（只读）访问权限。使用此方法管理租户级用户对所有 Panorama 组件的访问，但对您管理 Prisma Access 的云服务插件的访问除外。

如果要限制租户级用户在 Panorama 中配置 Prisma Access 组件，则不能使用管理员角色。要禁止用户配置特定于 Prisma Access 的配置任务，您必须阻止用户访问云服务插件，这也会阻止他们查看该插件。使用此方法，您可以为安全专业人员创建管理用户，该用户有权更改安全策略并将这些更改推送到 Panorama，但不能查看或更改 Prisma Access 配置。

您可以为用户启用或禁用对云服务插件的访问权限，但您不能授予用户只读访问权限；如果用户有权查看云服务插件，则用户还可以对其组件（包括 *Prisma Access*）进行配置更改。

下表列出了租户级管理角色示例以及您创建这些角色所需执行的步骤。

租户级配置示例	配置任务
创建以网络为中心的用户，该用户： • 可以编辑插件配置 • 可以提交到 Panorama • 可以将配置推送到 Prisma Access	创建租户级管理用户，在 **Admin Role Profile**（管理员角色配置文件）中启用 **Save**（保存）和 **Commit**（提交）权限，并禁用您不希望租户级管理用户拥有的任何权限或这些权限设置为 **Read Only**（只读）。
创建以安全为中心的用户，该用户： • 可以查看和更改安全策略 • 可以提交到 Panorama • 无法查看或更改云服务插件 • 无法将配置推送到 Prisma Access（需要超级用户角色才能推送配置）	为了防止租户级管理用户查看或访问插件，请删除租户级管理员的插件访问权限。对于所有其他与 Panorama 相关的权限，请更改用户的管理员角色权限。

©2025 Palo Alto Networks, Inc.

租户级配置示例	配置任务
创建混合用户，该用户： • 拥有对云服务插件的只读访问权限 • 拥有对安全策略的读写访问权限 • 无法将配置推送到 Prisma Access（需要超级用户角色才能推送配置）	此配置不可行。您无法将云服务插件的访问权限设置为只读。您只能向管理员用户提供查看访问权限，并且他们可以使用云服务插件来更改配置，或者禁止这些用户查看云服务插件。

删除租户级管理用户的插件访问权限

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama) • 有关在 Prisma Access (Managed by Strata Cloud Manager) 中管理多个租户的信息，请参阅 Prisma SASE。	❑ Prisma Access 许可证

在正常的多租户配置中，您使用访问域 向 Prisma Access 添加租户 并将每个访问域与一个租户关联。要防止租户级别的管理用户查看或更改 Prisma Access 的配置，请创建访问域，但不要将其与租户关联。

由于您将访问域关联到租户的设备组和模板堆栈，因此租户级别的管理用户在租户级别具有 RBAC 访问权限，并且只能为该租户执行配置。由于您未将访问域与 Prisma Access 中的租户关联，因此访问域无法查看云服务插件，该插件提供对 Prisma Access 的访问。通过这种方式，您可以创建一个可以执行租户级配置任务的用户，而无需访问、查看或更改 Prisma Access 的配置。

要为管理级别用户删除 Prisma Access，请完成以下任务。

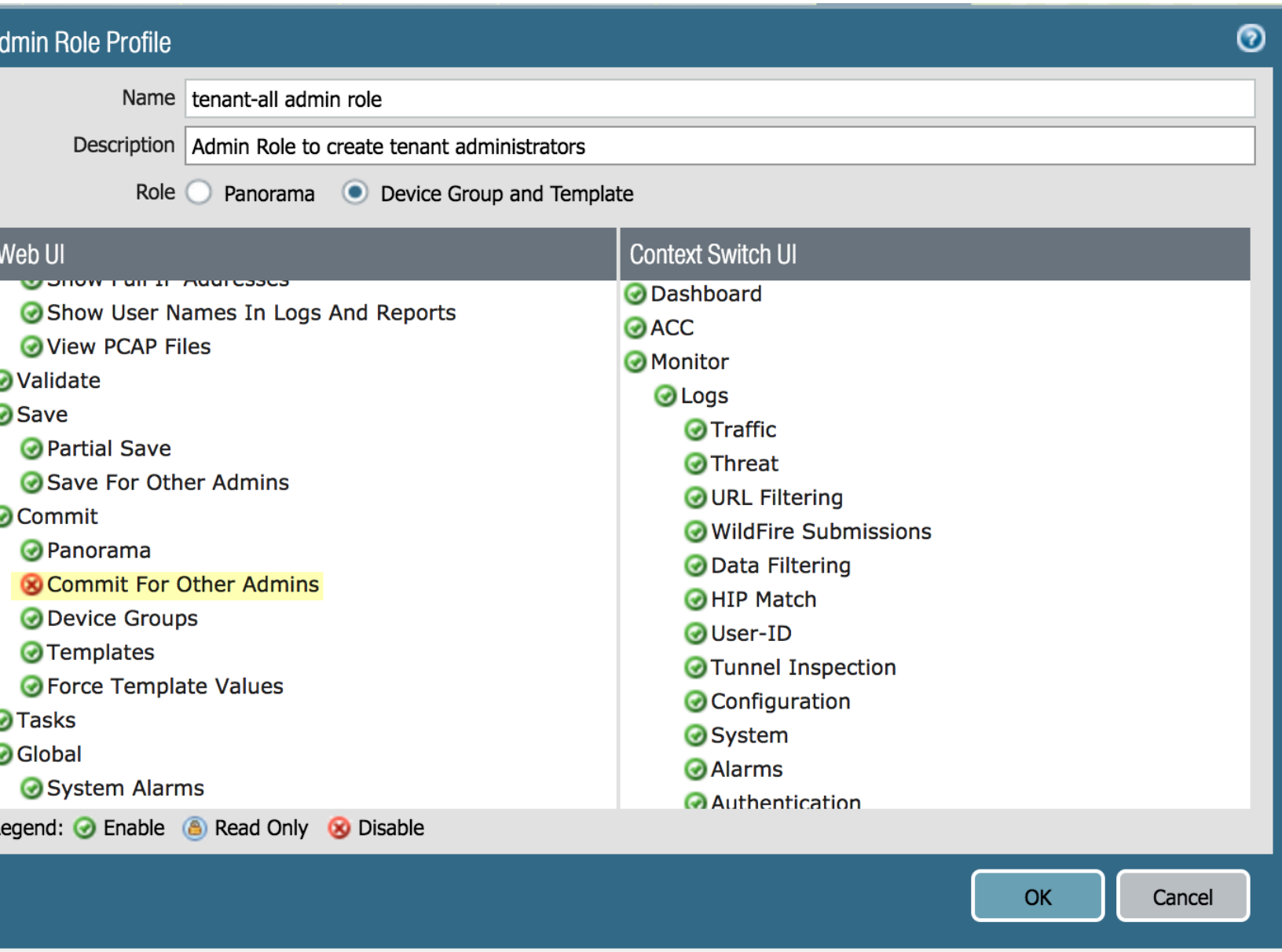
此任务假设您有租户的 向 Prisma Access 添加租户 模板、模板堆栈和设备组；您将把它们关联到租户级别的管理用户。

©2025 Palo Alto Networks, Inc.

STEP 1 | 创建类型为 **Device Group and Template**（设备组和模板）的管理员角色。

1. 选择 **Panorama** > **Admin Roles**（管理员角色）。
2. **Add**（添加）**Role**（角色）为 **Device Group and Template**（设备组和模板）的管理员角色配置文件。
3. 单击 **OK**（确定）。

   您可以创建一个管理员角色配置文件并在多个租户之间共享。

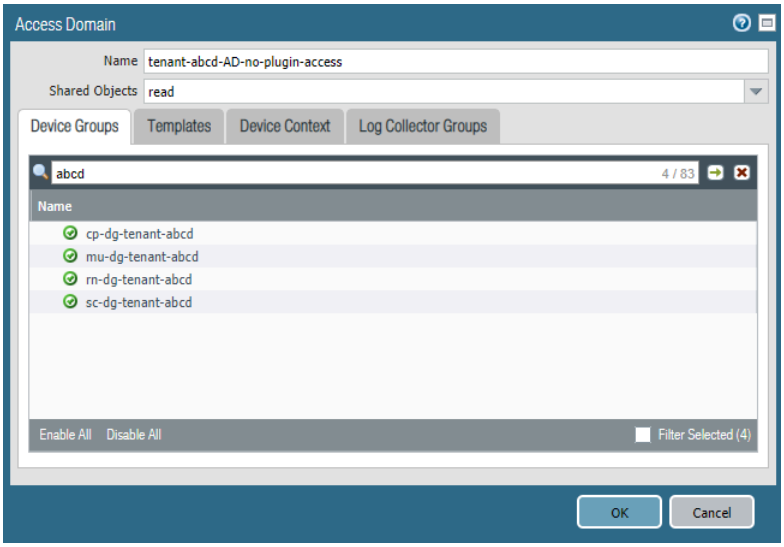


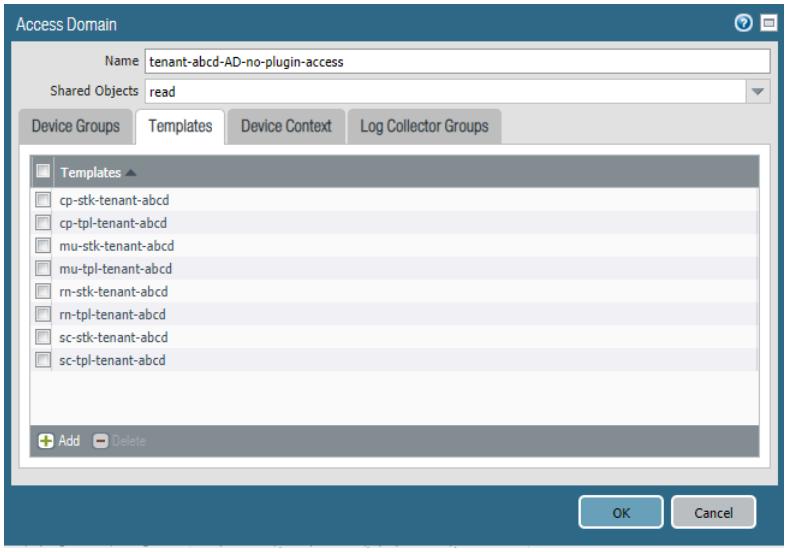
STEP 2 | 选择 **Panorama** > **Access Domain**（访问域）并 **Add**（添加）一个 Access Domain（访问域）。

 ©2025 Palo Alto Networks, Inc.

STEP 3 | 指定与该租户相关联的 **Device Groups**（设备组）和 **Templates**（模板）。

如果您创建的任何设备组是 ***Shared***（共享）父设备组下其他设备组的子设备组或孙设备组，请仅选择最低层次级别的设备组（子设备组或孙设备组）；不要选择父设备组，否则提交时会出现错误。



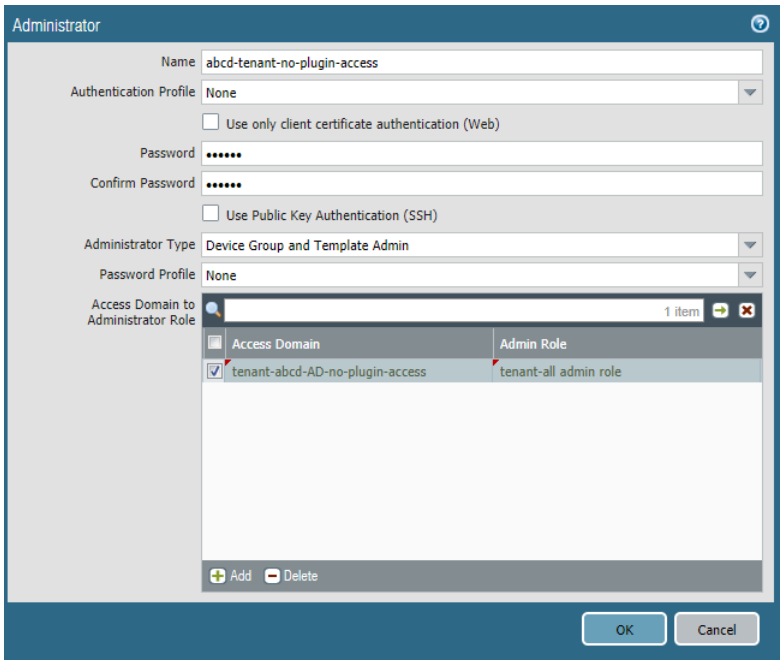


 ©2025 Palo Alto Networks, Inc.

STEP 4 | 为租户级管理用户创建并配置管理员，从而指定您刚才创建的访问域。

1. 选择 **Panorama** > **Administrators**（管理员）。
2. **Add**（添加）管理员。
3. 输入并确认新管理员的 **Password**（密码）。
4. 将 **Administrator Type**（管理员类型）指定为 **Device Group and Template Admin**（设备组和模板管理员）。
5. 指定与该租户的设备组关联的 **Access Domain**（访问域）。
6. 指定您在步骤 1 中为该租户创建的 **Admin Role**（管理员角色）。

   完成此示例后，**abcd-tenant-no-plugin-access** 管理用户将拥有基于您在管理员角色配置文件中定义的权限，但无法查看或配置云服务插件（包括 Prisma Access）。但是，请注意，他们将无法将他们所做的任何更改推送到云。



STEP 5 | 选择 **Commit**（提交） > **Commit to Panorama**（提交到 **Panorama**），并 **Commit**（提交）更改。

 ©2025 Palo Alto Networks, Inc.

在多租户部署中按设备组 ID 对日志进行排序

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama) • 有关管理多个租户的信息 Prisma Access (Managed by Strata Cloud Manager)请参阅 Prisma SASE。	❑ Prisma Access 许可证

要在 Panorama 中按租户手动对日志进行排序，请选择 “监控 > 日志”，然后选择与该租户关联的设备组 以显示该设备组的日志。但是，如果您将日志转发到外部设备，则可能需要在租户级别对这些日志进行排序。为此，请在与设备组关联的日志中找到设备组 ID，然后使用该组 ID 到设备组的映射将日志与租户关联。

日志中有四个与设备组相关的字段：**DG** 层次结构 **1** 级、**DG** 层次结构 **2** 级、**DG** 层次结构 **3** 级和 **DG** 层次结构 **4** 级。这些字段显示其层次结构中的设备组 ID。共享设备组（级别 0）不包含在此结构中。

DG 层次结构 **1** 级 是指层次结构中的第一个设备组级别。如果您添加了子设备组或孙设备组， 则 **DG** 层次结构级别 **2** 到 **DG** 层次结构级别 **4** 字段分别显示从子组到曾孙组的层次结构。

要按租户查找日志，请完成以下任务。

STEP 1 | 查找与设备组关联的设备组 ID。

- 要使用 CLI 命令查找此信息，请以超级用户（管理员级用户）身份登录 Panorama，在配置模式下输入 `show readonly` 命令，然后查看 设备组 标题中的值。设备组的 ID 显示在设备组名称下方。以下示例显示 **acme-sc** 设备组的设备 ID 为 **20**。

  请注意，这些设备组位于层次结构的第一级（**DG** 层次结构级别 **1**）；您将在下一步的查询中使用该信息。

  ```
  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 {
  ```

- 要使用 API 查询，请输入以下 API 命令：

  ```
  /api/?type=op&cmd=<show><dg-hierarchy></dg-hierarchy></show>
  ```

  有关使用带有日志的 *API* 的更多信息，请参阅 检索日志 (API)。

STEP 2 | 使用设备组 ID 到设备组名称映射将日志与租户关联。

STEP 3 | 添加 选择要转发的日志 的转发 参数。

 ©2025 Palo Alto Networks, Inc.

 ©2025 Palo Alto Networks, Inc.

FedRAMP 环境中的 Prisma Access

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证 ❑ 云服务插件版本 3.2.1-h94+、4.0.0-h88+、4.1.0-h58+、5.0.0-h31+

美国联邦风险和授权管理计划 (FedRAMP) 是一项美国政府范围的计划，为政府用户的云产品和服务提供标准化的安全评估、授权和持续监控方法。Palo Alto Networks 已证明符合 Prisma Access (Managed by Panorama) 的 FedRAMP 中等要求。阅读以下主题，详细了解如何设置 Prisma Access 以确保满足 FedRAMP 中等合规要求。

对于基于云的服务（如 Prisma Access），美国政府要求特定级别的保证，称为中等，在此级别下，若发生机密性、完整性和可用性的丧失，将对某个机构的运营、资产或个人造成严重的不利影响。严重的不利影响可能包括对机构资产的重大运营损失、财务损失或非生命或人身损失的个人伤害。

Prisma Access 符合 FedRAMP 中等安全要求，并已获得联邦政府颁发的运营授权 (ATO)。要确保 FedRAMP 中等安全要求，必须按照以下主题中列出的要求和准则安装和配置 Prisma Access。

Prisma Access FedRAMP 要求

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证 ❑ 云服务插件版本 3.2.1-h94+、4.0.0-h88+、4.1.0-h58+、5.0.0-h31+

FedRAMP 是美国政府使用的程序，它为云服务产品 (CSO) 提供标准的合规性方法。要确保您的 Prisma Access (Managed by Panorama) Access 符合 FedRAMP Moderate 要求，请在安装、激活、首次设置和配置 Prisma Access 时遵循这些指南和要求。

预安装和产品激活要求

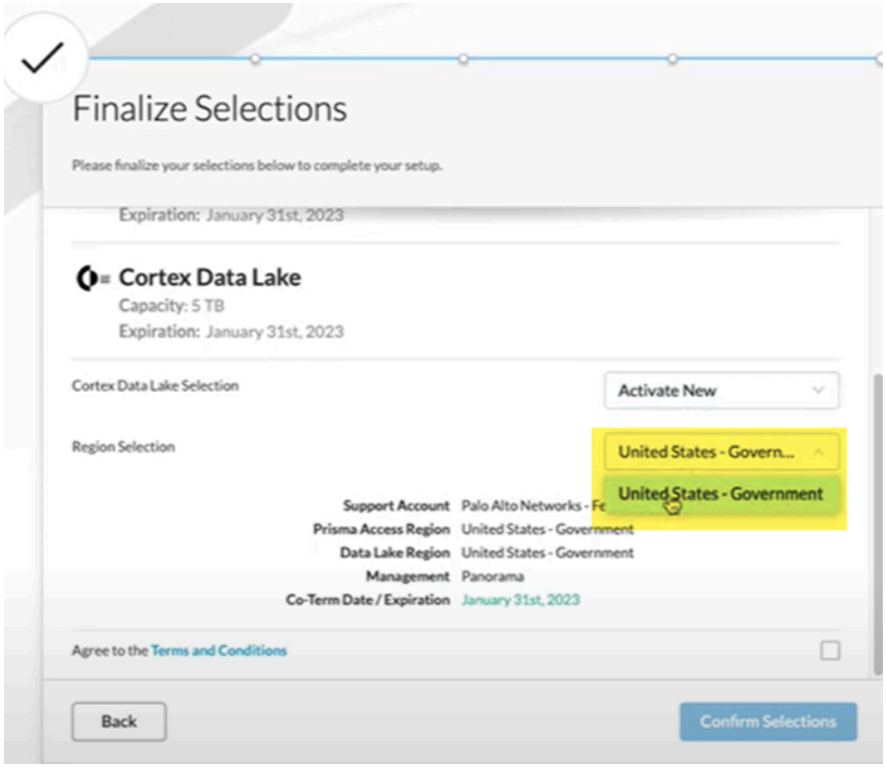
要确保您的 Prisma Access 部署保持合规性，请务必遵循这些安装和产品激活要求。

- 安装前要求：
  - 部署类型（新部署或现有部署）—在 FedRAMP Moderate 环境中支持新的 Prisma Access 部署。不支持从现有 Prisma Access 部署升级到 FedRAMP Moderate Prisma Access 部署。
  - 所需的 **SKU**—当您为 FedRAMP Moderate 部署购买 Prisma Access 时，Prisma Access 需要特定于 FedRAMP 环境的 SKU。与您的 Palo Alto Networks 授权代表或合作伙伴合作，确保为您的 FedRAMP Moderate 部署购买正确的 SKU。
  - 仅使用 所需的 Panorama、插件和 PAN-OS 数据平面版本 中列出的 Panorama 版本、GlobalProtect 版本和云服务插件版本。
  - 允许列表 **Strata Logging Service** 公共 **IP** 地址—Strata Logging Service联邦地区使用的 IP 地址块为 34.67.50.64/28。如果您的企业使用允许列表，请务必将这些 IP 地址添加到允许列表中，以确保 Strata Logging Service 可以从 Prisma Access 接收日志。
  - 更改为 **API URL**—运行 API 脚本检索 Prisma Access 使用的公用 IP 地址时，请将 API 的 URL 从 **`https://api.gpcloudservice.com/GetPrismaAccessIP/v2`** 更改为 **`https://api.fed.prismaaccess.com/GetPrismaAccessIP/v2`**。

    如果您的 Panorama 设备使用代理服务器（**Panorama** > **Setup**（设置） > **Service**（服务） > **Proxy Server**（代理服务器）），或者如果您通过 Prisma Access 启用 SSL 正向代理解密功能，请确保将 api.fed.prismaaccess.com URL 添加至代理服务器允许列表。
  - **GlobalProtect** 门户名称更改—Prisma AccessFedRAMP 移动用户—GlobalProtect 部署的默认门户主机名与非 FedRAMP 部署不同。门户名称为 *<portal-name>*.fed.prismaaccess.com. 而非 *<portal-name>*.gpcloudservice.com。
  - 支持要求—Prisma AccessFedRAMP Moderate 需要 Palo Alto Networks 美国政府支持服务，后者包括为在美国本土的美国人员提供全天候支持。

 ©2025 Palo Alto Networks, Inc.

- 激活要求—激活并安装 Prisma Access 部署时，激活和安装任务与非 FedRAMP 部署类似。但在产品激活期间，对于 **Strata Logging Service** 区域，必须选择 **United States—Government**（美国—政府）。



所需的 Panorama、插件和 PAN-OS 数据平面版本

为确保 Prisma Access 符合 FedRAMP Moderate 要求，请确保您的 Prisma Access (Managed by Panorama) 部署使用以下 Panorama、云服务插件和 GlobalProtect 版本。

组件	所需版本
Panorama PAN-OS 版本	10.2.8-h3 或更高版本 10.2.8 修补程序 PAN-OS 版本 10.2.9-h1 或更高版本 10.2.9 修补程序 PAN-OS 版本 推荐的最佳实践是在管理 Prisma Access 的 Panorama 上启用处理标准和通用条件 (FIPS-CC)，这也符合 FedRAMP 管控措施。在 Panorama 上启用 FIPS-CC 支持需要访问维护恢复工具 (MRT)。

©2025 Palo Alto Networks, Inc.

组件	所需版本
	为简化安装和激活过程，如果您已在客户支持门户 (CSP) 上注册 *Panorama*、安装许可证并激活了支持许可证，则可以选择已在 *FIPS* 模式下配置的现有 *Panorama*。如果已将 *Panorama* 序列号添加到要部署 *Prisma Access* 的同一 *CSP* 帐户，则可以在安装期间选择此 *Panorama* 设备的序列号。 不能使用已用来管理另一个 Prisma Access 或 Strata Logging Service 部署的Panorama。
云服务插件版本	• 3.2.1-h94+ • 4.0.0-h88+ • 4.1.0-h58+ • 5.0.0-h31+
GlobalProtect 版本	5.1.4+ 和 6.0.7+ 5.1.4 通过 FIPS 认证，是美国联邦政府部署使用的默认版本。如果您从 5.1.4 更改默认的 GlobalProtect 版本，则无法从 Panorama UI 中选择版本 5.1.4，并且必须向 Palo Alto Networks 技术支持部门提交支持案例才能将其添加回来。

支持的 Prisma Access FedRAMP 位置

以下位置已被授权在 FedRAMP 中等环境中与 Prisma Access 一起使用，其中包括对美国本土(CONUS) 和美国本土以外 (OCONUS) 位置的支持：

- 澳大利亚东南部
- 比利时
- 巴西南部
- 加拿大东部
- 芬兰
- 德国中部
- 印度西部
- 日本中部
- 日本南部
- 荷兰中部

©2025 Palo Alto Networks, Inc.

- 新加坡
- 瑞士
- 中国台湾
- 英国
- 美国中部
- 美国东部
- 美国西北部
- 美国东南部
- 美国西南部

Prisma Access FedRAMP 部署中支持和不支持的功能

Prisma Access FedRAMP Moderate 环境中支持使用IPv6 访问私有应用程序。

Prisma Access FedRAMP Moderate 环境中不支持使用以下应用程序和功能：

- Prisma Access 见解
- 自主 DEM
- 显式代理
- 适用于 Clean Pipe的 Prisma Access
- Enterprise DLP
- IoT Security
- SaaS 安全内联支持—可见性

©2025 Palo Alto Networks, Inc.

在 FedRAMP 环境中配置 Prisma Access

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证 ❑ 云服务插件版本 3.2.1-h94+、4.0.0-h88+、4.1.0-h58+、5.0.0-h31+

满足要求后，请完成以下步骤，以便为 FedRAMP Moderate 环境设置 Prisma Access 部署。

开始之前，请记下特定于 *Prisma Access FedRAMP* 部署的要求和指南，包括在 *FIPS-CC* 模式下配置 *Panorama* 设备以及 *Panorama*、云服务插件和 *GlobalProtect* 所需的特定版本。

STEP 1 | 确保您拥有客户支持门户 (CSP) 帐户，可专门用于 FedRAMP 部署。

您不能在单个 CSP 帐户中同时拥有 FedRAMP 和非 FedRAMP 部署。因此，Palo Alto Networks 建议您创建一个新的 CSP 帐户，仅用于 FedRAMP 帐户。

STEP 2 | 准备好要在 Prisma Access FedRAMP 环境中使用的 Panorama 设备。

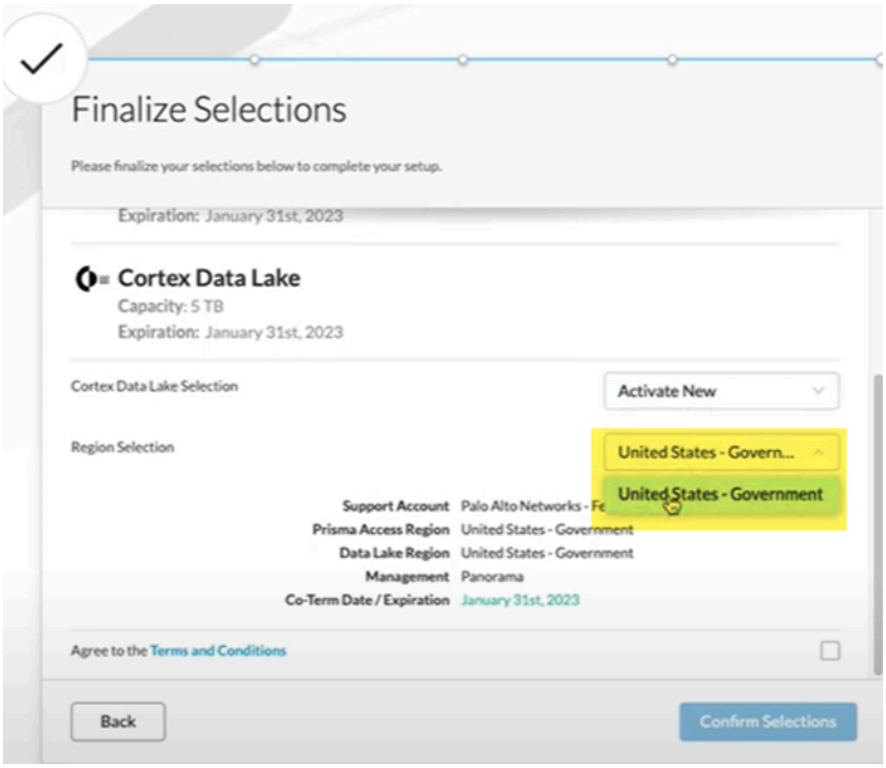
1. 安装 Panorama 设备（M 系列设备或虚拟设备）。
2. （可选，推荐）在 Panorama 设备上启用联邦信息处理标准和通用标准 (FIPS-CC) 支持。

   启用 FIPS-CC 支持需要访问维护恢复工具 (MRT)。
3. 将 Panorama 版本升级到 所需的 Panorama、插件和 PAN-OS 数据平面版本 中列出的版本。

©2025 Palo Alto Networks, Inc.

STEP 3 | 确定您的许可证要求；然后激活并安装 Prisma Access 许可证组件。

产品激活期间，在 **Strata Logging Service**（**Strata** 日志记录服务）区域中选择 **United States—Government**（美国—政府）。



STEP 4 | 将以下 URL、IP 地址和端口添加到与管理 Prisma Access 的 Panorama 设备一起使用的任何安全设备上的允许列表中。

此外，如果 Panorama 设备使用代理服务器（**Panorama** > **Setup**（设置） > **Service**（服务） > **Proxy Server**（代理服务器）），或者，如果您使用 Prisma Access 的 SSL 转发代理，请务必将以下 URL、IP 地址和端口添加到代理或代理服务器的允许列表中。

- api.gpcloudservice.com（对于 Prisma Access）
- api.paloaltonetworks.com（对于 Prisma Access）
- api.fed.prismaaccess.com（对于 Prisma Access）
- apitrusted.paloaltonetworks.com（对于 Prisma Access）
- Strata 日志记录服务所需的 FQDN 和端口
- 34.67.50.64/28

  Strata Logging Service 联邦地区使用的 IP 地址块为 34.67.50.64/28。将这些 IP 地址添加到允许列表中，以便 Strata Logging Service 可以接收来自 Prisma Access 的日志。
- Panorama 使用的端口。

©2025 Palo Alto Networks, Inc.

STEP 5 | 在客户支持门户 (CSP) 中提交案例，以便 Palo Alto Networks 允许列出 Strata Logging Service 的源和目标端口。

要在 Prisma Access 环境中使用 Strata Logging Service，您必须创建一个案例，以便 Palo Alto Networks 允许在内部列出源和目标端口。

STEP 6 | 选择 **Device**（设备） > **Setup**（设置） > **WildFire**，输入 **`wildfire.gov.paloaltonetworks.com`**。

FedRAMP 部署要求您使用 WildFire U.S.Government 云。

STEP 7 | 如果您的部署需要，请加入移动用户并使用 GlobalProtect 保护他们的安全。

我们建议第一步使用本地身份验证，以便验证是否已设置服务以及您的用户是否可以访问互联网。稍后可以切换为使用公司身份验证方法。

1. 设置 GlobalProtect 移动用户。
2. 为移动用户配置区域。
   1. 在移动用户模板中创建两个服务区。例如，“移动用户”和“互联网”。
   2. 映射区域。将任何未连接 Prisma Access 的用户或总部/分支机构的服务区映射到“不可信”。

      在 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Mobile Users**（移动用户）下，将“互联网”映射到“不可信；要信任的移动用户”。
3. 为设备组配置安全策略。

   要创建允许流量流向互联网的安全策略，请选择 Mobile_User_Device_Group **Policies**（策略） > **Security**（安全） > **Pre Rules**（预规则） > **Add**（添加）规则。例如：移动用户到互联网。
4. 提交并推送您的更改以开始使用该服务。
   1. 在 Panorama 上的本地 **Commit**（提交）。
   2. **Commit and Push**（提交并推送）到 Prisma Access。
   3. 选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Monitor**（监视） > **Mobile Users**（移动用户），以便查看 **Status**（状态）并验证是否可以 Ping 门户 FQDN。
5. 验证 Prisma Access 是否在保护移动用户的互联网流量。
   1. 下载和安装 GlobalProtect 应用。
   2. 使用该应用，以移动用户（本地用户）的身份连接到门户。
   3. 浏览互联网上的几个网站，并在 Panorama 上查看流量日志。

©2025 Palo Alto Networks, Inc.

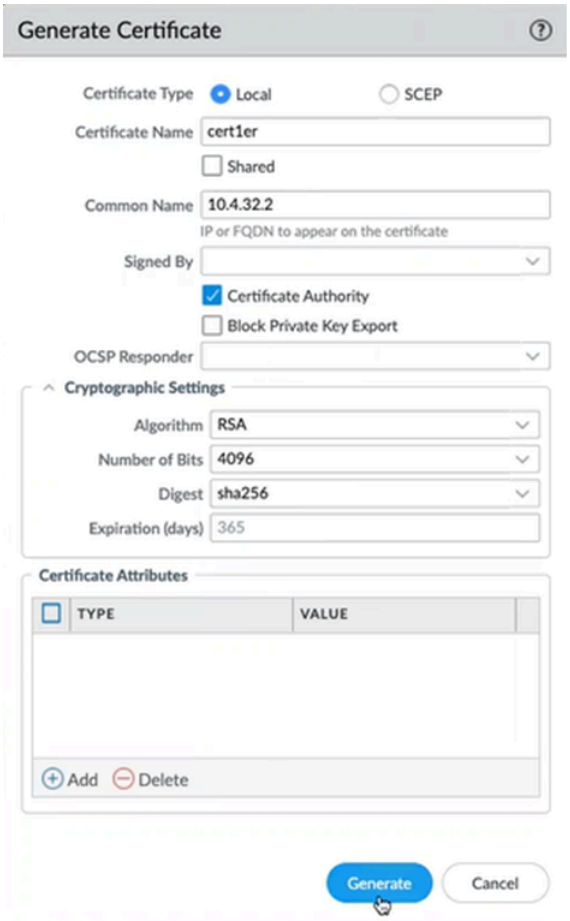
STEP 8 | （仅限移动用户—GlobalProtect 部署）在移动用户—GlobalProtect 部署中创建身份验证覆盖证书，该证书满足在 FIPS 模式下运行的 Panorama 的要求，并将该证书应用于您的部署。

生成新证书，因为移动用户—GlobalProtect 的默认证书，即 **Authentication Cookie CA**（身份验证 **Cookie CA**），不符合在 FIPS-CC 模式下运行的 Panorama 的最低密码套件要求。

1. 在管理 Prisma Access 的 Panorama 中，选择 **Device**（设备） > **Certificate Management**（证书管理） > **Certificates**（证书） > **Device Certificates**（设备证书）。

   确保您位于 **Mobile_User_Template** 中。

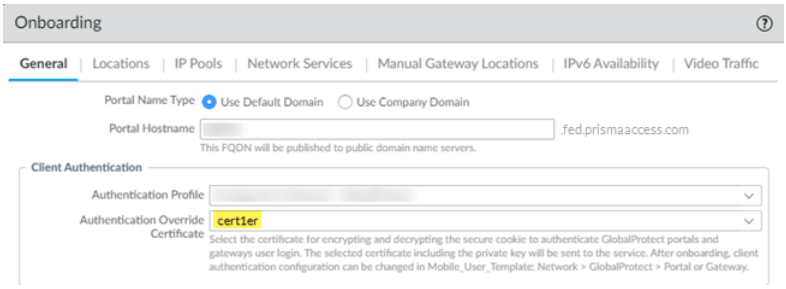
2. 生成证书，该证书需符合 FIPS-CC 模式下 Panorama 的最低密码套件要求。



3. 选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Mobile Users—GlobalProtect**（移动用户—**GlobalProtect**），选择 **Hostname**（主机名），然

 ©2025 Palo Alto Networks, Inc.

后在 **Client Authentication**（客户端身份验证）区域中，选择您创建的 **Authentication Override Certificate**（身份验证覆盖证书）。



如果您已经创建了移动用户—*GlobalProtect* 配置，则此区域将显示为灰色。要更改身份验证覆盖证书，请选择 ***Network***（网络）**>** ***GlobalProtect*** **>** ***Portals***（门户）**>** ***<portal-config>*** **>** ***Agent***（代理）**>** ***DEFAULT***（默认）**>** ***Authentication***（身份验证），在 ***Certificate to Encrypt/Decrypt Cookie***（用于加密/解密 ***Cookie*** 的证书）下选择此证书。

STEP 9 | 启用服务基础架构和允许 Prisma Access 元素之间进行通信的服务连接。

1. 计划启用服务基础架构和服务连接。
2. 启用服务基础架构。
3. 创建服务连接以允许访问公司资源。

   即使您不需要访问公司资源，仍应创建服务连接以支持移动用户与远程网络之间的访问。

STEP 10 | 规划、创建和配置远程网络连接。

1. 向 Prisma Access 添加一个或多个远程网络。

   您可以上线一个地点，然后使用批量导入功能添加其他地点。
2. 创建安全策略规则以允许流量从远程网络流向总部（例如：信任到信任）。
3. 验证服务连接、远程网络连接和移动用户之间的连接。

STEP 11 | 检索 Prisma Access 公共和专用 IP 地址。

将这些地址添加到组织网络的允许列表中，以限制对企业网络和应用程序的入站访问。

如果您有移动用户—*GlobalProtect* 部署，则可以使用 *Prisma Access UI*（而不是此 *API*）来管理公共 *IP* 地址的分配，并在 *Prisma Access* 释放这些 *IP* 地址之前确认已将其添加到允许列表中。这样，*Prisma Access* 就只会配置允许列表中的 *IP* 地址。

©2025 Palo Alto Networks, Inc.

STEP 12 | （可选）将身份验证方法从本地身份验证更改为组织的身份验证方法。

使用以下方法之一为移动用户设置 SAML 身份验证：

- 为移动用户部署配置 Azure AD SAML 身份验证

  仅配置此配置的 GlobalProtect 组件并忽略显式代理配置。
- 使用 Okta 作为 IdP 为移动用户配置 SAML 身份验证
- 将 ADFS 配置为移动用户的 SAML 提供商

设置身份验证后，虽然您可以使用 Cloud Identity Engine 检索用户和组信息，但您不能仅使用 Cloud Identity Engine 对用户进行身份验证。

STEP 13 | （可选）通过设置日志转发应用程序，将日志从 Strata Logging Service 转发到外部 Syslog 接收器。

©2025 Palo Alto Networks, Inc.

©2025 Palo Alto Networks, Inc.

Prisma Access 高级部署

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

某些 Prisma Access 路由和网络部署要求您透彻了解组织的拓扑和路由设备，以及 Prisma Access 路由的工作原理。在本节中了解这些高级部署及其配置方法。

适用于服务连接、移动用户和远程网络的高级部署：

- 为已部署的 Prisma Access 位置添加新的计算位置
- IPv6 支持
- “移动用户 — GlobalProtect”和远程网络部署的 DNS 解析
- BGP 如何为服务连接和远程网络连接通告移动用户 IP 地址池
- Prisma Access 和 Strata Logging Service 对代理的支持情况
- 阻止来自特定国家/地区的传入连接
- 确保来自 AWS WorkSpace 的互联网流量安全
- 适用于无默认路由网络的 Prisma Access

服务连接高级部署：

- 服务连接多云冗余
- 使用流量导向将互联网绑定流量转发到服务连接
- 服务连接流量的路由
- 为具有源 NAT 的服务连接保留 User-ID 和 Device-ID 映射

移动用户—GlobalProtect 高级部署：

- 在 Prisma Access 中配置多个门户
- 支持动态 DNS 注册，实现远程故障排查与更新
- 对“移动用户—GlobalProtect”的动态 DNS 注册支持
- 在 Prisma Access GlobalProtect 部署中识别和隔离感染设备
- 移动用户中的 IPv6 流量陷坑 — GlobalProtect 部署
- 使用 Prisma Access 重新分发 HIP 信息
- 查看 HIP 报告
- 无客户端 VPN 中支持 Gzip 编码
- Prisma Access 中的流量复制

远程网络高级部署：

- 提供对远程网络地点的安全入站访问
- 为远程站点创建高带宽网络

©2025 Palo Alto Networks, Inc.

为已部署的 Prisma Access 位置添加新的计算位置

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

为了优化性能和改善延迟，作为插件升级的一部分，Prisma Access 可以为您已经部署的位置引入新的计算位置。升级插件时，计算位置到位置的现有映射不会改变，但您可以选择利用新的计算位置。如果更改计算位置，Prisma Access 会更改与新计算位置关联的一个或多个位置的网关和门户 IP 地址（针对移动用户）以及 服务 IP 地址（针对远程网络）。如果您在网络中使用允许列表来让用户访问 SaaS 应用程序或可公开访问的合作伙伴应用程序等互联网资源，那么您需要将这些新的 IP 地址添加到您的允许列表中。

要在新的计算位置可用后升级到该位置，请完成以下任务。

由于您需要留出时间来删除和添加现有位置，并更改您的允许列表（针对移动用户）或对等 IPSec 隧道 IP 地址（针对远程网络部署），Palo Alto Networks 建议您将计算位置更改安排在维护窗口期间或非高峰时段。



要减少移动用户部署的停机时间，请在执行这些步骤之前，使用 API 预分配新的移动用户网关和门户 *IP* 地址。

STEP 1 | 为新的远程网络计算位置增加带宽。

1. （仅按计算位置分配远程网络带宽的远程网络部署）选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Remote Networks**（远程网络）。
2. 单击 **Bandwidth Allocation**（带宽分配）区域的齿轮图标，为新的计算位置添加 **Bandwidth Allocation (Mbps)**（带宽分配 **(Mbps)**）。
3. 等待带宽反映在页面顶部的“Allocated Total（分配的总带宽量）”字段中；然后单击 **OK**（确定）。

STEP 2 | （仅限移动用户部署）使用 API 脚本检索新的网关和门户 IP 地址并将其添加到您的允许列表中。

STEP 3 | 删除与新计算位置关联的服务连接、远程网络连接或移动用户位置。

STEP 4 | 提交并推送更改。

STEP 5 | 重新添加刚刚删除的位置。

STEP 6 | 提交并推送更改。

STEP 7 | （仅限远程网络和服务连接部署）将您的 CPE 配置为指向用于远程网络连接或服务连接的 IPsec 隧道的新 IP 地址。

对于远程网络连接，选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详情） > **Remote Networks**（远程网络），记录下 **Service IP Address**（服务 IP

 ©2025 Palo Alto Networks, Inc.

地址），并将新的 **Service IP Address**（服务 **IP** 地址） 配置为您的 CPE 上远程网络 IPSec 隧道的对等 地址。

对于服务连接，选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息） > **Service Connection**（服务连接），记下 **Service IP Address**（服务 **IP** 地址），并将新的 **Service IP Address**（服务 **IP** 地址） 配置为您的 CPE 上服务连接 IPSec 隧道的对等 IP 地址。

STEP 8 | 选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息） > **Remote Networks**（远程网络），记下 **Service IP Address**（服务 **IP** 地址），并将新的 **Service IP Address**（服务 **IP** 地址） 配置为您的 CPE 上远程网络 IPSec 隧道的对等 地址。

删除并重新添加远程网络连接时，Prisma Access 端 IPSec 隧道的 IP 地址会发生更改。

STEP 9 | （仅限移动用户部署）重新映射位置后，检索新的网关 FQDN 并将其添加到 SAML 提供商的身份验证配置中。

如果移动用户的位置被重新映射，在导致重新映射的基础设施升级之后，网关 FQDN 可能会发生变化，这可能会引发 SAML 身份验证问题。要查找网关名称：

- 在 Prisma Access (Managed by Strata Cloud Manager) 中，选择 **Workflows**（工作流） > **Prisma Access Setup**（设置） > **GlobalProtect** > **GlobalProtect Setup**（**GlobalProtect** 设置） > **Infrastructure**（基础设施） > **Infrastructure Settings**（基础设施设置），单击齿轮图标查看基础设施设置，然后在网关 FQDN 区域复制重命名后的网关。
- 在 Prisma Access (Managed by Panorama) 中，选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息） > **Mobile Users**—**GlobalProtect**（移动用户—**GlobalProtect**），然后在“Gateways（网关）”区域复制重命名后的网关。

 ©2025 Palo Alto Networks, Inc.

IPv6 支持

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证版本 2.2 Preferred 和更高版本 ❑ 对公共和私有应用程序的原生 IPv6 访问需要以下最低版本： • Prisma Access (Managed by Strata Cloud Manager)：2024 年 6 月发布 • Prisma Access (Managed by Panorama)：Prisma Access 5.1.1仅适用于新部署。 任何其他部署（包括现有 Prisma Access (Managed by Panorama) 部署）仅支持私有应用访问。

如果您的组织使用 IPv6 寻址，则 Prisma Access 使您可以访问位于 IPv6 地址之后的内部（专用）应用程序。根据您的 Prisma Access 版本，您可以使用 IPv6 访问私有（内部）应用程序，也可以同时访问 GlobalProtect 和远程网络的内部和公共（外部）应用程序。

为了访问外部应用程序，默认情况下，某些 *Prisma Access* 组件未启用 *IPv6* 功能。在为公共应用程序访问启用本机 *IPv6* 之前，请联系您的 *Palo Alto Networks* 客户团队，并为开始启用流程提交 *TAC* 工单。

原生 IPv6 支持的一个优点是，仅 IPv6 和双堆栈端点的移动用户能够使用 GlobalProtect 通过 IPv6 连接连接到 Prisma Access。另一个优点是，当互联网目标需要 IPv6 连接时，GlobalProtect 和远程网络能够通过互联网访问互联网以及公共 SaaS 应用程序。

IPv6 提供的地址空间远远大于 IPv4，几乎可以实现无限数量的唯一 IP 地址。同时，双栈是一种过渡性方法，允许网络和设备同时使用 IPv4 和 IPv6。有了原生 IPv6 支持，Prisma Access 便能同时兼容 IPv6 和双堆栈连接，从而简化从 IPv4 到 IPv6 的迁移过程，确保向后兼容性，并助力您向云端和支持 IPv6 的网络迁移。

在以下 Prisma Access 网络组件中配置 IPv6：

- 在基础设施子网中启用 IPv6 并指定 IPv6 子网，以建立 IPv6 网络基础结构来启用远程网络（分支位置）、移动用户和服务连接（数据中心或总部位置）之间的通信。

  为了获得最佳效果，请提供您自己的 *IPv6*（公共或私有）地址池，前缀长度为 */64*，例如 *3005:10:209:55::/64*。

©2025 Palo Alto Networks, Inc.

- 对于“移动用户—GlobalProtect”部署，指定是否应将 IPv6 网络用于与移动用户位置关联的计算位置。

  您可以根据需要指定 IPv6 移动用户IP 地址池和 IPv6 DNS 服务器地址。

  为获得最佳结果，请提供您自己的 *IPv6*（公共或私有）地址池，前缀长度为*/64*，如 *3001:192:168:32::/64*，在全球级别应用。

  Prisma Access 为每个计算区域分配一个来自 */80* 子网中的池，为每个位置（网关）分配一个来自 */112* 子网中的池。由于每个 *GlobalProtect* 连接都使用池中的一个 *IP* 地址，因此这种分配允许为每个位置的用户端点分配超过 *65,000* 个可用 *IPv6* 地址 *(/128)*。
- 对于服务连接和远程网络连接，您可以为连接使用的路由类型（静态路由或 BGP 路由）指定 IPv6 寻址。
  - 对于静态路由，请为用于静态路由的子网指定 IPv6 地址。
  - 对于BGP路由，请指定 IPv6 的 **Peer Address**（对端地址）和 **Local Address**（本地地址）。

    还可以指定用于交换 BGP 对等信息的传输方法。您可以指定使用 IPv4 来交换所有 BGP 对等信息（包括 IPv4 和 IPv6），使用 IPv6 来交换所有 BGP 对等信息，或使用 IPv4 来交换 IPv4 且使用 IPv6 来交换 IPv6 BGP 信息。

  为了获得最佳效果，请提供您自己的 *IPv6*（公共或私有）地址池，最大前缀长度为 */64*，例如 *2005:10:209:79::/64*。
- 对于远程网络，您可以为 DNS 服务器添加 IPv6 地址。

  为了获得最佳效果，请提供您自己的 *IPv6*（公共或私有）地址池，最大前缀长度为 */64*，例如 *2001:10:209:65::/64*。

  每个分支办公室应使用唯一的 */112*（最大长度）子网，这样可以允许超过 *65,000* 个唯一主机。

- 您提供的 *IPv6* 地址不应与 *Prisma Access BYOIP* 公用 *IPv6* 地址空间重叠。
- 您的 *IP* 池、分支机构（远程网络）子网、公司（服务连接）子网和基础设施子网不应相互重叠（应相互排斥）。

以下 计算位置 不支持 IPv6：

- 韩国
- 亚洲东北部
- 南美洲东部
- 巴林
- 南非西部
- 欧洲北部（斯德哥尔摩）
- 中东中部（阿联酋）

以下位置不支持 IPv6：

 ©2025 Palo Alto Networks, Inc.

- 所有本地区域位置
- 加拿大西部
- 南非中部

以下部署不支持 IPv6 地址：

- 远程网络 — 高性能
- IP 优化

  IP 优化部署不支持使用 IPv6 访问公共（外部）应用程序；支持私有应用程序访问。要为您的新 Prisma Access 部署启用 IPv6，请联系您的 Palo Alto Networks 客户团队，他们将创建一个 TAC 案例来满足您的请求。
- Clean Pipe 部署
- 流量控制（使用流量控制规则，通过服务连接重定向互联网流量）
- 适用于服务连接和远程网络连接的服务出站路由

Prisma Access 不会通告 *IPv6* 默认路由。

原生 IPv6 支持概述

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证版本 2.2 Preferred 及更高版本 ❑ 对公共和私有应用程序的原生 IPv6 访问需要以下最低版本： • Prisma Access (Managed by Strata Cloud Manager)：2024 年 6 月发布 • Prisma Access (Managed by Panorama)：Prisma Access 5.1.1仅适用于新部署。 任何其他部署（包括现有 Prisma Access (Managed by Panorama) 部署）仅支持私有应用程序访问。

Prisma Access 扩展了对 IPv6 的支持，使其不仅可以访问私有应用程序，还可以本机支持 GlobalProtect 和远程网络的 IPv6。

原生 IPv6 支持的一个优点是，仅 IPv6 和双堆栈端点的移动用户能够使用 GlobalProtect 通过 IPv6 连接连接到 Prisma Access。另一个优点是，当互联网目标需要 IPv6 连接时，GlobalProtect 和远程网络能够通过互联网访问互联网以及公共 SaaS 应用程序。

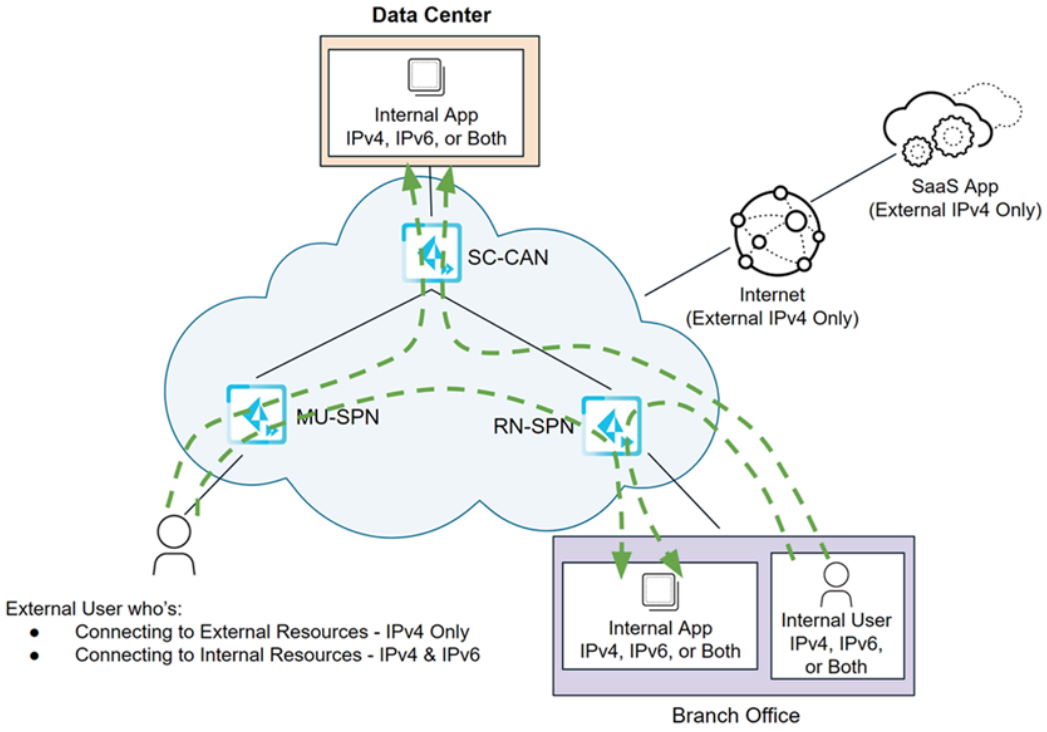
IPv6 提供的地址空间远远大于 IPv4，几乎可以实现无限数量的唯一 IP 地址。同时，双栈是一种过渡性方法，允许网络和设备同时使用 IPv4 和 IPv6。有了原生 IPv6 支持，Prisma Access 便能同时

 ©2025 Palo Alto Networks, Inc.

兼容 IPv6 和双堆栈连接，从而简化从 IPv4 到 IPv6 的迁移过程，确保向后兼容性，并助力您向云端和支持 IPv6 的网络迁移。

私有应用程序支持

某些 Prisma Access 部署支持与内部私有应用程序之间使用 IPv6 连接。Prisma Access 使用底层连接到数据中心（服务连接）和分支机构（远程网络），其中 IPv6 流量通过 IPv4 隧道传输。



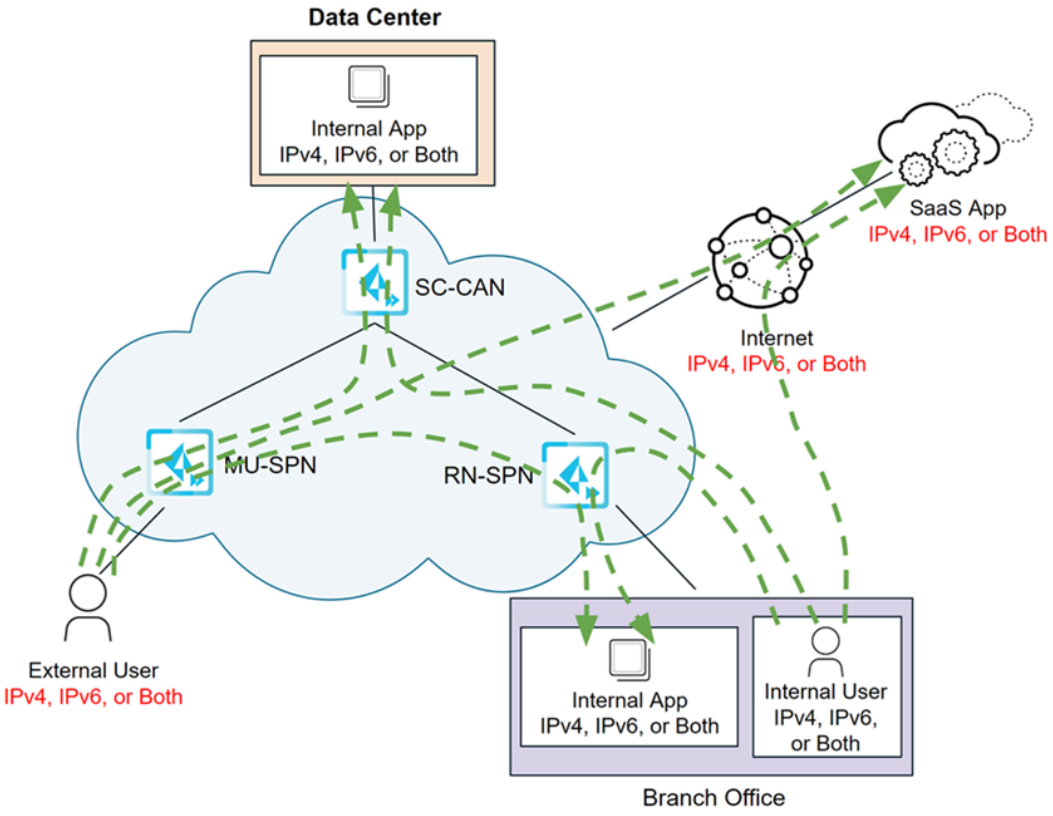
Prisma Access 中的原生 IPv6

Prisma Access

- 与 Prisma Access 的双栈 IPv4/IPv6 入站连接
- 双栈 IPv4/IPv6 通过互联网与互联网和 SaaS 应用程序建立出站连接

现在，用户可以使用 IPv6 通过互联网连接到互联网和“公共”SasS 应用程序。

©2025 Palo Alto Networks, Inc.



外部用户（移动用户）需要使用以下受支持的 *GlobalProtect* 版本之一才能运行原生 *IPv6*：

- *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)*

下表显示了 IPv4 和 IPv6 Prisma Access 部署支持的连接。复选标记表示支持此连接，破折号表示不支持。

©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

按照这些工作流在您的配置中启用 IPv6。

- ❑ 在 Prisma Access 基础设施中启用和配置 IPv6 网络和 IP 池
- ❑ 为“移动用户—GlobalProtect 部署”启用 IPv6 网络
- ❑ 为服务连接启用 IPv6 网络
- ❑ 为远程网络启用 IPv6 网络

在 Prisma Access 基础设施中启用和配置 IPv6 网络和 IP 池

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证版本 2.2 Preferred 和更高版本

©2025 Palo Alto Networks, Inc.

在何处可以使用？	需要提供什么？
	❑ 对公共和私有应用程序的原生 IPv6 访问需要以下最低版本： • Prisma Access (Managed by Strata Cloud Manager)：2024 年 6 月发布 • Prisma Access (Managed by Panorama)：Prisma Access 5.1.1仅适用于新部署。 任何其他部署（包括现有 Prisma Access (Managed by Panorama) 部署）仅支持私有应用程序访问。

对于任何 Prisma Access 部署，您都需要全局启用 IPv6 并在基础设施子网中指定 IPv6 子网，以便 Prisma Access 可以在远程网络位置、移动用户和服务连接之间建立 IPv6 网络基础设施。为此，请完成以下步骤。

- Strata Cloud Manager
- Panorama

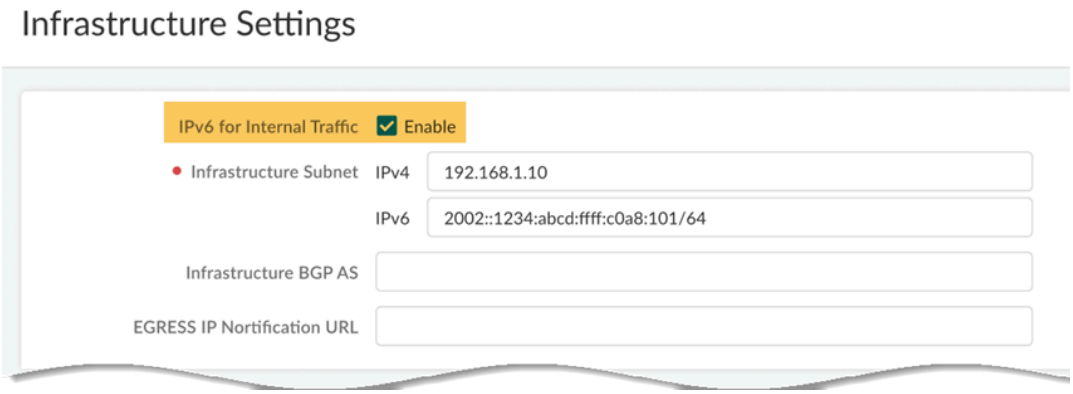
在 Prisma Access 基础设施中启用和配置 IPv6 网络和 IP 池 (Strata Cloud Manager)

STEP 1 | 选择 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Prisma Access**，然后选择齿轮图标来编辑设置。

STEP 2 | 为内部流量选中 **Enable IPv6**（启用 **IPv6**）复选框。

当数据平面准备接受或拒绝 Prisma Access 主干上的 IPv6 路由时，启用或禁用 IPv6 会导致短暂的流量中断（最长 120 秒）。我们建议您在维护时段或非高峰时段推送此配置更改。

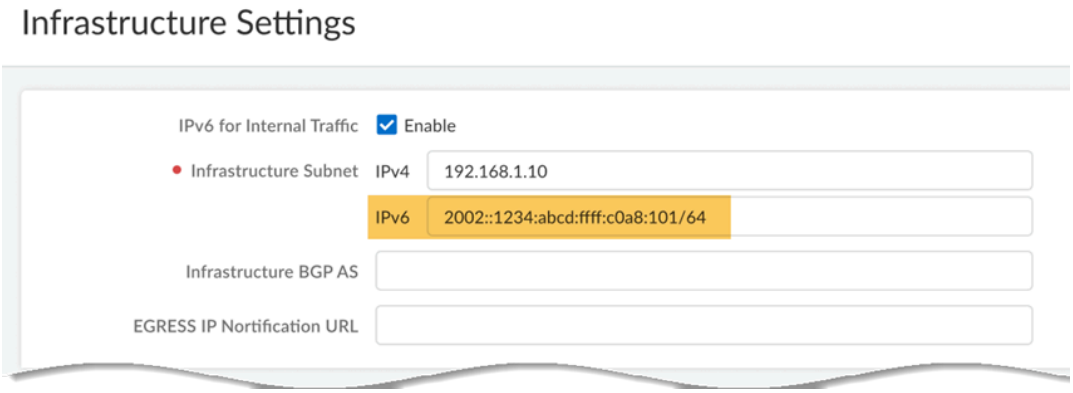
如果需要删除 *IPv6*，请删除所有配置（根据需要，包括移动用户、远程网络和服务连接的配置），然后为内部流量取消选中 ***Enable IPv6***（启用 ***IPv6***）复选框。



 ©2025 Palo Alto Networks, Inc.

STEP 3 | 指定 **IPv6** 基础设施子网和基础设施 **BGP AS**。

- 指定最小子网 /96。
- 您还必须输入 IPv4 子网；Prisma Access 要求其网络基础设施中存在 IPv4 和 IPv6 子网才能使用 IPv6。有关详细信息，请参阅Prisma Access 基础设施管理。
- Palo Alto Networks 建议您使用私有（而非公共）IPv4 和 IPv6 地址。
- 不要使用 IPv6 链路本地地址 (fe80::/10)。



STEP 4 | 输入要在 Prisma Access 基础设施中使用的基础设施 **BGP AS**。

如果要使用动态路由，以便 Prisma Access 能够动态发现远程网络和总部/数据中心位置上资源的路由，请指定自治系统 (AS) 编号。如果您不提供 AS 编号，则将使用默认 AS 编号 65534。

STEP 5 | 如果尚未执行此操作，请考虑添加内部 DNS 服务器，以使 Prisma Access 能够解析内部域以访问公司网络上的服务，例如 LDAP 和 DNS 服务器。

有关详细信息，请参阅Prisma Access 基础设施管理。

©2025 Palo Alto Networks, Inc.

STEP 6 | （仅限移动用户部署）为您的移动用户 — GlobalProtect 部署添加 IPv6 IP 地址池。

移动用户 — GlobalProtect 部署需要 IP 地址池。要启用 IPv6 功能，需要 IPv4 和 IPv6 IP 地址池。您可以在区域或全球级别应用程序 IPv4 地址；您可以在全球级别应用程序 IPv6 地址。指定最小 /80 子网。

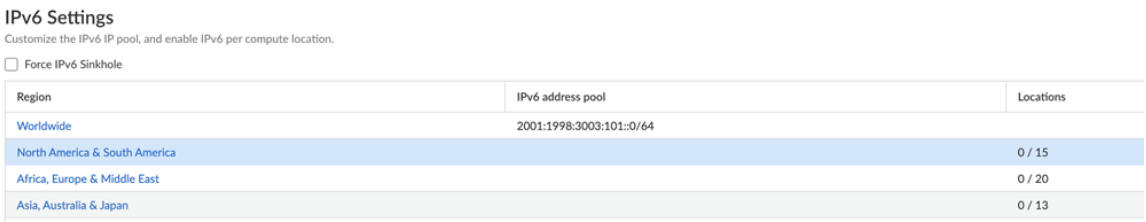
Prisma Access 使用以下方法细分全球 IPv6 地址：

- Prisma Access 为每个位置（网关）分配一个 /112 子网中的池。由于每个 GlobalProtect 连接都使用池中的一个 IP 地址，因此这种分配允许为每个位置的用户端点分配超过 65,000 个可用 IPv6 地址。

  如果您遇到自动缩放事件（如果大量用户登录到单个 Prisma Access 地点），Prisma Access 可以再添加一个具有另一 /112 子网的位置。
- 当您启用某个位置以使用 IPv6 时，Prisma Access 会将 IPv6 地址池分配给该位置所属的区域，并在已启用 IPv6 的区域总数之间划分该池。

不要在 *IP* 地址池中使用本地链路地址 *(fe80::/10)*。

1. 选择 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **GlobalProtect**，然后选择齿轮图标来编辑“Infrastructure Settings（基础设施设置）”。
2. 在“Client IP Pools（客户端 IP 池）”部分中，选择 **Region**（区域），或者选择 **Add IP Portal**（添加 **IP** 门户）。
3. 在 **IPv6 Address Pool**（**IPv6** 地址池）中输入值。
   - 对于移动用户，必须输入 IPv4 和 IPv6 IP 地址。使用 IPv6 时，Prisma Access 需要 IPv4 和 IPv6 地址来支持其内部基础设施。
   - 输入最小 IPv6 子网 /80。
   - Prisma Access 按区域细分每个子网。



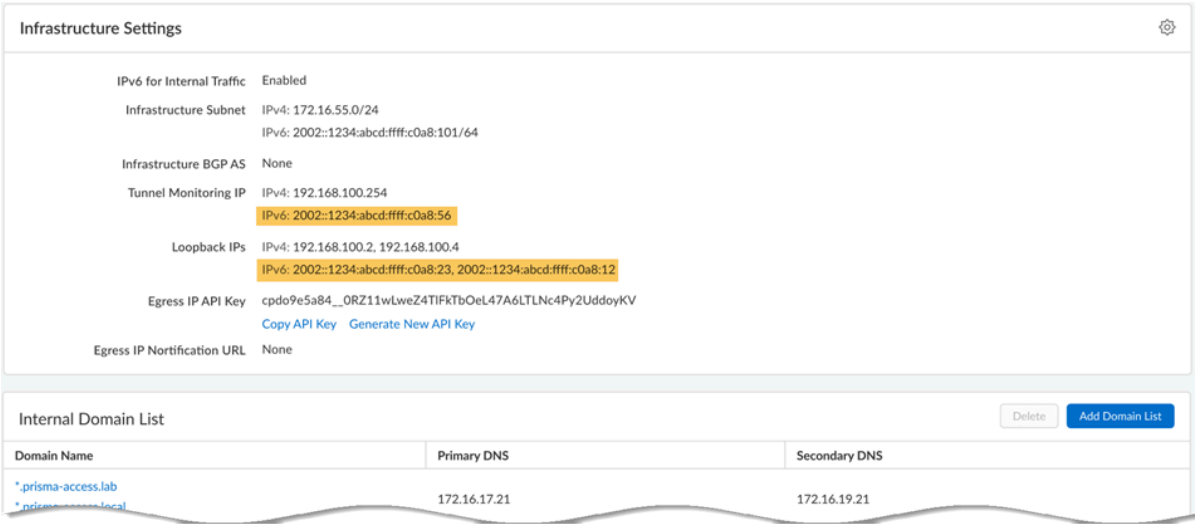
STEP 7 | 依次单击 **Save**（保存）和 **Push Config**（推送配置）。

 ©2025 Palo Alto Networks, Inc.

STEP 8 | 选择 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Prisma Access**，然后在“Infrastructure Settings（基础设施设置）”中记下以下 IPv6 地址：

- **Captive Portal Redirect IP Addresses**（强制门户重定向 **IP** 地址）— 与基于身份验证门户的 User-ID 地址映射一起使用
- **Tunnel Monitor IP Address**（隧道监视 **IP** 地址） — 用于隧道监视

由于 GlobalProtect 移动用户需要 IPv4 地址来建立 VPN 隧道，因此环回地址（其 IP 地址取自基础设施子网）仍然使用 IPv4 地址。



在 Prisma Access 基础设施中启用和配置 IPv6 网络和 IP 池 (Panorama)

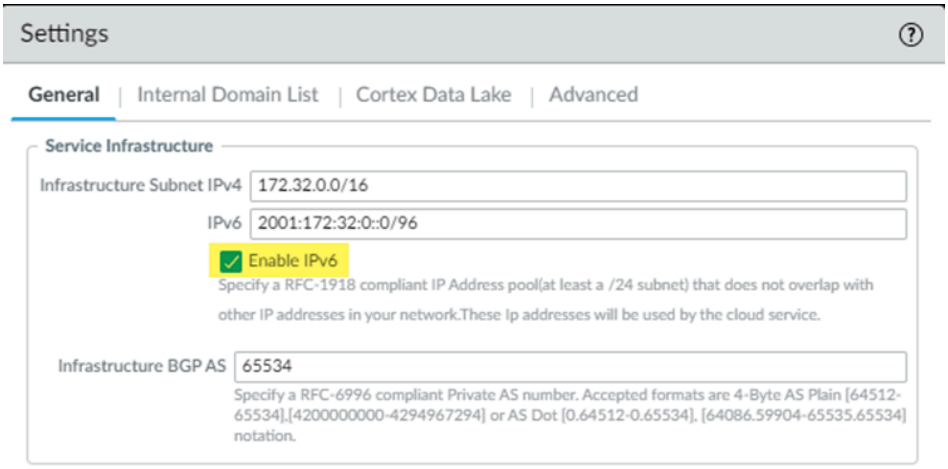
STEP 1 | 选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Service Setup**（服务设置），然后单击齿轮图标来编辑“Settings（设置）”。

©2025 Palo Alto Networks, Inc.

STEP 2 | 在 **General**（常规）选项卡上，选择 **Enable IPv6**（启用 **IPv6**）。

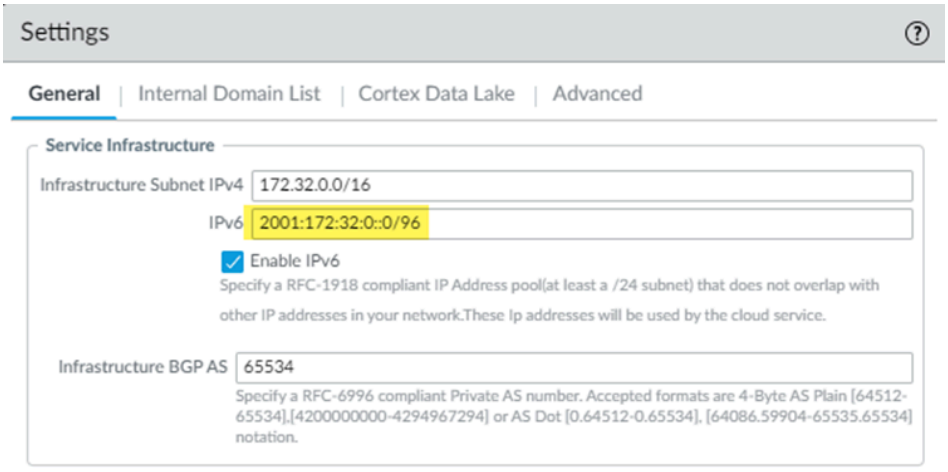
当数据平面准备接受或拒绝 Prisma Access 主干上的 IPv6 路由时，启用或禁用 IPv6 会导致短暂的流量中断（最长 120 秒）。Palo Alto Networks 建议您在维护时段或非高峰时段提交此配置更改。

如果需要删除 *IPv6*，请删除所有配置（根据需要，包括移动用户、远程网络和服务连接的配置），然后取消选中 ***Enable IPv6***（启用 ***IPv6***）复选框。



STEP 3 | 指定 **IPv6** 基础设施子网和基础设施 **BGP AS**。

- 指定最小子网 /96。
- 您还必须输入 IPv4 子网；Prisma Access 要求其网络基础设施中存在 IPv4 和 IPv6 子网才能使用 IPv6。有关详细信息，请参阅配置 Prisma Access 服务基础设施 (Panorama)。
- Palo Alto Networks 建议您使用私有（而非公共）IPv4 和 IPv6 地址。
- 不要使用 IPv6 链路本地地址 (fe80::/10)。



STEP 4 | 输入要在 Prisma Access 基础设施中使用的基础设施 **BGP AS**。

如果要使用动态路由，以便 Prisma Access 能够动态发现远程网络和总部/数据中心位置上资源的路由，请指定自治系统 (AS) 编号。如果您不提供 AS 编号，则将使用默认 AS 编号 65534。

 ©2025 Palo Alto Networks, Inc.

STEP 5 | 如果尚未完成服务设置配置，请在 **Internal Domain List**（内部域列表）、**Strata Logging Service** 和**Advanced**（高级）设置中输入值。

有关详细信息，请参阅配置 Prisma Access 服务基础设施 (Panorama)。

STEP 6 | （仅限移动用户部署）为您的移动用户 — GlobalProtect 部署添加 IPv6 IP 地址池。

移动用户 — GlobalProtect 部署需要 IP 地址池。要启用 IPv6 功能，需要 IPv4 和 IPv6 IP 地址池。您可以在区域或全球级别应用程序 IPv4 地址；您可以在全球级别应用程序 IPv6 地址。指定最小 /80 子网。

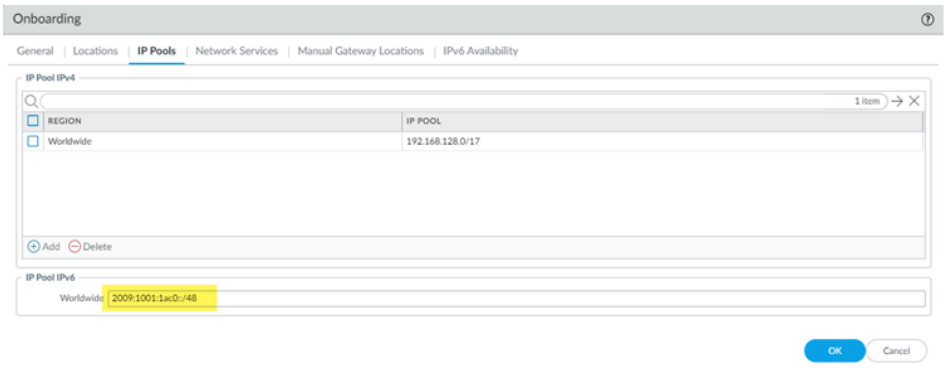
Prisma Access 使用以下方法细分全球 IPv6 地址：

- Prisma Access 为每个位置（网关）分配一个 /112 子网中的池。由于每个 GlobalProtect 连接都使用池中的一个 IP 地址，因此这种分配允许为每个位置的用户端点分配超过 65,000 个可用 IPv6 地址。

  如果您遇到自动缩放事件（如果大量用户登录到单个 Prisma Access 地点），Prisma Access 可以再添加一个具有另一 /112 子网的位置。
- 当您启用某个位置以使用 IPv6 时，Prisma Access 会将 IPv6 地址池分配给该位置所属的区域，并在已启用 IPv6 的区域总数之间划分该池。

不要在 *IP* 地址池中使用本地链路地址 *(fe80::/10)*。

1. 选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Mobile Users—GlobalProtect**（移动用户 — **GlobalProtect**）。
2. 在“Onboarding（接入）”部分中，选择门户的 **Hostname**（主机名）或选择 **Configure**（配置）。
3. 选择 **IP Pools**（**IP** 池）选项卡。
4. 在 **IP Pool IPv6**（**IP** 池 **IPv6**）中输入值。
   - 对于移动用户，必须输入 IPv4 和 IPv6 IP 地址。使用 IPv6 时，Prisma Access 需要 IPv4 和 IPv6 地址来支持其内部基础设施。
   - 输入最小 IPv6 子网 /80。
   - Prisma Access 按区域细分每个子网。



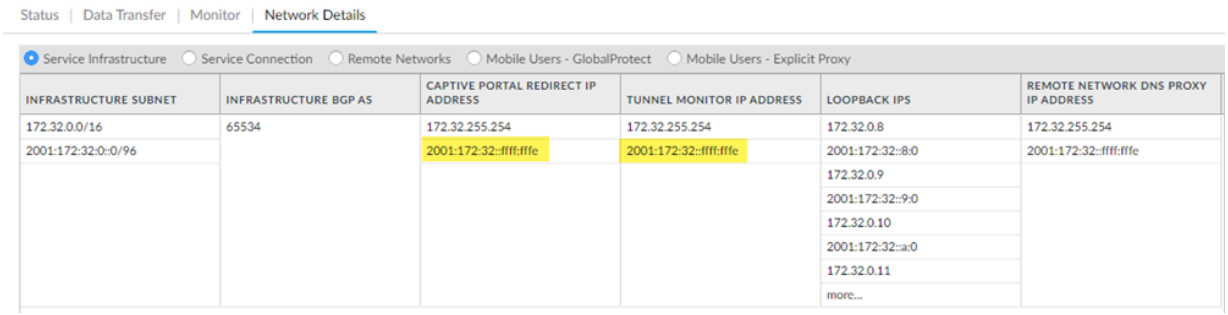
STEP 7 | **Commit and Push**（提交并推送）更改。

 ©2025 Palo Alto Networks, Inc.

STEP 8 | 选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息） > **Service Infrastructure**（服务基础设施），然后记下以下 IPv6 地址：

- **Captive Portal Redirect IP Addresses**（强制门户重定向 **IP** 地址）— 与基于身份验证门户的 User-ID 地址映射一起使用
- **Tunnel Monitor IP Address**（隧道监视 **IP** 地址） — 用于隧道监视

由于 GlobalProtect 移动用户需要 IPv4 地址来建立 VPN 隧道，因此环回地址（其 IP 地址取自基础设施子网）仍然使用 IPv4 地址。



为“移动用户 — GlobalProtect 部署”启用 IPv6 网络

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证版本 2.2 Preferred 和更高版本 ❑ 对公共和私有应用程序的原生 IPv6 访问需要以下最低版本： • Prisma Access (Managed by Strata Cloud Manager)：2024 年 6 月发布 • Prisma Access (Managed by Panorama)：Prisma Access 5.1.1仅适用于新部署。 任何其他部署（包括现有 Prisma Access (Managed by Panorama) 部署）仅支持私有应用程序访问。

除了指定移动用户的 IP 地址池之外，还必须为“移动用户 — GlobalProtect”部署配置 **IPv6 Availability**（**IPv6** 可用性）选项。如果您的网络使用 IPv6 DNS 服务器来解析内部域名，您还可以为首选和备用 DNS 服务器指定 IPv6 地址，具体内容如下节所示。

- Strata Cloud Manager
- Panorama

 ©2025 Palo Alto Networks, Inc.

为“移动用户 — GlobalProtect”部署启用 IPv6 网络 (Strata Cloud Manager)

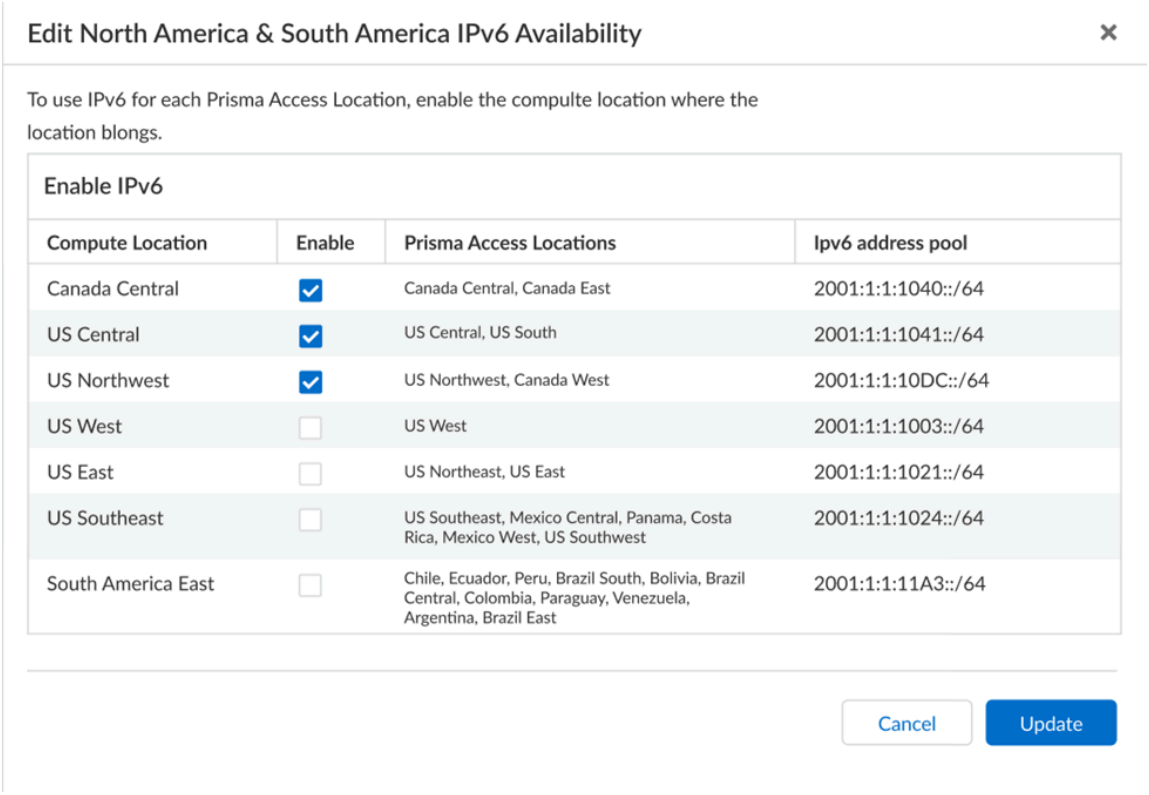
除了指定移动用户的 IP 地址池之外，还必须为“移动用户 — GlobalProtect”部署配置 **IPv6 Availability**（**IPv6** 可用性）选项。如果您的网络使用 IPv6 DNS 服务器来解析内部域名，您还可以为首选和备用 DNS 服务器指定 IPv6 地址，具体内容如下节所示。

STEP 1 | 计划是要在整个 Prisma Access 部署中部署 IPv6，还是仅在特定数量的计算位置中部署 IPv6。

STEP 2 | 为想要部署 IPv6 的区域配置 IPv6 可用性。

1. 选择 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **GlobalProtect**，然后选择齿轮图标来编辑 **Infrastructure Settings**（基础设施设置）。
2. 在 **IPv6 Settings**（**IPv6** 设置）部分中，针对要启用 IPv6 的位置选择 **Enable**（启用）。

   所有位置都与计算位置相关联。如果计算位置中的位置未启用 IPv6，请取消选择该计算位置。



STEP 3 | （可选）如果您使用的内部 DNS 服务器可通过 IPv6 地址访问，请从 **Client DNS**（客户端 **DNS**）部分选择 **Add Region**（添加区域），选中 **Resolve Internal Domains**（解析内部域）复选框，选择 **Add**（添加）以添加规则或指定默认规则，然后选择 **Custom**（自定义），从而为主 **DNS** 和辅助 **DNS** 服务器指定自定义 DNS 服务器 IPv6 地址。

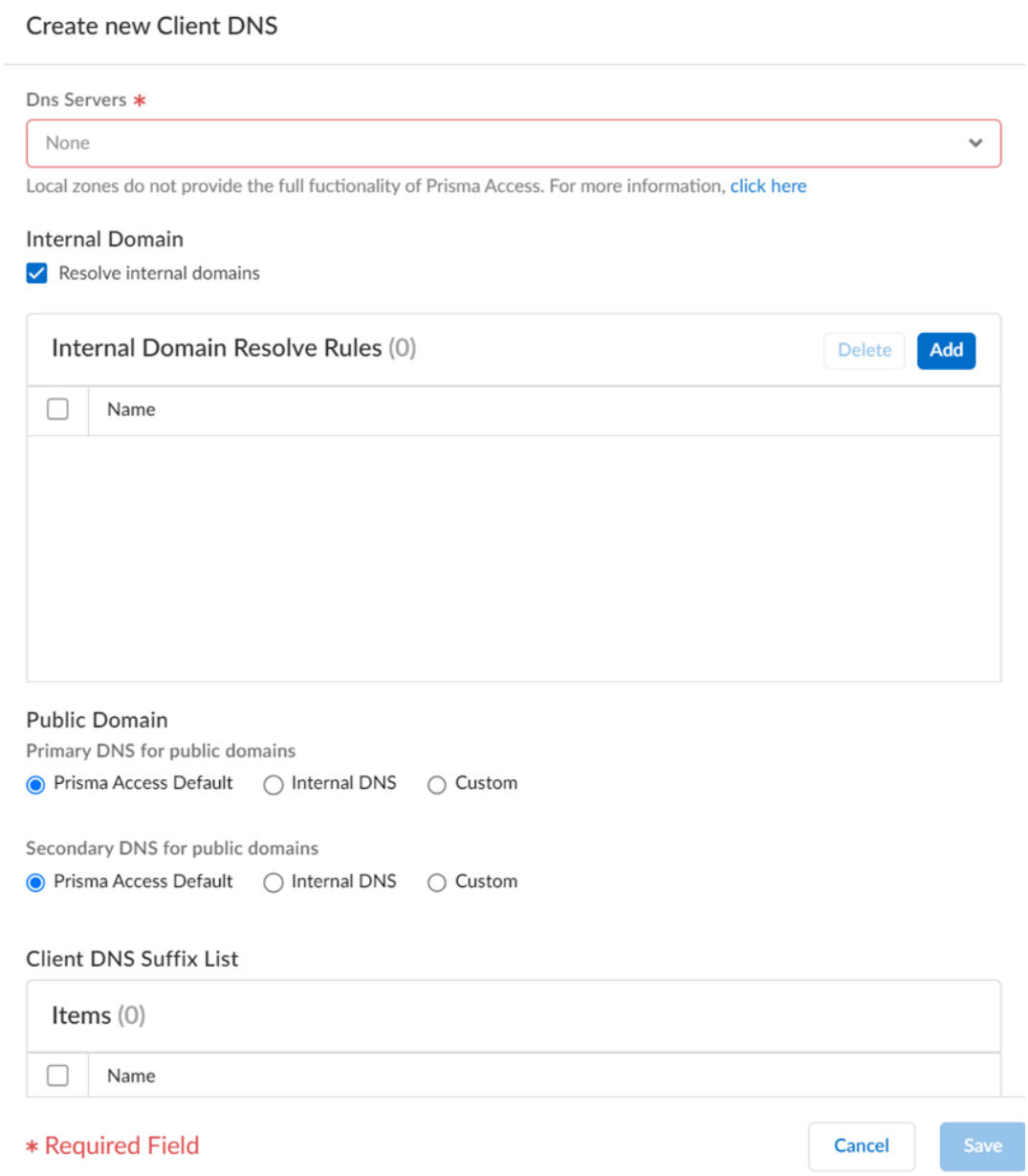
如果您为 DNS 服务器输入 IPv6 地址，则您的移动用户 IP 地址池中也必须有 IPv6 地址。

您可以输入主 DNS 服务器和辅助 DNS 服务器的 IPv4 或 IPv6 地址的任意组合。如果为主 DNS 服务器输入 IPv6 地址，为辅助 DNS 服务器输入 IPv4 地址，并且从尚未启用 **IPv6**

 ©2025 Palo Alto Networks, Inc.

Availability（**IPv6** 可用性）的计算位置接收 DNS 查询，则 Prisma Access 将使用辅助 DNS 服务器，因为服务 NDS 服务器使用 IPv4 地址。

IPv4 地址使用 *A* 记录，而 *IPv6* 地址使用 *AAAA* 记录。某些 *DNS* 服务器可以通过 *IPv4* 传输执行 *AAAA DNS* 查找；因此您可能就不再具有 *IPv6 IP* 地址的服务器。



STEP 4 | （可选）如果您尚未完成移动用户配置，请立即完成。有关详细信息，请参阅 设置 GlobalProtect 移动用户。

STEP 5 | 选择 **Push Config**（推送配置）以将您的更改部署到您的网络。

©2025 Palo Alto Networks, Inc.

为“移动用户 — GlobalProtect”部署启用 IPv6 网络 (Panorama)

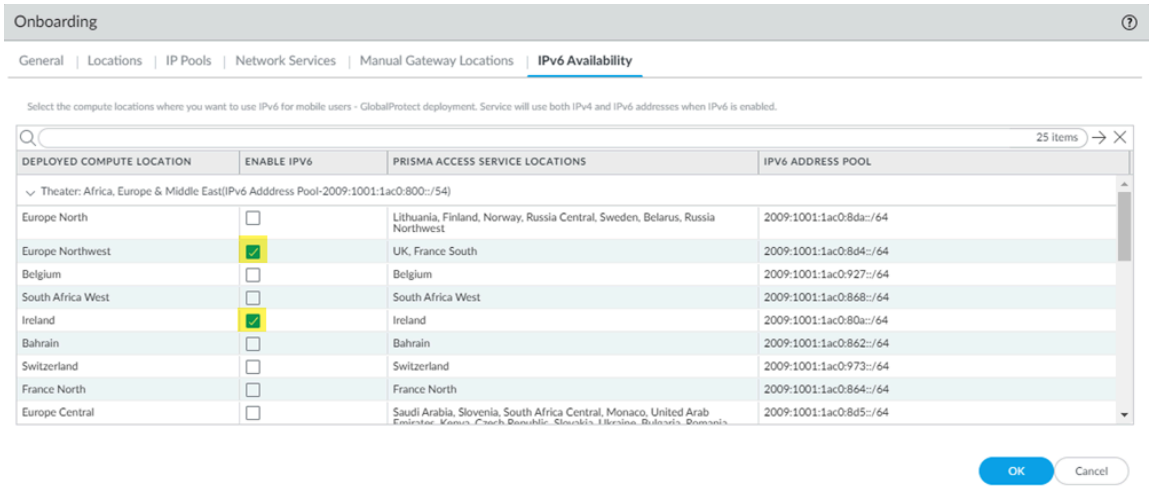
除了指定移动用户的 IP 地址池之外，还必须为“移动用户 — GlobalProtect”部署配置 **IPv6 Availability**（**IPv6** 可用性）选项。如果您的网络使用 IPv6 DNS 服务器来解析内部域名，您还可以为首选和备用 DNS 服务器指定 IPv6 地址，具体内容如下节所示。

STEP 1 | 计划是要在整个 <ph keyref="pa"/> 部署中部署 IPv6，还是仅在特定数量的计算位置中部署 IPv6。

STEP 2 | 为想要部署 IPv6 的区域配置 IPv6 可用性。

1. 在 **IPv6 Availability**（**IPv6** 可用性）选项卡中，为想要启用 IPv6 的位置选择 **Enable IPv6**（启用 **IPv6**）。

   所有位置都与计算位置相关联。如果计算位置中的位置未启用 IPv6，请取消选择该计算位置。



STEP 3 | （可选）如果使用的内部 DNS 服务器可通过 IPv6 地址访问，请单击 **Network Services**（网络服务）选项卡，单击 **Add**（添加）以添加规则或指定默认规则，然后单击 **Custom DNS Server**（自定义 **DNS** 服务器），为 **Primary DNS**（主 **DNS**）和 **Secondary DNS**（辅助 **DNS**）服务器指定自定义 DNS 服务器 IPv6 地址。

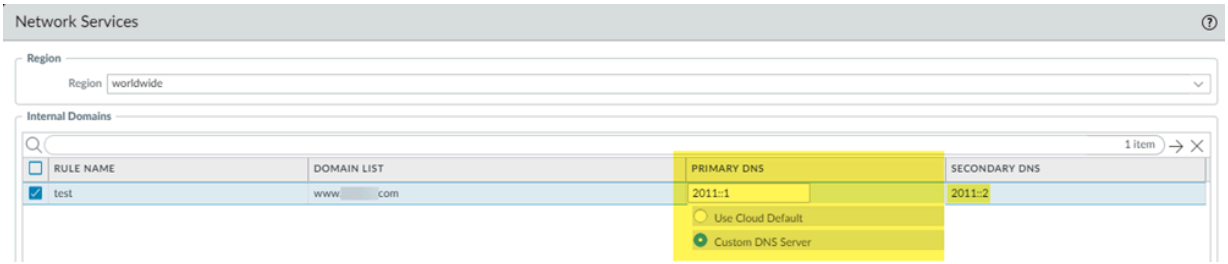
如果您为 DNS 服务器输入 IPv6 地址，则您的移动用户 IP 地址池中也必须有 IPv6 地址。

您可以输入主 DNS 服务器和辅助 DNS 服务器的 IPv4 或 IPv6 地址的任意组合。如果为主 DNS 服务器输入 IPv6 地址，为辅助 DNS 服务器输入 IPv4 地址，并且从尚未启用 **IPv6**

©2025 Palo Alto Networks, Inc.

Availability（**IPv6** 可用性）的计算位置接收 DNS 查询，则 <ph keyref="pa"/> 将使用辅助 DNS 服务器，因为服务 NDS 服务器使用 IPv4 地址。

IPv4 地址使用 *A* 记录，而 *IPv6* 地址使用 *AAAA* 记录。某些 *DNS* 服务器可以通过 *IPv4* 传输执行 *AAAA DNS* 查找；因此您可能就不再具有 *IPv6 IP* 地址的服务器。



STEP 4 | （可选）如果您尚未完成移动用户配置，请立即完成。有关详细信息，请参阅 设置 GlobalProtect 移动用户。

STEP 5 | **Commit and Push**（提交并推送）更改。

为服务连接启用 IPv6 网络

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证版本 2.2 Preferred 和更高版本 ❑ 对公共和私有应用程序的原生 IPv6 访问需要以下最低版本： • Prisma Access (Managed by Strata Cloud Manager)：2024 年 6 月发布 • Prisma Access (Managed by Panorama)：Prisma Access 5.1.1仅适用于新部署。 任何其他部署（包括现有 Prisma Access (Managed by Panorama) 部署）仅支持私有应用程序访问。

对于服务连接，您可以使用 IPv6 子网进行静态或 BGP 路由。对于 BGP 路由，您可以输入 IPv6 对等地址并指定 IPv4 和 IPv6 路由选项。

要为服务连接配置 IPv6 网络，请完成以下任务。

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

为服务连接启用 IPv6 网络 (Strata Cloud Manager)

 ©2025 Palo Alto Networks, Inc.

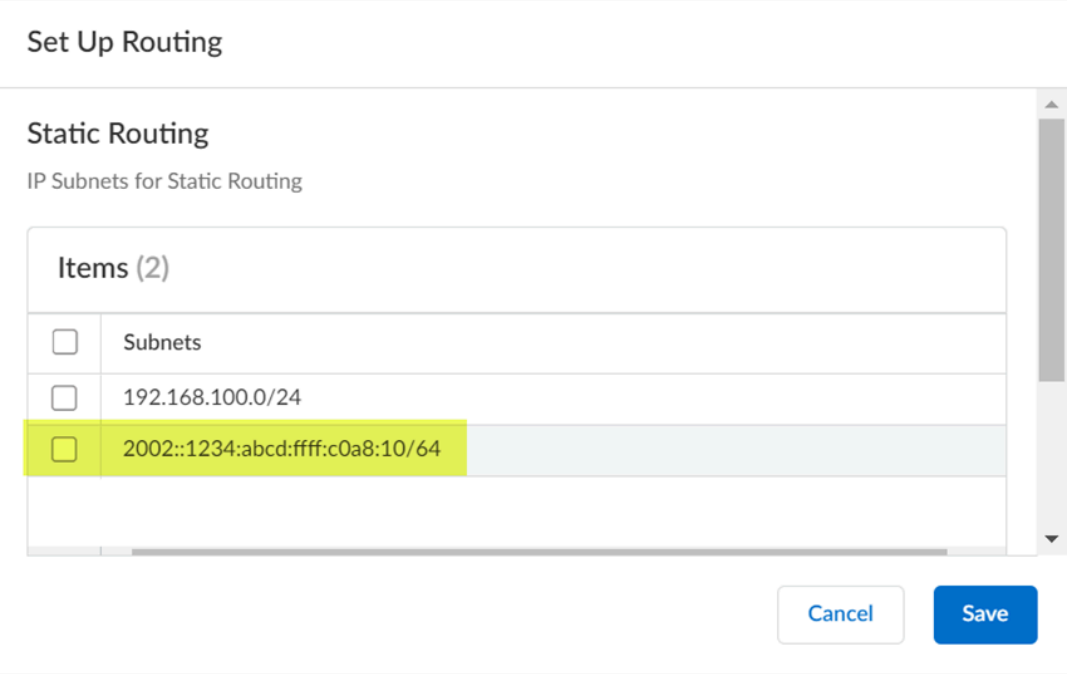
STEP 1 | 选择 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Service Connections**（服务连接），然后选择 **Add Service Connection**（添加服务连接）。

STEP 2 | 添加新服务连接或选择现有服务连接以对其进行编辑。

 ©2025 Palo Alto Networks, Inc.

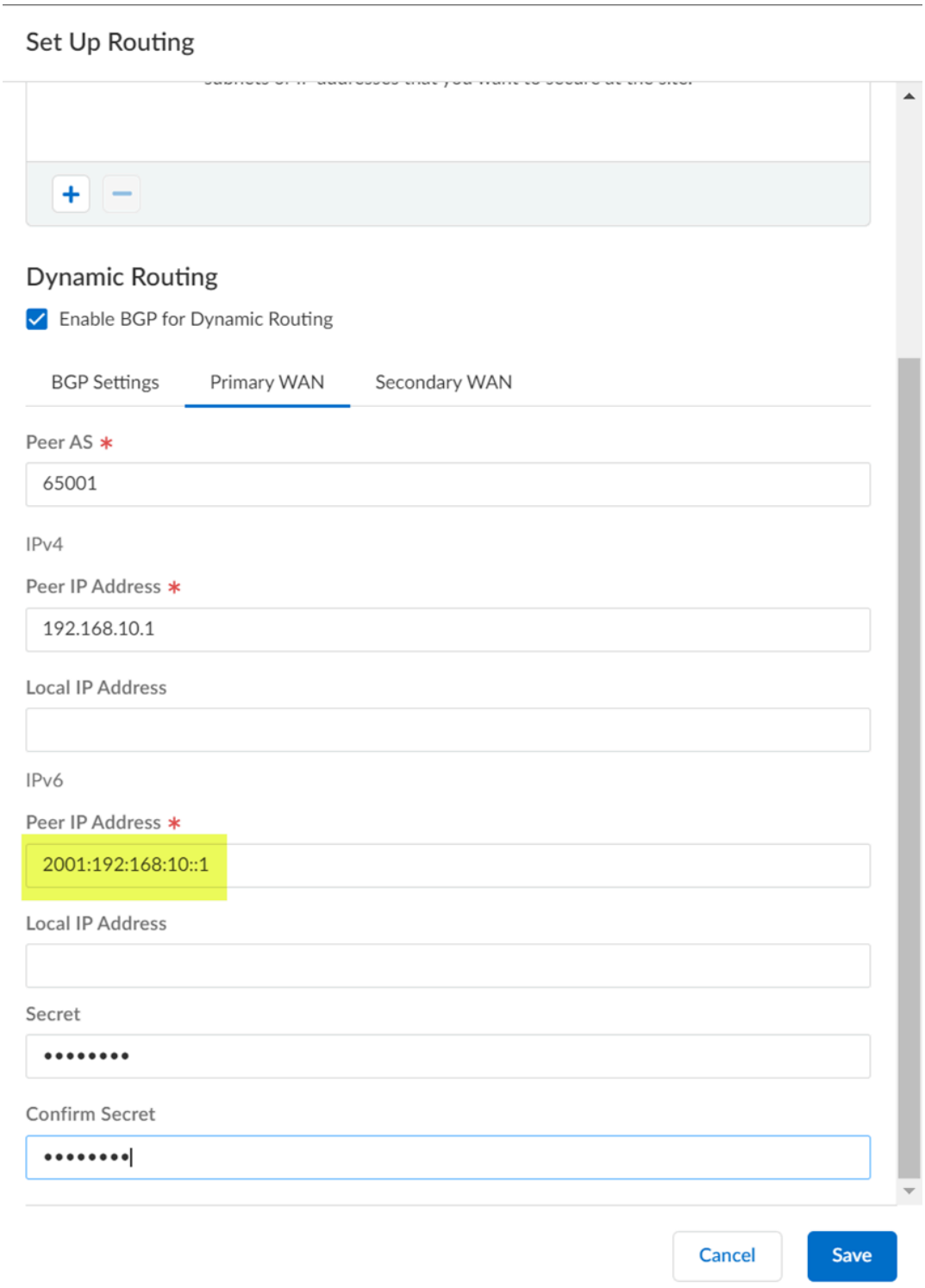
STEP 3 | 为服务连接设置 IPv6 路由。

1. (仅限静态路由部署）在 **Static Routes**（静态路由）中的 **Corporate Subnets**（企业子网）中，输入一个或多个企业子网。



2. (仅限 BGP 路由部署）指定 IPv4 和 IPv6 BGP 路由的交换方法；然后在 **Peer Address**（对等地址）和 **Local Address**（本地地址）中输入 IPv6 地址。
   - 要使用单个 IPv4 BGP 会话同时交换 IPv4 和 IPv6 BGP 对等连接信息，请选择 **Exchange both IPv4 and IPv6 routes over IPv4 peering**（通过 **IPv4** 对等连接交换 **IPv4** 和 **IPv6** 路由）。
   - 对于交换 IPv4 BGP 对等连接信息的 IPv4 BGP 会话和交换 IPv6 BGP 对等信息的 IPv6 会话，请选择 **Exchange IPv4 routes over IPv4 peering and IPv6 routes over IPv6 peering**（通过 **IPv4** 对等连接交换 **IPv4** 路由，通过 **IPv6** 对等连接交换 **IPv6** 路由）。
   - 要使用单个 IPv6 BGP 会话交换 IPv6 BGP 对等连接信息，请选择 **Exchange IPv6 routes over IPv6 peering**（通过 **IPv4** 对等连接交换 **IPv6** 路由）。
3. 如果您的辅助 WAN 使用不同的对等地址或本地地址，请取消选择 **Same as Primary WAN**（与主 **WAN** 相同），并在辅助 WAN 的 **Peer Address**（对等地址）和 **Local Address**（本地地址）中输入 IPv6 地址。

 ©2025 Palo Alto Networks, Inc.



STEP 4 | 如果您尚未完成服务连接设置，请立即完成。请参阅配置服务连接Prisma Access以了解详细信息。

服务连接的 *IPv6* 互联网访问由底层连接启用，在底层连接中，*IPv6* 流量通过 *IPv4* 隧道传递。

©2025 Palo Alto Networks, Inc.

STEP 5 | 选择 **Push Config**（推送配置）以将您的更改部署到您的网络。

STEP 6 | 如果您尚未完成移动用户配置，请立即完成。

为服务连接启用 IPv6 网络 (Panorama)

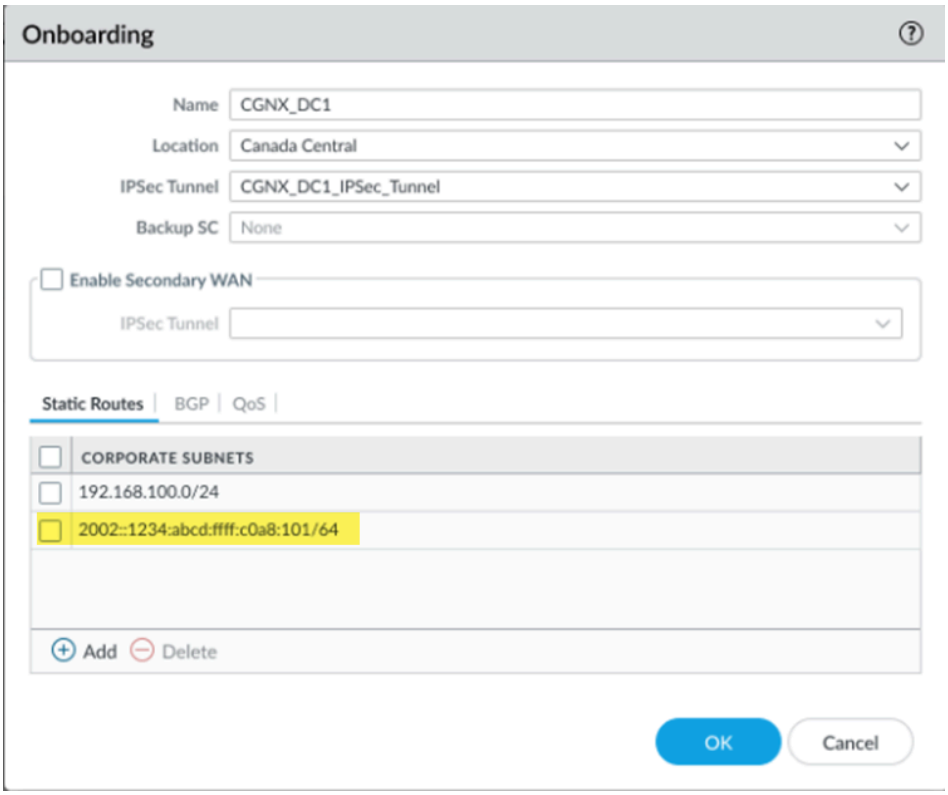
STEP 1 | 选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Service Connection**（服务连接）。

STEP 2 | 选择 **Add**（添加）以添加新服务连接或选择现有服务连接以对其进行编辑。

 ©2025 Palo Alto Networks, Inc.

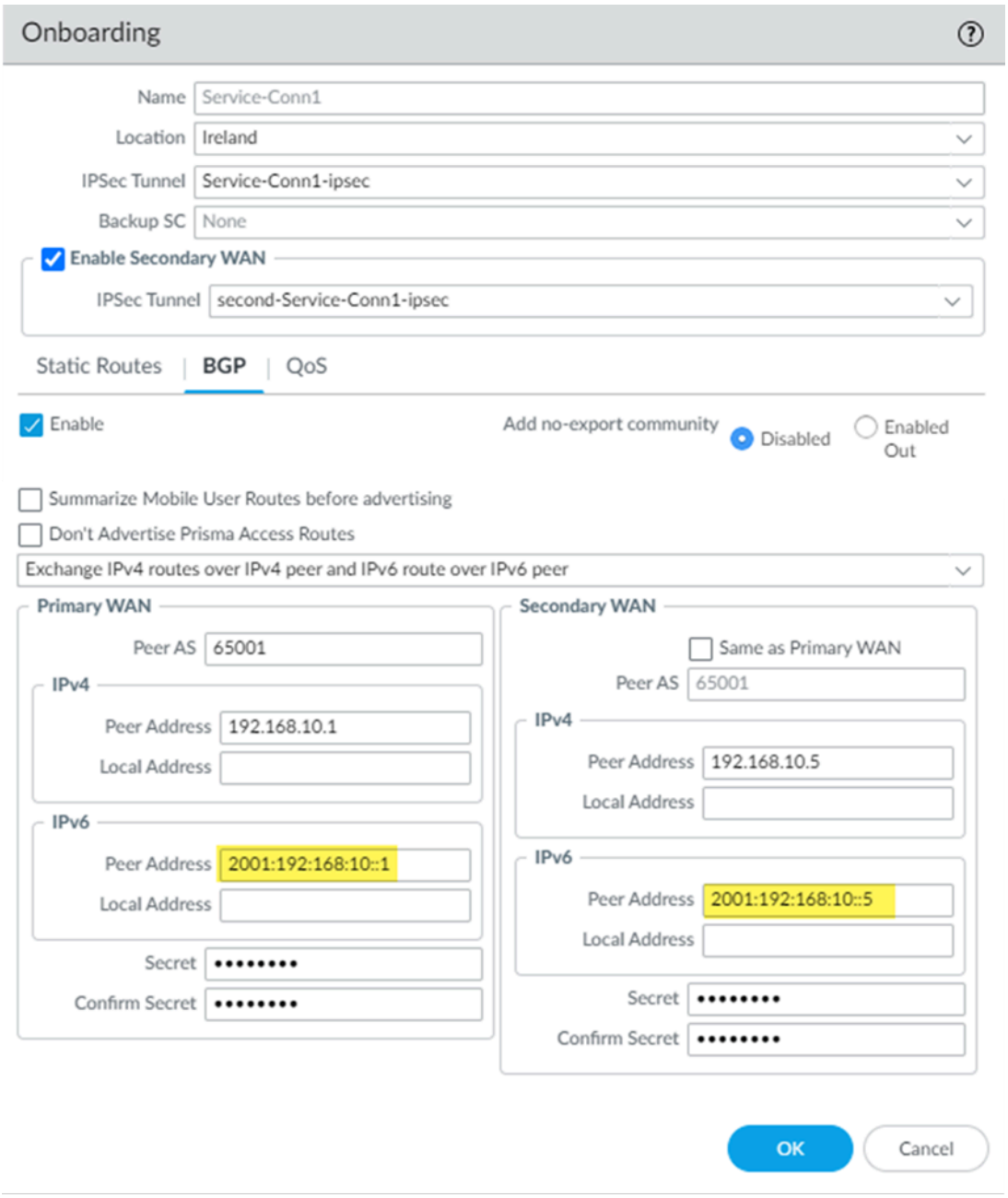
STEP 3 | 为服务连接设置 IPv6 路由。

1. (仅限静态路由部署）在 **Static Routes**（静态路由）中的 **Corporate Subnets**（企业子网）中，输入一个或多个企业子网。



2. (仅限 BGP 路由部署）指定 IPv4 和 IPv6 BGP 路由的交换方法；然后在 **Peer Address**（对等地址）和 **Local Address**（本地地址）中输入 IPv6 地址。
   - 要使用单个 IPv4 BGP 会话同时交换 IPv4 和 IPv6 BGP 对等连接信息，请选择 **Exchange both IPv4 and IPv6 routes over IPv4 peering**（通过 **IPv4** 对等连接交换 **IPv4** 和 **IPv6** 路由）。
   - 对于交换 IPv4 BGP 对等连接信息的 IPv4 BGP 会话和交换 IPv6 BGP 对等信息的 IPv6 会话，请选择 **Exchange IPv4 routes over IPv4 peering and IPv6 routes over IPv6 peering**（通过 **IPv4** 对等连接交换 **IPv4** 路由，通过 **IPv6** 对等连接交换 **IPv6** 路由）。
   - 要使用单个 IPv6 BGP 会话交换 IPv6 BGP 对等连接信息，请选择 **Exchange IPv6 routes over IPv6 peering**（通过 **IPv4** 对等连接交换 **IPv6** 路由）。
3. 如果您的辅助 WAN 使用不同的对等地址或本地地址，请取消选择 **Same as Primary WAN**（与主 **WAN** 相同），并在辅助 WAN 的 **Peer Address**（对等地址）和 **Local Address**（本地地址）中输入 IPv6 地址。

 ©2025 Palo Alto Networks, Inc.



STEP 4 | 如果您尚未完成服务连接设置，请立即完成。有关详细信息，请参阅在 Prisma Access 中配置服务连接。

STEP 5 | **Commit and Push**（提交并推送）更改。

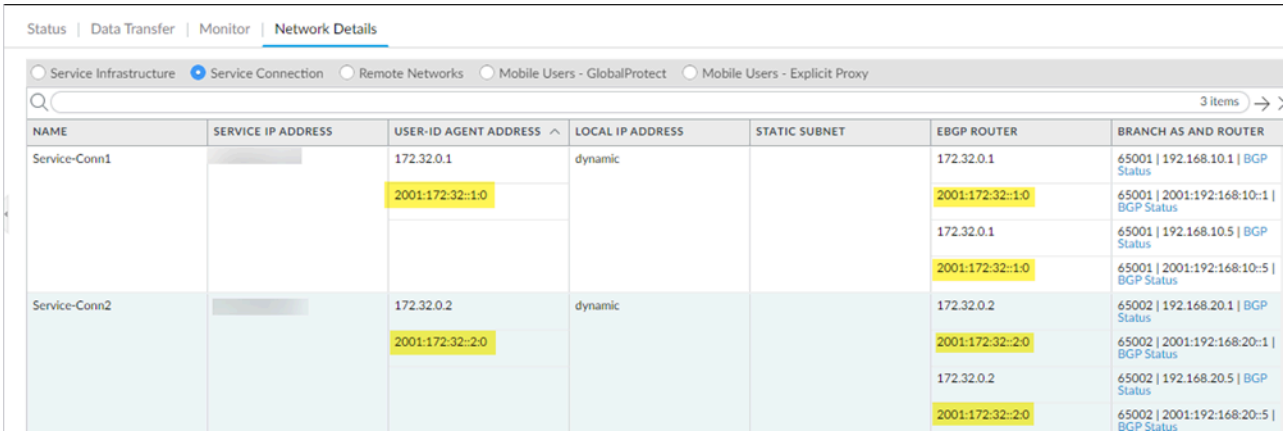
 ©2025 Palo Alto Networks, Inc.

STEP 6 | 选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息） > **Service Connection**（服务连接），然后记下 IPv6 **User-ID** 代理地址和 **EBGP** 路由器地址。

提交更改后，您将获得 IPv6 **User-ID** 代理地址（用于 User-ID 检索和分发）和 **EBGP** 路由器地址（用于服务连接）。

由于用于服务连接的 IPSec 隧道使用 IPv4 地址，因此服务 **IP** 地址是 IPv4 地址。

服务连接的 IPv6 互联网访问由底层连接启用，在底层连接中，IPv6 流量通过 IPv4 隧道传递。



STEP 7 | 如果您尚未完成移动用户配置，请立即完成。

为远程网络启用 IPv6 网络

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证版本 2.2 Preferred 和更高版本 ❑ 对公共和私有应用程序的原生 IPv6 访问需要以下最低版本： • Prisma Access (Managed by Strata Cloud Manager)：2024 年 6 月发布 • Prisma Access (Managed by Panorama)：Prisma Access 5.1.1仅适用于新部署。 任何其他部署（包括现有 Prisma Access (Managed by Panorama) 部署）仅支持私有应用程序访问。

对于远程网络连接，您可以将 IPv6 子网用于静态路由。对于 BGP 路由，您可以输入 IPv6 对等地址，并规定 BGP 仅使用 IPv6 路由或同时使用 IPv4 和 IPv6 路由。

要为远程网络连接配置 IPv6 网络，请完成以下任务。

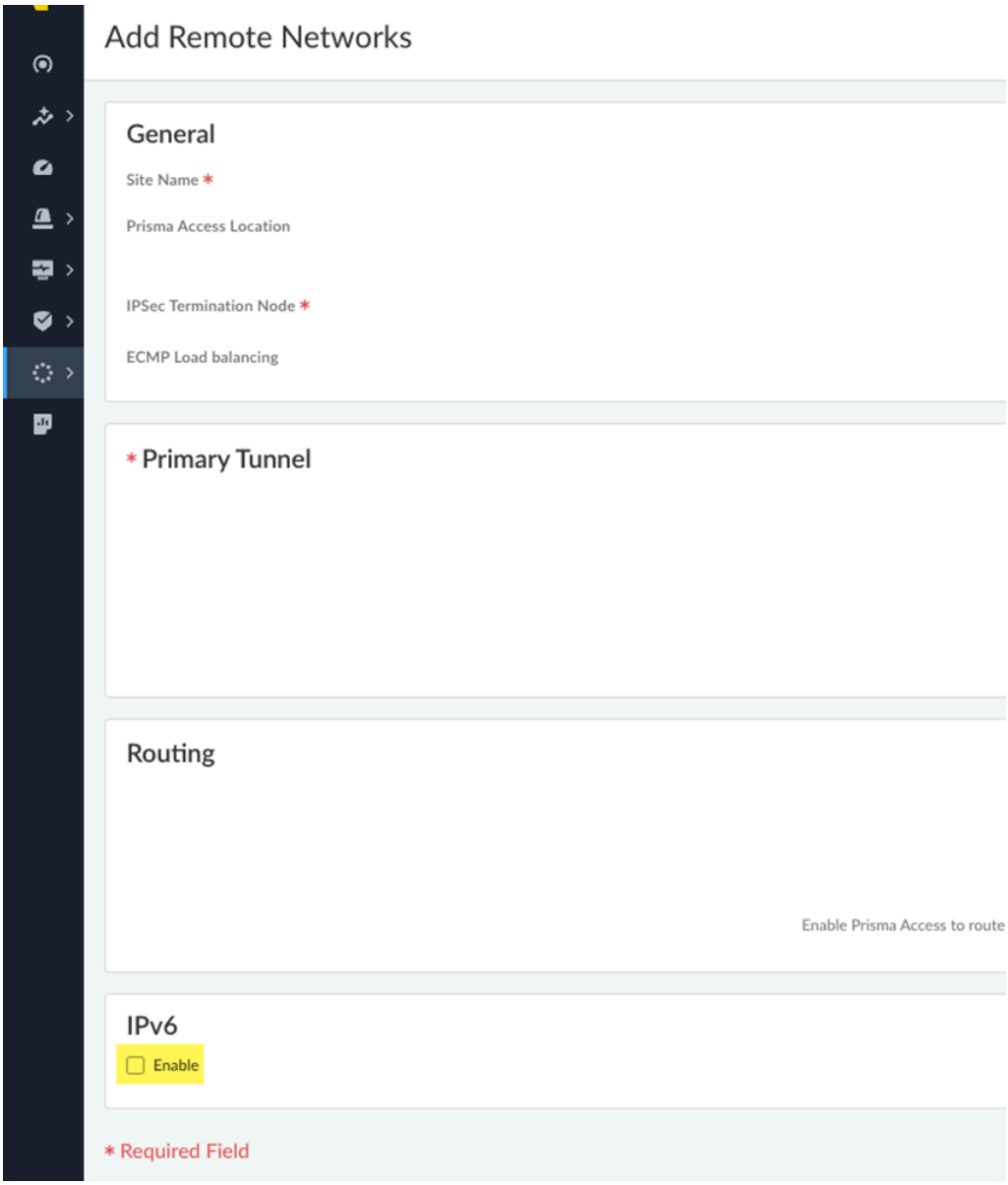
 ©2025 Palo Alto Networks, Inc.

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

为远程网络启用 IPv6 联网 (Strata Cloud Manager)

STEP 1 | 选择 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > 远程网络和 **Add Remote Networks**（添加远程网络）。

STEP 2 | 启用 IPv6。

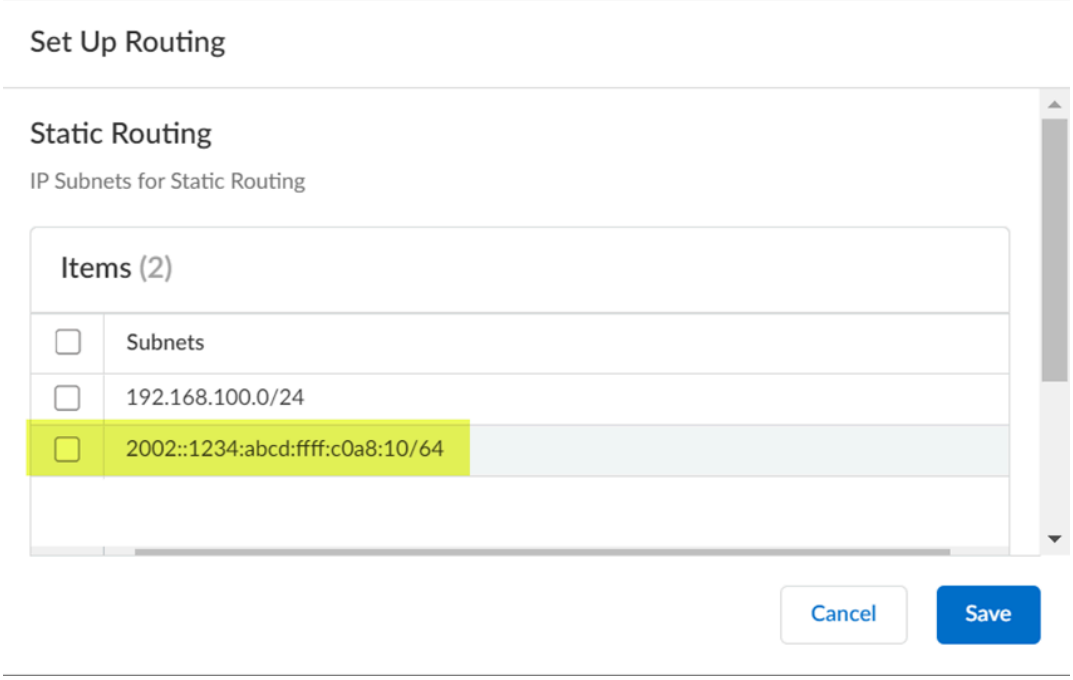


STEP 3 | 添加新的远程网络连接或选择现有远程网络连接进行编辑。

 ©2025 Palo Alto Networks, Inc.

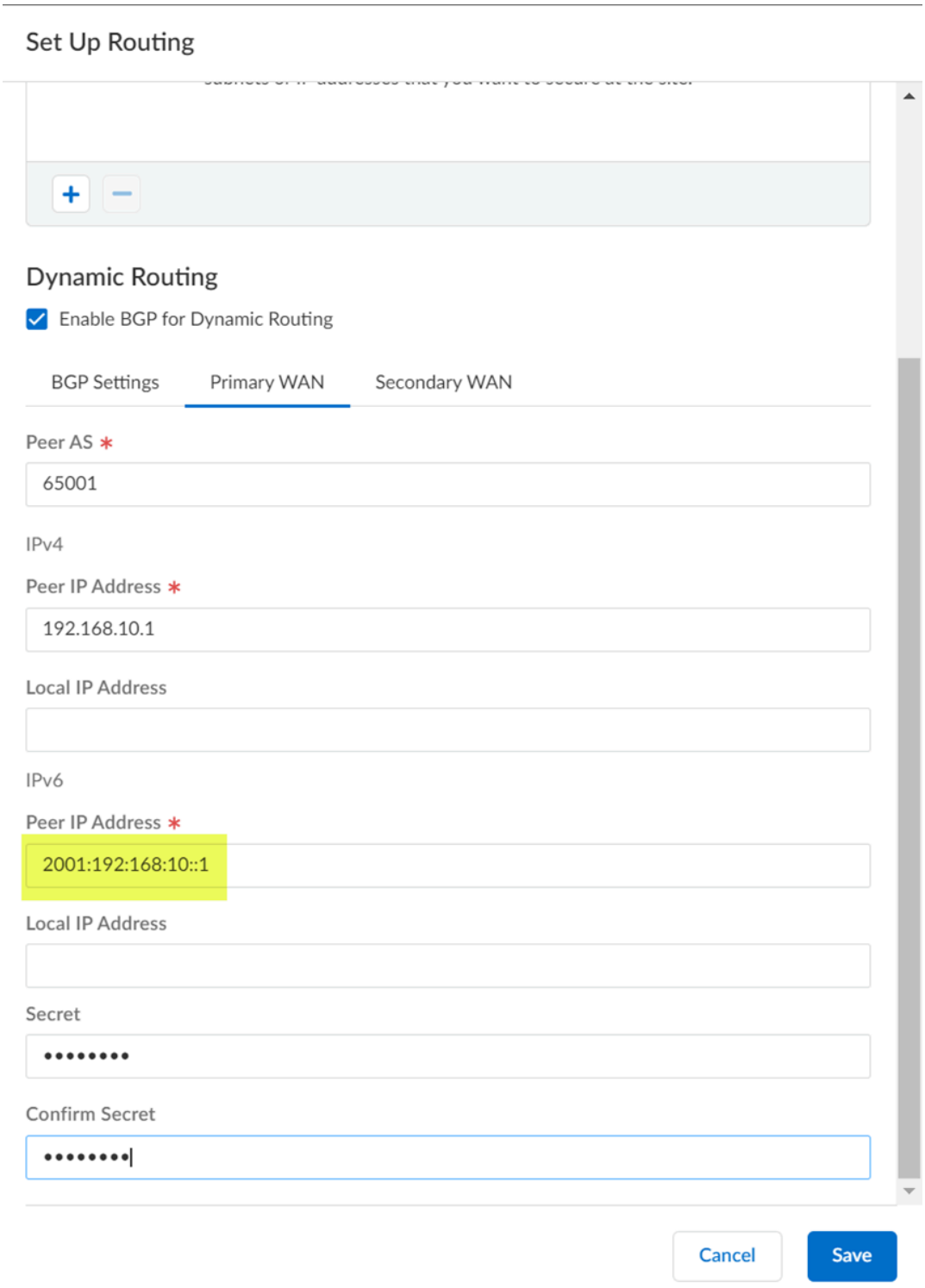
STEP 4 | 为您的远程网络设置 IPv6 路由。

1. (仅限静态路由部署）在 **Static Routes**（静态路由）中的 **Corporate Subnets**（企业子网）中，输入一个或多个企业子网。



2. (仅限 BGP 路由部署）指定 IPv4 和 IPv6 BGP 路由的交换方法；然后在 **Peer Address**（对等地址）和 **Local Address**（本地地址）中输入 IPv6 地址。
   - 要使用单个 IPv4 BGP 会话同时交换 IPv4 和 IPv6 BGP 对等连接信息，请选择 **Exchange both IPv4 and IPv6 routes over IPv4 peering**（通过 **IPv4** 对等连接交换 **IPv4** 和 **IPv6** 路由）。
   - 对于交换 IPv4 BGP 对等连接信息的 IPv4 BGP 会话和交换 IPv6 BGP 对等信息的 IPv6 会话，请选择 **Exchange IPv4 routes over IPv4 peering and IPv6 routes over IPv6 peering**（通过 **IPv4** 对等连接交换 **IPv4** 路由，通过 **IPv6** 对等连接交换 **IPv6** 路由）。
   - 要使用单个 IPv6 BGP 会话交换 IPv6 BGP 对等连接信息，请选择 **Exchange IPv6 routes over IPv6 peering**（通过 **IPv4** 对等连接交换 **IPv6** 路由）。
3. 如果您的辅助 WAN 使用不同的对等地址或本地地址，请取消选择 **Same as Primary WAN**（与主 **WAN** 相同），并在辅助 WAN 的 **Peer Address**（对等地址）和 **Local Address**（本地地址）中输入 IPv6 地址。

©2025 Palo Alto Networks, Inc.



STEP 5 | （可选）如果使用的内部 DNS 服务器可通过 IPv6 地址访问，请选择 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Remote Networks**（远程网络） > **Advanced Settings**（高级设置），找到 **DNS Proxy**（**DNS** 代理），单击 **Add**（添加）以添

 ©2025 Palo Alto Networks, Inc.

加规则或指定默认规则，然后单击 **Custom DNS Server**（自定义 **DNS** 服务器），为 **Primary DNS**（主 **DNS**）和**Secondary DNS**（辅助 **DNS**）服务器指定自定义 DNS 服务器 IPv6 地址。

Prisma Access 允许您指定 DNS 服务器来解析组织内部域和外部域。如果未指定任何设置，则 Prisma Access 不会代理远程网络的 DNS 请求。您还需要选择一个 **Region**（区域）。

您可以输入主 DNS 服务器和辅助 DNS 服务器的 IPv4 或 IPv6 地址的任意组合。

- *IPv4* 地址使用 *A* 记录，而 *IPv6* 地址使用 *AAAA* 记录。某些 *DNS* 服务器可以通过 *IPv4* 传输执行 *AAAA DNS* 查找；因此您可能就不再具有 *IPv6 IP* 地址的服务器。

STEP 6 | 如果您尚未完成远程网络连接设置，请立即完成。

远程网络连接的 *IPv6* 互联网访问由底层连接启用，在底层连接中，*IPv6* 流量通过 *IPv4* 隧道传递。

STEP 7 | 选择 **Push Config**（推送配置）以将您的更改部署到您的网络。

为远程网络启用 IPv6 联网 (Panorama)

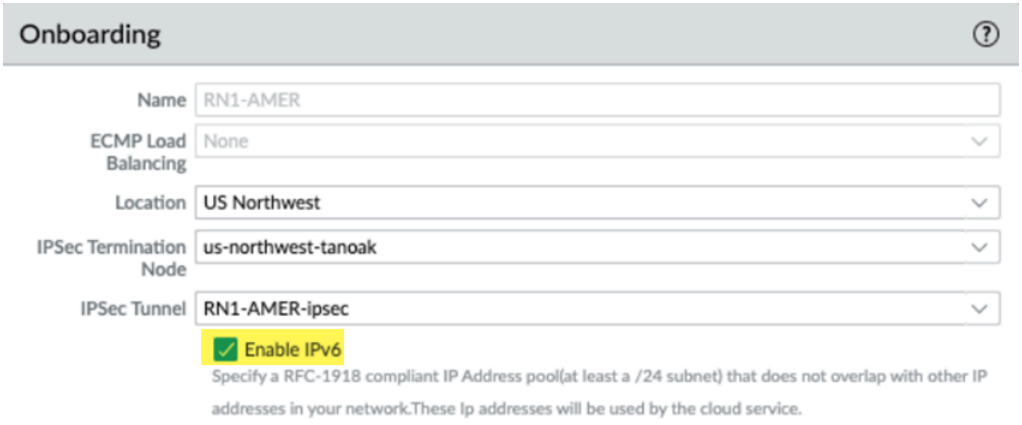
STEP 1 | （可选）在自定义 DNS 服务器代理配置中输入 IPv6 地址。

1. 选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Remote Networks**（远程网络），然后单击 **Settings**（设置）区域中的齿轮图标以编辑设置。
2. 在 **DNS Proxy**（**DNS** 代理）区域中的 **Custom DNS Server**（自定义 **DNS** 服务器）中，为您的 DNS 代理设置 IPv6 地址。

STEP 2 | 选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Remote Networks**（远程网络）。

STEP 3 | 单击 **Add**（添加）以添加一个新的远程网络连接或选择现有远程网络连接进行编辑。

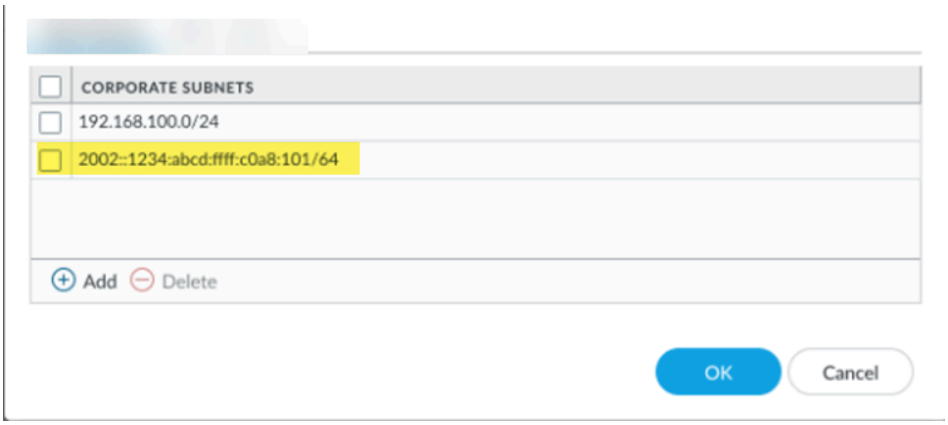
STEP 4 | 启用 **IPv6**。



 ©2025 Palo Alto Networks, Inc.

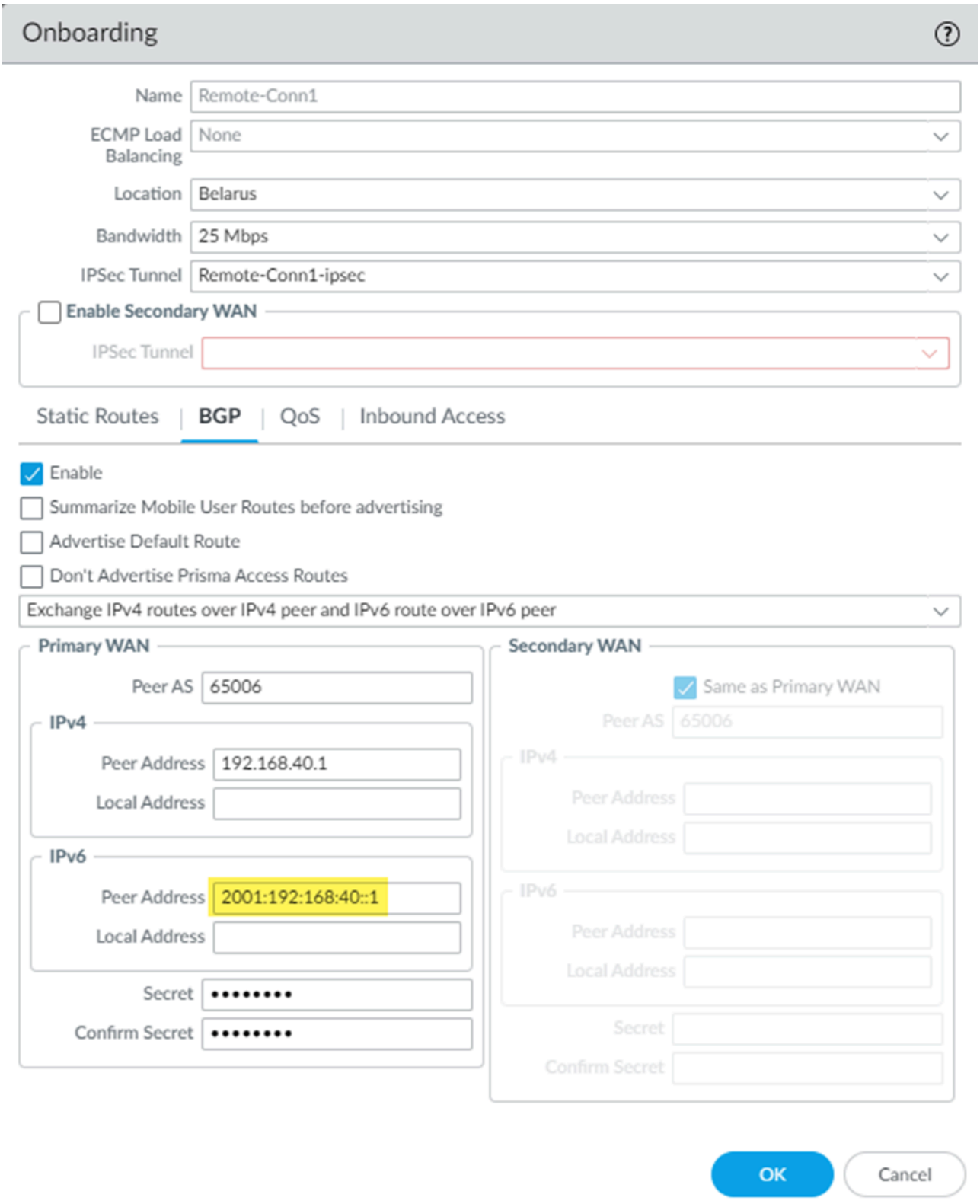
STEP 5 | 为您的远程网络设置 IPv6 路由。

1. (仅限静态路由部署）在 **Static Routes**（静态路由）中的 **Corporate Subnets**（企业子网）中，输入一个或多个企业子网。



2. (仅限 BGP 路由部署）指定 IPv4 和 IPv6 BGP 路由的交换方法；然后在 **Peer Address**（对等地址）和 **Local Address**（本地地址）中输入 IPv6 地址。
   - 要使用单个 IPv4 BGP 会话同时交换 IPv4 和 IPv6 BGP 对等连接信息，请选择 **Exchange both IPv4 and IPv6 routes over IPv4 peering**（通过 **IPv4** 对等连接交换 **IPv4** 和 **IPv6** 路由）。
   - 对于交换 IPv4 BGP 对等连接信息的 IPv4 BGP 会话和交换 IPv6 BGP 对等信息的 IPv6 会话，请选择 **Exchange IPv4 routes over IPv4 peering and IPv6 routes over IPv6 peering**（通过 **IPv4** 对等连接交换 **IPv4** 路由，通过 **IPv6** 对等连接交换 **IPv6** 路由）。
   - 要使用单个 IPv6 BGP 会话交换 IPv6 BGP 对等连接信息，请选择 **Exchange IPv6 routes over IPv6 peering**（通过 **IPv4** 对等连接交换 **IPv6** 路由）。
3. 如果您的辅助 WAN 使用不同的对等地址或本地地址，请取消选择 **Same as Primary WAN**（与主 **WAN** 相同），并在辅助 WAN 的 **Peer Address**（对等地址）和 **Local Address**（本地地址）中输入 IPv6 地址。

 ©2025 Palo Alto Networks, Inc.



STEP 6 | （可选）如果您使用的内部 DNS 服务器可通过 IPv6 地址访问，请选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Remote Network**（远程网络） > **Settings**（设置），单击齿轮图标以编辑设置，选择 **DNS Proxy**（**DNS** 代理）选项卡，单击

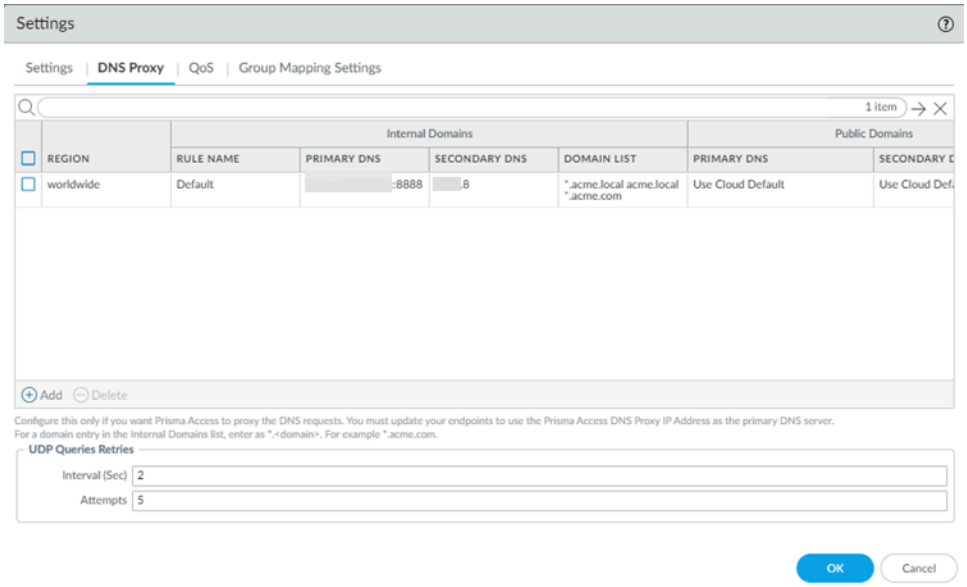
©2025 Palo Alto Networks, Inc.

Add（添加） 以添加规则或指定默认规则，然后单击 **Custom DNS Server**（自定义 **DNS** 服务器），为 **Primary DNS**（主 **DNS**）和 **Secondary DNS**（辅助 **DNS**）服务器指定自定义 DNS 服务器 IPv6 地址。

Prisma Access 允许您指定 DNS 服务器来解析组织内部域和外部域。如果未指定任何设置，则 Prisma Access 不会代理远程网络的 DNS 请求。您还需要选择一个 **Region**（区域）。

您可以输入主 DNS 服务器和辅助 DNS 服务器的 IPv4 或 IPv6 地址的任意组合。

IPv4 地址使用 *A* 记录，而 *IPv6* 地址使用 *AAAA* 记录。某些 *DNS* 服务器可以通过 *IPv4* 传输执行 *AAAA DNS* 查找；因此您可能就不再具有 *IPv6 IP* 地址的服务器。



STEP 7 | 如果您尚未完成远程网络连接设置，请立即完成。

STEP 8 | **Commit and Push**（提交并推送）更改。

STEP 9 | 选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息） > **Remote Networks**（远程网络），然后记下 **EBGP** 路由器地址：

提交更改后，您将获得用于服务连接的 IPv6 **EBGP** 路由器 地址。

由于用于远程网络连接的 IPSec 隧道使用 IPv4 寻址，因此 **Service IP Address**（服务 **IP** 地址）仍为 IPv4 地址。

远程网络连接的 IPv6 互联网访问由底层连接启用，在底层连接中，IPv6 流量通过 IPv4 隧道传递。

 ©2025 Palo Alto Networks, Inc.

“移动用户 — GlobalProtect”和远程网络部署的 DNS 解析

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证版本 2.2 Preferred 和更高版本 ❑ 对公共和私有应用程序的原生 IPv6 访问需要以下最低版本： • Prisma Access (Managed by Strata Cloud Manager)：2024 年 6 月发布 • Prisma Access (Managed by Panorama)：Prisma Access 5.1.1仅适用于新部署。 任何其他部署（包括现有 Prisma Access (Managed by Panorama) 部署）仅支持私有应用程序访问。

Prisma Access 允许您指定 DNS 服务器来解析组织内部域和外部域。Prisma Access 根据 DNS 服务器的配置代理 DNS 请求。下表显示了内部域和外部域支持的 DNS 解析方法，并指出了 Prisma Access 在什么情况下会代理 DNS 请求。

内部 **DNS** 解析方法	外部 **DNS** 解析方法	**Prisma Access** 代理 **DNS** 请求（是/否）
单一规则，为内部域配置的 DNS 服务器	云默认值（Google IPv6 公共 DNS64）	是
单一规则，为内部域配置的 DNS 服务器	与内部域相同	否
单一规则，为内部域配置的 DNS 服务器	自定义 DNS 服务器（Google IPv6 公共 DNS64）	是
单一规则，为域设置的云默认值	云默认值（Google IPv6 公共 DNS64）	是
单一规则，为域设置的云默认值	与内部域名相同（Google IPv6 公共 DNS64）	是
单一规则，为域设置的云默认值	自定义 DNS 服务器（Google IPv6 公共 DNS64）	是

 ©2025 Palo Alto Networks, Inc.

内部 DNS 解析方法	外部 DNS 解析方法	Prisma Access 代理 DNS 请求（是/否）
多个规则，为内部域配置的 DNS 服务器	云默认值（Google IPv6 公共 DNS64）	是
多个规则，为内部域配置的 DNS 服务器	与内部域相同	是
多个规则，为内部域配置的 DNS 服务器	自定义 DNS 服务器（Google IPv6 公共 DNS64）	是
无配置	自定义 DNS 服务器（Google IPv6 公共 DNS64）	是
无配置	云默认值（适用于 IPv6，主要 =Google 公共 DNS64，次要 = 云默认值）	否
无配置	无配置	否
未指定 DNS 解析（存在使用云默认值的默认配置）	未指定 DNS 解析	否
ZTNA 连接器（无论采用何种 *DNS* 解析方法）	不适用	是
启用 ZTNA 连接器后，Prisma Access 将使用为远程网络和移动用户 — GlobalProtect 设置的 DNS 规则来代理所有 DNS 请求。		

DNS 请求的源 IP 地址取决于 Prisma Access 是否代理 DNS 请求。

- 当 Prisma Access 不代理 DNS 请求时，DNS 请求的源 IP 地址将更改为请求 DNS 查找的设备的 IP 地址。此源 IP 地址允许您实施基于源 IP 地址的 DNS 策略或识别与恶意域通信的终结点。此行为同时适用于移动用户和远程网络部署。
- 当 Prisma Access 代理 DNS 请求时，DNS 请求的源 IP 地址将更改为以下地址：
  - 移动用户部署 — DNS 请求的源 IP 地址是从 移动用户 IP 地址池 （对于内部请求）和移动用户位置的网关 IP 地址（对于外部请求）中获取的 IP 地址。
  - 远程网络部署 — 对于内部请求，DNS 请求的源 IP 地址是 **EBGP** 路由器地址；对于外部请求，则是远程网络连接的服务 IP 地址。

将 DNS 解析与 PRISMA Access 一起使用时，请遵守以下准则和限制：

- Prisma Access 支持的最大并发挂起 TCPDNS 请求数（**Max Pending Requests**（最大挂起请求数））为 64。
- 对于 UDP 查询，如果 DNS 代理在 2 秒内未收到响应，则会发送另一个请求，并在尝试下一个 DNS 服务器之前最多重试 5 次。

 ©2025 Palo Alto Networks, Inc.

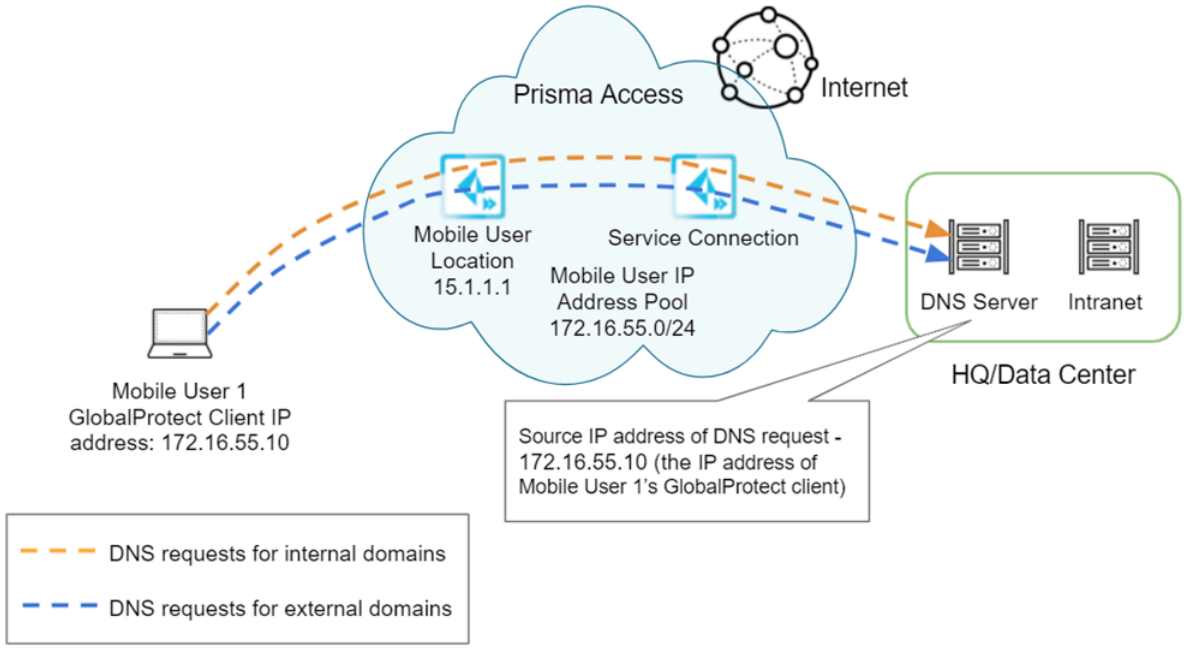
- Prisma Access 缓存生存时间 (TTL) 值为 300 秒的 DNS 条目。EDNS 响应也会被缓存。

“移动用户 — GlobalProtect”部署的 DNS 解析

在何处可以使用？	需要提供什么？
• Panorama	• Prisma Access 许可证

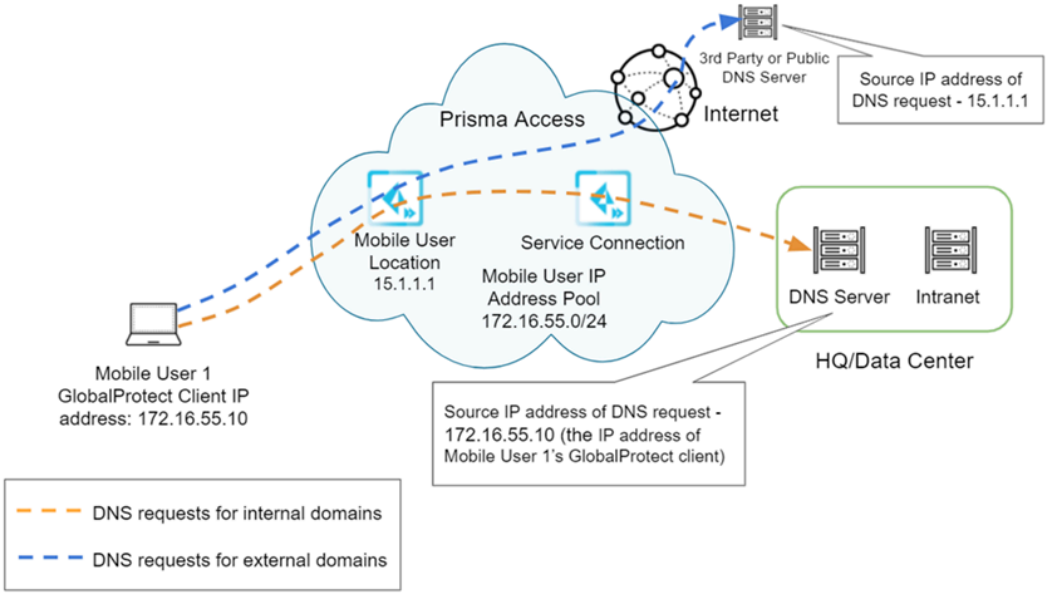
以下部分提供了一些示例，说明在您为移动用户和远程网络配置 DNS 解析后，Prisma Access 如何处理 DNS 请求的源 IP 地址。

下图显示了您已分配内部 DNS 服务器来解析内部和外部域的部署。在这种情况下，Prisma Access 不会代理 DNS 请求，DNS 请求来自移动用户 1 的 GlobalProtect 客户端 IP 地址。GlobalProtect 客户端将此 IP 地址分配给移动用户，该地址取自移动用户位置的网关 IP 地址。

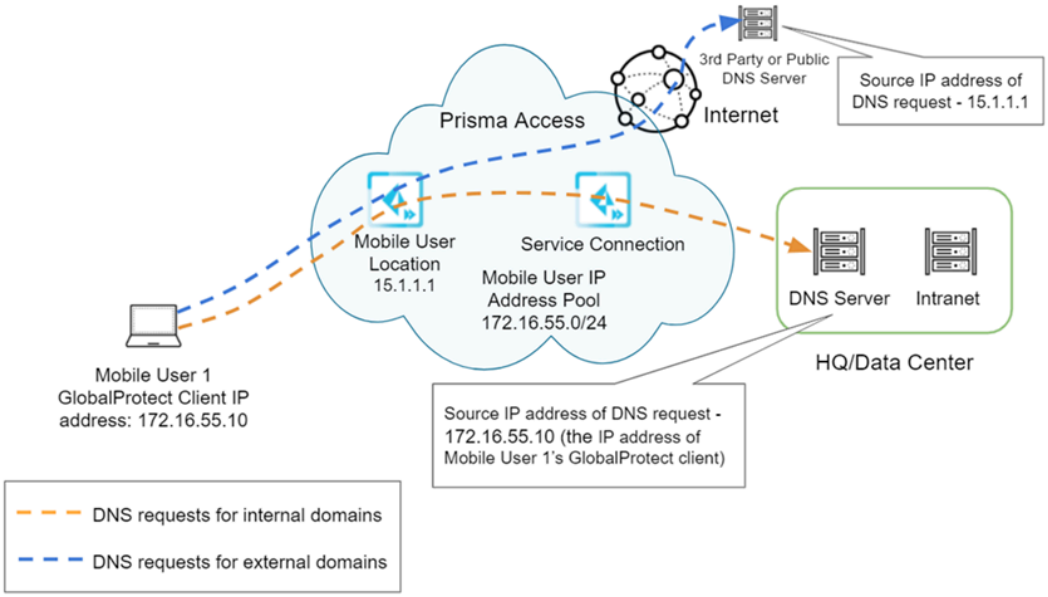


下图显示了由总部或数据中心位置的 DNS 服务器解析的内部域的 DNS 请求，而由 Prisma Access 的云默认 DNS 服务器解析的外部域的请求。在这种情况下，Prisma Access 代理外部请求的请求，源 IP 地址是 Prisma Access 网关 IP 地址（在此示例中为 15.1.1.1），而内部源 IP 仍然是移动用户 1 的 GlobalProtect 客户端 IP 地址。

 ©2025 Palo Alto Networks, Inc.



下图显示了组织使用可通过互联网访问的第三方或公共 DNS 服务器来处理对外部域的请求。Prisma Access 也会代理这些请求。



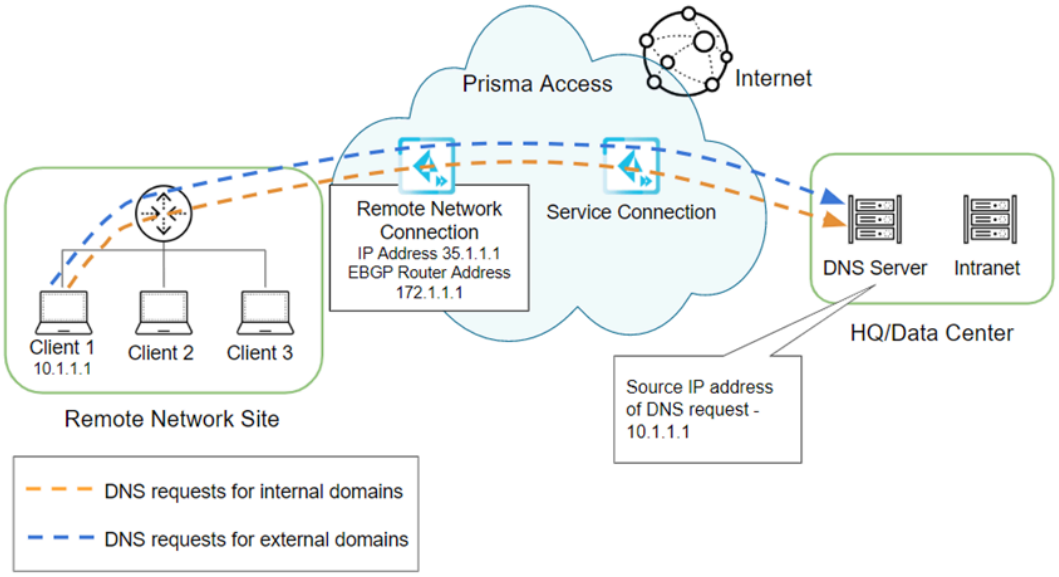
远程网络的 DNS 解析

在何处可以使用？	需要提供什么？
• Panorama	• Prisma Access 许可证

如果已有远程网络部署，则可以继续使用已有的 DNS 解析方法，也可以使用 Prisma Access 代理 DNS 请求。代理 DNS 请求允许您将公共域的 DNS 请求发送到一个服务器，并将内部域的 DNS 请求发送到另一个服务器。

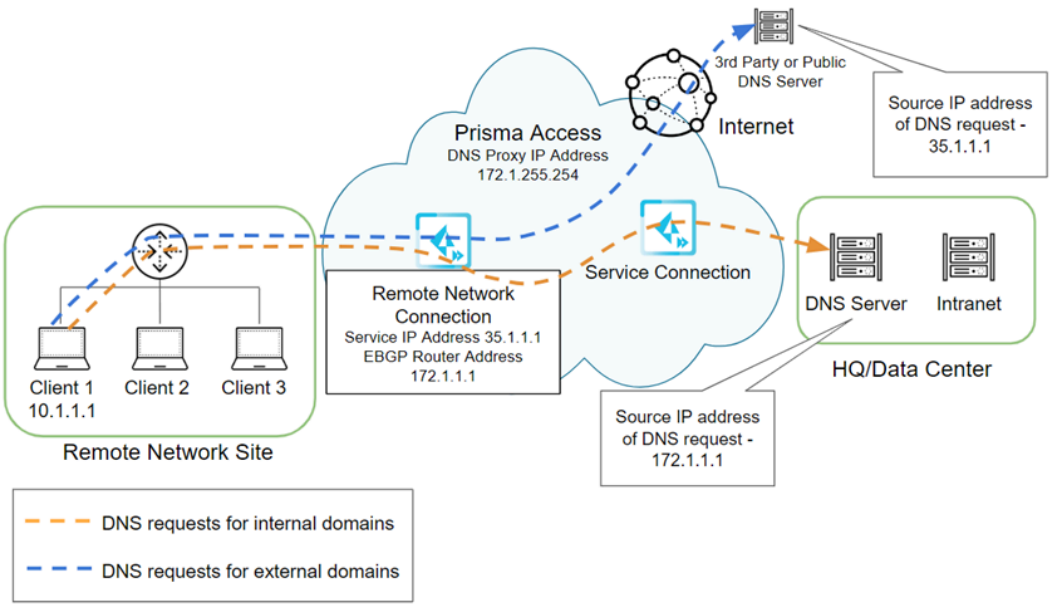
 ©2025 Palo Alto Networks, Inc.

下图显示了对部署的 DNS 请求，其中内部 DNS 服务器用于处理内部和外部域的请求。远程网络 IP 地址为 35.1.1.1，**EBGP** 路由器的 IP 地址为 172.1.1.1。在这种情况下，Prisma Access 不会代理请求，并且如果内部 DNS 服务器不使用 NAT，则 DNS 请求的源 IP 为 10.1.1.1（远程网络站点中客户端 1 设备的 IP 地址）。



如果 Prisma Access 代理 DNS 请求，则对于内部请求，代理的 DNS 请求的源 IP 地址将更改为 **EBGP** 路由器地址，对于外部请求，则更改为远程网络连接的服务 IP 地址，如下图所示。

在网络中配置用于 *Prisma Access* 代理的外部请求的 *DNS* 地址时，请指定 ***Remote Network DNS Proxy IP Address***（远程网络 ***DNS*** 代理 ***IP*** 地址）（***Panorama*** > ***Cloud Services***（云服务）> ***Status***（状态）> ***Service Infrastructure***（服务基础设施）> ***Remote Network DNS Proxy IP Address***（远程网络 ***DNS*** 代理 ***IP*** 地址））。在以下示例中，您将为网络中为 *DNS* 服务器指定 *172.1.255.254*。



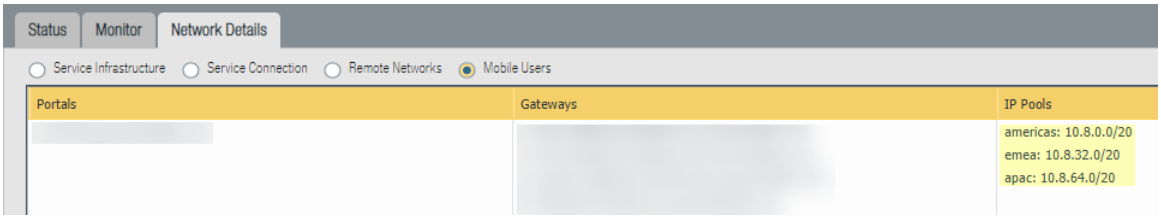
 ©2025 Palo Alto Networks, Inc.

BGP 如何为服务连接和远程网络连接通告移动用户 IP 地址池

在何处可以使用？	需要提供什么？
• Panorama	• Prisma Access 许可证

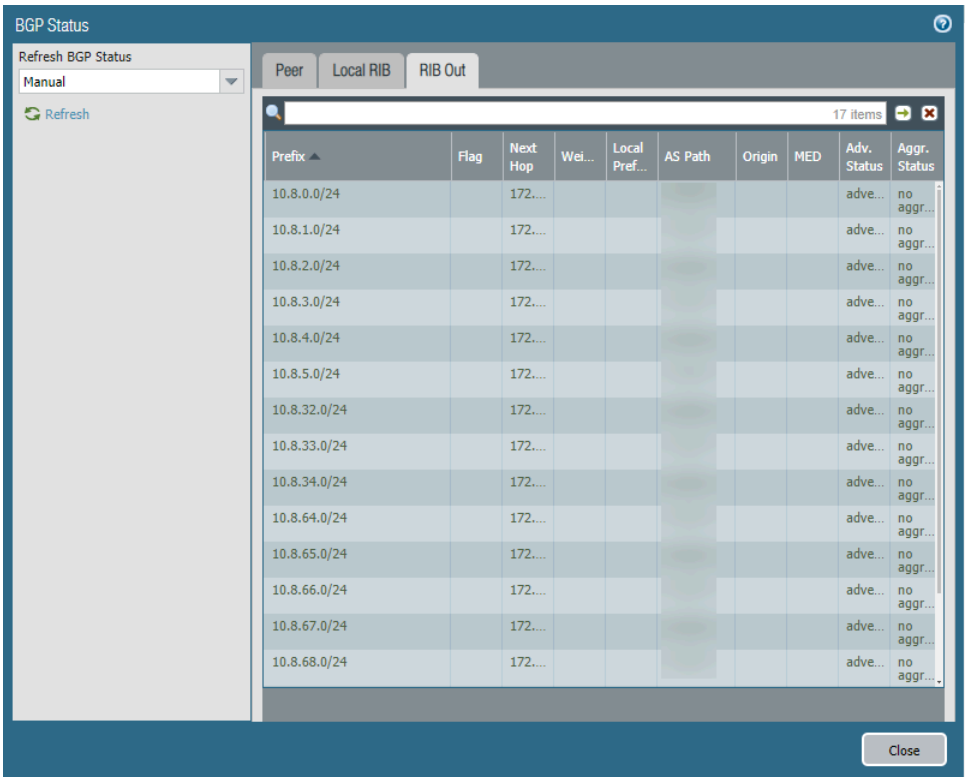
如果为服务连接或远程网络连接启用 BGP，则在您设置 GlobalProtect 移动用户(Panorama)之后，Prisma Access 将使用 C 类 (/24) 地址块分配您指定的移动用户 IP 地址池。因此，BGP 以 /24 的区块通告分配的移动用户子网，而不是通告与该区域相关的整个池。Prisma Access 为 Prisma Access 网关添加一个 /24 子网后，它会自动发送一条 BGP 通告。添加和删除子网后，Prisma Access 会自动更新其 BGP 通告。这种分配方法在通告公 BGP 路由时提供了更大的灵活性，尤其是在您配置了 **Worldwide**（全球）池而不是按区域分配池的情况下。将 IP 地址池划分为更小的子网，这样能在已分配的地址空间耗尽时添加、移除或删除相同的子网，然后在不同的区域中重复使用。

以下屏幕截图来自 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息） > **Mobile Users**—**GlobalProtect**（移动用户—**GlobalProtect**），展示了 /20 IP 地址池，可供按区域划分的三个供移动用户使用。



来自 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息） > **Service Connection**（服务连接） > **Show BGP Status**（显示 **BPG** 状态）（在**Branch AS and Router**（分支 **AS** 和路由器）区域中）的 **RIB Out**（路由信息库输出）表，展示了划分为 /24 子网块（用于 BGP 路由通告）的移动用户地址池。请注意，并不会通告整个 /20 子网。

©2025 Palo Alto Networks, Inc.



 ©2025 Palo Alto Networks, Inc.

Prisma Access 和 Strata Logging Service 对代理的支持情况

在何处可以使用？	需要提供什么？
• Panorama	• Prisma Access 许可证

如果在 Panorama、Prisma Access 基础设施和 Strata Logging Service 之间部署代理服务器，请参阅下表以了解有关预期行为的详细信息：

功能	通过不执行 **SSL** 解密的代理服务器提供支持	通过执行 **SSL** 解密的代理服务器提供支持
首次接入 **Strata Logging Service**，使用 **OCSP** 进行证书吊销状态检查	支持	仅支持直通代理；不支持任何使用 SSL 解密的代理。
Panorama 查询 **Strata Logging Service** 以获取报告和日志	如果代理服务器是 Panorama 上的默认路由，则无法在 ACC 和 **Monitor**（监控） > **Logs**（日志）页面上查看数据。 如果 Panorama 存在通往 Strata Logging Service 的备用路由，并且您可以绕过代理服务器，那么您可以在 ACC 以及 监控（**Monitor**） > 日志（**Logs**）页面上查看数据。	

©2025 Palo Alto Networks, Inc.

阻止来自特定国家/地区的传入连接

Prisma Access 允许您创建安全策略规则，以阻止来自您指定国家/地区的远程网络、移动用户—GlobalProtect 和移动用户—显式代理部署的登录尝试。Prisma Access 根据客户端源 IP 地址的地理位置信息阻止来自您指定国家/地区的传入连接。

要阻止来自这些国家/地区的传入连接，请完成以下任务。

STEP 1 | 使用特定规则名称之一创建安全策略前置规则：

请务必将此规则配置为前置规则。

- 要阻止某个国家/地区的移动用户—GlobalProtect 部署，请创建名为 **Mobile_User_EMBG_Source_Countries** 的规则。
- 要阻止某个国家/地区的移动用户—显式代理部署，请创建名为 **Explicit_Proxy_EMBG_Source_Countries** 的规则。
- 要阻止某个国家/地区的远程网络部署，请创建名为 **Remote_Network_EMBG_Source_Countries** 的规则。

STEP 2 | 为名为 **PA_predefined_embargo_rule** 的规则添加 **Tag**（标签）。

STEP 3 | 在 **Source**（源）中添加一个或多个要阻止的国家/地区。

STEP 4 | 将 **Action**（操作）指定为 **Drop**（丢弃）。

 ©2025 Palo Alto Networks, Inc.

确保来自 AWS WorkSpace 的互联网流量安全

组织需要重新考虑他们保护远程员工、承包商、医院工作人员和通过基于 Amazon WorkSpace 云的虚拟机访问互联网的呼叫中心用户的方法。这些用户需要能够安全地访问互联网，并在组织对通过这些云托管虚拟机生成的互联网流量保持完全可见性的同时，保护自己免受基于互联网的威胁。

为远程工作和资源设计的传统网络模型已经不足以应对当今复杂和创新的经济发展要求，在这种经济形势下，劳动力、数据和云应用程序变得更加分散。组织需要云服务的灵活性和可扩展性，但这些服务需要旨在满足其独特需求的云安全解决方案。

了解有关 Prisma SASE 和 AWS WorkSpace 的更多信息。

使用 Palo Alto Networks Strata Cloud Manager，您可以通过以下方法为 AWS WorkSpace 提供安全的互联网访问：

- 在 AWS WorkSpace 客户端上配置 PAC 文件
- 在 AWS 和 Prisma Access 之间配置站点到站点隧道

在 AWS WorkSpace 客户端上配置 PAC 文件

保护来自 Amazon WorkSpaces 的互联网流量的一种方法是使用代理自动配置 (PAC) 文件。PAC 文件是 JavaScript 代码，它告诉 Web 浏览器如何连接到代理服务器。企业环境使用 PAC 文件来控制 Web 流量并实施安全策略规则。Web 服务器通常用于存储 PAC 文件，Web 浏览器则在启动时下载 PAC 文件。

STEP 1 | 如果您尚未设置 Prisma SASE 显式代理，请进行设置。

您可以在 Prisma SASE 或 Web 服务器中托管 PAC 文件。使用 Web 浏览器访问 PAC URL，以验证是否可从 WorkSpace 客户端访问 PAC 服务器。

STEP 2 | 自定义 Prisma SASE 显式代理 PAC 文件，以更新代理 FQDN 并定义排除项。

1. 在 Strata Cloud Manager 中，选择 **Workflows**（工作流） > **Prisma Access** 设置 > **Explicit Proxy**（显式代理） > **Forwarding Rules**（转发规则）。
2. 根据 PAC 文件指导原则编辑 PAC 文件。

STEP 3 | 下载 Prisma SASE 显式代理根证书以安装在 AWS WorkSpace 上。

STEP 4 | 在 AWS WorkSpace 客户端上安装证书，以应用基于用户的策略规则、流量检查和报告。

这将允许 WorkSpace 客户端与 Prisma SASE 显式代理进行通信。

 ©2025 Palo Alto Networks, Inc.

STEP 5 | 在 AWS WorkSpace 上配置 PAC 文件。

执行此操作的方式取决于您所使用的浏览器。

- Google Chrome：
  1. 打开 Chrome。
  2. 选择窗口右上角的三个点。
  3. 选择 **Settings**（设置）。
  4. 选择 **Advanced**（高级）。
  5. 在 **System**（系统）下，选择 **Open proxy settings**（打开代理设置）。
  6. 在局域网 (LAN) 设置窗口中，选择 **Use automatic configuration script**（使用自动配置脚本）。
  7. 在 **Address**（地址）字段中，输入 PAC 文件的 URL。
  8. 选择 **OK**（确定）以保存更改。
- Firefox
  1. 打开 Firefox。
  2. 选择窗口右上角的三条线。
  3. 选择 **Options**（选项）。
  4. 选择 **Advanced**（高级）。
  5. 在 **Network**（网络）中，选择 **Settings**（设置）。
  6. 在 **Connection Settings**（连接设置）窗口中，选择 **Automatic proxy configuration URL**（自动代理配置 **URL**）。
  7. 在 **URL** 字段中，输入 PAC 文件的 URL。
  8. 选择 **OK**（确定）以保存更改。

应用 PAC 文件后，Chrome 和 Firefox 将使用该文件来确定每个网站要使用哪个代理服务器。

STEP 6 | 重新启动 AWS WorkSpace 浏览器。

WorkSpace 浏览器重新启动后，它将获取新的 PAC 文件并开始通过 Prisma SASE 代理路由流量。

 ©2025 Palo Alto Networks, Inc.

STEP 7 | 测试并验证流量。

将 WorkSpace 客户端配置为使用 Prisma SASE 显式代理后，您可以通过在浏览器中验证证书以及在 Prisma Access 上查看日志来测试流量。

1. 如果使用的是 Google Chrome，请选择地址栏中的挂锁。



   1. 选择 **Connection is secure**（连接安全）。
   2. 选择 **Certificate is valid**（证书有效）。
   3. 验证弹出窗口中显示的证书详细信息是否正确。
2. 如果使用的是 Safari，请选择地址栏中的挂锁图标。
   1. 选择 **Connection secure**（连接安全）。
   2. 选择 **More information**（更多信息）。
   3. 选择 **View Certificate**（查看证书）。
   4. 验证弹出窗口中显示的证书详细信息是否正确。

在 AWS 和 Prisma Access 之间配置站点到站点隧道

随着业务规模的扩大，您需要运行多个 AWS WorkSpace 客户端，因此 Prisma Access 远程网络允许您快速加入 WorkSpace 并为用户提供同类最佳的安全性。它提供一个使用便捷的选项，简化了 WorkSpace 的配置和管理过程。

组织可以通过在 AWS 和 Prisma Access 之间建立 IPSec 隧道，将 AWS WorkSpace 用户加入 Prisma Access。

使用远程网络的好处在于，它可以保护通过 Prisma Access 连接以访问互联网的用户的出站互联网流量。

STEP 1 | 为 Amazon WorkSpace 配置虚拟私有云 (VPC) 或将现有 VPC 用于 Amazon WorkSpace。

STEP 2 | 将 AWS Transit Gateway 连接到 VPC 以配置 AWS 和 Prisma Access 之间的站点到站点 IPSec 隧道。

STEP 3 | 在 AWS Transit Gateway 和 Prisma Access 远程网络 之间配置 IPSec VPN。

STEP 4 | 在 Prisma Access 远程网络上，您可以定义安全规则来限制互联网流量，以保护 AWS WorkSpace 用户。

 ©2025 Palo Alto Networks, Inc.

适用于无默认路由网络的 Prisma Access

在何处可以使用？	需要提供什么？
• Prisma Access	❑ Prisma Access 许可证

什么是无默认路由网络？

“无默认路由网络”是指没有配置默认路由的网络。当网络没有配置默认路由时，它会丢弃发往未知目标的数据包。企业通常使用“无默认路由网络”来限制其用户的访问。如果无默认路由网络上的某个设备需要访问特定目标（IP 地址或子网），则管理员需要为该目标手动配置路由。企业还需要对无默认路由分支网络上的用户、服务器和设备进行受限且安全的互联网访问。

配置无默认路由网络的原因有以下几种：

- 阻止从网络上受感染端点到随机目标的出站恶意和 DDoS 流量来提高安全性，从而防止拒绝服务攻击和其他恶意流量。
- 减少要处理的路由数量，从而提高路由设备的性能。
- 通过为特定目标配置特定的路由来实施满足用户特定需求的路由策略。

无默认路由网络注意事项

在保护无默认网络的互联网流量时，企业必须清楚地评估分支网络中可能与互联网通信的用户、端点、服务器和设备。

在无默认路由分支中，可能存在具有各种不同操作系统的设备、多用户或共享端点（如 VDI）以及无头设备（如服务器和物联网设备）。所有这些设备产生的互联网流量都需要加以保护。关键是要有一个解决方案，能够涵盖所有这些使用情形，通过不同的连接方法提供灵活性，并提供一个统一的平台，无论设备类型如何，都能始终如一地保护互联网访问。

关于保护无默认路由网络的互联网访问安全的部署建议

如果您设置了无默认路由网络，我们建议采取下列措施来保护互联网流量的安全：

设备	建议
Windows、macOS	代理模式下的 GlobalProtect 代理
ChromeOS、VDI	无代理 PAC 文件
iOS、Android	无代理 PAC 文件
Linux	无代理 PAC 文件
servers	无代理 PAC 文件

©2025 Palo Alto Networks, Inc.

物联网设备（代理感知）	无代理 PAC 文件
物联网设备（代理不感知）	远程网络 (IPSec)

关键注意事项

在无默认路由网络中部署 GlobalProtect 时，请考虑以下几点：

- 在外围设备中添加路由，将用户的互联网流量路由至 Prisma Access显式代理 IP 地址。
- 在内部托管 PAC 文件，以将 IdP URL 和 Prisma Access 门户 URL 转发到显式代理，从而允许 GlobalProtect 连接到门户和 IdP。
- 如果无默认路由网络中的 DNS 服务器无法解析外部 FQDN，则添加内部 DNS 记录以解析显式代理、PAC 文件和 Prisma Access 门户 FQDN。
- 将内部 Prisma Access 显式代理 IP 地址和 Prisma Access 门户 IP 地址的 DNAT 配置为实际的显式代理 IP 地址和门户 IP 地址。

对于基于 *PAC* 的部署，无需将 *Prisma Access* 门户 *URL* 转发到显式代理，也无需将其从 *Prisma Access* 显式代理设置中的身份验证设置中排除。

©2025 Palo Alto Networks, Inc.

Prisma Access 服务连接高级部署

在何处可以使用？	需要提供什么？
• Panorama	• Prisma Access 许可证

以下部分介绍了可用于 Prisma Access 服务连接的高级部署：

- 服务连接多云冗余
- 使用流量导向将互联网绑定流量转发到服务连接
- 服务连接流量的路由
- 使用多个服务连接创建高带宽网络

服务连接多云冗余

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

从 *Prisma Access 3.1 Innovation* 开始，支持服务连接多云冗余。

如果您使用 Prisma Access 服务连接 为移动用户和远程站点的用户提供访问总部或数据中心的内部资源和应用程序的权限，则可以通过在不同的云提供商中创建活动和备用服务连接，确保以更灵活的方式访问这些资源。您可以在同一地点或不同地理区域的不同地点指定这些活动和备用服务连接，这样，即使云提供商或区域不可用，您也可以通过服务连接访问资源。

在站点中指定活动和备用服务连接。站点是一个或多个服务连接终止的客户数据中心或总部位置（内部部署或公共云中）。创建服务连接后，请创建站点，并向该站点添加服务连接，然后将添加的服务连接指定为活动连接或备用连接。

如果云提供商或区域中断，导致站点中的活动服务连接关闭，Prisma Access 将使用这些规则重新路由流量，从而允许您的移动用户继续访问该总部或数据中心的资源：

- 如果站点中存在单个活动服务连接，则 Prisma Access 会选择该站点中的备用服务连接来路由流量。
- 如果站点中存在多个活动服务连接，则 Prisma Access 会选择另一个活动服务连接来路由流量，而备用服务连接仅在所有活动服务连接关闭时才会用于路由流量。

要利用在同一国家/地区使用活动和备用位置的站点，请使用国内首选和备用位置来载入服务连接，然后创建站点并将这些国内地点添加到站点中。

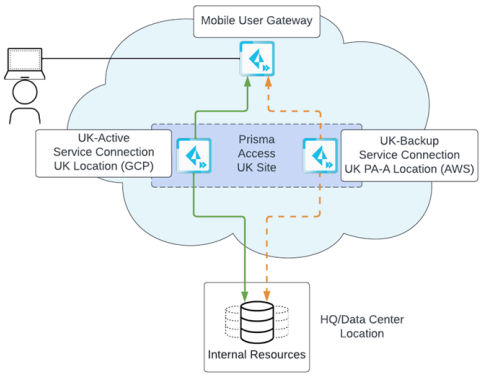
Prisma Access 还提供有关您在站点中已载入的服务连接的状态消息（例如，如果站点中的所有服务连接都部署在单个区域中）。

以下示例说明了如何利用创建站点并向其中添加服务连接的优势：

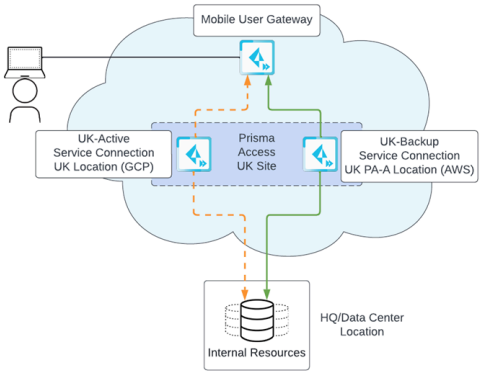
©2025 Palo Alto Networks, Inc.

- 同一地理区域中的不同云提供商 — 如果您是需要在特定国家/地区访问您的数据的组织（如银行），则可以从该国家/地区选择首选位置，并从同一国家/地区选择备用位置。以下示例显示了英国的一个组织，该组织在英国载入其服务连接以遵循数据地点法规。在这种情况下，该组织的管理员在英国载入两个服务连接，即位于英国地点的 UK-Active 和位于英国 PA-A 地点的 UK-Backup。英国地点由英国的首选云提供商 (GCP) 托管，英国 PA-A 地点由该国家的备用云提供商 (AWS) 托管。国内地点列表显示一个国家的首选和备用云提供商。然后，管理员会创建一个站点，并将 UK-Active 指定为活动位置，而将 UK-Backup 指定为该站点的备用位置。

  在正常运行期间，移动用户使用 UK-Active 服务连接访问总部或数据中心的内部资源。



  如果 GCP 中断影响 UK-Active 服务连接，则 Prisma Access 将故障切换到托管在 AWS 上的 UK-Backup 服务连接。这样，Prisma Access 就允许移动用户访问数据中心或总部的资源，即使在云提供商服务中断的情况下也是如此。下图显示了流量流。

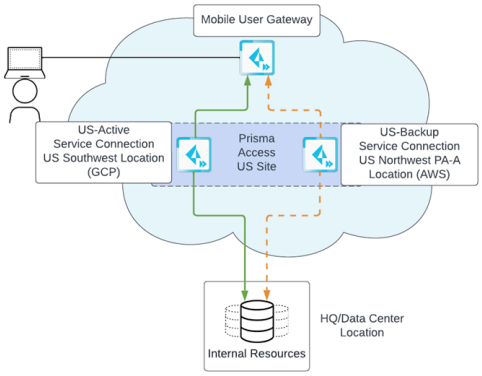


- 不同地理区域 — 如果要确保在区域服务中断时保持冗余，可以在不同的计算地点以及不同的云提供商中指定两个或多个服务连接，以便在地理区域服务中断时为您提供备用访问。在下图中，管理员已经载入了来自美国境内地点的服务连接（美国西南地点为 US-Active，美国西北

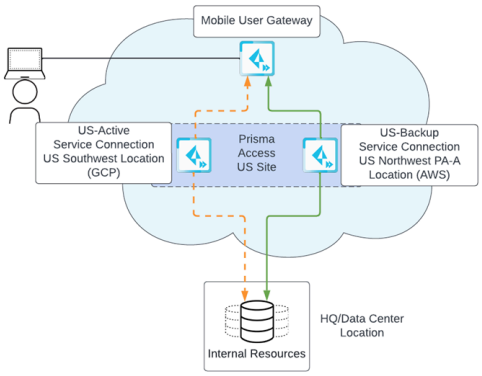
 ©2025 Palo Alto Networks, Inc.

PA-A 地点为 US-Backup），并创建了一个站点，将 US-Active 作为站点的活动服务连接，并将 US-Backup 作为备用。

您有位于不同计算位置以及不同云提供商的已载入服务连接，因此，您配置了一个站点，该站点为您提供了地理和云提供商冗余。



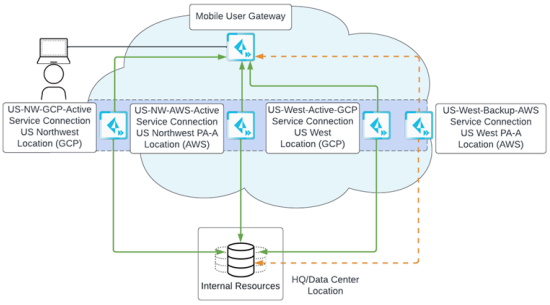
如果 US-Active 地点出现故障（无论是由于云提供商，还是由于区域服务中断），服务连接将故障转移到 US-Backup 地点，后者将使用不同于 US-Active 服务连接的云提供商和计算地点，如下图所示。



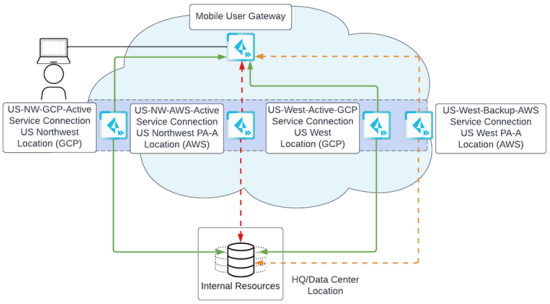
 ©2025 Palo Alto Networks, Inc.

- 使用多个服务连接的高带宽连接 — 如果您需要与内部资源建立更高带宽的连接，则可以创建具有多个活动连接的站点。下图显示正在载入四个站点，同时使用了 GCP 和 AWS 云提供商：
  - US-NW-GCP-Active，使用美国西北 (GCP) 地点
  - US-NW-AWS-Active，使用美国西北 PA-A (AWS) 地点
  - US-West-Active-GCP，使用美国西部 (GCP) 地点
  - US-West-Backup-AWS，使用美国西部 PA-A (AWS) 地点

  在站点中，三个服务连接被指定为活动服务连接，第四个服务连接被指定为备用连接。与单个服务连接相比，将三个服务连接指定为活动连接可以有效地为您提供三倍于内部资源的带宽。

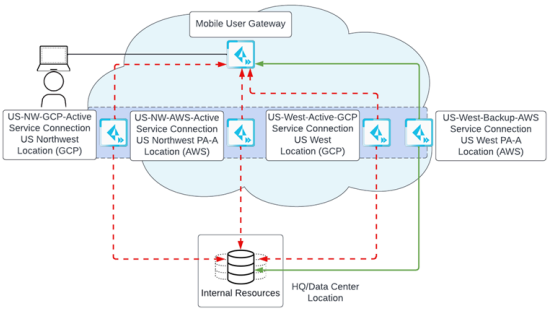


如果其中一个活动服务连接断开，备用连接不会投入使用；相反，Prisma Access 会将流量转移到其余处于打开状态的活动服务连接，如下图所示。



如果所有活动服务连接都断开，则备用服务连接将投入使用，并成为活动连接。

如果将多个服务连接配置为备用服务连接，则 *Prisma Access* 会将所有备用服务连接置于使用中，并加载共享服务连接流量。



 ©2025 Palo Alto Networks, Inc.

配置冗余云提供商服务连接时，请使用以下指南：

- 您可以使用站点中的首选或备用地点添加服务连接。

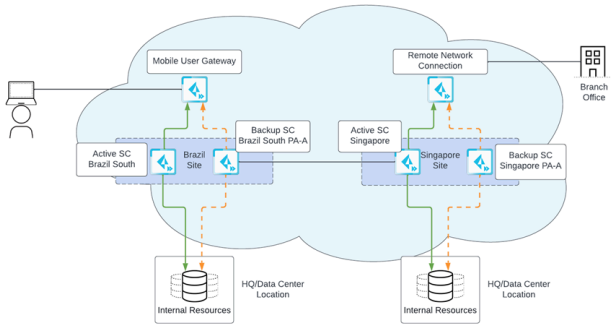
  Palo Alto Networks 强烈建议您使用首选云提供商作为站点中的主动服务连接。
- 站点中的所有服务连接都必须指向同一总部或数据中心地点的同一资源。站点中不能有指向不同地点的不同资源的服务连接。
- 站点中必须至少选择一个活动服务连接；但是，单个站点中也可以有多个活动服务连接。以下站点配置有效：
  - US Central（活动）
  - US Central PA-A（备用）
  - US East（活动）
  - US East PA-A（备用）
- 如果您在一个站点中有多个活动服务连接，并且一个活动服务连接断开，则流量会转移到另一个活动服务连接（也就是说，只要其中一个活动服务连接处于打开状态，就不会使用备用服务连接）。
- 按照以下指导原则使用静态和动态服务连接路由：
  - 如果对服务连接使用静态路由，请确保为服务连接指定的子网指向相同的子网。

    例如，如果您有一个站点使用 192.168.41.0/24、192.168.44.0/24 和 192.168.47.0/24 作为活动服务连接的子网，请确保为备用服务连接指定相同的子网。
  - 如果将动态 (BGP) 路由用于服务连接，请确保所有服务连接都向同一数据中心或总部通告相同的前缀。
- Prisma Access 使用 BGP 多出口鉴别器 (MED) 值来区分站点中的活动服务和备用服务连接，如下表所示。请注意，活动服务连接的 MED 值会根据您是否为活动服务连接启用了辅助 IPSec 隧道而更改。Prisma Access 将这些 MED 值通告给 CPE（BGP 对等体）。

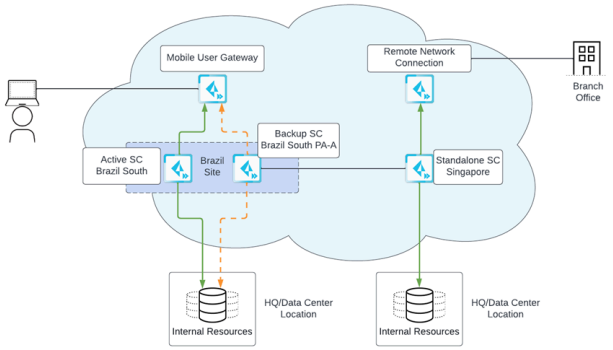
连接类型	MED 值
站点中的活动 **IPSec** 服务连接	
活动服务连接，未配置辅助 IPSec 隧道	0
活动服务连接，已配置辅助 IPSec 通道，主通道	100
活动服务连接，已配置辅助 IPSec 隧道，辅助隧道	200
备用站点中的 **IPSec** 服务连接	
备用服务连接，主隧道（无论是否已配置辅助 IPSec 隧道）	500
备用服务连接，已配置辅助 IPSec 隧道，辅助隧道	600

©2025 Palo Alto Networks, Inc.

- 您可以在单个 Prisma Access 部署中添加多个站点，如下图所示。



- 您仍然可以使用单个独立服务连接访问内部资源。您还可以将独立服务连接与活动和备用服务连接混合使用，如下图所示。



- 为服务连接使用热土豆路由时，不支持服务连接多云冗余。
- 不要使用 CLI 载入和配置服务连接。如果您需要使用 CLI 实现载入服务连接，请与 Palo Alto Networks 团队联系。

配置和激活服务连接云提供商冗余

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

要为云提供商配置多个服务连接，请完成以下步骤。

STEP 1 | （仅限现有 Prisma Access 部署）如果您已将插件升级到支持云提供商冗余的版本，请在升级到受支持的插件后执行 **Commit and Push**（提交并推送）操作

从 Prisma Access 3.1 Preferred 和 Innovation 开始，支持服务连接多云冗余。升级云服务插件后，必须执行 **Commit and Push**（提交并推送）操作，才能使云冗余更改显示在 UI 中。

如果您有新部署（而非升级），请跳过此步骤。

©2025 Palo Alto Networks, Inc.

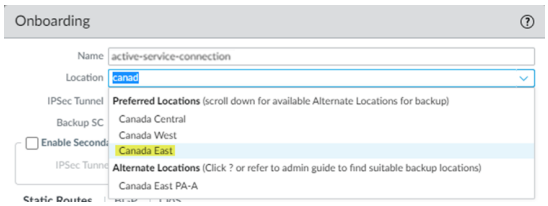
STEP 2 | 创建要用作站点中的活动和备份服务连接的服务连接。

创建首选位置和备用位置并提交和推送更改后，无法更改这些位置。例如，您无法将首选位置从加拿大东部更改为加拿大东部 *PA-A*，也无法将备用位置从加拿大东部 *PA-A* 更改为加拿大东部。

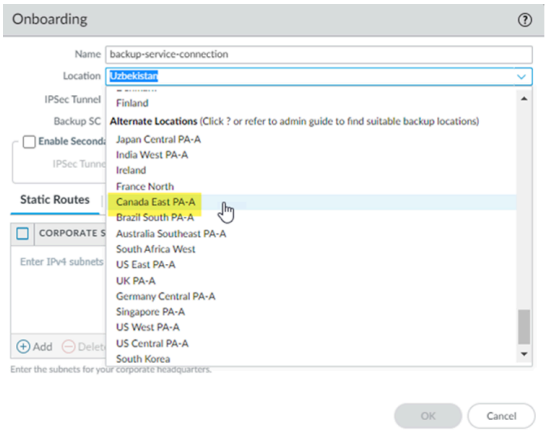
1. 选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Service Connection**（服务连接）。
2. **Add**（添加）您将指定为站点中的活动服务连接的服务连接。

   从首选位置或备用位置列表中选择。

   要搜索某个位置，请开始输入 ***Location***（位置）名称。



3. **Add**（添加）您将指定为站点中的备份服务连接的服务连接。



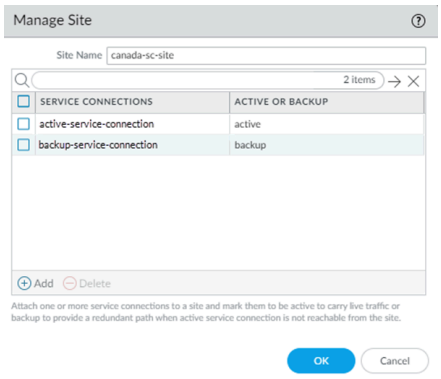
4. （可选）根据需要继续加入要指定为活动站点和备份站点的服务连接。

 ©2025 Palo Alto Networks, Inc.

STEP 3 | 创建一个站点；然后，将您添加的服务连接指定为站点中的活动或备份服务连接。

1. 在 **Manage Sites**（管理站点）中，**Add**（添加）新站点。
2. **Add**（添加）您已加入的服务连接。
3. 将您添加的服务位置指定为 **active**（活动）和 **backup**（备份）站点。

   您可以创建多个活动站点和备份站点。指定至少一个站点作为活动站点。
4. 单击 **OK**（确定）。
5. （可选）根据需要继续为活动和备份服务连接添加站点。



STEP 4 | **Commit and Push**（提交并推送）更改。

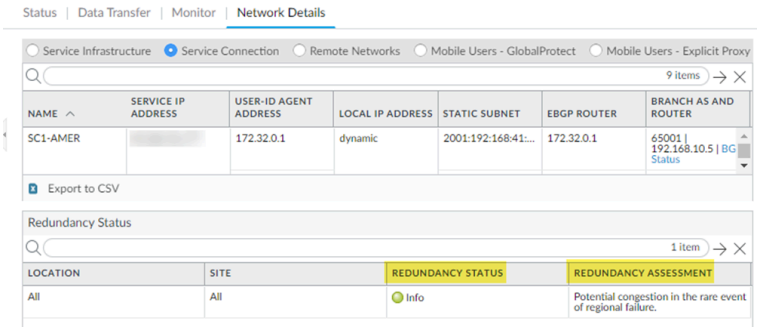
STEP 5 | 检查站点的状态。

1. 选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息） > **Service Connection**（服务连接） > **Redundancy Status**（冗余状态）。
2. 检查 **Redundancy Status**（冗余状态）和 **Redundancy Assessment**（冗余评估）字段中的信息。冗余状态提供您部署的站点的状态，冗余评估提供有关站点中部署的服务连接的更多详细信息。

冗余状态	冗余评估
信息	如果发生区域故障，您的服务连接可能会出现拥塞。
警告	所有服务连接均部署在一个区域中。请考虑在附近的位置部署服务连接。 此消息通知您，所有服务连接均部署在一个区域中。
小心	连接到该站点的所有服务连接均部署在一个区域中。请考虑在附近的位置部署服务连接。

 ©2025 Palo Alto Networks, Inc.

冗余状态	冗余评估
	此消息通知您，连接到站点的所有服务连接均部署在一个区域中。



受支持的国内主动和备份云提供商冗余位置

在何处可以使用？	需要提供什么？
• Panorama	• Prisma Access 许可证

如果您想要配置活动位置和备份位置位于同一国家/地区的部署，请从该国内首选位置和备用位置列表中进行选择。

首选地点	替代地点
澳大利亚东南部	澳大利亚东南部 PA-A
巴林 PA-A	巴林
巴西南部	巴西南部 PA-A
加拿大东部	加拿大东部 PA-A
法国北部 PA-A	法国北部
德国中部	德国中部 PA-A
印度西部	印度西部 PA-A
爱尔兰 PA-A	爱尔兰
日本中部	日本中部 PA-A
新加坡	新加坡 PA-A
南非西部 PA-A	南非西部

©2025 Palo Alto Networks, Inc.

首选地点	替代地点
韩国PA-A	韩国
英国	英国 PA-A
阿拉伯联合酋长国 PA-A	阿拉伯联合酋长国
美国中部	美国中部 PA-A
美国东部	美国东部 PA-A
美国西北部	美国西北部 PA-A
美国西部	美国西部 PA-A

使用流量导向将互联网绑定流量转发到服务连接

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证 ❑ 将证书吊销列表 (CRL) 和在线证书状态协议 (OCSP) 直接发送到互联网的功能至少需要 Prisma Access 版本 5.1.1。

Prisma Access 允许您创建流量导向规则，以指定来自移动用户和远程网络连接的互联网绑定流量的目标。您可以指定在发送到互联网之前要重定向到服务连接的流量，也可以指定直接传出至互联网的流量。这个功能称为 流量导向 *(Traffic Steering)*。

或者，您可以将 Prisma Access 配置为接受从 CPE 到 Prisma Access 的默认路由，以便 Prisma Access 将绑定互联网的移动用户流量转发到部署中的最佳服务连接。

具有 Prisma Access 流量控制的默认路由

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

使用 Prisma Access 中的默认路由功能接受从您的 CPE 到服务连接通告的默认路由。可以使用 BGP 或静态路由来通告默认路由。Prisma Access 使用 BGP 在多个服务连接上通告这些路由，这让 Prisma Access 能够通过给定移动用户位置的最佳服务连接来路由移动用户流量。若要使服务连接接受默认路由，请在在 Prisma Access 中配置流量导向时指定 **Accept Default Route over Service Connections**（接受服务连接上的默认路由）设置。

©2025 Palo Alto Networks, Inc.

启用默认路由后，您的互联网流量将被引导到服务连接，而不是从移动用户位置流出。如果要将互联网流量重定向到数据中心，则此功能非常有用。例如，如果您的数据中心中有第三方安全堆栈，并且您希望该堆栈执行额外的筛选或检查。

实现默认路由时请遵循以下准则：

- 默认路由仅适用于移动用户部署；启用默认路由后，远程网络连接将正常运行，不会发生任何变化。
- 尽管支持将目标服务连接和流量控制规则与默认路由一起使用，但如果您允许默认路由，则不需要这两者。
- 如果指定了 **Accept Default Route over Service Connections**（接受服务连接上的默认路由）设置时，则所有 Prisma Access 服务连接（专用服务连接除外）都将接受默认路由，并在流量控制决策中使用这些路由。
- 在启用此设置之前，请确保数据中心正在发送默认路由。否则，通过服务连接的路由将失败。
- Palo Alto Networks 建议所有数据中心都通告默认路由；当 Prisma Access 收到路由时，它可以选择用于远程网络位置的最佳服务连接。
- 配置服务连接 时，请对连接使用“仅静态路由”或“仅 BGP”。在使用默认路由时，Palo Alto Networks 不建议将使用 BGP 的服务连接与使用静态路由的服务连接混合使用。
- （仅适用于 Prisma Access (Managed by Panorama) 部署）多租户部署支持使用默认路由。
- Prisma Access 不会使用默认路由将无客户端 VPN、门户或网关 SAML 身份验证流量转发到公共身份提供程序 (IdP)。

有关使用流量控制实现默认路由的详细信息和示例，请参阅 具有流量控制的默认路由示例、流量定向控制到互联网的默认路由示例和具有流量控制和专用服务连接的默认路由示例。

Prisma Access 中的流量导向

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

在标准 Prisma Access 部署中，服务连接提供对内部网络资源的访问，例如您总部或数据中心的身份验证服务和私有应用程序。服务连接处理内部流量，无需互联网访问。在某些情况下，您可能希望将互联网流量重定向到数据中心。流量引导允许您在将移动用户或远程网络流量发送到互联网之前，将其重定向到服务连接。

您可以在移动用户部署、远程网络部署或两者的组合中使用流量引导。使用流量引导根据多种标准（包括IP地址、用户、URL、自定义URL类别、服务类型（HTTP或HTTPS）、用户ID、动态地址组（DAGs）、动态用户组（DUGs）和基于IP的外部动态列表（EDLs））来引导互联网流量。https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/url-filtering/custom-url-categorieshttps://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-panorama-admin/configure-user-based-policies-with-prisma-accesshttps://docs.paloaltonetworks.com/pan-os/10-1/pan-os-web-interface-help/objects/objects-address-groupshttps://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/policy/use-an-external-dynamic-list-in-policy/external-dynamic-list

 ©2025 Palo Alto Networks, Inc.

支持两种流量引导的操作类型：

- 转发到目标—使用流量引导规则中的标准，通过您创建的目标转发互联网流量，该目标使用一个或多个服务连接。
- 转发到互联网 — 使用流量引导规则中的标准，直接将流量从其源（移动用户位置或远程网络连接）转发到互联网，而不经过服务连接。

如果您转发到目标，您可以选择创建两种类型的目标组：专用和非专用。

- 仅用于流量引导相关流量的服务连接称为专用服务连接。要将服务连接设置为专用服务连接，请在 Panorama 中选择仅用于流量引导的专用选项。在 Prisma Access 中配置流量导向仅在您设置流量引导规则时选择专用 PBF。Strata Cloud Manager

  如果您使用的第三方安全堆栈位于您组织的内部网络之外，以在将流量发送到公共SaaS应用程序或互联网之前处理流量，您可能需要配置专用的服务连接。因为安全堆栈不是您组织网络的一部分，因此您不希望此服务连接处理任何内部网络流量。
- 用于流量引导和标准服务连接相关流量（例如，前往数据中心的身份验证服务器的流量）的服务连接是非专用服务连接。

将服务连接设置为专用服务连接会导致以下更改：

- （仅适用于 Prisma Access (Managed by Strata Cloud Manager) 部署）服务连接对转发的流量应用源NAT。源IP地址是服务连接的EBGP路由器地址，该地址来自基础设施子网。
- 与此目标相关的所有服务连接的区域从信任变为不信任。检查您的区域映射，以确保您的网络反映此更改。Prisma Access 区域为流量导向专用连接配置服务区映射和安全策略
- 配置为专用服务连接的服务连接不参与内部或外部的BGP路由。
- （仅适用于部署）CYR-13358如果您的专用服务连接使用 BGP，当您打开状态页面（Panorama云服务状态监控服务连接），选择一个区域，然后选择状态选项卡时，BGP 状态显示为未启用。Prisma Access (Managed by Panorama) > > > > 要检查服务连接的BGP状态，请检查服务连接配置页面（Panorama云服务配置服务连接）。 > > >
- （仅适用于 Prisma Access (Managed by Panorama)部署）默认情况下，服务连接对转发的流量应用源NAT。源IP地址是服务连接的用户ID代理地址（Panorama云服务状态网络详细信息服务连接用户ID代理地址），该地址来自基础设施子网（Panorama云服务状态网络详细信息服务基础设施）。 > > > > > > > > >

  （仅适用于部署）您可以禁用源 NAT，并使用您组织的源 IP 地址用于专用服务连接；要做到这一点，请在流量引导区域的目标服务连接中添加目标时选择禁用专用 SC 的源 NAT。Prisma Access (Managed by Panorama)

交通引导要求

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

在实施流量引导之前 Prisma Access 部署时，请确保您的网络环境具有以下基础架构要求：

 ©2025 Palo Alto Networks, Inc.

- Prisma Access 必须能够连接到贵组织用于终止服务连接的支持 IPSec 的 CPE（例如路由器或 SD-WAN 设备），并且该设备的 IP 地址必须可以从 Prisma Access。

  您可以使用标准 IPSec 和 IKE 加密配置文件在堆栈位置和 Prisma Access。配置服务连接 和使用流量控制时，您可以使用静态路由、BGP 或两者的组合。如果您使用具有流量控制的默认路由，Palo Alto Networks 建议您仅使用 BGP 或仅使用静态路由。如果使用静态路由，请在 创建 IKE 网关时指定组织 CPE 使用的公网 IP 地址作为 对等地址 。
- Prisma Access 可能与流量控制规则中 URL 类别的 URL 的前几个数据包不匹配，这意味着网络会话的前几个数据包（例如，TCP 握手）可能与规则不匹配。Palo Alto Networks 建议，对于在流量控制规则中使用的 URL，创建安全策略规则以允许它们通过不信任区域，以便在新会话开始时握手可以完成。
- 如果您将此配置与安全堆栈一起使用，则必须可以通过标准 IPSec 隧道配置从服务连接访问堆栈位置。

配置流量导向时，请遵循以下准则：

- 您可以在流量引导配置中指定最多 1,000 个 URL（聚合），包括 自定义 URL 类别中的常规 URL 和通配符 (*.example.com) URL。

  此数字包括手动输入的 URL、通配符 URL 以及在自定义 URL 类别中输入的 URL。
- 如果您在流量控制规则中使用此类别，Prisma Access 会在自定义 URL 类别中的 URL 前面添加星号。如果对流量引导和其他安全策略规则使用相同的 URL 类别策略，则这些更改将同时适用于流量引导规则和其他安全策略规则。

  如果您有未在流量控制规则中使用的自定义 URL 类别， Prisma Access 不会更改这些类别中的 URL。
- 在流量转发规则中输入 URL 以及在自定义 URL 类别中添加 URL 时，请使用全部小写的 URL。
- 最多可以配置100条流量转发规则。
- 如果您配置了主隧道和备份隧道，则从主隧道（活动隧道）故障转移到备份隧道后，使用流量控制规则的流量控制将不起作用。 具有 Prisma Access 流量控制的默认路由 在具有主隧道和备份隧道的故障转移场景中工作。

具有流量控制的默认路由示例

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

以下示例显示了以下组件的 Prisma Access 部署示例：

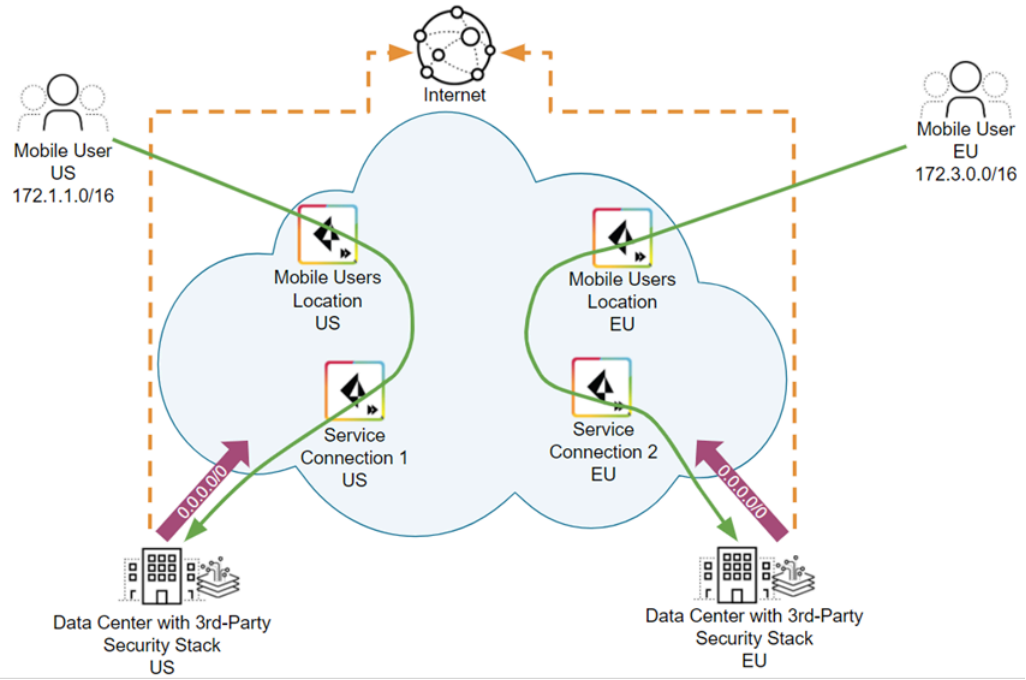
- 有两个 Prisma Access 移动用户位置；一个在美国，一个在欧洲。
- 两个 Prisma Access 服务连接；一个在美国，一个在欧洲，两个数据中心都向服务连接发送默认路由（启用了 **Accept Default Route over Service Connections**（通过服务连接接受默认路由））。
- 两个数据中心；一个在美国，一个在欧洲。

  每个数据中心都有一个第三方安全堆栈；因此，您希望所有与互联网连接的流量在进入互联网之前都通过数据中心。

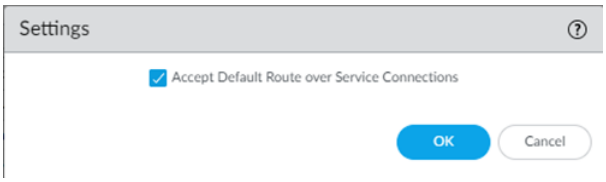
 ©2025 Palo Alto Networks, Inc.

当移动用户发送数据中心流量时，Prisma Access 会检查其路由表，确定最近的服务连接，并将流量转发到该服务连接。在以下示例中，Prisma Access 将来自美国移动用户的数据中心流量发送到服务连接，将来自欧洲移动用户的流量发送到服务连接 2。

请勿将流量控制专用的的服务连接与默认路由一起使用；专用服务连接不参与 *BGP* 路由，因此无法接收来自总部或数据中心的 *BGP* 通告。



要启用默认路由，请在配置流量控制设置时选择 **Accept Default Route over Service Connections**（通过服务连接接受默认路由）。配置此设置并提交和推送更改后，Prisma Access 将通过服务连接发送发往互联网的流量。

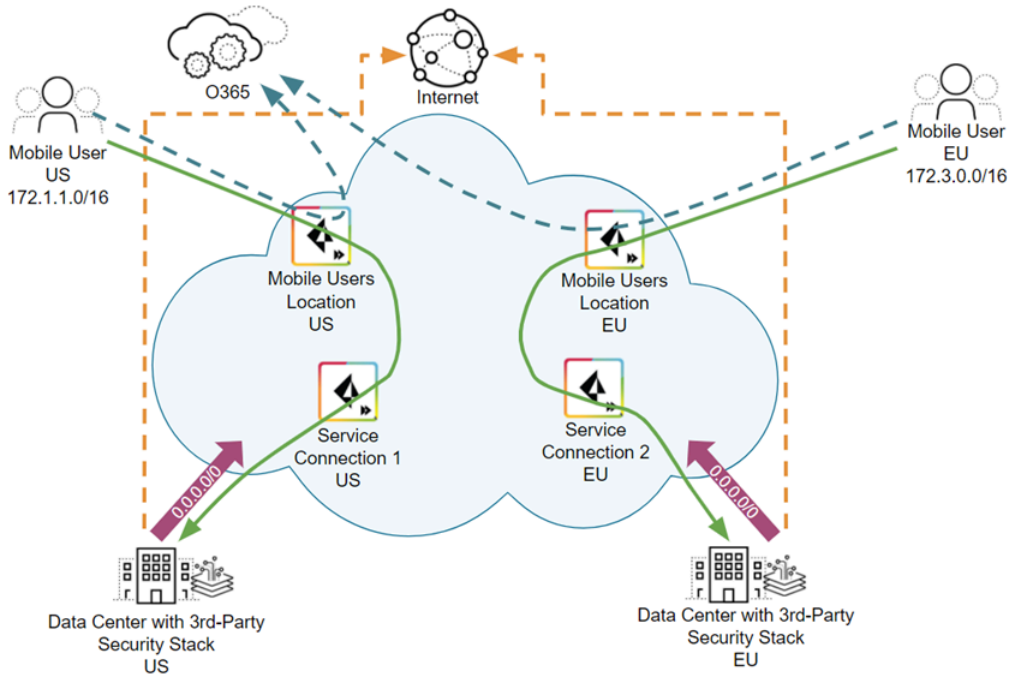


流量定向控制到互联网的默认路由示例

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

以下示例显示了如何对外部 SaaS 应用程序绑定流量进行更精细的控制。在这种情况下，您希望将 Office 365 流量直接从移动用户位置发送到互联网出口，而不是将其发送到数据中心进行进一步处理。对于此配置，可将流量控制与默认路由一起使用。

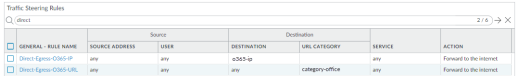
 ©2025 Palo Alto Networks, Inc.



若要允许 Prisma Access 将 Office 365 流量直接路由到互联网，请执行以下操作：

- 使用与 Office 365 地址匹配的 IP 地址创建 EDL（**Object**（对象） > **External Dynamic Lists**（外部动态列表））
- 使用与 Office 365 URL 匹配的 URL 创建自定义 URL 类别（**Objects**（对象） > **Custom Objects**（自定义对象） > **URL Category**（**URL** 类别））
- 创建 在 Prisma Access 中配置流量导向，并且将您创建的 EDL 和 URL 类别指定为目标匹配条件（将 **Action**（操作）设置为 **Forward to the internet**（转发到互联网））。

此配置将 Office 365 流量直接发送到互联网，而其他互联网流量则发送到数据中心进行进一步处理，然后再发送到互联网。

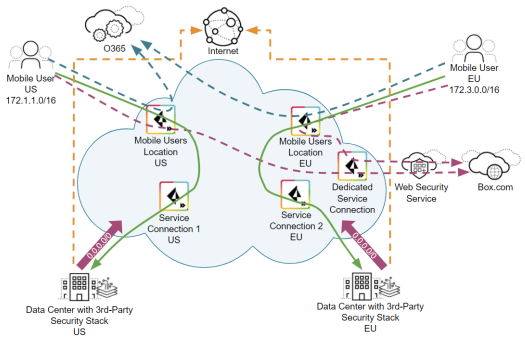


具有流量控制和专用服务连接的默认路由示例

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

在此示例中，除了前面的配置外，您还有一个第三方互联网安全服务，并且您希望将来自 box.com 的流量先发送到安全服务进行处理，然后再发送到互联网。您不想将任何其他发往互联网的流量发送到该安全服务；基于此，要为 box.com 的流量创建一条专用服务连接。配置完成后，Prisma Access 会将 *.box.com 目标流量发送到堆栈。

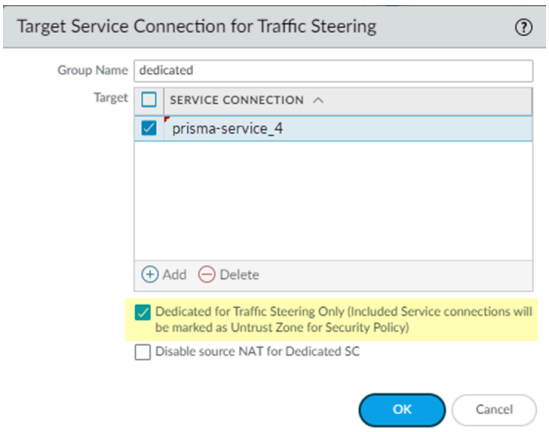
 ©2025 Palo Alto Networks, Inc.



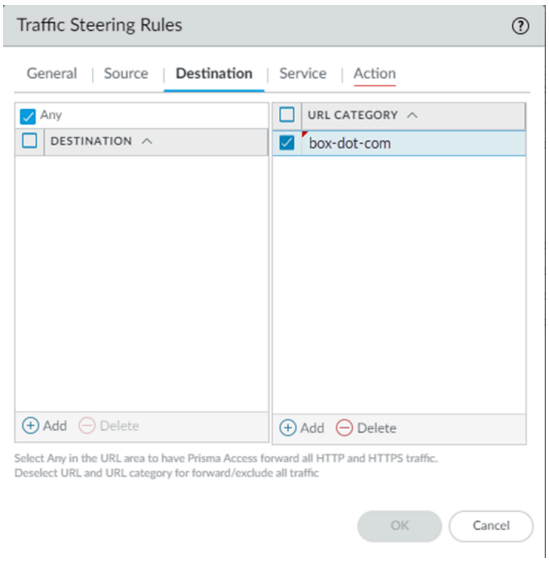
要启用此部署，请在“Traffic Steering（流量控制）”选项卡中执行以下操作：

- 创建将一个或多个服务连接分配给目标的目标服务连接组，然后选择 **Dedicated for Traffic Steering Only**（流量控制专用），使一个或多个目标服务连接成为专用连接。

  如果您创建具有多个服务连接的目标，*Prisma Access* 会选择最佳服务连接来转发发往互联网的流量。

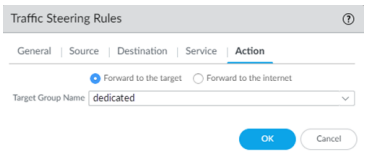


- 创建用于将流量转发到 URL 的流量控制规则。下面的屏幕截图显示了为流量目的地分配的自定义 URL 类别，其中包含 URL *.box.com。



 ©2025 Palo Alto Networks, Inc.

- 在流量控制规则中创建一个 **Action**（操作），内容为 **Forward to the target**（转发到目标），然后指定您已创建的目标组名称（本例中为 **dedicated**）。



Prisma Access 交通引导规则指南

在何处可以使用？	需要提供什么？
• Panorama	• Prisma Access 许可证

流量引导可以处理各种可能的配置；然而，重要的是要了解如何 Prisma Access 处理规则，这样您就可以创建易于维护和管理的规则。为了帮助您创建最适合您的部署的规则，请遵循以下准则：

- Prisma Access 按照创建规则的顺序（从上到下）评估规则。在顶部指定更具体的规则，在底部指定更一般的规则。
- 创建具有较少匹配条件的多个规则，而不是创建具有多种类型条件的较少规则。创建更简单的规则既可以加快规则创建速度，又可以使修改规则变得更容易。
- 由于创建规则后无法在列表中上下移动规则，因此在创建规则之前请仔细规划规则顺序。
- 不支持指定 任何源 地址和用户、 任何源 目标和 URL 类别以及 任何 服务的规则。使用更具体的规则；例如，指定包含 任何源 或目标流量以及 **service-http** 和 **service-https**服务的规则。
- 如果您要在 源用户 字段中为用户指定规则，请确保 Prisma Access 通过以 域/用户名 的格式对 LDAP 用户进行身份验证、以 用户名 （不带域名）的格式对本地用户进行身份验证，可以区分在本地身份验证的用户和使用 LDAP 进行身份验证的用户之间是否共享相同的用户名。
- 如果您已将本地下一代防火墙配置为主设备，则可以通过选择 **Panorama** > 云服务 > 配置 > 移动用户，单击齿轮图标编辑设置，然后在设备组区域中选择 主设备，自动填充流量控制和安全策略规则中移动用户设备组的用户和组信息。虽然这会在每个设备组中填充主设备，但它只会在安全策略规则中填充移动用户的用户和组信息。
- 如果在流量控制规则中使用了 EDL（类型 IP 列表），并且 EDL 的 EDL 源 URL 更新为不可访问的 URL， Prisma Access 可以继续使用以前 URL 的缓存 IP 列表。
- 如果您对 TCP 端口 80 和 443 使用应用程序覆盖策略， 则 Prisma Access 会绕过服务类型为 HTTP 或 HTTPS 的规则的流量控制。

  此外，如果您为 TCP 端口 80 或 443 配置了应用程序覆盖策略，则流量转向不适用于流量转向规则中引用的 URL 类别的 URL。
- 您可以在同一规则中指定目标 IP 地址和 URL 类别。如果你这么做了， Prisma Access 使用逻辑或来处理规则中的目标条件，但基于 HTTP 的 TCP 端口 80 和 8080 以及 HTTPS 的 TCP 端口 443 处理 URL 和 URL 类别流量。

  对于具有 IP 地址和 URL 类别的规则，只要 IP 地址或 URL 类别匹配，流量就与规则匹配，但仅根据端口 80、443 和 8080 处理 URL 类别流量。Palo Alto Networks 不建议创建此类规则；而是创建更简单的规则。

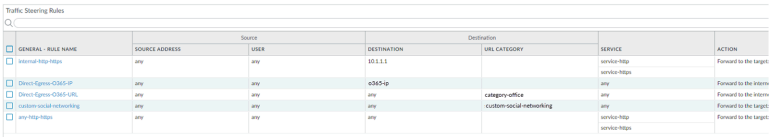
 ©2025 Palo Alto Networks, Inc.

例如，您想对网络流量实施以下规则：

- 您在数据中心有一个 IP 地址为 10.1.1.1 的内部 HTTP 服务器，并且您想将内部 HTTP 和 HTTPS 流量引导至该服务器。服务器 IP 地址为 10.1.1.1。

  到该服务器的流量不应该流向互联网，而应该在内部处理；因此，为此流量选择一个非专用目标，因为这种类型的目标同时处理内部流量和互联网流量。
- 您希望将 office365.com 流量直接路由到互联网。
- 您希望来自 *.example.com 的流量或在 **custom-social-networking** 的自定义 URL 类别中定义的任何流量被路由到专用连接。
- 您希望任何其他 HTTP 和 HTTPS 流量使用与内部 HTTP 服务器相同的非专用服务连接目标。

对于此示例，请创建从最具体到最不具体的规则，如下面的屏幕截图所示。不要首先添加允许所有 HTTP 和 HTTPS 流量的规则，否则 Prisma Access 会将所有 HTTP 和 HTTPS 流量引导到非专用连接，而不会评估任何其他规则。



为流量导向专用连接配置服务区映射和安全策略

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

如果您创建使用专用服务连接的目标，则专用服务连接的服务区将从 **Trust**（可信）更改为 **Untrust**（不可信）（非专用服务连接目标不会更改其服务区）。由于您无法为服务连接创建服务区或配置服务区映射，因此您可以对移动用户和设备组的专用服务连接进行服务区映射和安全策略更改。完成以下步骤，配置专用连接的服务区映射。

这些步骤显示的是示例配置；您可以根据自己的部署定制此示例。

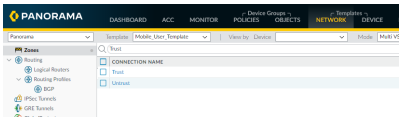
STEP 1 | 选择 **Network**（网络） > **Zones**（区域）。

STEP 2 | 从下拉列表中选择正确的 **Template**（模板）（对于移动用户，选择 **Mobile_User_Template**；对于远程网络，选择 **Remote_Network_Template**）。

如果您有移动用户和远程网络部署，则需要执行这些步骤两次；一次在 **Mobile_User_Template** 中执行，一次在 **Remote_Network_Template** 中执行。

STEP 3 | 为可信和不可信服务区 **Add**（添加）两个服务区。

在此示例中，创建两个服务区，分别称为 **Trust**（可信）和 **Untrust**（不可信）服务区。



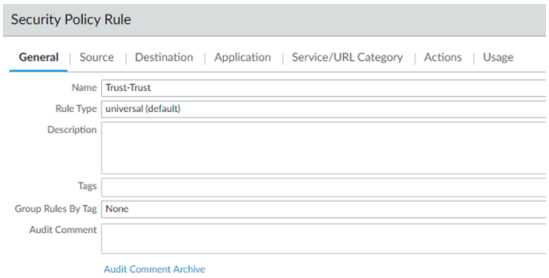
 ©2025 Palo Alto Networks, Inc.

STEP 4 | 为您创建的服务区创建默认策略。

1. 选择 **Policies**（策略） > **Security**（安全） > **Post Rules**（后置规则）。
2. 从下拉列表中选择正确的 **Device Group**（设备组）（对于远程网络，选择 **Mobile_User_Device_Group**；对于移动用户，选择 **Remote_Network_Device_Group**）。

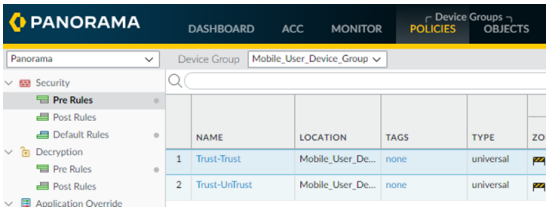
   如果您有移动用户和远程网络部署，则需要执行这些步骤两次；一次在 **Mobile_User_Device_Group** 中执行，一次在 **Remote_Network_Device_Group** 中执行。
3. **Add**（添加）用于可信区到可信区流量的默认策略。

   对于所有 **Source**（源）、**User**（用户）、**Destination**（目标）、**Application**（应用程序）和 **Service/URL Category**（服务/URL 类别）流量，此策略允许 **Any**（任何）流量通过。



4. **Add**（添加）用于可信区到不可信区流量的默认策略，使用与可信区到可信区策略相同的参数。

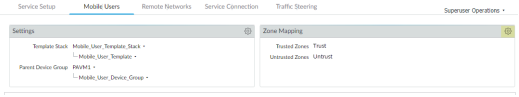
   完成后，您将拥有两个安全策略，一个策略用于可信区到可信区流量，另一个策略用于可信区到不可信区流量。



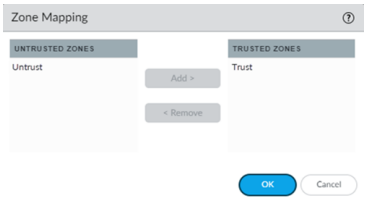
 ©2025 Palo Alto Networks, Inc.

STEP 5 | 根据部署需要，为远程网络、移动用户或两者定义服务区映射。

1. 为远程网络、移动用户或两者设置服务区映射。
   - 对于移动用户，选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Mobile Users**（移动用户）。
   - 对于远程网络，选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Remote Networks**（远程网络）。
2. 单击 **Zone Mapping**（服务区映射）旁边的齿轮图标以编辑设置。



3. 为您的部署设置 **Zone Mapping**（服务区映射），将可信区流量移动到 **Trusted Zones**（可信区），将不可信区流量移动到 **Untrusted Zones**（不可信区）；然后，单击 **OK**（确定）。



在 Prisma Access 中配置流量导向

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证 ❑ 将证书吊销列表 (CRL) 和在线证书状态协议 (OCSP) 直接发送到互联网的功能至少需要Prisma Access 版本 5.1.1。

流量导向允许您配置 Prisma Access 以创建流量导向规则，从而指定来自移动用户和远程网络连接的互联网绑定流量的流向目标。您可以指定在发送到互联网之前将流量重定向到服务连接，也可以指定将流量直接传出到互联网。完成以下步骤，为 Prisma Access 部署配置流量导向。

- Strata Cloud Manager
- Panorama

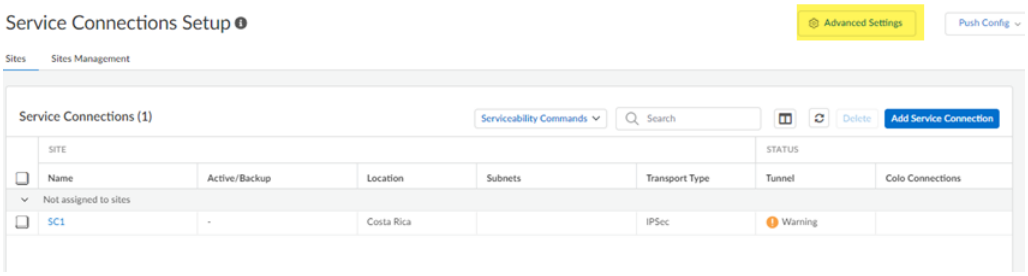
在 Prisma Access 中配置流量导向 (Strata Cloud Manager)

在 Prisma Access 部署中，服务连接提供对内部网络资源的访问，例如总部或数据中心的身份验证服务和私有应用程序。服务连接会处理内部流量，无需互联网访问。在某些情况下，您可能希望将互联网绑定流量重定向到数据中心。流量导向允许您将移动用户或远程网络流量重定向到服务连接，然后再发送到互联网。完成以下步骤，为 Prisma Access 部署配置流量导向。

STEP 1 | 根据您的部署情况，加入服务连接、移动用户和远程网络。

 ©2025 Palo Alto Networks, Inc.

STEP 2 | 转到 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Service Connections**（服务连接） > **Advanced Settings**（高级设置）。



STEP 3 | 配置 **Traffic Steering**（流量导向）规则。

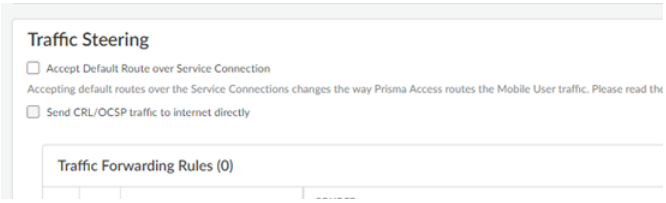
1. （可选，仅限移动用户部署）通过单击齿轮图标打开“设置”，然后选择 **Accept Default Route over Service Connections**（接受通过服务连接通告的默认路由），允许 Prisma Access 接受并安装 CPE 通过一个或多个服务连接通告的默认路由。

   默认路由具有您在使用时必须遵循的准则；例如，默认路由仅支持移动用户部署，并且对远程网络部署不起作用。通过流量导向实施默认路由之前，请务必查看这些准则。

STEP 4 | （可选）通过选择 **Send CRL/OCSP traffic to internet directly**（直接向互联网发送 **CRL/OCSP** 流量），允许 Prisma Access 将证书吊销列表 (CRL) 和在线证书状态协议 (OCSP) 流量直接发送到互联网。

如果公共互联网中有 OCSP 或 CRP 服务器，并且您想要使用非可信区将该流量直接发送到互联网，请选择此选项。如果不选择此选项，Prisma Access 会将该流量发送到服务连接。

在选择 ***Send CRL/OCSP traffic to internet directly***（直接向互联网发送 ***CRL/OCSP*** 流量）之前，请确保将 *Prisma Access* 部署至少升级到版本 *5.1.1*。



 ©2025 Palo Alto Networks, Inc.

STEP 5 | 为您创建的目标创建规则，并将这些规则应用于该目标。

1. **Add Rule**（添加规则）。
2. 为该规则输入唯一的 **Name**（名称）。
3. 在 **Source**（源）区域中：
   - 指定要匹配的用户列表。

     您可以 **Match Any User**（匹配任何用户），**Match Pre-logon**（匹配预登录用户），**Match known-user**（匹配已知用户），**Match unknown**（匹配未知用户），或者 **Add Users**（添加用户）并选择要匹配的一名或多名用户。
   - 选择 **Source Address Entities**（源地址实体）。您可以选择以下一个或多个对象：
     - IP 地址
     - 地址组
     - 使用 IP 地址或 URL 的外部动态列表 (EDL)
4. 在 **Destination**（目标）区域中，指定以下 **Destination Address Entities**（目标地址实体）之一，或选择 **Any**（任意）以通过“URL 类别”字段中的规则处理流量：
   - IP 地址
   - 地址组
   - 使用 IP 地址或 URL 的外部动态列表 (EDL)
5. 指定 **URL Category**（**URL** 类别）。

   如果创建自定义 URL 类别，请输入全部小写的 URL。流量导向支持自定义 URL 和预定义 URL 类别。您可以在 URL 类别中的 URL 中使用通配符。支持以下通配符格式：
   - *.example.com
   - *.fqdn.example.com

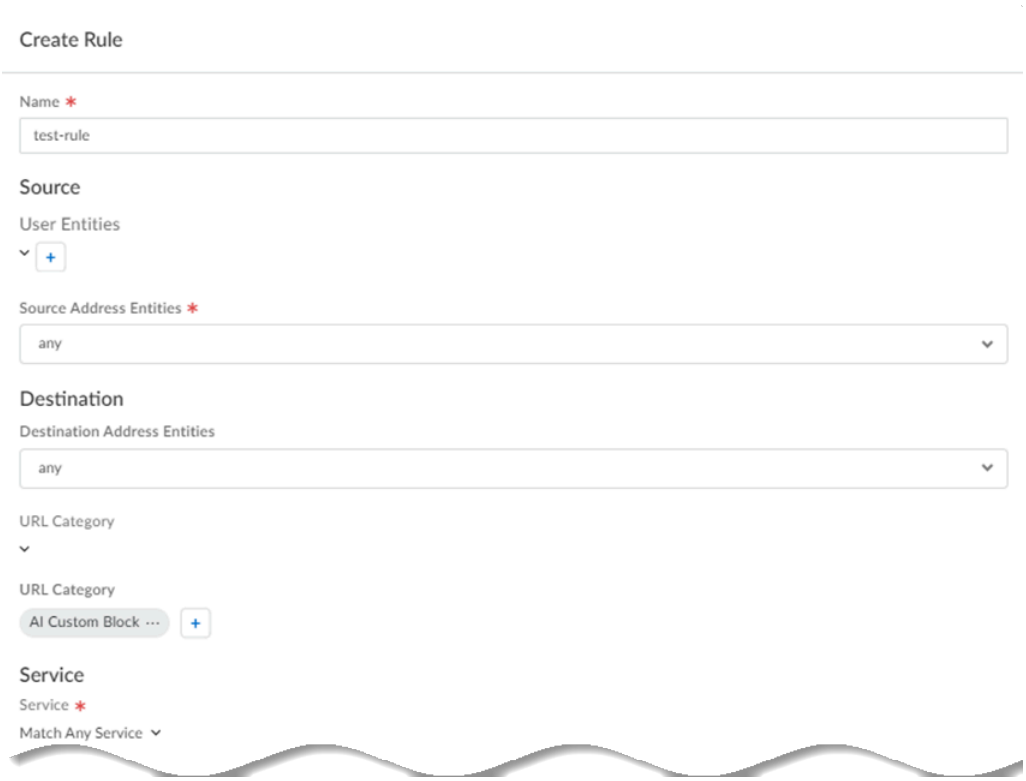
   不支持以下格式：
   - *
   - *.*
   - *example.com
   - example.com/（用于流量导向的 URL 类别不支持 URL 中的尾部斜杠）
   - example.com/path（仅支持域名）
   - *fqdn.example.com
   - fqdn.example.*

   配置目标选项时，请遵循以下准则：
   - 如果指定 URL 类别，Prisma Access 仅匹配 HTTP 和 HTTPS 流量，即使服务设置为 **Any**（任意）也是如此。
   - 请勿创建类型为 **Category Match**（类别匹配）的自定义 URL 类别。

   请勿创建名称为 **Custom_URL_Category_TFR** 的自定义 URL 类别。
6. 指定 **Service**（服务）类型并 **Add Service**（添加服务）。

 ©2025 Palo Alto Networks, Inc.

指定 **service-http** 以转发 HTTP 流量，指定 **service-https** 以指定 HTTPS 流量。选择 **Match Any Service**（匹配任何服务），以转发任何服务类型的流量。



7. 创建服务连接组并指定 **Action**（操作）。
   1. **Create New**（新建）或 **Manage**（管理）组，或为其指定唯一的 **Name**（名称）。
   2. 指定要用于该目标的 **Service Connection**（服务连接）。

      Palo Alto Networks 不建议在流量导向规则提及的目标服务连接组中使用多个服务连接（无论是专用连接还是非专用连接）。此外，给定的服务连接只能存在于一个目标中，并且您不能将单个服务连接添加到两个不同的目标。
   3. （可选）可以使用专用服务连接将流量引导至非本地部署且不需要参与路由的安全堆栈或云。要将您要使用的服务连接设置为专用服务连接，请选择 **Dedicated for Traffic Steering Only**（仅用于流量导向）。

      专用服务连接会更改其服务区，并被标记为安全策略规则的非可信区。

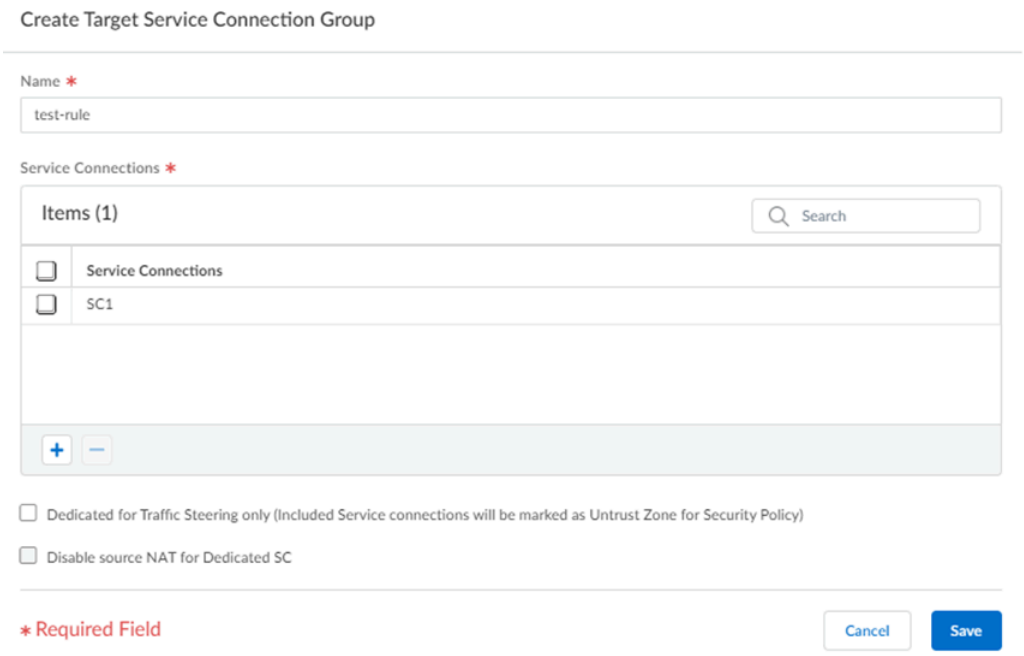
      如果您要通过服务连接发送与正常服务连接相关的流量和流量导向流量，请取消选择 **Dedicated for Traffic Steering Only**（仅用于流量导向）；选择此选项后，该服务连接的服务区仍为可信区。
   4. 要禁用专用服务连接的源 NAT，请选择 **Disable Source NAT for Dedicated SC**（禁用专用 **SC** 的源 **NAT**）。默认情况下启用源 NAT（取消选中该复选框）。

      如果禁用源 NAT，Prisma Access 会使用组织的源 IP 地址进行专用服务连接。如果启用源 NAT，Prisma Access 会将服务连接的 **EBGP Router**（**EBGP** 路由器）地址（**Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络

 ©2025 Palo Alto Networks, Inc.

详细信息） > **Service Connection**（服务连接） > **EBGP Router**（**EBGP** 路由器））用作源 IP 地址，即使流量从专用服务连接传出后也是如此。

5. **Save**（保存）更改。



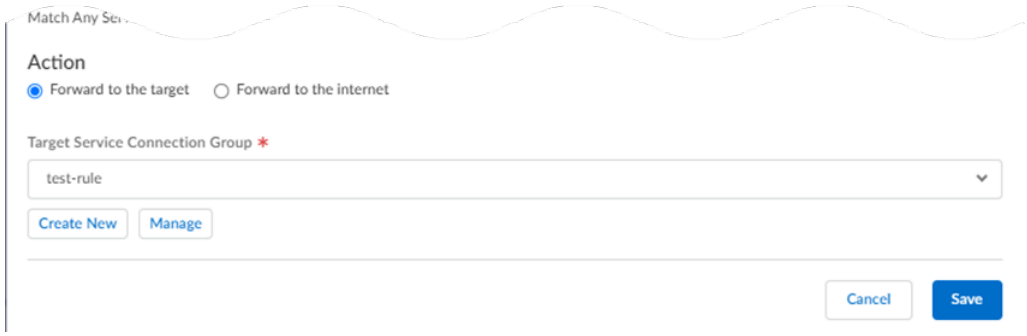
8. 将流量转发到指定的服务连接目标，或将流量直接发送到互联网而无需通过服务连接发送。

   - 要让 Prisma Access 将流量转发到服务连接目标，请选择 **Forward to the target**（转发到目标）；然后选择 **Target Service Connection Group**（目标服务连接组）。

     如果您由于 SaaS 应用程序允许列表限制而需要将流量发送到现有或旧版环境，或者您想要创建流量流以将指定的互联网流量引导回本地网络，请指定此选项。

   - 要让 Prisma Access 将流量直接转发到互联网而不是先发送到服务连接，请选择 **Forward to the internet**（转发到互联网）。

     如果要将默认路由发送到 Prisma Access 并且您想将一些流量直接引导至互联网，请指定此选项。



STEP 6 | 选择 **Push Config**（推送配置）以保存更改。

©2025 Palo Alto Networks, Inc.

在 **Prisma Access** 中配置流量导向 **(Panorama)**

STEP 1 | 根据您的部署情况，加入服务连接、移动用户和远程网络。

STEP 2 | 选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Traffic Steering**（流量导向）。

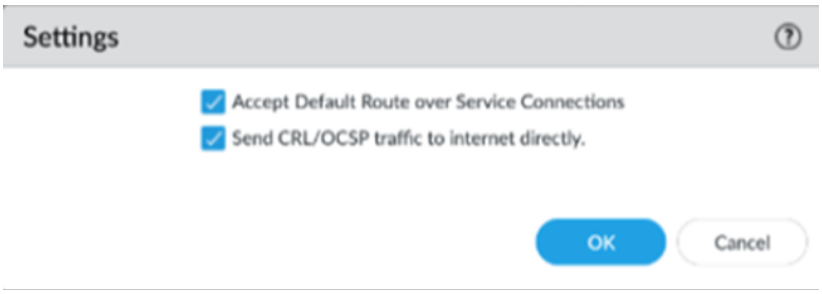
STEP 3 | （可选，仅限移动用户部署）通过单击齿轮图标打开“设置”，然后选择 **Accept Default Route over Service Connections**（接受通过服务连接通告的默认路由），允许 Prisma Access 接受并安装 CPE 通过一个或多个服务连接通告的默认路由。

默认路由具有您在使用时必须遵循的准则；例如，默认路由仅支持移动用户部署，并且对远程网络部署不起作用。通过流量导向实施默认路由之前，请务必查看这些准则。

STEP 4 | （可选）通过选择 **Send CRL/OCSP traffic to internet directly**（直接向互联网发送 **CRL/OCSP** 流量），允许 Prisma Access 将证书吊销列表 (CRL) 和在线证书状态协议 (OCSP) 流量直接发送到互联网。

如果公共互联网中有 OCSP 或 CRP 服务器，并且您想要使用非可信区将该流量直接发送到互联网，请选择此选项。如果不选择此选项，Prisma Access 会将该流量发送到服务连接。

在选择 ***Send CRL/OCSP traffic to internet directly***（直接向互联网发送 ***CRL/OCSP*** 流量）之前，请确保将 *Prisma Access* 部署至少升级到版本 *5.1.1*。



 ©2025 Palo Alto Networks, Inc.

STEP 5 | （可选）创建目标组并为其分配服务连接。

1. 在 **Target Service Connections for Traffic Steering**（流量导向的目标服务连接）区域中，**Add**（添加）一个组并为其指定 **Group Name**（组名称）。
2. 为流量 **Add**（添加）**Target**（目标），指定要用于该目标的 **Service Connection**（服务连接）；然后单击 **OK**（确定）。

   Palo Alto Networks 不建议在流量导向规则提及的目标服务连接组中使用多个服务连接（无论是专用连接还是非专用连接）。此外，给定的服务连接只能存在于一个目标中，并且您不能将单个服务连接添加到两个不同的目标。
3. 选择是否将与此目标关联的服务连接设为专用服务连接。
   - 可以使用专用服务连接将流量引导至非本地部署且不需要参与路由的安全堆栈或云。要将您要使用的服务连接设置为专用服务连接，请选择 **Dedicated for Traffic Steering Only**（仅用于流量导向）。

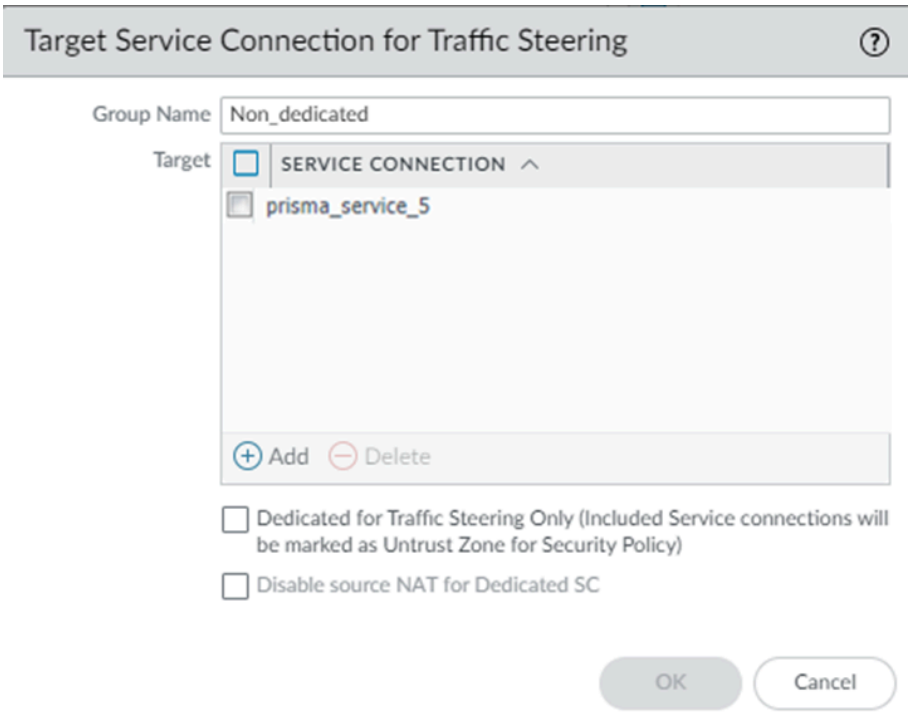
     专用服务连接会更改其服务区。
   - 如果您要通过服务连接发送与正常服务连接相关的流量和流量导向流量，请取消选择 **Dedicated for Traffic Steering Only**（仅用于流量导向）；选择此选项后，该服务连接的服务区仍为可信区。
4. 选择是启用还是禁用源 NAT。

   要禁用专用服务连接的源 NAT，请选择 **Disable Source NAT for Dedicated SC**（禁用专用 **SC** 的源 **NAT**）。默认情况下启用源 NAT（取消选中该复选框）。

   如果禁用源 NAT，Prisma Access 会使用组织的源 IP 地址进行专用服务连接。如果启用源 NAT，Prisma Access 会将服务连接的 **EBGP Router**（**EBGP** 路由器）地址（**Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详

 ©2025 Palo Alto Networks, Inc.

细信息） > **Service Connection**（服务连接） > **EBGP Router**（**EBGP** 路由器））用作源 IP 地址，即使流量从专用服务连接传出后也是如此。



 ©2025 Palo Alto Networks, Inc.

STEP 6 | 为您创建的目标创建规则，并将这些规则应用于该目标。

1. 在 **Traffic Steering Rules**（流量导向规则）区域中，**Add**（添加）流量导向规则。
2. 在 **General**（常规）选项卡中，指定流量导向规则的 **Name**（名称）。
3. 在 **Source**（源）选项卡中，指定源流量的规则。
   - 在 **Source Address**（源地址）字段中，指定以下一个或多个对象，或选择 **Any**（任意）以使来自任何源的流量流向此目标：
     - IP 地址
     - 您在 Panorama 中创建的地址对象（**Objects**（对象） > **Addresses**（地址））
     - 动态地址组 (DAG)
     - 使用 IP 地址或 URL 的外部动态列表 (EDL)
   - 在 **Source User**（源用户）字段中，指定源用户流量的规则。您可以指定以下用户信息：
     - 用户

       以域名/用户或用户@域名 的格式输入用户。
     - 用户组

       输入用户组时使用完整的专有名称 (DN)。
     - 在 Panorama 上配置的用户（**Device**（设备） > **Local User Database**（本地用户数据库） > **Users**（用户））
     - 在 Panorama 上配置的用户组（**Device**（设备） > **Local User Database**（本地用户数据库） > **User Groups**（用户组））

   如果使用地址对象、DAG、EDL、用户或用户组，请将其指定为 **Shared**（共享），以便与 Prisma Access 中的所有设备组共享。此外，不要在地址对象、DAG 或 EDL 中输入 0.0.0.0/0；而是直接在规则中输入 0.0.0.0/0。

   Prisma Access 仅自动填充移动用户设备组中的用户。
4. 在 **Destination**（目标）选项卡中，指定以下值：
   - 在 **Destination**（目标）区域中，指定以下条件之一，或选择 **Any**（任意）以通过 **URL Category**（**URL** 类别）字段中的规则处理流量：
     - IP 地址或前缀
     - 您在 Panorama 中创建的地址对象（**Objects**（对象） > **Addresses**（地址））
     - 动态地址组 (DAG)
     - 基于 IP 地址的外部动态列表 (EDL)

       请勿在地址对象、*DAG* 或 *EDL* 中输入 *0.0.0.0/0*；而是直接在规则中输入 *0.0.0.0/0*。

     将 **Any**（任意）保持选中状态，以传递通过 **URL Category**（**URL** 类别）区域中的规则处理的所有流量。如果您在 **Destination**（目标）和 **URL Category**（**URL** 类别）区域中指定规则，Prisma Access 会首先处理 **Destination**（目标）类别中的规则。

 ©2025 Palo Alto Networks, Inc.

- 在 **URL Category**（**URL** 类别）字段中，输入自定义 URL 类别（**Objects**（对象） > **Custom Objects**（自定义对象） > **URL Category**（**URL** 类别））创建自定义 URL 类别时，请输入全部小写的 URL。流量导向支持自定义 URL 和预定义 URL 类别。

  可以在 URL 类别中的 URL 中使用通配符。支持以下通配符格式：

  - *.example.com
  - *.fqdn.example.com

  不支持以下格式：

  - *
  - *.*
  - *example.com
  - example.com/（用于流量导向的 URL 类别不支持 URL 中的尾部斜杠）
  - example.com/*path*（仅支持域名）
  - *fqdn.example.com
  - fqdn.example.*

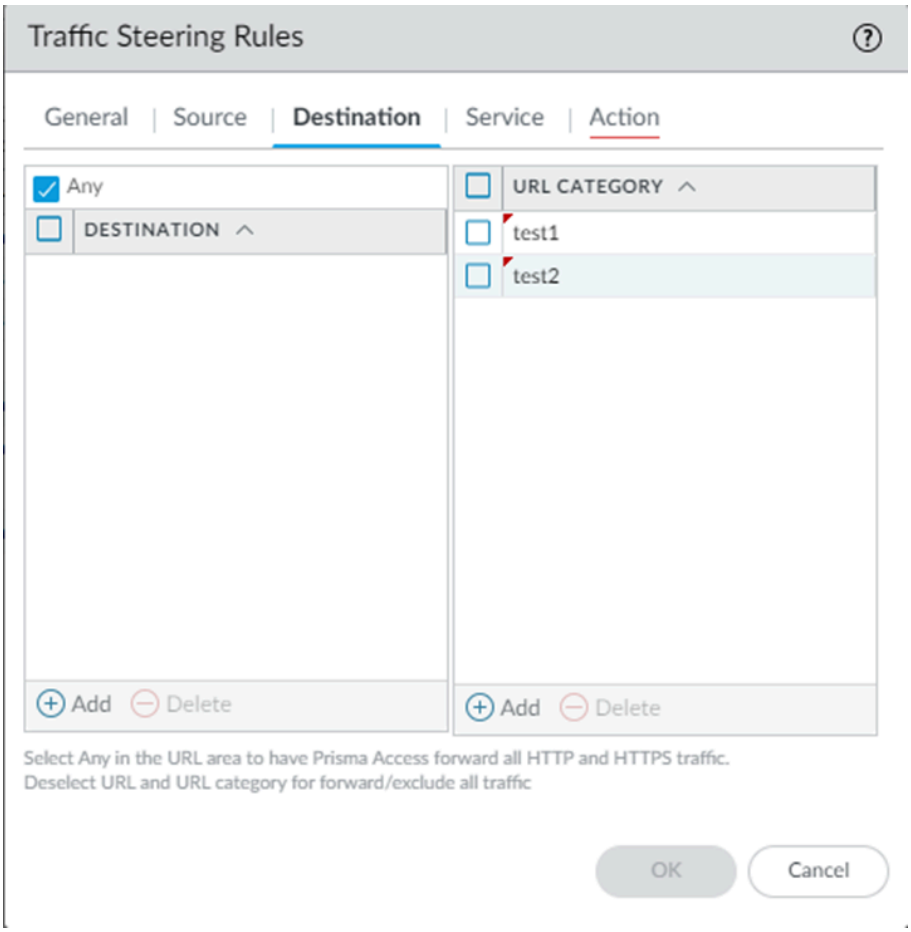
  自定义 URL 类别中的 URL 使用与新一代防火墙相同的 URL 模式匹配。

配置目标选项时，请遵循以下准则：

- 如果指定 URL 类别，Prisma Access 仅匹配 HTTP 和 HTTPS 流量，即使服务设置为“任意”也是如此。
- 请勿创建类型为 **Category Match**（类别匹配）的自定义 URL 类别。
- 请勿创建名称为 **Custom_URL_Category_TFR** 的自定义 URL 类别，因为对于从 Prisma Access 1.7 迁移到 2.0 的部署，在 URL 区域中输入的 URL 从 1.7 迁移到名称

 ©2025 Palo Alto Networks, Inc.

为 **Custom_URL_Category_TFR***number* 的自定义 URL 类别，其中 *number* 是附加到自定义 URL 类别的数字。



5. 在 **Service**（服务）选项卡中，指定服务类型。

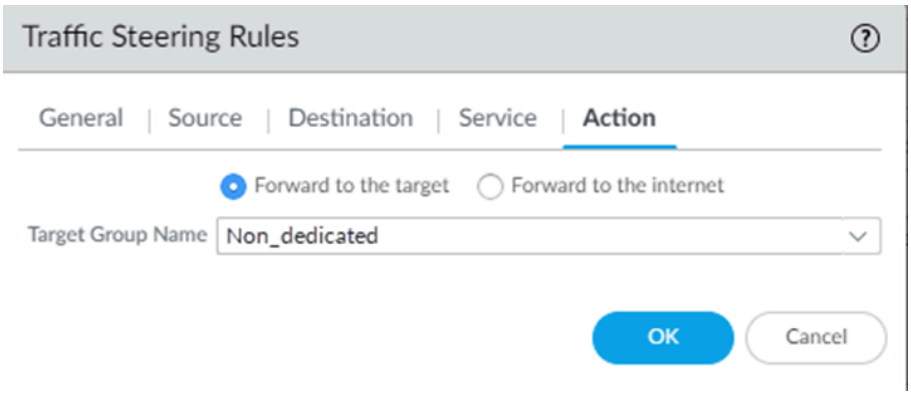
   指定 **service-http** 以转发 HTTP 流量，指定 **service-https** 以指定 HTTPS 流量。选择 **Any**（任意）可转发任意服务类型的流量。

6. 在 **Action**（操作）选项卡中，选择要应用于流量导向规则的 **Target Group Name**（目标组名称）。

7. 将流量转发到指定的服务连接目标，或将流量直接发送到互联网而无需通过服务连接发送。

   - 要让 Prisma Access 将流量转发到服务连接目标，请选择 **Forward to the target**（转发到目标）；然后选择 **Target Group Name**（目标组名称）。
   - 要让 Prisma Access 将流量直接转发到互联网而不是先发送到服务连接，请选择 **Forward to the internet**（转发到互联网）。

©2025 Palo Alto Networks, Inc.



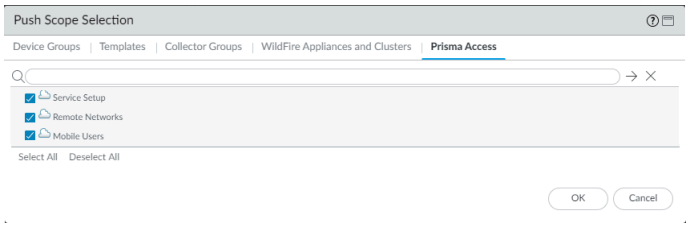
8. 单击 **OK**（确定）保存更改。

STEP 7 | 可选 指定额外的流量导向规则。

Prisma Access 按照创建的顺序（从上到下）处理多个规则。

STEP 8 | 提交并推送更改，以使其在 Prisma Access 中生效。

1. 选择 **Commit**（提交） > **Commit and Push**（提交并推送）和推送范围中的 **Edit Selections**（编辑选择）。
2. 选择 **Prisma Access**，然后选择 **Service Setup**（服务设置）、**Remote Networks**（远程网络）和 **Mobile Users**（移动用户）。



3. 单击 **OK**（确定）保存对推送范围所作的更改。
4. **Commit**（提交）并 **Push**（推送）更改。

服务连接流量的路由

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

Prisma Access 使用 BGP 进行动态路由，并使用 BGP 路径选择在路由表中安装路由。当 Prisma Access 使用服务连接将流量路由到您的总部或数据中心时，它使用能够有效引导流量的路由方法。Prisma Access 使用默认路由模型，该模型旨在适应大多数网络部署；但是，并非所有组织的网络都是一样的。为了适应更广泛的部署，Prisma Access 允许您选择另一种模式进行服务连接路由。

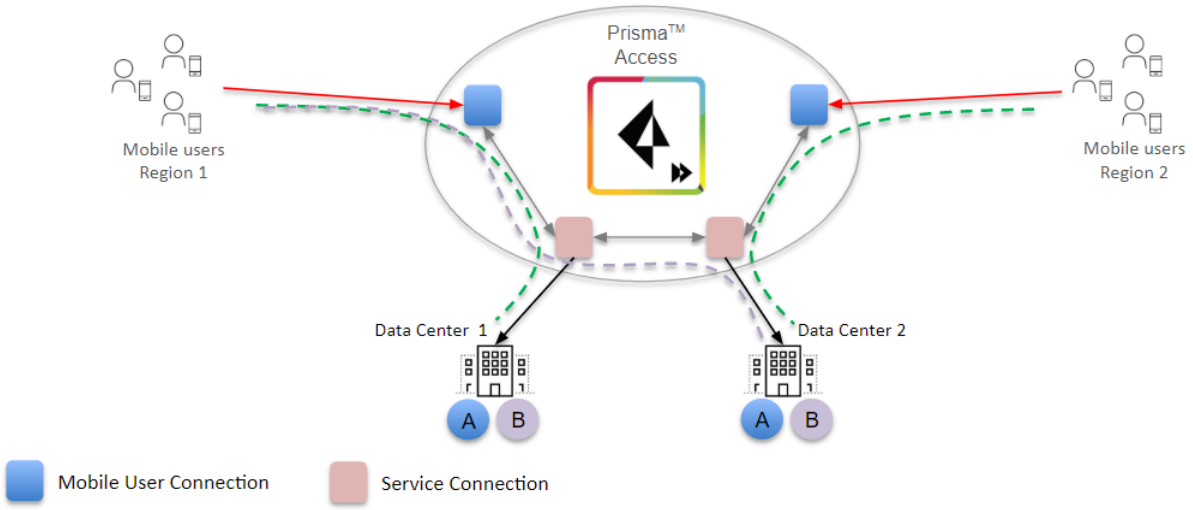
 ©2025 Palo Alto Networks, Inc.

要更改 *Prisma Access* 服务连接路由方法，需要彻底了解组织的拓扑和路由设备，同时了解 *Prisma Access* 的工作原理，如本节所述。从默认设置更改路由方法之前，请仔细阅读本节。

Prisma Access 支持静态路由和使用BGP进行服务连接和远程网络连接的动态路由。当您对连接使用 BGP 路由时，您的组织网络会从 Prisma Access 获取 BGP 信息。

在决定使用哪种服务连接路由之前，您应该了解 Prisma Access 如何在移动用户、远程网络和服务连接之间路由流量，因为移动用户流量使用的路由和服务连接之间的远程网络流量使用的路由是不同的。

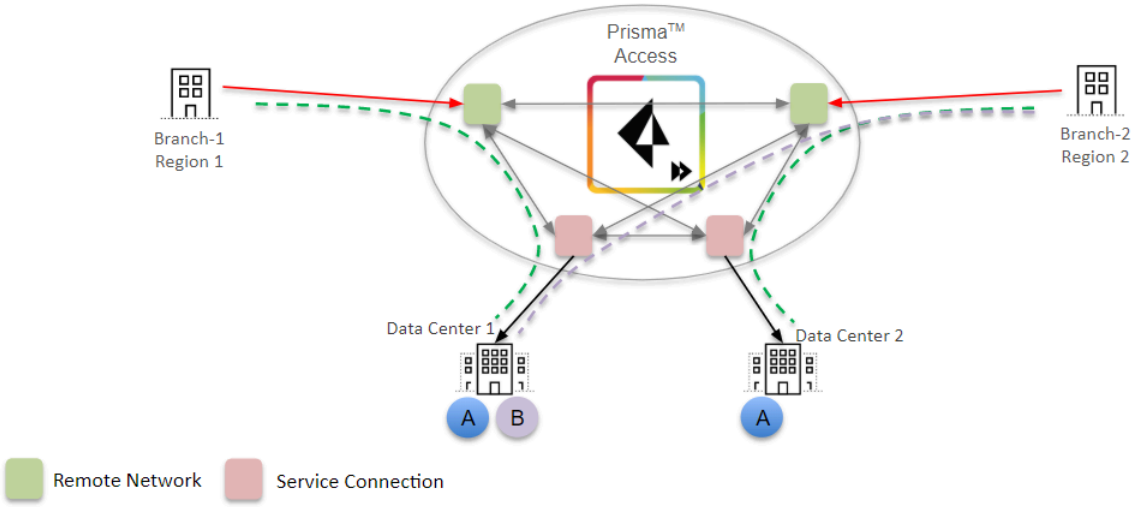
移动用户-服务连接路由 — 移动用户连接与最近的服务连接形成 IPSec 隧道。Prisma Access 使用 iBGP 进行内部路由，使用 eBGP 与数据中心的客户本地设备对等。下图显示了区域 1 和 2 中的移动用户被路由到该区域的相应服务连接。区域 1 中的移动用户正在访问位于数据中心 1 的应用程序 **A** 和 **B**。如果您组织的网络在其服务连接中使用 BGP 路由，并且数据中心 1 的一个服务连接出现了 ISP 故障，Prisma Access 会检测到该故障，并在 BGP 融合后将应用程序 **A** 和应用程序 **B** 的流量路由到数据中心 2，从而为您网络的数据中心提供冗余保障。



当 *Prisma Access* 检测到故障时，会对 *BGP* 使用以下计时：如果您配置了 *BGP* 路由并启用了隧道监视，则确定安全参数索引 *(SPI)* 失败的最短默认保持时间是使用隧道监视器，当它检测到连续 *15* 秒的隧道失败时，将删除指向对等设备的所有路由。通过这种方式，隧道监控器确定 *BGP* 路由的行为。如果未配置隧道监控，保持计时器将确定在删除路由之前隧道关闭的时间。*Prisma Access* 使用 *RFC 4271* 定义的默认 *BGP HoldTime* 值 *90* 秒，这是 *Prisma Access* 删除非活动 *SPI* 的路由之前的最长等待时间。如果对等 *BGP* 设备的配置保持时间较短，*BGP* 保持计时器将使用较低的值。成功安装辅助隧道后，辅助路由将优先使用，直到主隧道恢复。如果主路由和辅助路由都已启动，则主路由优先。

远程网络服务连接路由—Prisma Access与其他远程网络和服务连接构建了一个全互联网络。与移动用户一样，Prisma Access 使用 iBGP 进行内部路由，使用 eBGP 与客户本地设备建立对等连接，以交换路由。如果分支机构 1 中的一名用户正在访问您组织数据中心中数据中心 1 的应用程序 **A**，且分支机构 1 与数据中心 1 之间的链路中断，那么在 BGP 融合后，Prisma Access 会将应用程序 **A** 的流量路由到数据中心 2。

 ©2025 Palo Alto Networks, Inc.



在了解 Prisma Access 服务连接路由及其与网络的关系后，您可以选择以下服务连接的路由模式之一：

- 默认路由 — 这是 Prisma Access 使用的默认路由模型。

  如果您希望 Prisma Access 使用 BGP 最佳路径选择机制而不调整任何 BGP 属性，请使用此路由模式。在此模式下，Prisma Access 将遵从客户本地设备 (CPE) 发布的任何属性。
- 热土豆路由 — Prisma Access 以最快的速度将流量切换到您组织的网络。

  如果您希望组织的网络执行大多数路由决策，请使用此路由方法。

Prisma Access 默认路由

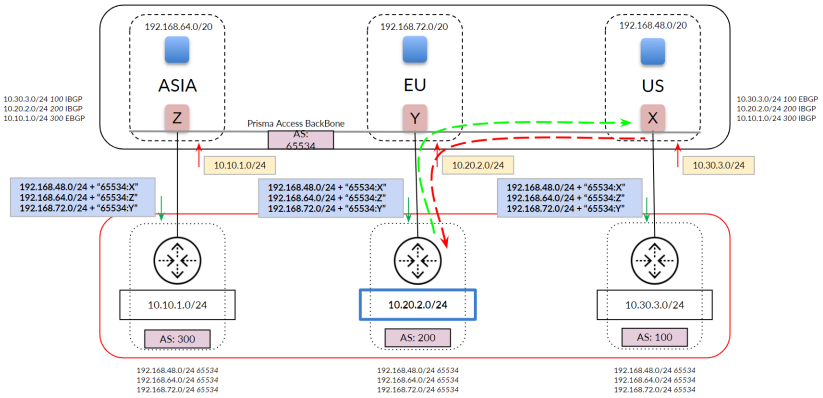
下图展示了在默认路由模式下，Prisma Access 对服务连接流量进行路由的一个示例。该组织的网络在三个数据中心有三个独立的网络，并且没有连接网络的主干网。在默认路由模式下，移动用户池在三个网络上平等地进行通告，如下图所示。

请注意，当 Prisma Access 通告移动用户路由时，它会在通告之前将子网划分为 C 类 /24 地址块；因此，当网关使用这些前缀时，它会以 /24 为单位分块通告 /20 移动用户子网。

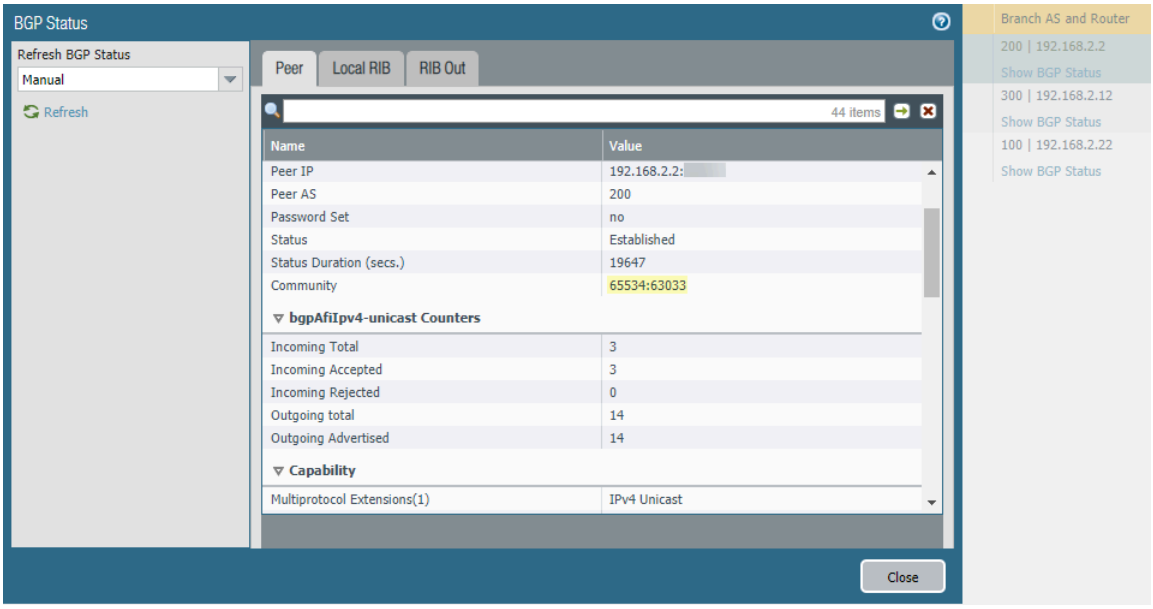
记下 Prisma Access 如何使用 BGP 路由通告：

- Prisma Access 不调整移动用户通告路由的默认 BGP 属性（Prisma Access 将其 AS 编号添加到路由通告中）。
- Prisma Access 以 /24 子网块为单位通告移动用户路由，并在通过服务连接所通告的路由中添加 BGP 社区值。下图显示了具有三个服务连接和为移动用户 IP 地址池指定的三个不同 IP 地址块的移动用户部署：`192.168.64.0/20` 用于亚洲、澳大利亚和日本地区，`192.168.72.0/20` 用于非洲、欧洲和中东地区，`192.168.48.0/20` 用于 **N**北美和南美地区。Prisma Access 将这些路由划分为 /24 块，并使用 **65534** 的 AS 编号通告这些路由，但还将 BGP 社区值附加到通告中（**Z** 代表亚洲，**Y** 代表欧洲，**X** 代表美国）。这些路线显示在图中间。通过这种方式，您可以区分网络中的服务连接，即使 Prisma Access 为它们分配相同的 AS 编号。

 ©2025 Palo Alto Networks, Inc.



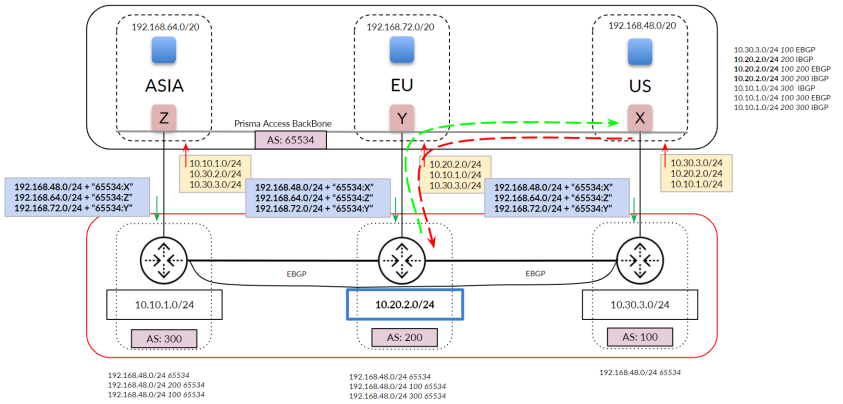
您可以选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息） > **Service Connection**（服务连接） > **Show BGP Status**（显式 **BGP** 状态），并在 **Peer**（对端设备）选项卡中找到 **Community**（社群）字段，从而查看社群字符串。



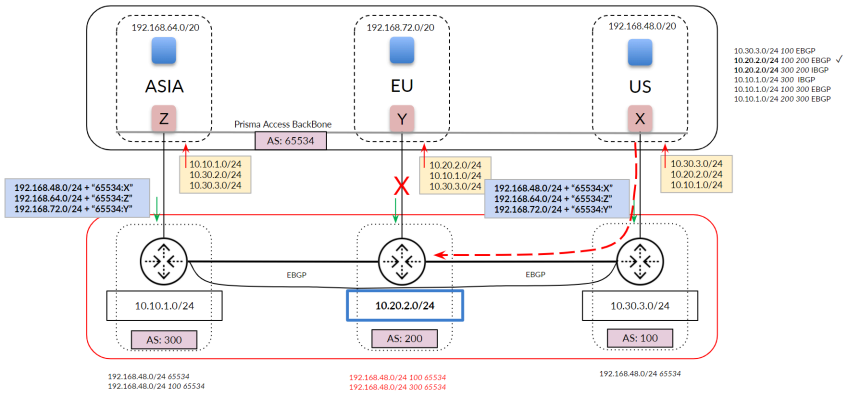
下图显示了具有全网状 eBGP 主干的更常见的网络。该图展示了 Prisma Access 从您所在组织的网络中学习到的路由信息（右上角）。请注意 Prisma Access 通过 Prisma Access 骨干网 (iBGP) 和您组织的骨干网 (eBGP) 学习到的额外路由。

对于北美和南美地区（图中为美国）的移动用户与贵组织的非洲、欧洲和中东地区（图中为欧盟）的数据中心之间的流量，Prisma Access 选择了通过欧盟服务连接的路径，因为它更倾向于 AS-PATH 更短的路由。

 ©2025 Palo Alto Networks, Inc.



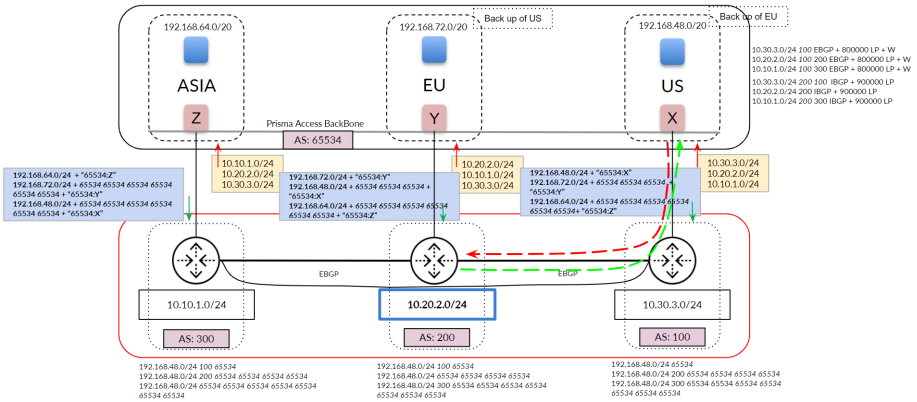
在具有全网状 eBGP 骨干网的部署中，以下情况可能会出现不对称：由于客户数据中心的 ISP/CPE 故障，Prisma Access 无法访问特定数据中心。下图显示了当欧盟服务链路中断时可能发生的情况。您的网络检测到链路故障并为 AS 200 建立新的路由表。从美国服务连接到 AS 200 的流量会经过 AS 100，这是因为 AS 200 和 AS 100 之间骨干网络的 eBGP 路由优先于欧盟和美国服务连接之间的 iBGP 路由。然而，返程流量并不一定会采用相同路径，因为 CPE 可以选择任意一条路径（图中以红色显示）来返回流量。



前面的示例展示了一个路由未进行聚合的网络（也就是说，在向 Prisma Access 发送 BGP 路由通告之前，您尚未进行路由汇总）。以下示例显示的网络中，网络在发送到 Prisma Access 之前汇总其到 10.0.0.0/8 的路由。如果选择默认路由，此配置可能会导致非对称路由问题，因为 Prisma Access 无法通过汇总路由确定正确的返回路径。

如果您的 *Prisma Access* 部署有远程网络，*Palo Alto Networks* 不建议在服务连接上使用路由汇总。服务连接上的路由汇总仅适用于移动用户部署。

©2025 Palo Alto Networks, Inc.



如果对移动用户使用路由聚合，则强烈建议您启用热土豆路由而不是默认路由，在热土豆路由中，Prisma Access 会尽快将流量转交给组织的网络。此外，我们建议您为每个服务连接选择备份 **SC**（如以下部分所述），以使其具有确定性路由行为。

Prisma Access 热土豆路由

当您选择 **Hot Potato Routing**（热土豆路由）时，Prisma Access 系统会尽快将绑定到服务连接/数据中心的流量从其内部网络流出。

采用热土豆路由时，Prisma Access 会在从网关发送的 BGP 前缀通告中添加自治系统路径 (AS-PATH) 的信息。当这些前缀从服务连接通告到组织的本地 CPE 时，会执行这种前置操作。Prisma Access 会对 AS-PATH 进行前置处理，以便您的 CPE 能正确区分主隧道和备用隧道的优先级。这样一来，如果主隧道出现故障，您的 CPE 就会选择备用隧道作为备份。

如果您为备用（备份）BGP 对端指定了不同的 IP 地址，则 Prisma Access 会根据隧道类型添加更多前缀，如下表所示。

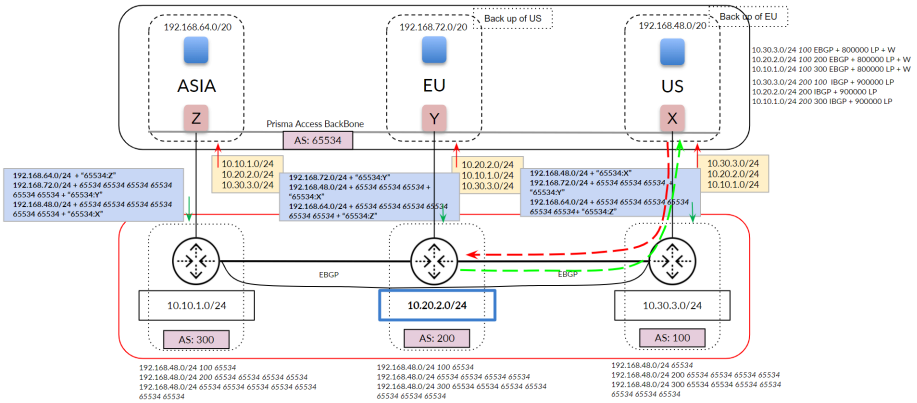
前缀类型	服务连接隧道类型	**AS-PATH** 前置的次数	在 **CPE** 上看到的 **AS-PATH** 总数
来自主服务连接的网关前缀	具有相同 BGP 对端 IP 地址的主隧道或备用隧道	0	1
来自备份服务连接的网关前缀	具有相同 BGP 对端 IP 地址的主隧道或备用隧道	3	4
来自所有其他服务连接的网关前缀	具有相同 BGP 对端 IP 地址的主隧道或备用隧道	6	7
来自主服务连接的网关前缀	具有不同 BGP 对端 IP 地址的备用隧道	1	2
来自备份服务连接的网关前缀	具有不同 BGP 对端 IP 地址的备用隧道	4	5

 ©2025 Palo Alto Networks, Inc.

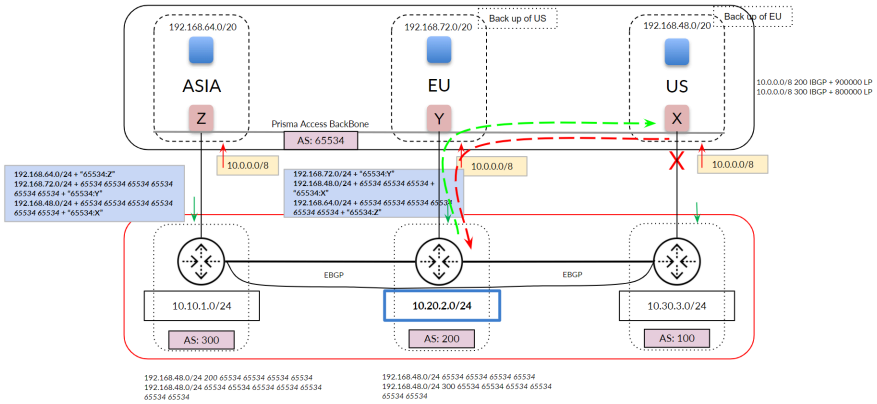
前缀类型	服务连接隧道类型	AS-PATH 前置的次数	在 CPE 上看到的 AS-PATH 总数
来自所有其他服务连接的网关前缀	具有不同 BGP 对端 IP 地址的备用隧道	7	8

在热土豆路由模式中，Prisma Access 允许您在接入过程中指定备份服务连接。指定备份服务连接会在服务连接链路出现故障时通知 Prisma Access 使用该服务连接作为备份。

下图展示了美国服务连接与 AS 200 之间流量的热土豆路由配置，其中欧盟服务连接被配置为美国连接的备份服务连接。使用热土豆路由时，Prisma Access 会通过美国服务连接从最近的出口路径发送流量。回程流量会采用沿着 AS100 的相同路径，因为对于位于美国地区的移动用户群而言，这条路径的 AS-PATH 更短。Prisma Access 会根据隧道是主隧道还是备份隧道，或者既非主隧道也非备份隧道的情况，在其前缀通告中前置 AS-PATH。

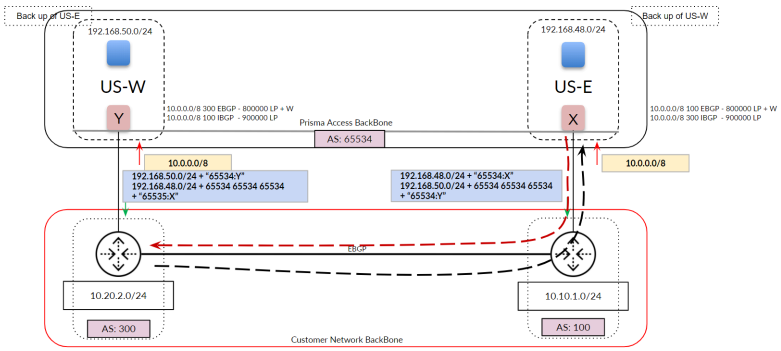


由于您已经设置了备份服务连接，因此，如果指向美国服务连接的链路中断，热土豆路由将使用通过欧盟服务连接的最短路径将流量发送出去。此路由方案也适用于使用路由聚合的网络。



还可以将备份服务连接用于单个区域中的多个服务连接。下图显示了在北美地区使用两个服务连接的 Prisma Access 部署。在这种情况下，可为美国西部 (US-W) 服务连接指定一个美国东部 (US-E) 作为 **Backup SC**（备份服务连接），反之亦然，以确保路由对称。

©2025 Palo Alto Networks, Inc.



配置路由首选项

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

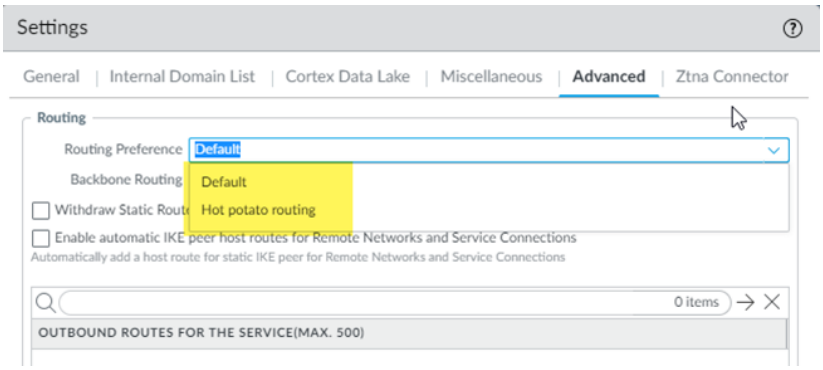
要启用路由首选项，请完成以下步骤。

要配置这些路由首选项，必须对服务连接使用 *BGP* 路由，而不是静态路由。

STEP 1 | 配置您的服务连接。

STEP 2 | （可选）选择用于服务连接的路由。

1. 在管理 Prisma Access 的 Panorama 中，转到 **Panorama** > **Cloud Services**云服务）> **Configuration**（配置） > **Service Setup**（服务设置），然后单击齿轮来编辑 **Settings**（设置）。
2. 在 **Advanced**（高级）设置中，选择您的 **Routing Preference**（路由首选项）（**Default**（默认）或 **Hot Potato**（热土豆））。

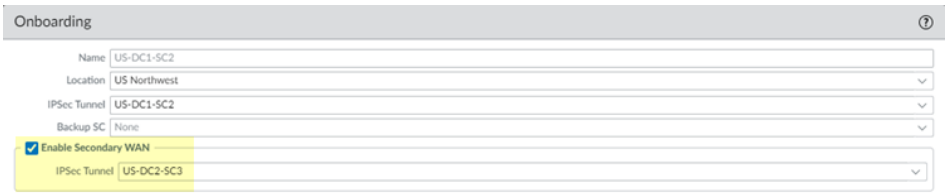


 ©2025 Palo Alto Networks, Inc.

STEP 3 | （可选，仅限热土豆路由部署）要指定在链路发生故障时使用的首选服务连接，请在配置服务连接时配置 **Backup SC**（备份 **SC**）。

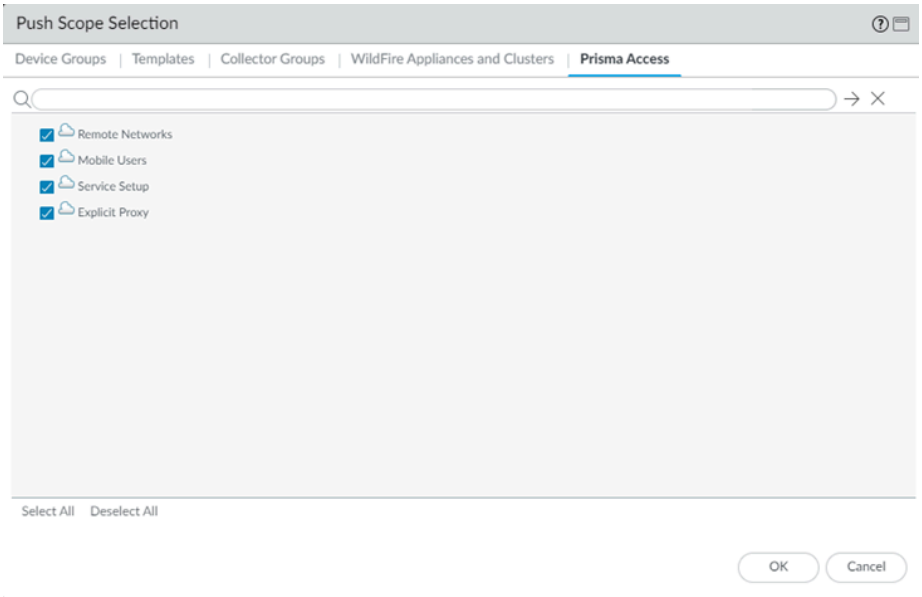
您可以选择已添加的任何服务连接。Prisma Access 使用您选择的 **Backup SC**（备份 **SC**）作为发生链路故障时的首选服务连接。选择备份服务连接后，可以防止在加入了两个以上的服务连接的情况下出现非对称路由问题。仅在热土豆路由模式下提供此选项。

1. 转到 **Panorama** > **Cloud Service**（云服务） > **Configuration**（配置） > **Service Connection**（服务连接）
2. 选择要配置的服务连接，或 **Add**（添加）新的服务连接。
3. 选择要用作首选备份的服务连接（**Backup SC**（备份 **SC**））。



STEP 4 | 将更改提交到 Panorama 并将配置更改推送到 Prisma Access。

1. 单击 **Commit**（提交） > **Commit and Push**（提交并推送）。
2. **Edit Selections**（编辑选择），在 Prisma Access 选项卡中，确保在 **Push Scope**（推送范围）中选择 **Service Setup**（服务设置），然后单击 **OK**（确定）。

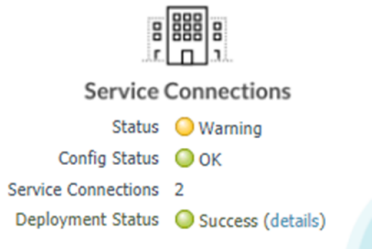


3. 单击 **Commit and Push**（提交并推送）。

 ©2025 Palo Alto Networks, Inc.

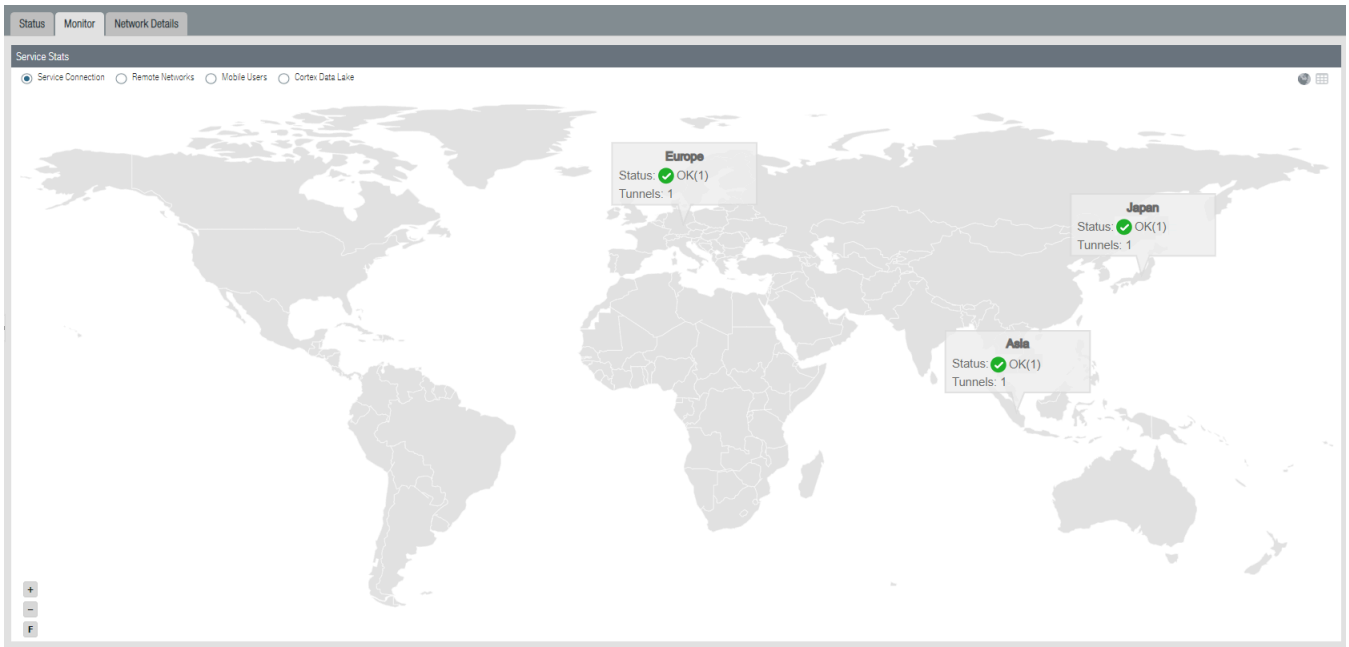
STEP 5 | 通过选择 **Panorama > Cloud Services**（云服务）**> Status**（状态）**> Status**（状态）并检查其状态是否显示 **OK**（正常），验证您的服务连接是否正常运行。

在 **Deployment Status**（部署状态）区域中，您可以在载入和部署作业完成前查看其进度，以及查看有关已完成作业的状态的更多信息。



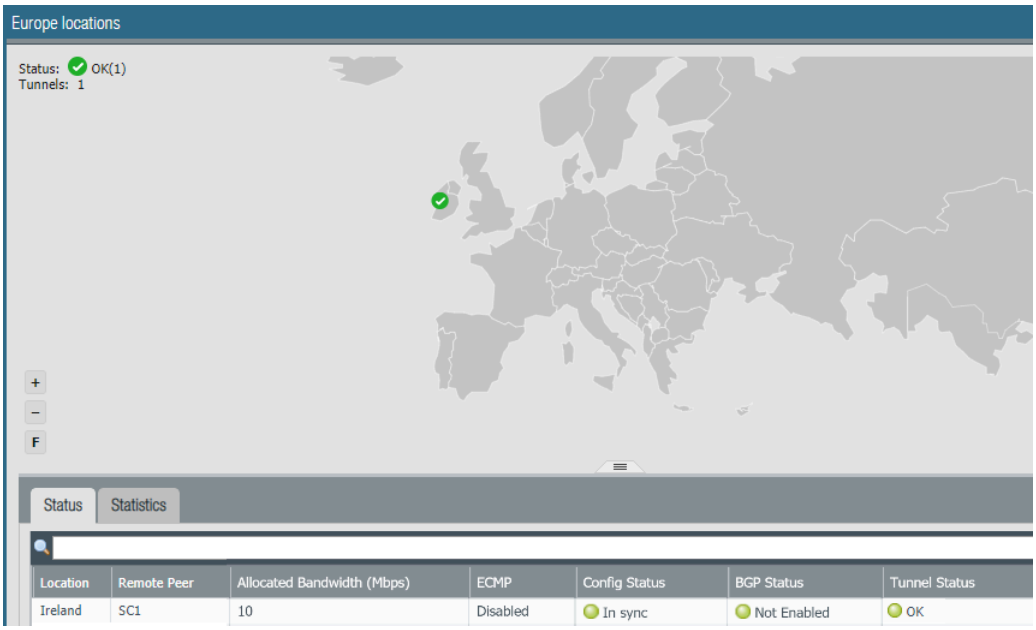
如果状态并非显示 **OK**（正常），请将鼠标悬停在状态图标上以查看任何错误。

要查看服务连接的图形表示以及状态详细信息，请在 **Monitor**（监控）选项卡上选择 **Service Connection**（服务连接）。



选择一个区域以获取该区域的更多详细信息。

 ©2025 Palo Alto Networks, Inc.



单击地图下方的选项卡，以查看有关服务连接的更多信息。

Status（状态）选项卡：

- **Location**（位置）— 部署服务连接的位置。
- **Remote Peer**（远程对等体）— 此服务基础架构设置 IPSec 隧道的公司位置。
- **Allocated Bandwidth**（分配的带宽）— 分配的服务连接数量乘以 300 Mbps。

  此数字不反映可用的服务连接带宽。

  虽然每个服务连接提供约 *1 Gbps* 的吞吐量，但实际吞吐量取决于多个因素，包括：

  - 流量组合（例如，帧大小）
  - 服务连接与总部位置或数据中心之间的延迟和数据包丢失
  - 服务提供商性能限制
  - 客户终端设备性能限制
  - 其他客户数据中心流量
- **ECMP** — 如果您为此服务连接配置了等价多路径 (ECMP)。由于 ECMP 不用于服务连接，因此此状态为 **Disabled**（禁用）。
- **Config Status**（配置状态）— 您上次推送到服务的配置的状态。如果本地配置和云端配置匹配，则配置状态为 **In sync**（同步）。如果您在本地进行了更改，但尚未将配置推送到云端，则显示状态 **Out of sync**（不同步）。将鼠标悬停在状态指示器上，以获取更多详细信息。提交配置并将其推送到 Prisma Access 后，配置状态更改为 **In sync**（同步）。
- **BGP Status**（**BGP** 状态）— 显示公司/总部位置的防火墙或路由器与建立服务连接的 Prisma Access 之间的 BGP 状态的相关信息。虽然您可能会暂时看到状态经历各种 BGP 状态

 ©2025 Palo Alto Networks, Inc.

（**Idle**（空闲）、**Active**（活跃）、**Open sendOpen** 消息发送）、**Open pend**（**Open** 消息待处理）、**Open confirm**（**Open** 消息确认），但最常见的情况是，BGP 状态显示：

- **Connect**（连接）— 数据中心/总部的路由器正在尝试与 Prisma Access 建立 BGP 对等体关系。

©2025 Palo Alto Networks, Inc.

- **Established**（已建立）— BGP 对等体关系已建立。

如果 BGP 连接处于错误状态，此字段还会显示：

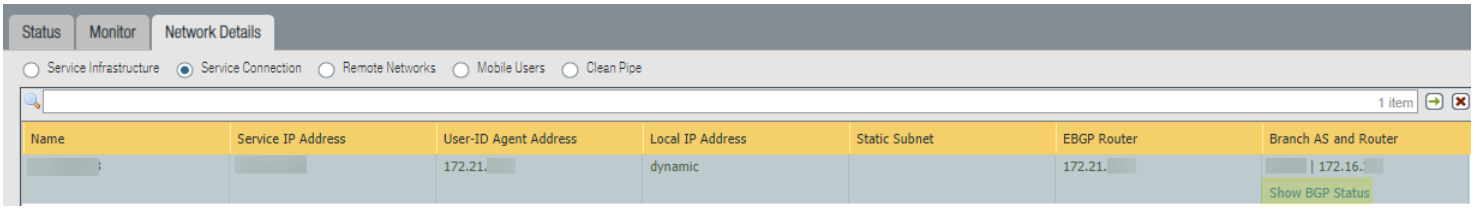
- 警告 — 超过八分钟没有 BGP 状态更新。这可能表示防火墙中断。
- **Error**（错误）— BGP 状态未知。

- **Tunnel Status**（隧道状态）— Prisma Access 与服务连接之间的连接的运行状态。

Statistics（统计信息）选项卡：

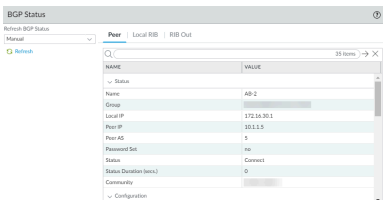
- **Location**（位置）— 部署服务连接的位置。
- **Remote Peer**（远程对等体）— 服务连接设置 IPSec 隧道的公司位置。
- **Ingress Bandwidth (Mbps)**（入口带宽 **(Mbps)**）— 从总部/数据中心位置流入 Prisma Access 的带宽。
- **Ingress Peak Bandwidth (Mbps)**（入口峰值带宽 **(Mbps)**）— 从总部/数据中心位置流入云服务的峰值负载。
- **Egress Bandwidth (Mbps)**（出口带宽 **(Mbps)**）— 从总部/数据中心位置流入 Prisma Access 的带宽。
- **Egress Peak Bandwidth (Mbps)**（出口峰值带宽 **(Mbps)**）— 从 Prisma Access 流入总部/数据中心位置的峰值负载。
- **QoS** — 选择此按钮可显示图形图表，其中显示实时和历史 QoS 统计信息，包括每个类的丢包数。此图表仅显示启用了 QoS 的服务连接或远程网络连接。

如果配置了 BGP，则可以通过选择 **Panorama** > **Cloud Services**（云服务）> **Status**（状态）> **Network Details**（网络详细信息）> **Service Connection**（服务连接）> **Show BGP Status**（显示 **BGP** 状态）来检查其状态。



此时显示 BGP 状态对话框。此表为您提供以下信息：

- **Peer**（对等体）— BGP 对等体的路由信息，包括状态、路由总数、配置以及运行时统计信息和计数器。在 **bgpAfiIpv4-unicast Counters**（**bgpAfiIpv4-unicast** 计数器）的 **Incoming Total**（传入总数）和 **Outgoing Total**（传出总数）字段中显示路由总数。



- **Local RIB**（本地 **RIB**）— Prisma Access 本地使用的 BGP 路由。Prisma Access 从 BGP RIB-In 表中选择此信息，该表存储相邻网络设备发送的信息，应用本地 BGP 导入策略和路由决策，并将本地 RIB 信息存储在路由信息库 (RIB) 中。

 ©2025 Palo Alto Networks, Inc.

请注意，仅显示前 256 个条目。要查看其他条目，请在“筛选器”字段中输入子网或 IP 地址，然后单击“应用筛选器”以查看路由条目的子集（最多显示 256 个）。



- **RIB Out**（**RIB** 传出）— Prisma Access 通过 BGP 更新消息向其对等体通告的路由信息。

使用多个服务连接创建高带宽网络

如果您的总部或数据中心位置需要额外的服务连接带宽，则可以配置到该位置的多个服务连接。

每个 Prisma Access 服务连接都没有带宽上限，但 Palo Alto Networks 预计每个服务连接可提供约 1 Gbps 的吞吐量。虽然此带宽通常足以访问总部或数据中心位置的内部资源，但您的部署可能需要额外的带宽；例如，如果您在数据中心托管内部或私有 SaaS 应用程序。

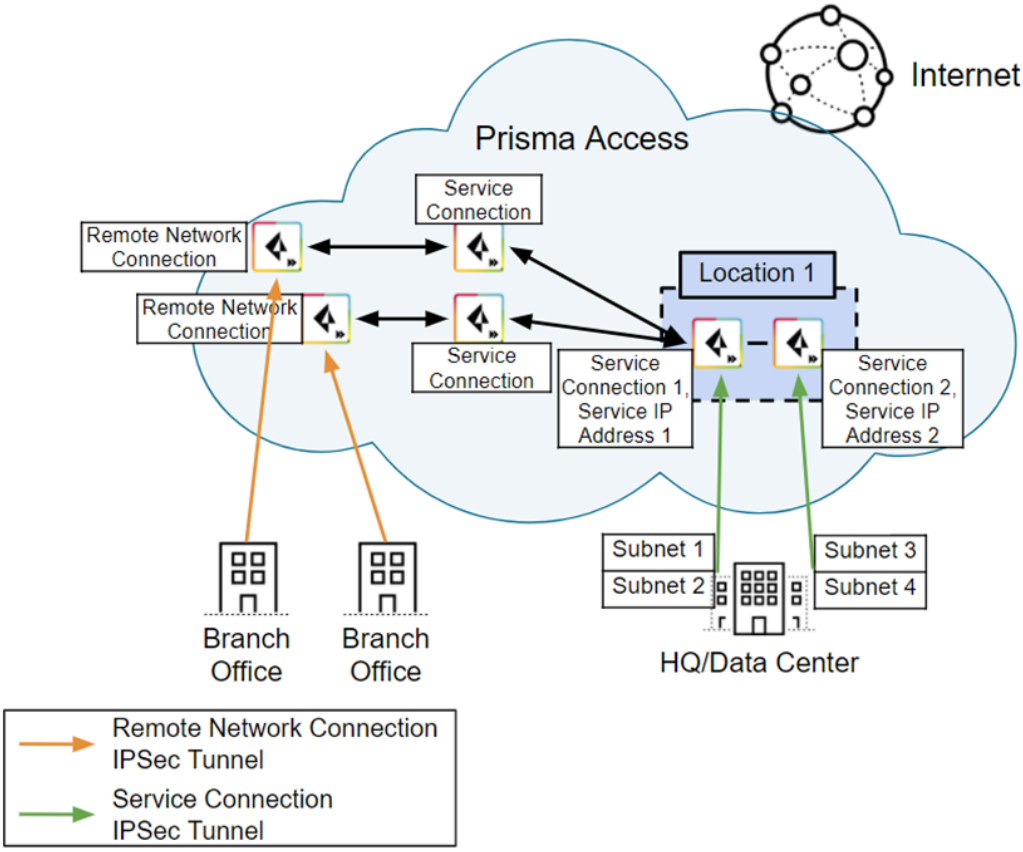
要创建到总部或数据中心站点的高带宽服务连接，您可以使用同一 Prisma Access 地点的多个服务连接来加入该站点。

尽管 *Prisma Access* 不限制可以加入到单个总部或数据中心远程网络位置的最大服务连接数，但 *Palo Alto Networks* 建议在高带宽部署中使用的服务连接不要超过四个。如果您需要更多带宽来访问内部应用程序，请使用 ZTNA 连接器或 Colo-Connect，而不是使用多个服务连接。

下图显示了总部或数据中心站点的 Prisma Access 远程网络部署，该部署具有来自同一 Prisma Access 地点的两个服务连接，从而在该站点和 Prisma Access 地点之间有效地提供了 2 Gbps 的带宽。

除了为实现高带宽访问而部署的服务连接外，该图还显示了另一组服务连接。这些服务连接为 Prisma Access 提供常规路由功能（在此图中，它们提供远程网络连接和高带宽服务连接之间的内部路由访问）。Palo Alto Networks 建议，在部署高带宽连接时，保留服务连接以仅提供对总部或数据中心位置的资源的访问，并部署其他服务连接以用于远程网络、移动用户和数据中心资源之间的内部路由。

©2025 Palo Alto Networks, Inc.



每个服务连接都处于活动状态，并具有其自己的 **Service IP Address**（服务 **IP** 地址） ；您可以使用该地址终止每个服务连接的 IPSec 隧道。

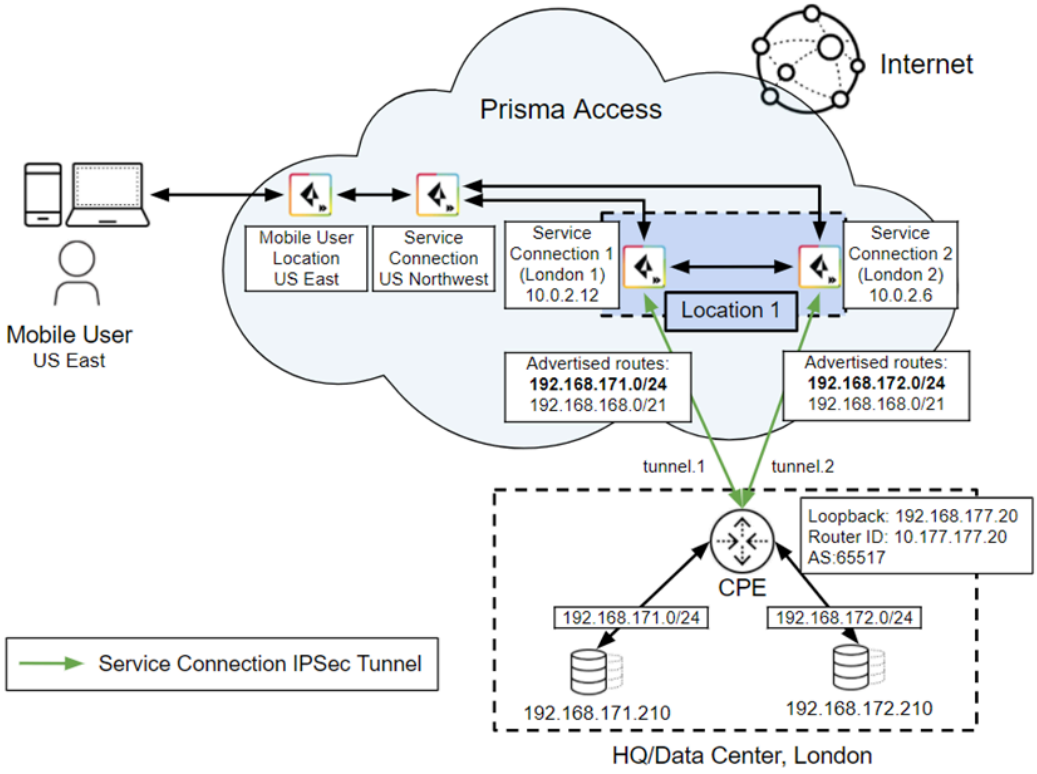
创建总部或数据中心位置的高带宽连接

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

要配置单个总部或数据中心位置的多个服务连接，请完成以下步骤。

本节中的步骤使用下图所示的部署示例。在此示例中，伦敦总部位置使用两个不同的 IPSec 隧道连接到两个不同的服务连接（London 1 和 London 2），这两个隧道在两个不同的客户终端设备 (CPE) 接口（tunnel.1 和 tunnel.2）上终止。

 ©2025 Palo Alto Networks, Inc.



此示例和本节中的步骤使用新一代防火墙来终止 CPE 上的服务连接；但是，您可以使用任何支持对称路由和 PBF 或基于策略的路由的 CPE 作为 CPE。

使用这些步骤作为指南；每个用例都可能需要额外的设计和规划，这超出了本文档的范围。

STEP 1 | 在部署从单个 Prisma Access 地点到单个站点的多个服务连接之前，请确保您的网络满足以下先决条件：

- 您必须在总部或数据中心位置划分子网，并在每个服务连接上通告唯一的子网。
- 客户终端设备 (CPE) 必须支持以下网络功能，并且您必须能够配置这些功能：
  - 基于策略的转发 (PBF) 或基于策略的路由 — 您的 CPE 必须能够有选择地为特定的本地源 IP 地址和子网选择特定路径。
  - 对称返回 — 您必须能够配置 CPE，以确保对称流量流向和流出特定 IP 地址和子网，并且如果其中一个隧道出现故障，则为故障转移隧道配置对称返回。

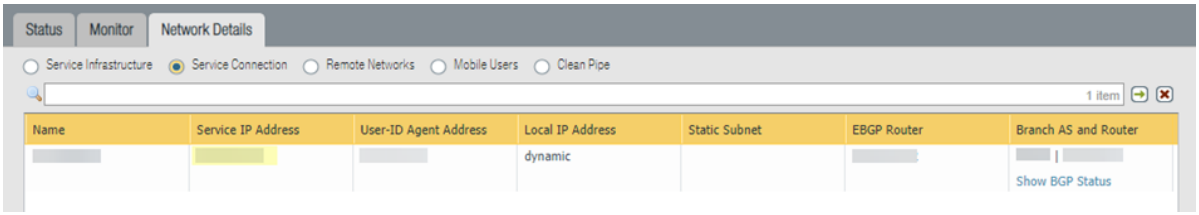
STEP 2 | 创建服务连接并为用于服务连接的 IPSec 隧道建立连接。

1. 在管理 Prisma Access 的 Panorama 中，创建服务连接，包括创建新的 IPSec 隧道配置、IKE 网关、IPSec 加密配置文件以及隧道监控设置。

   Prisma Access 提供预定义的 IPSec 模板，您可以使用这些模板来简化 *IPSec* 隧道的创建过程。
2. 找到要用作从 CPE 到 Prisma Access 的 IPSec 隧道远程端的 IP 地址，方法是选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详

 ©2025 Palo Alto Networks, Inc.

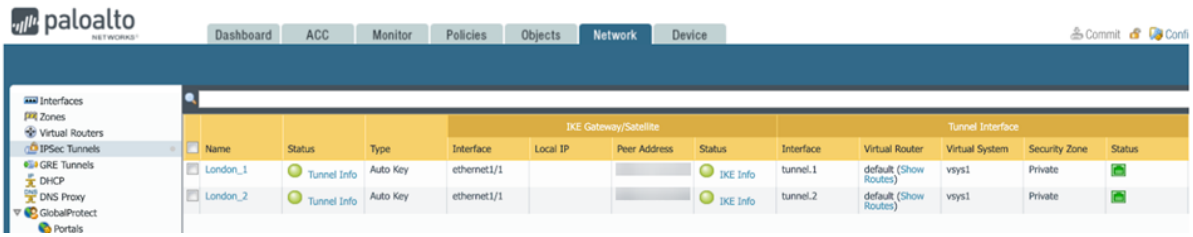
细信息），单击 **Service Connection**（服务连接）单选按钮并记下该站点的 **Service IP Address**（服务 **IP** 地址）。



3. 在 CPE 上，创建到服务连接的 IPSec 隧道

   1. 验证 IKE 和 IPSec 隧道是否使用相同的加密配置文件在对等体之间进行身份验证和加密。
   2. 使用 **Service IP Address**（服务 **IP** 地址）作为该隧道的对等体 IP 地址。

   如果使用新一代防火墙作为 CPE，请选择 **Network**（网络） > **IPSec Tunnels**（**IPSec** 隧道），并为服务连接创建两个隧道（以下屏幕截图中的 **tunnel.1** 和 **tunnnel.2**）。



STEP 3 | 为 CPE 创建虚拟路由器设置。

您创建 BGP 路由实例，在一个隧道上通告一个子网，在另一个隧道上通告另一个子网，从而确保两个活动隧道上的负载均衡。

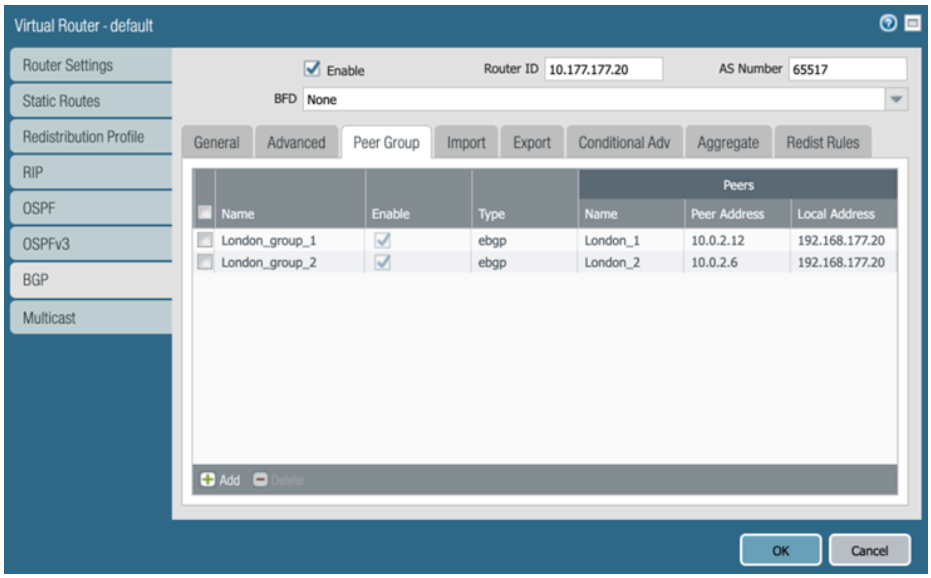
如果将新一代防火墙用作 CPE，请选择 **Network**（网络） > **Virtual Routers**（虚拟路由器），**Add**（添加）虚拟路由器设置，然后为每个隧道 **Add**（添加）**BGP Peer Group**（**BGP** 对等体组），并指定以下设置：

- 指定 CPE 路由器的 **Router ID**（路由器 **ID**）和 **AS Number**（**AS** 编号）（在此示例中分别为 10.177.177.20 和 65517）。
- 将服务连接的 **EBGP Router**（**EBGP** 路由器）地址（**Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息） > **Service Connection**（服务连接）

 ©2025 Palo Alto Networks, Inc.

> **EBGP Router**（**EBGP** 路由器））指定为服务连接的 **Peer Address**（对等体地址）（在此示例中，服务连接 1 的对等体地址为 10.0.2.12，服务连接 2 的对等体地址为 10.0.2.6）。

- 对于 **Local Address**（本地地址），您可以指定 CPE 的回环地址（在此示例中为 192.168.177.20）。



STEP 4 | 为用于两个隧道的 IP 地址创建汇总子网。

提供汇总子网可保证冗余。当两个隧道都正常运行时，流量使用最具体的路由到达其目标；例如，192.168.171.0/24 使用 tunnel.1 到达目标。添加覆盖所有通告子网（在此示例中为 192.168.168.0/21）的汇总子网，确保如果 tunnel.1 发生故障，来自 192.168.171.0/24 的

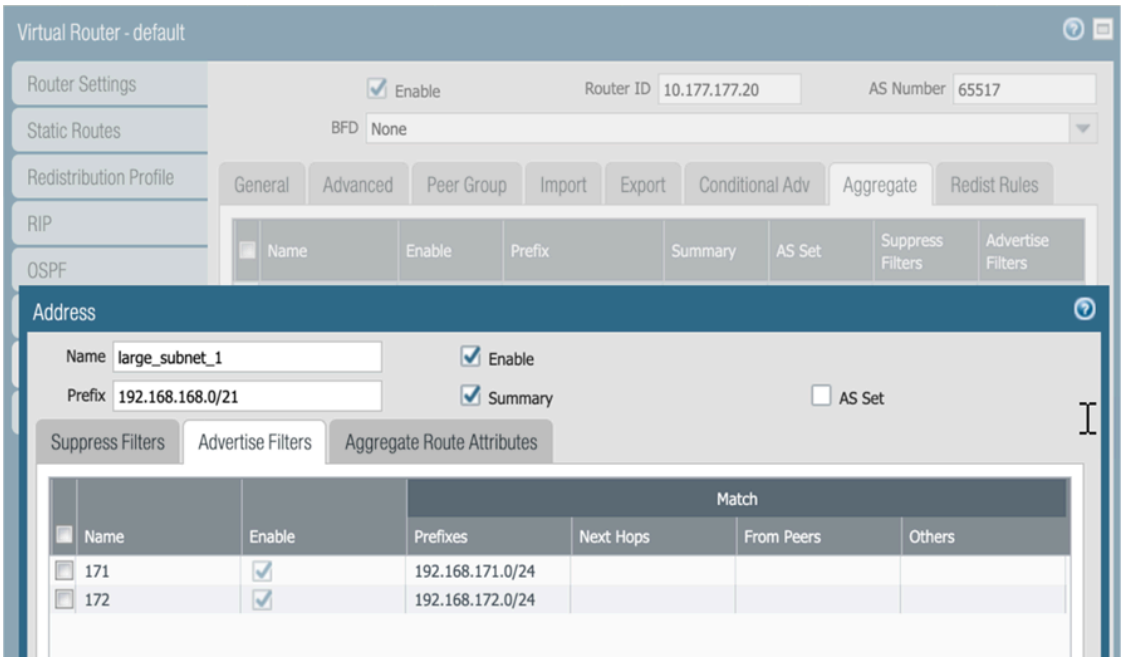
 ©2025 Palo Alto Networks, Inc.

流量可从 tunnel.2 到达目标，如果 tunnel.2 发生故障，来自 192.168.172.0/24 的流量可从 tunnel.1 到达目标。

如果使用新一代防火墙作为 CPE，请完成以下步骤。

1. 继续修改虚拟路由器配置文件并 **Add**（添加）路由聚合参数（**Network**（网络） > **Virtual Routers**（虚拟路由器） > **BGP** > **Aggregate**（聚合））。
2. 输入您为服务连接通告的子网的汇总子网。

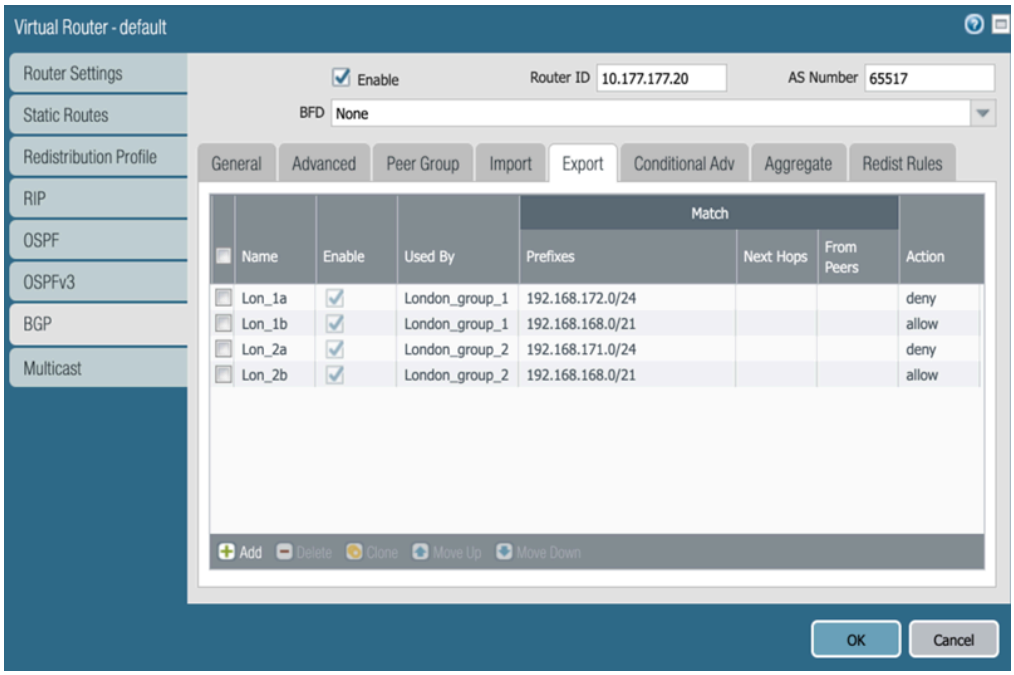
   在此示例中，输入 **Prefix**（前缀）**192.168.168.0/21**，它汇总了两个数据中心子网。



3. 输入 **Export**（导出）设置以确保隧道通告正确的子网。

   在此示例中，您为子网指定 **deny**（拒绝）和 **allow**（允许）**Action**（操作），以便从 tunnel.1 访问第一个子网 (192.168.171.0/24)，从 tunnel.2 访问第二个子网 (192.168.172.0/24)。

©2025 Palo Alto Networks, Inc.

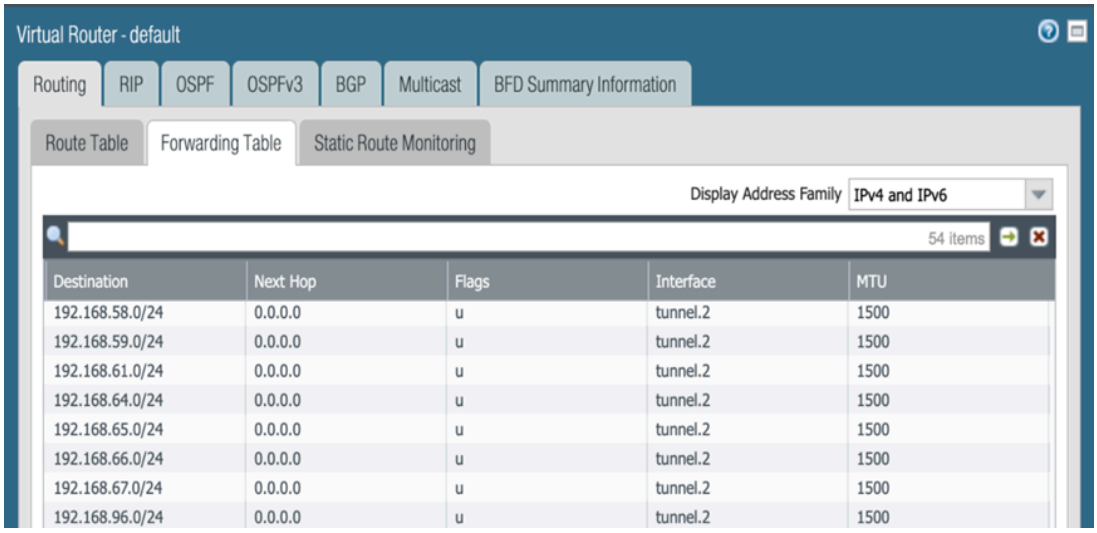


STEP 5 | （仅限具有两个以上的服务连接的部署）如果您需要两个以上的服务连接来将用户连接到专用资源以获得超过 2 Gbps 的带宽，请为导出的路由添加 AS-PATH 前缀，以便在发生故障转移时服务连接使用往返数据中心的对称路由。有关详细信息，请参阅配置总部或数据中心位置的两个以上的服务连接。

©2025 Palo Alto Networks, Inc.

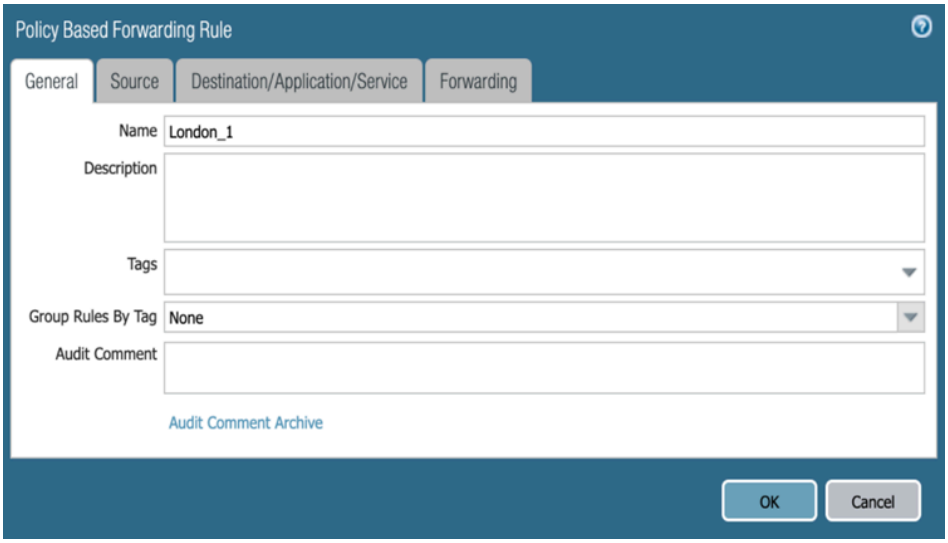
STEP 6 | 为了确保对称返回（确保来自 192.168.171.0/24 的流量始终使 用tunnel.1，来自 192.168.172.0 的流量始终使用 tunnel.2），请输入 PBF 或基于策略的路由规则。

默认情况下，无论首选隧道是什么，BGP 都会为所有不同的目标安装路由表中的路由。以下屏幕截图显示，BGP 向 tunnel.2 通告来自 192.168.168.0/21 子网的所有目标，这可能导致来自 192.168.171.0/24 的流量出现非对称路由。



为了确保对称路由，请配置一组 PBF 或基于路由的转发规则。如果使用新一代防火墙作为 CPE，请完成以下步骤。

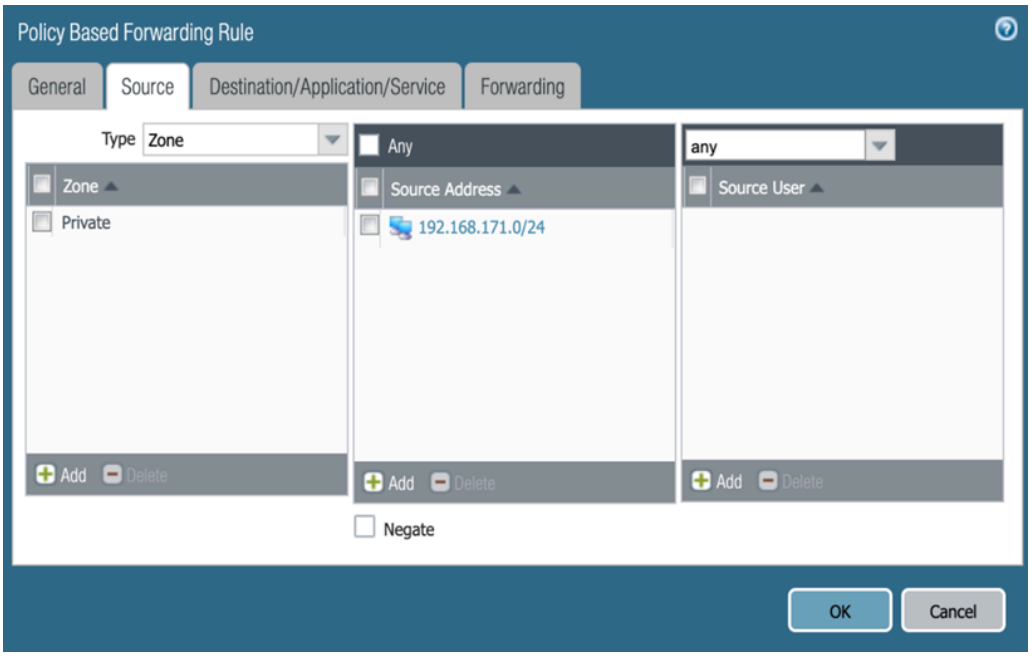
1. 选择 **Policies**（策略） > **Policy Based Forwarding**（基于策略的转发），然后 **Add**（添加）PDB 策略规则。



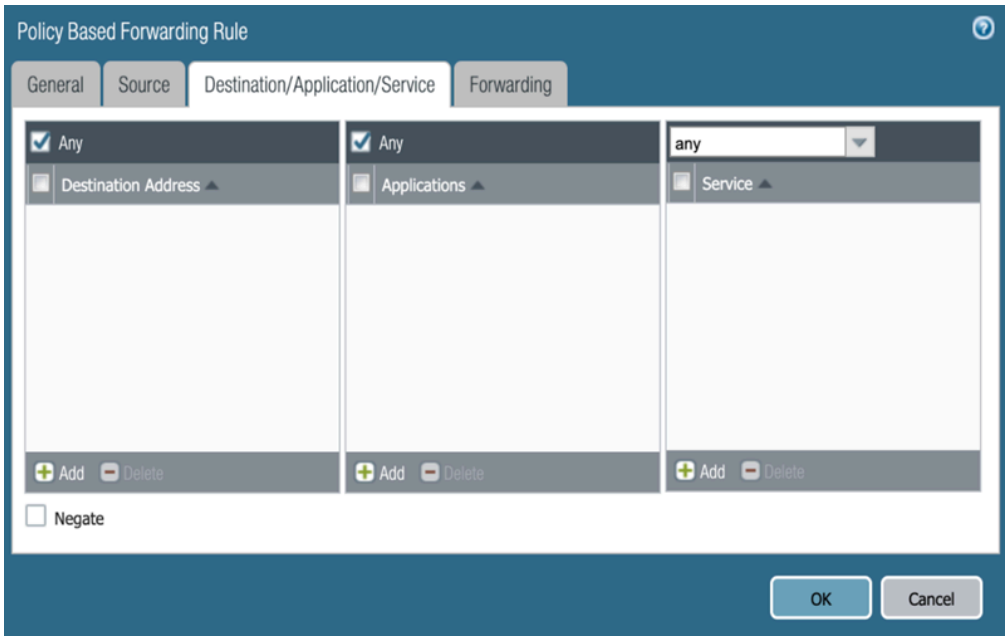
2. 选择 **Source**（源）并 **Add**（添加）用于 PBF 的 **Source Address**（源地址）。

   在本例中，您想要为 tunnel.1 创建 PBF，因此输入 192.168.171.0/24 子网。

 ©2025 Palo Alto Networks, Inc.



3. 选择 **Destination/Application/Service**（目标/应用程序/服务），选择 **Any**（任意）目标地址和 **Any**（任意）应用程序。

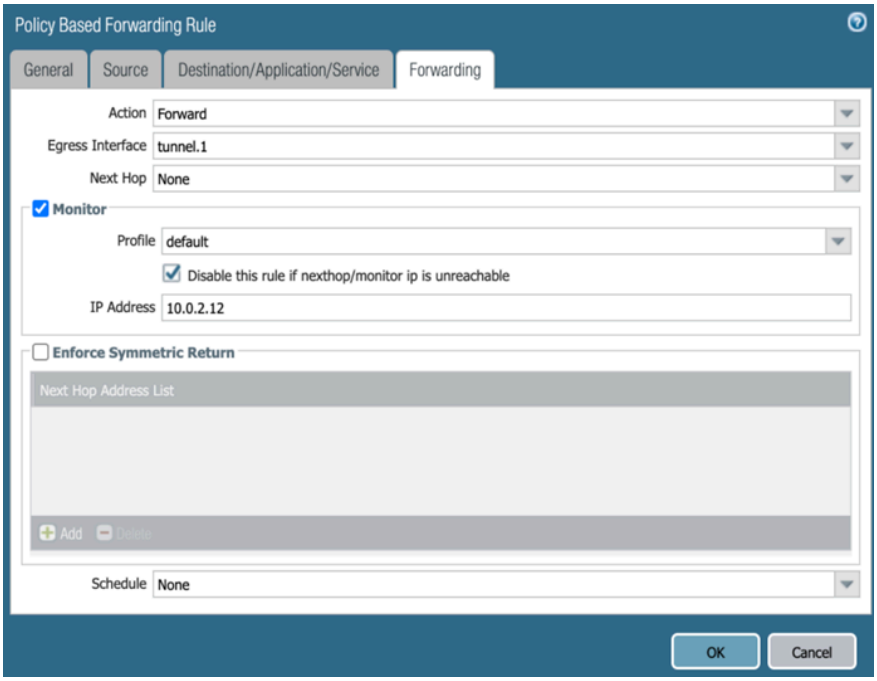


4. 选择 **Forwarding**（转发），并指定以下参数；然后单击 **OK**（确定）：
   - 在 **Action**（操作）中选择 **Forward**（转发）。
   - 选择要将该 IP 子网转发到的隧道的 **Egress Interface**（出口接口）（在本例中为 **tunnel.1**）。
   - 选择 **Monitor**（监控）并选择以下监控配置文件：
     - 在 **Profile**（配置文件）中选择 **default**（默认）。

©2025 Palo Alto Networks, Inc.

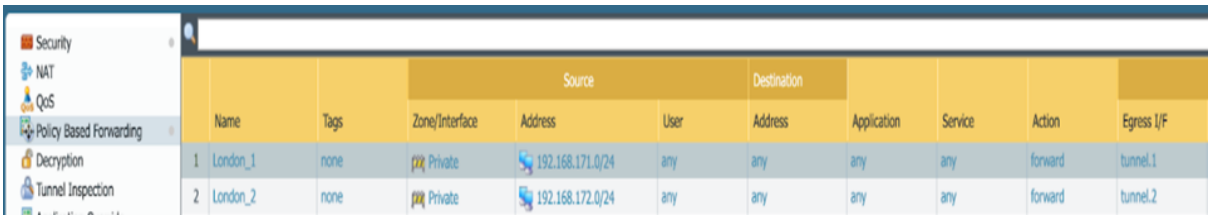
- 选择 **Disable this rule if nexthop/monitor ip is unreachable**（下一个跃点/监控 **IP** 无法访问时禁用此规则）。
- 指定服务连接的 **EBGP Router**（**EBGP** 路由器）地址的 **IP Address**（**IP** 地址）（**Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息） > **Service Connection**（服务连接） > **EBGP Router**（**EBGP** 路由器））。

通过启用监控并选择服务连接的 EBGP 路由器地址，可确保如果 tunnel.1 出现故障，防火墙将禁用 PBF 策略并路由仍处于正常运行状态的隧道 (tunnel.2) 上的流量。



5. 重复步骤 6，将服务连接 1 的 **EBGP Router**（**EBGP** 路由器）地址替换为服务连接 2 的 **EBGP Router**（**EBGP** 路由器）地址，并将 tunnel.1 的子网替换为 tunnel.2 的子网。

   完成后，您将拥有两个 PBF 策略，一个策略用于 tunnel.1，另一个策略用于 tunnel.2。

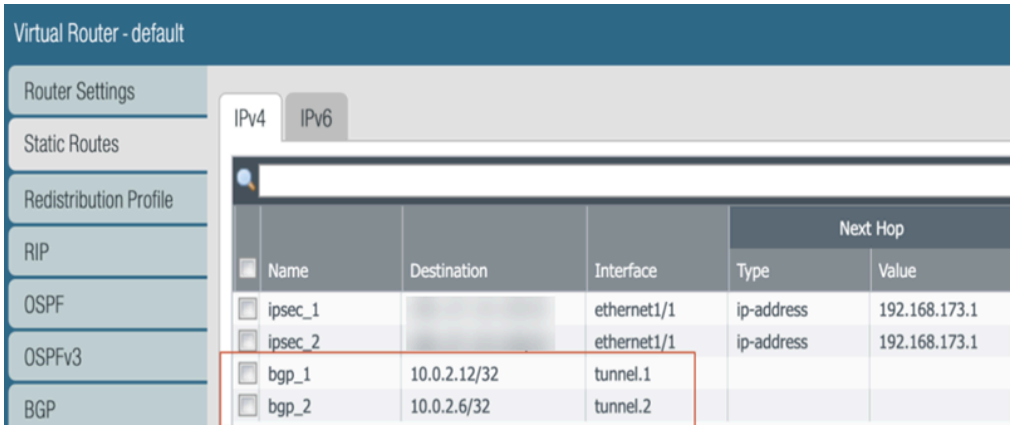


STEP 7 | 选择 **Network**（网络） > **Virtual Routers**（虚拟路由器） > **Static Routes**（静态路由），将服务连接 1 的 **EBGP Routerr**（**EBGP** 路由器）地址分配给 **tunnel.1** 的 **Interface**（接口）；

 ©2025 Palo Alto Networks, Inc.

然后，将服务连接 2 的 **EBGP Router**（**EBGP** 路由器）地址分配给 **tunnel.2** 的 **Interface**（接口）

为每个路由器 BGP 地址输入特定的静态路由，确保隧道监控正常工作，因为服务连接 1 的 EBGP 路由器 IP 地址仅可通过 tunnel.1 访问，而服务连接 2 的 EBGP 路由器 IP 地址仅可通过 tunnel.2 访问。



配置总部或数据中心位置的两个以上的服务连接

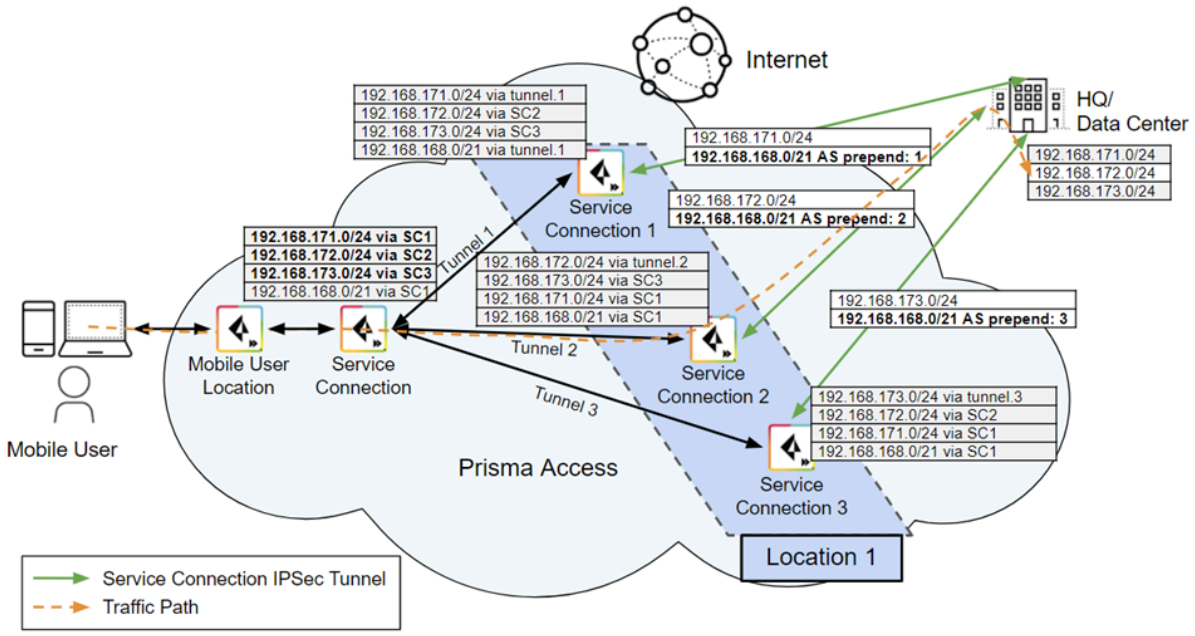
在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

将两个隧道用于高带宽服务连接时，如果一个隧道发生故障，则只剩下一个可用的流量路径，从而简化了故障转移路径的配置。如果将两个以上的连接用于高带宽连接，则需要执行其他配置以确保隧道故障转移的行为一致。

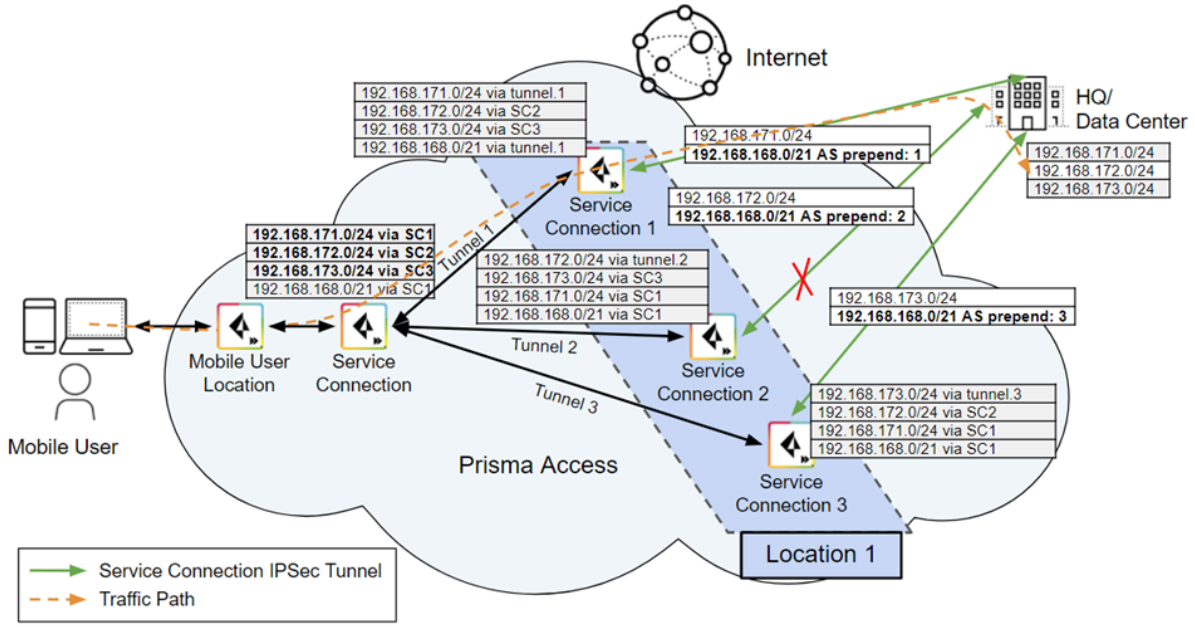
由于您使用汇总子网进行隧道故障转移，因此需要明确说明发生故障转移时要使用的服务连接隧道。由于 BGP 路由为路由选择最短的 AS-PATH 数，因此您可以将 AS-PATH 添加到路由的前面，以便在发生故障转移时让 BGP 优先使用某个隧道。

以下示例显示了使用三个服务连接的高带宽服务连接的路由表。如果所有三个隧道均已启动，Prisma Access 将使用更具体的路由到达总部或数据中心位置的子网。由于用户要访问 192.168.172.0/24 子网中的资源，因此离移动用户最近的服务连接会检查其路由表并选择隧道 2 作为访问数据中心资源的路径。

 ©2025 Palo Alto Networks, Inc.



如果隧道 2 发生故障，则通往 192.168.172.0/24 子网中资源的特定路由将不可用，因此离用户最近的服务连接将使用汇总的 192.168.168.0/21 子网。您只为服务连接 1 配置了一个 AS-PATH 前缀；因此，Prisma Access 选择隧道 1 作为故障转移路径，因为它的 AS-PATH 前缀较少。

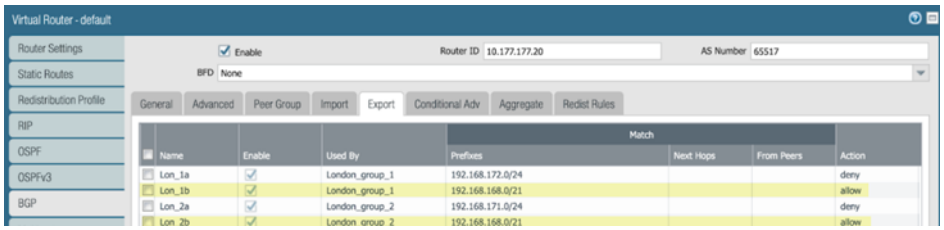


如果使用新一代防火墙作为 CPE，要为路由添加前缀，请完成以下任务。

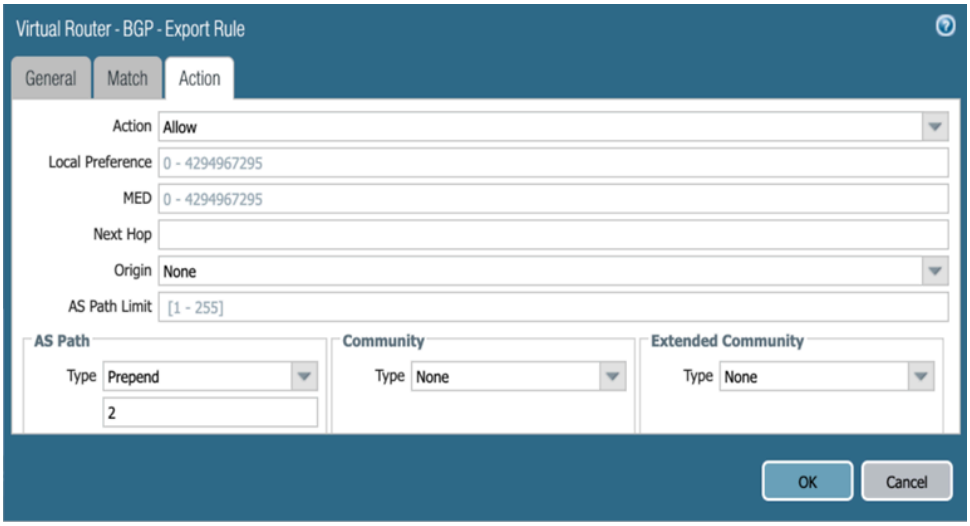
STEP 1 | 选择虚拟路由器 BGP 导出配置文件（**Network**（网络） > **Virtual Routers**（虚拟路由器） > **BGP** > **Export**（导出））。

 ©2025 Palo Alto Networks, Inc.

STEP 2 | 修改您在配置服务连接时创建的导出规则，该规则将 **Action**（操作）设置为 **Allow**（允许）。



STEP 3 | 在 AS 路径区域中，添加 **Prepend**（前缀），然后输入要添加的 AS-PATH 前缀的数量（在本示例中输入 **2**）。



STEP 4 | 对于将 **Action**（操作）设置为 **Allow**（允许）的每个导出规则，重复步骤 2 和 3，添加 AS-PATH 前缀以匹配您为部署规划的故障转移方案。

在本节使用的示例中，您将为服务连接 1 的通往数据中心位置的隧道添加 AS-PATH 前缀 1 (tunnel.1)，为用于服务连接 2 的隧道添加 AS-PATH 前缀 2 (tunnel.2)，为用于服务连接 3 的隧道添加 AS-PATH 前缀 3 (tunnel.3)。

完成后，此示例在发生故障转移时使用以下隧道：

- 如果 tunnel.2 或 tunnel.3 发生故障，则相应子网的流量将故障转移到具有最短通告 AS-PATH 的 tunnel.1。
- 如果 tunnel.1 发生故障，则其子网 (192.168.171.0/24) 的流量将故障转移到具有最短通告 AS-PATH 的 tunnel.2。

STEP 5 | 添加备份 PBF 或基于策略的路由策略，以确保在隧道发生故障时的对称返回流量。

尽管 AS-PATH 前缀可确保在发生故障转移时从 Prisma Access 传输到数据中心的流量使用特定隧道，但您还必须确保从数据中心流向 Prisma Access 的流量具有对称返回路径。为了确保对称返回，请使用 PBF 或基于策略的路由策略，为您针对从 Prisma Access 流向数据中心的流量创建的故障转移场景生成镜像。

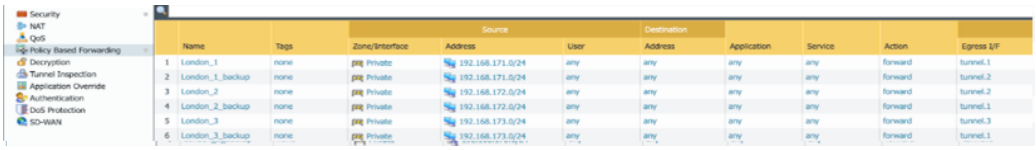
在此示例中，对于源 IP 为 192.168.171.0/24 的 tunnel.1 流量，您可以创建备份 PBF 策略，在发生故障转移时强制返回流量使用 tunnel.2。如果无法访问隧道监视器 IP 地址，则第一个 PBF

 ©2025 Palo Alto Networks, Inc.

规则将被禁用；发生此故障转移时，CPE（在本示例中为新一代防火墙）将评估列表中的下一个规则。



然后，添加更多 PBF 规则，以匹配您针对从 Prisma Access 流向数据中心的流量创建的故障转移场景。



为具有源 NAT 的服务连接保留 User-ID 和 Device-ID 映射

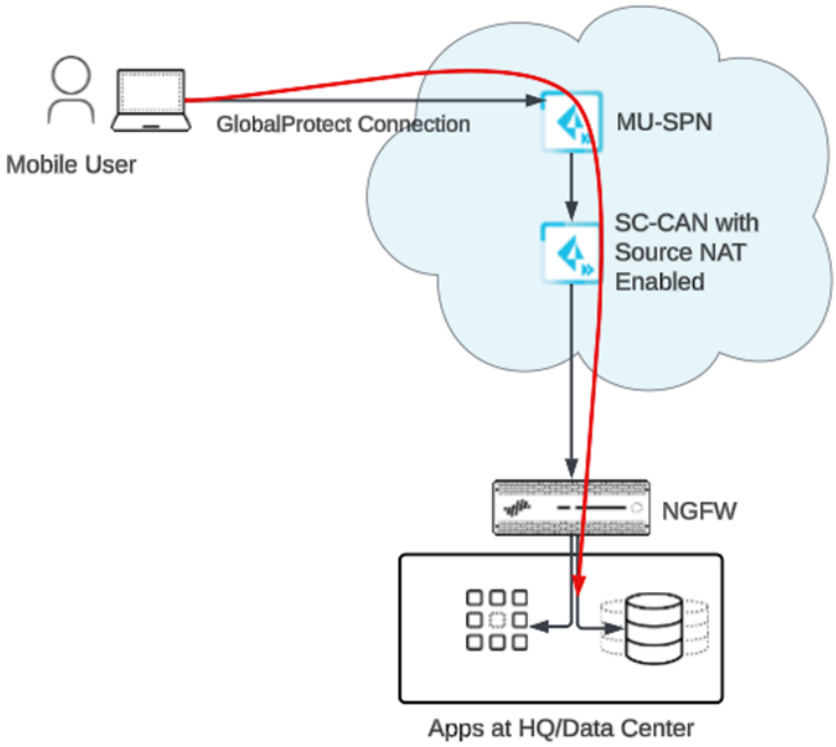
在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证 ❑ 运行最低版本的 PAN-OS 11.2 的新一代防火墙 (NGFW) ❑ 此功能使用 Geneve 封装。确保除运行 PAN-OS 11.2 或更高版本的 NGFW 之外的任何下游防火墙都能够解封装 Geneve。 动态特权访问不支持此功能。

可以在 Prisma Access 中使用服务连接（也称为服务连接，企业访问节点 (SC-CAN)）来保护私有应用。要根据 User-ID 或 Device-ID 限制对应用的访问，可以在私有应用所在的数据中心或总部位置部署新一代防火墙 (NGFW)；然后根据 User-ID 映射和/或 Device-ID 映射在 NGFW 上配置策略规则。

要使用这些规则，NGFW 必须从 SC-CAN 接收 User-ID 或 Device-ID；但如果用户使用 GlobalProtect 连接到 Prisma Access，并且 SC-CAN 启用了数据流量源 **NAT**，则 NGFW 无法获得此映射。如果在 SC-CAN 上启用了数据流量源 **NAT**，则将对移动用户 IP 地址池执行 NAT，并且不会在数据中心或总部位置通告这些 IP 地址。

在这种情况下，NGFW 无法检索 GlobalProtect 用户的 User-ID 或 Device-ID，这意味着您无法根据 User-ID 或 Device-ID 执行策略。

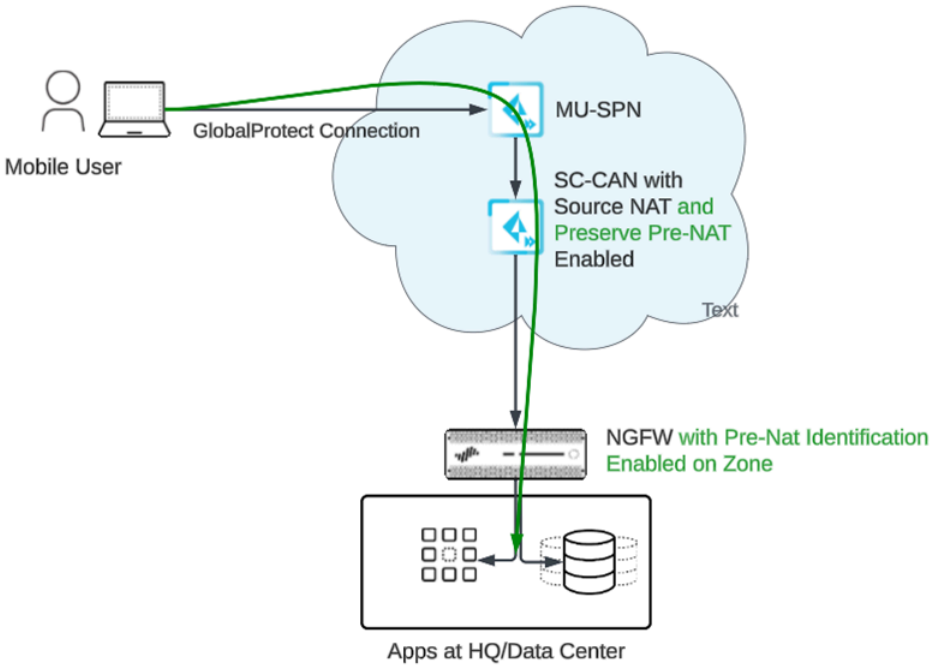
 ©2025 Palo Alto Networks, Inc.



为确保您的网络将 User-ID 或 Device-ID 映射分发到总部或数据中心，请完成以下其中一个部分列出的步骤，这些步骤可使 NGFW 根据从 GlobalProtect 获知的 User-ID 映射来实施安全策略规则。

需要至少具有 *PAN-OS* 版本 *11.2* 的 *NGFW*。服务连接不一定要在 *NGFW* 上终止，也可以在另一个支持 *IPSec* 的设备上终止，只要 *NGFW* 位于服务连接终止处的下游即可。

©2025 Palo Alto Networks, Inc.



- Strata Cloud Manager
- Panorama

为具有源 NAT 的服务连接保留 User-ID 和 Device-ID 映射 (Strata Cloud Manager)

要让 Prisma Access 在 Prisma Access (Managed by Strata Cloud Manager) 中将 User-ID 映射从 GlobalProtect 用户分发到总部或数据中心的 NGFW，请完成以下步骤。

此过程假定您已实施以下网络配置：

- 您已在服务连接上启用数据通信源 **NAT**。
- 您已经在私有应用程序所在的总部或数据中心部署了NGFW。
- 您已根据在 NGFW 中创建的区域在 NGFW 上应用了 Prisma Access 的安全策略规则。

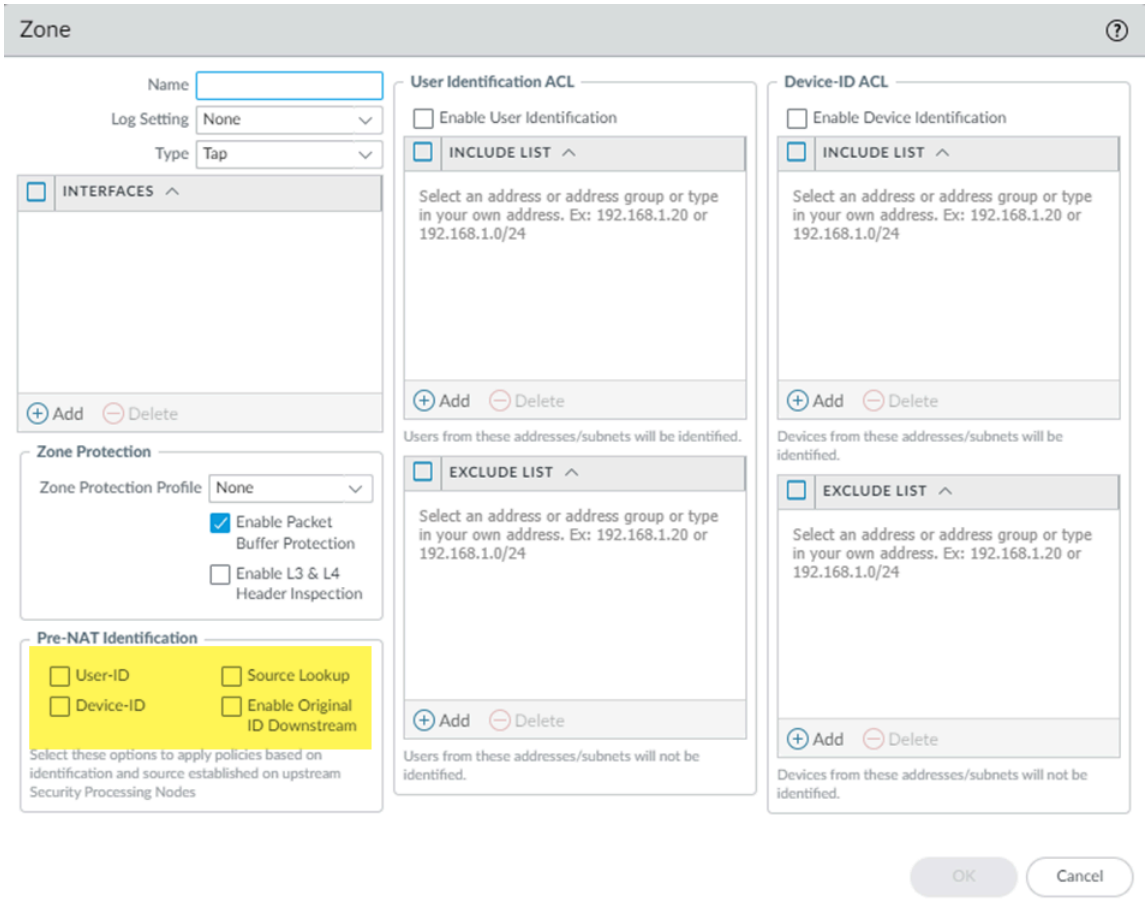
STEP 1 | 在 NGFW 上输入 NAT 前标识参数。

1. 登录到 NGFW，或登录到管理 NGFW 的 SCM 或 Panorama，然后转到 **Network**（网络） > **Zones**（区域）。
2. 选择 **Add**（添加）以添加区域或选择现有区域。
3. 选择一个或多个 **Pre-NAT Identification**（**NAT** 前标识）参数：
   - **User-ID**—保留在对 IP 地址进行 NAT 转换之前使用的移动用户 User-ID 映射。如果在安全策略规则中使用 User-ID，请启用此选项。
   - **Device-ID**—保留在对 IP 地址进行 NAT 转换之前使用的移动用户 Device-ID 映射。如果您在安全策略规则中使用 Device-ID，请启用此参数。
   - **Source Lookup**（来源查找）—可以匹配从 GlobalProtect 收到的原始来源 IP 地址。如果您在 QoS 或基于策略的转发 (PBF) 策略中使用来源查找，则源 IP 比较将基于进行 NAT 转换之前的源 IP 地址。例如，如果您的安全策略允许源 IP 地址为 1.1.1.1 且允许

 ©2025 Palo Alto Networks, Inc.

目标 IP 地址为任意值，则会将 1.1.1.1 与数据包标头中进行 NAT 转换之前的源 IP 地址进行比较。

- **Enable Original ID Downstream**（启用下游原始 **ID**）—如果连续部署了两个 NGFW，请指定此选项，让第一个 NGFW 在检查流量并对流量应用了策略之后，再将 NAT 转换前的信息发送给第二个 NGFW。这是 SC-CAN 的默认配置。



4. 单击 **OK**（确定）并 **Commit**（提交）更改。

STEP 2 | 使用 NGFW 创建命令行界面 (CLI) 会话，并在配置模式下输入以下命令：

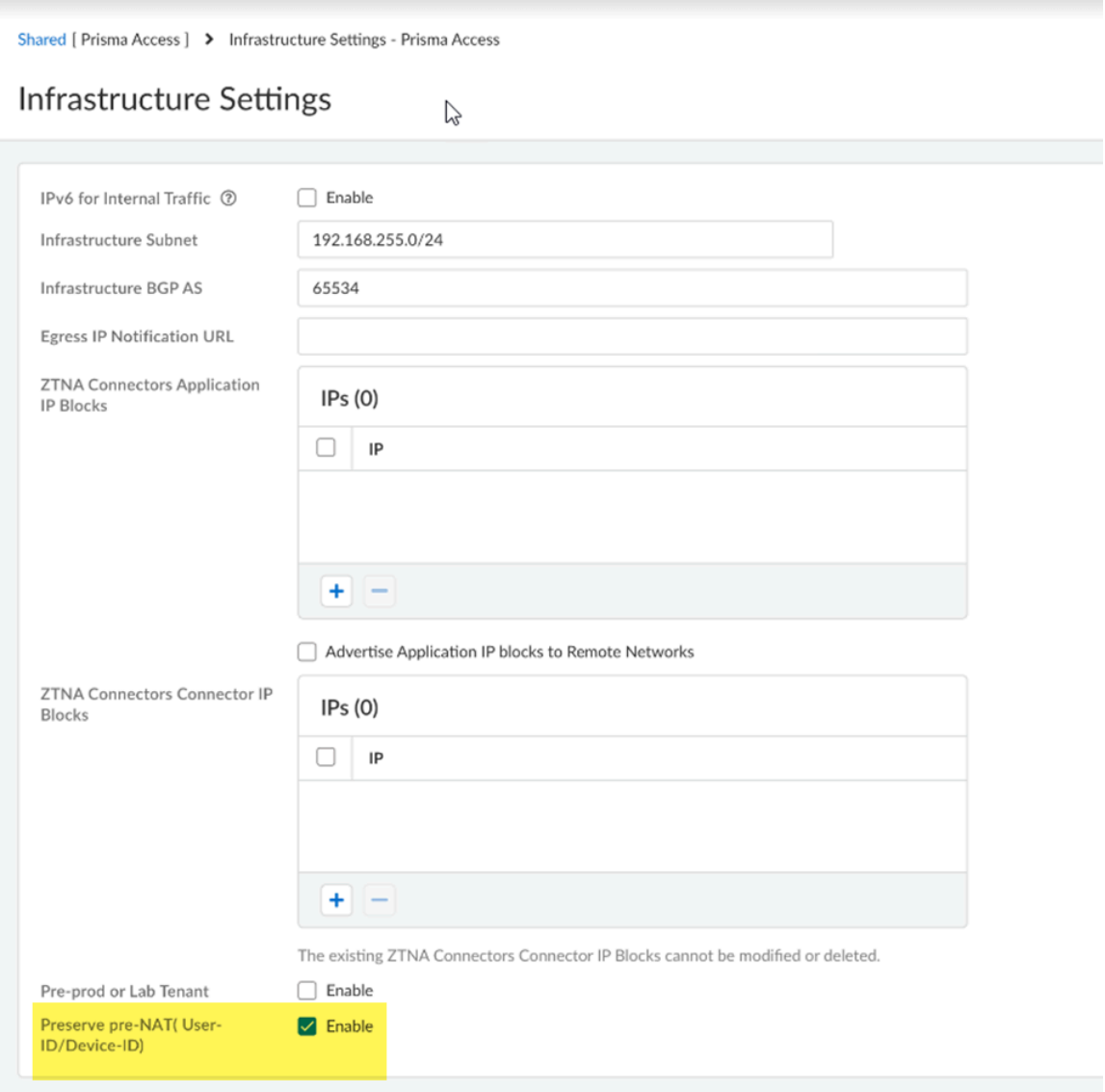
```
set deviceconfig setting preserve-prenat-feature yes
```

如果您将来需要禁用此功能，请输入 `set deviceconfig setting retain-prenat-feature no`。

 ©2025 Palo Alto Networks, Inc.

STEP 3 | 在 Strata Cloud Manager 中启用 NAT 前设置。

1. 转到 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Prisma Access** > **Infrastructure Settings**（基础设施设置）。
2. **Enable**（启用） **Preserve pre-NAT (User-ID/Device-ID)**（保留 **NAT** 之前 **(User-ID/Device-ID)**）。



3. 选择 **Push Config**（推送配置）以保存更改。

为具有源 NAT 的服务连接保留 User-ID 和 Device-ID 映射 (Panorama)

要让 Prisma Access 在 Prisma Access (Managed by Panorama) 中将 User-ID 映射从 GlobalProtect 用户分发到总部或数据中心的 NGFW，请完成以下步骤。

此过程假定您已实施以下网络配置：

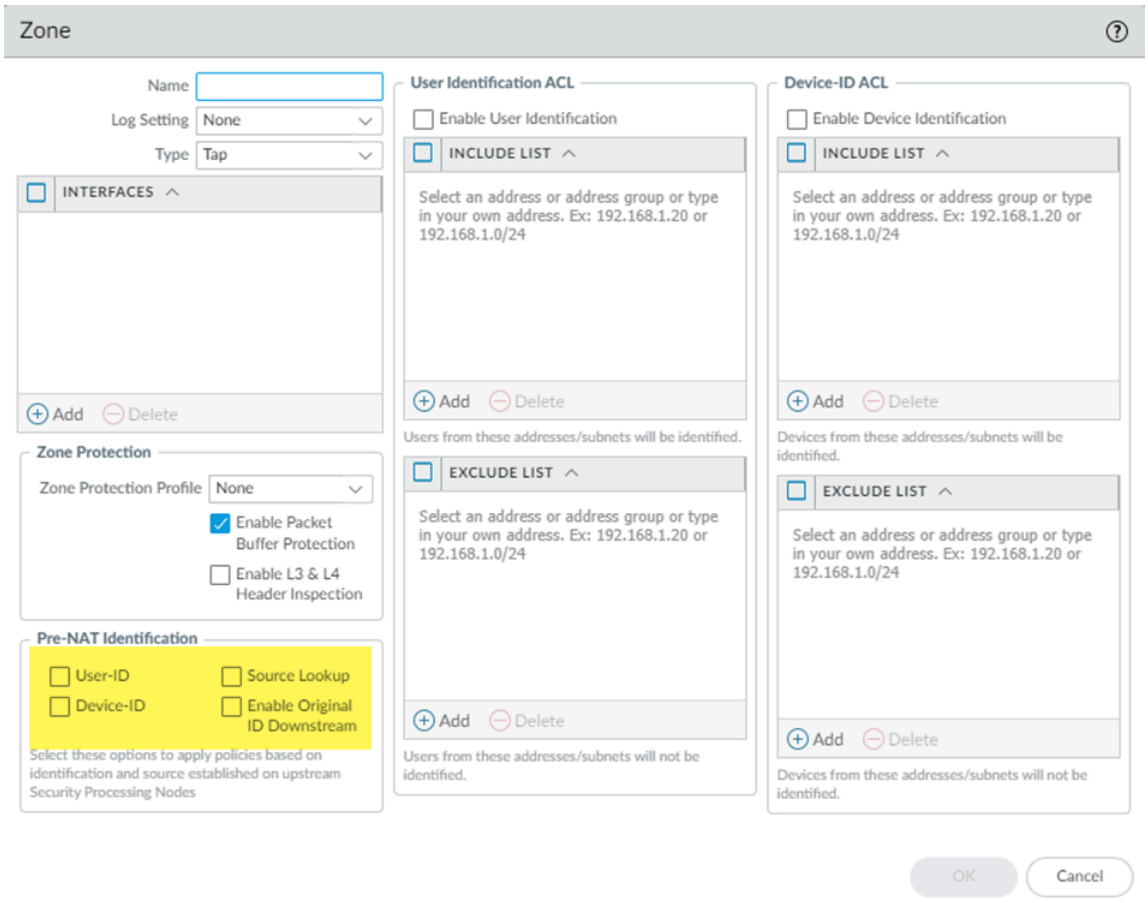
- 您已在服务连接上启用数据通信源 **NAT**。
- 您已经在私有应用程序所在的总部或数据中心部署了NGFW。

 ©2025 Palo Alto Networks, Inc.

- 您已根据在 NGFW 中创建的区域在 NGFW 上应用了 Prisma Access 的安全策略规则。

STEP 1 | 在 NGFW 上输入 NAT 前标识参数。

1. 登录到 NGFW，或登录到管理 NGFW 的 SCM 或 Panorama，然后转到 **Network**（网络）> **Zones**（区域）。
2. 选择 **Add**（添加）以添加区域或选择现有区域。
3. 选择一个或多个 **Pre-NAT Identification**（**NAT** 前标识）参数：
   - **User-ID**—保留在对 IP 地址进行 NAT 转换之前使用的移动用户 User-ID 映射。如果在安全策略规则中使用 User-ID，请启用此选项。
   - **Device-ID**—保留在对 IP 地址进行 NAT 转换之前使用的移动用户 Device-ID 映射。如果您在安全策略规则中使用 Device-ID，请启用此参数。
   - **Source Lookup**（来源查找）—可以匹配从 GlobalProtect 收到的原始来源 IP 地址。如果您在 QoS 或基于策略的转发 (PBF) 策略中使用来源查找，则源 IP 比较将基于进行 NAT 转换之前的源 IP 地址。例如，如果您的安全策略允许源 IP 地址为 1.1.1.1 且允许目标 IP 地址为任意值，则会将 1.1.1.1 与数据包标头中进行 NAT 转换之前的源 IP 地址进行比较。
   - **Enable Original ID Downstream**（启用下游原始 **ID**）—如果连续部署了两个 NGFW，请指定此选项，让第一个 NGFW 在检查流量并对流量应用了策略之后，再将 NAT 转换前的信息发送给第二个 NGFW。这是 SC-CAN 的默认配置。



4. 单击 **OK**（确定）并 **Commit**（提交）更改。

 ©2025 Palo Alto Networks, Inc.

STEP 2 | 使用 NGFW 创建命令行界面 (CLI) 会话，并在配置模式下输入以下命令：

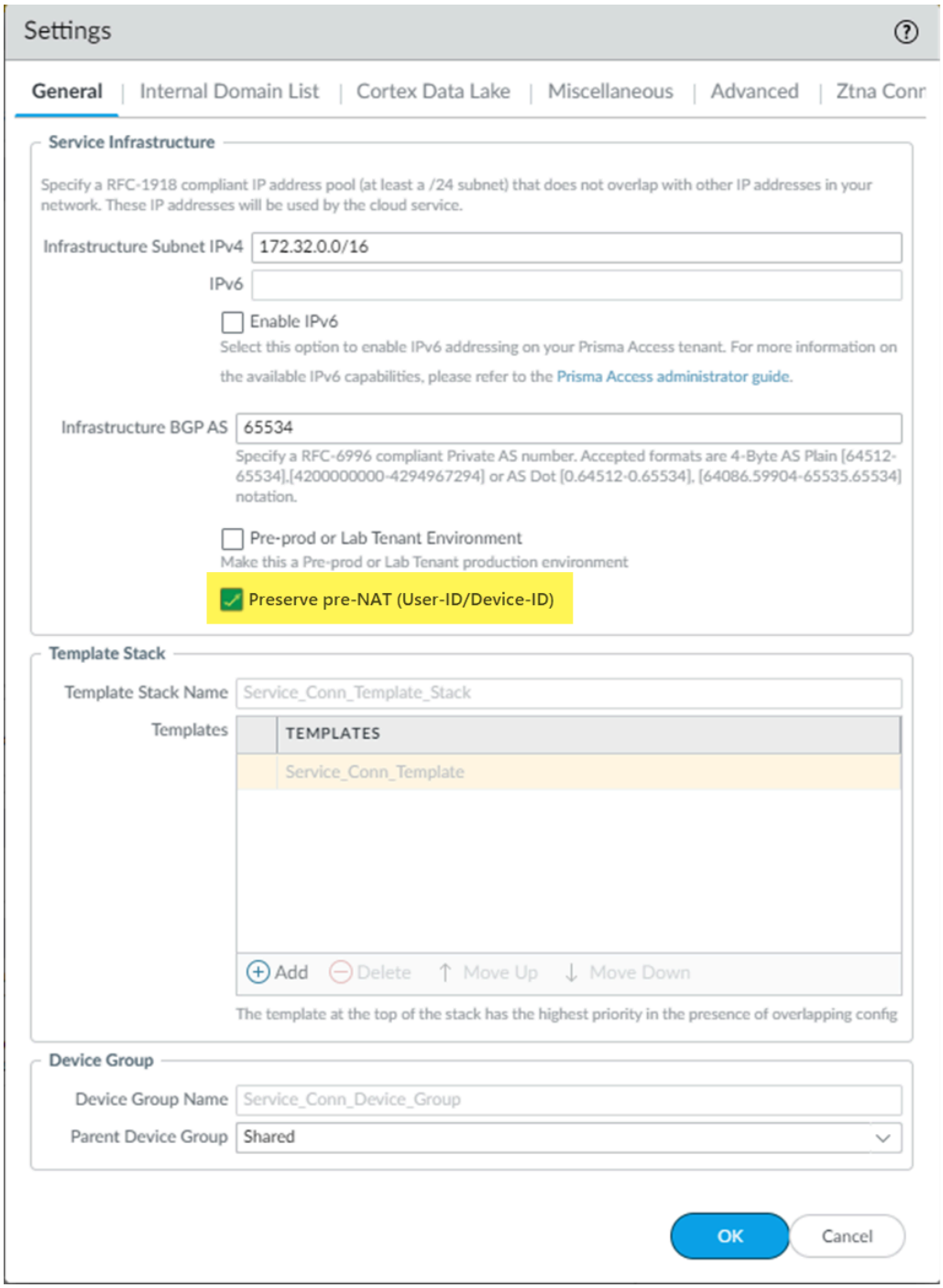
```
set deviceconfig setting preserve-prenat-feature yes
```

如果您将来需要禁用此功能，请输入 `set deviceconfig setting retain-prenat-feature no`。

 ©2025 Palo Alto Networks, Inc.

STEP 3 | 从管理 Prisma Access 的 Panorama 中启用 NAT 前设置。

1. 转到 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Service Setup**（服务设置），然后单击齿轮来编辑 **Settings**（设置）。
2. 选择 **Preserve pre-NAT (User-ID/Device-ID)**（保留 NAT 之前 **(User-ID/Device-ID)**）。



3. **Commit and Push**（提交并推送）更改。

 ©2025 Palo Alto Networks, Inc.

Prisma Access 移动用户—GlobalProtect 高级部署

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

以下部分显示了在“移动用户—GlobalProtect”部署中可用的高级部署：

- 对“移动用户—GlobalProtect”的动态 DNS 注册支持
- 在 Prisma Access GlobalProtect 部署中识别和隔离感染设备
- 移动用户中的 IPv6 流量陷坑 — GlobalProtect 部署
- 使用 Prisma Access 重新分发 HIP 信息
- 查看 HIP 报告
- 无客户端 VPN 中支持 Gzip 编码
- Prisma Access 中的流量复制

在 Prisma Access 中配置多个门户

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证 ❑ 最低要求的 GlobalProtect 客户端版本：6.1（仅限 Windows 和 macOS）

您可以在同一 Prisma Access 租户中基于端口号配置两个门户，每个门户支持不同的身份验证方法。启用此功能可将移动用户从一种身份验证方法迁移到另一种身份验证方法，而无需创建新的 Prisma Access 租户。此配置允许您逐步将用户迁移到基于云的身份验证，从而提高身份验证的灵活性，而无需创建单独的 Prisma Access 实例。

具有多个 GlobalProtect 门户的 Prisma Access 对同一租户内的每个门户使用不同的端口号。使用标准端口 443 配置第一个 GlobalProtect 门户。启用多门户功能时，Prisma Access 使用备用端口 8443 配置第二个 GlobalProtect 门户，并允许使用与第一个门户相同的 FQDN 连接到第二个门户。多个门户功能仅支持每个 FQDN 连接两个门户。

当用户使用端口 443 连接到门户时，流量将发送到第一个身份验证门户，IP 地址不变。此流程与不具备 GlobalProtect 多门户功能的配置是相同的。当用户使用端口 8443 连接时，流量将改为匹配目标 NAT 规则。这会将用户引导至其他 IP 地址的第二个身份验证门户。在任一门户上进行身份验证后，通过身份验证覆盖 Cookie 将用户转发到网关。此功能取决于身份验证覆盖 Cookie 设置，并且在门户和网关上均已启用。

下表介绍了 GlobalProtect 多门户支持以及使用主门户上的传统身份验证（如 RADIUS 或 LDAP）和辅助门户上的云身份验证（如 SAML 或带 CAS 的 SAML）的身份验证方法和证书组合。

©2025 Palo Alto Networks, Inc.

主门户用户身份验证	辅助门户用户身份验证	连接方法选项
传统，无证书	云，无证书	用户登录（始终在线、按需）
传统、<auth profile selection> 和客户端证书 注意：证书配置文件必须是相同的。	云、<auth profile selection> 和客户端证书 注意：证书配置文件必须是相同的。	用户登录（始终在线、按需） 预登录（始终在线、按需）
传统，无证书	云、<auth profile selection> 或客户端证书	用户登录（始终在线、按需）
传统、<auth profile selection> 或客户端证书 多门户配置不支持仅使用客户端证书进行身份验证的客户端	云，无证书	用户登录（始终在线、按需） 预登录（始终在线、按需），如有证书
传统、<auth profile selection> 或客户端证书 多门户配置不支持仅使用客户端证书进行身份验证的客户端	云、<auth profile selection> 或客户端证书 多门户配置不支持仅使用客户端证书进行身份验证的客户端	用户登录（始终在线、按需） 预登录（始终在线、按需），如有证书

在配置多个门户之前，请确保以下事项：

- 两个门户具有相同的证书配置文件或没有证书配置文件
- 与身份验证配置文件关联的允许列表应是相同的
- 当您在门户上接受用于身份验证覆盖的 Cookie 时，请确保门户和网关上的 Cookie 生命周期是相同的
- 多门户配置不支持仅使用基于客户端证书的身份验证

在多门户部署中，不支持在辅助门户上使用无客户端 VPN；但是，无客户端 VPN 可以在主门户上运行以使用现有身份验证方法。

- Strata Cloud Manager
- Panorama

在 Prisma Access 中配置多个门户 (Strata Cloud Manager)

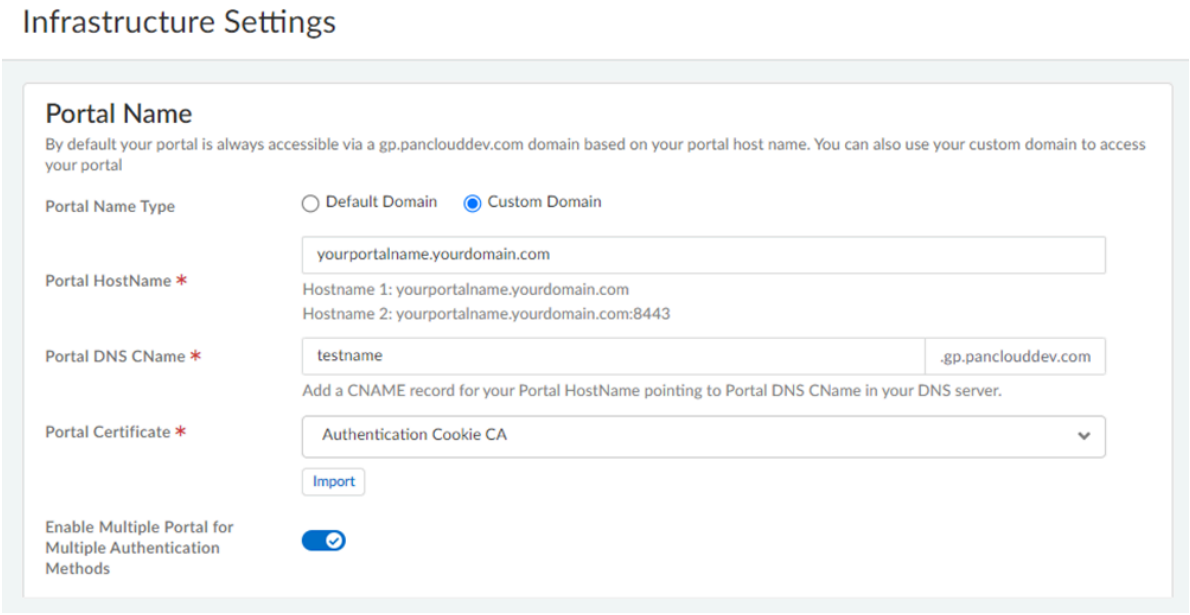
STEP 1 | 请联系 Palo Alto Networks 支持部门以激活此功能。

STEP 2 | 配置移动用户及其身份验证方法。

©2025 Palo Alto Networks, Inc.

STEP 3 | 为同一个网关启用多个门户。

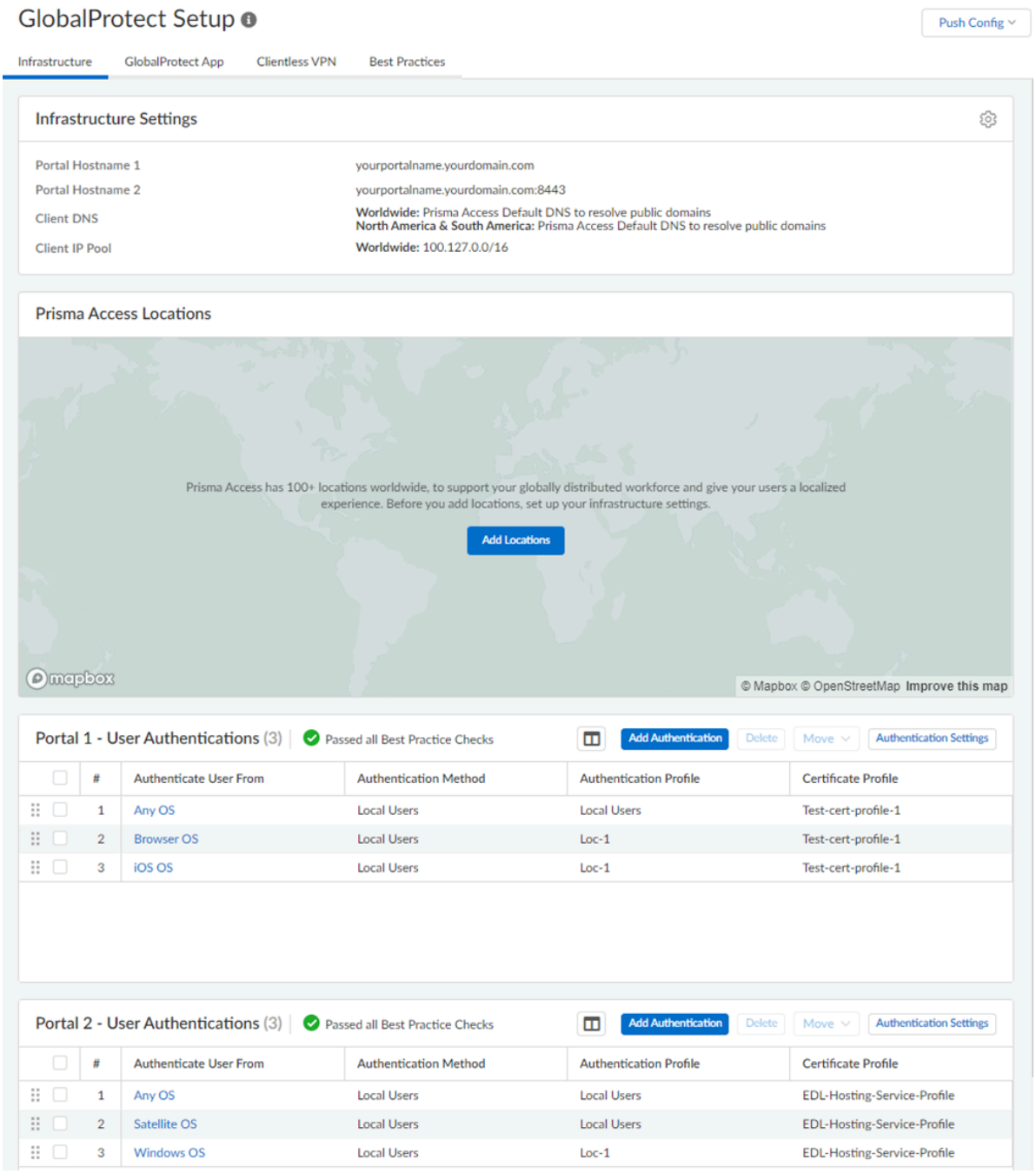
1. 选择 **Workflows**（工作流） > **Prisma Access** 设置 > **GlobalProtect** > **GlobalProtect Setup**（**GlobalProtect** 设置） > **Infrastructure**（基础架构）。
2. 编辑 **Infrastructure Settings**（基础架构设置）。
3. **Enable Multiple Portal for Multiple Authentication Methods**（为多种身份验证方法启用多个门户）。



同一租户的 8443 端口上会出现新门户。此门户从原始端口（即端口 443）继承配置设置。

 ©2025 Palo Alto Networks, Inc.

STEP 4 | 编辑门户配置以更新身份验证设置。

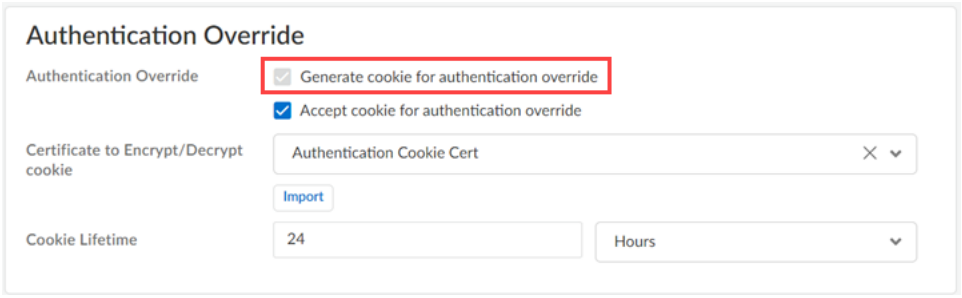


您只能编辑门户的 **Authentication Settings**（身份验证设置）和 **Certificate Profile**（证书配置文件）身份验证设置。

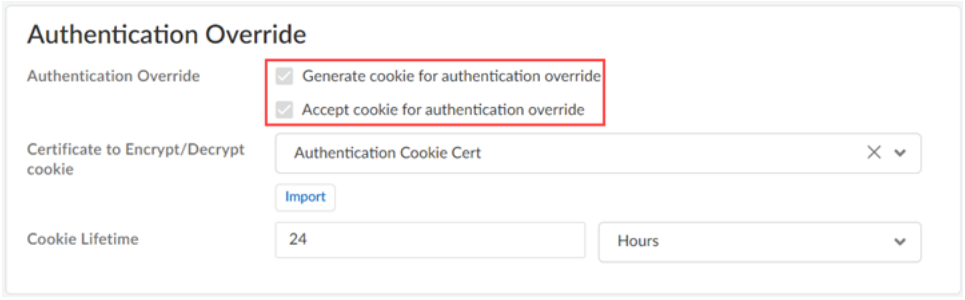
如果您在两个门户中均使用基于证书的身份验证，请确保这两个门户使用相同的客户端证书配置文件进行身份验证。

此功能启用身份验证覆盖设置，以便在 GlobalProtect 应用程序设置中为两个门户生成 Cookie。

©2025 Palo Alto Networks, Inc.



此功能启用身份验证覆盖设置，以便在隧道设置中为两个门户生成并接受 Cookie。



STEP 5 | 保存所有更改并将配置更改 **Push**（推送）到 Prisma Access。

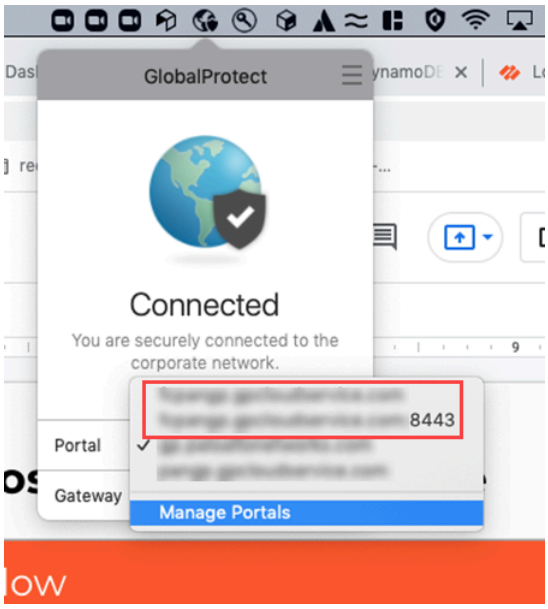
STEP 6 | 手动添加门户或使用 GlobalProtect 应用程序中的端点管理软件添加门户。

 ©2025 Palo Alto Networks, Inc.

STEP 7 | 验证您是否可以连接到该网关使用不同的身份验证配置文件的两个门户。

1. 登录到 Windows 计算机。
2. 连接到 GlobalProtect 应用程序中的门户。

   当您更改使用不同的身份验证方法的门户之间的连接时，请对用户登录进行身份验证。



如果在连接到 *8443* 门户并切换到手动网关时身份验证 *Cookie* 过期，*GlobalProtect* 将连接到 ***Best Available Gateway***（最佳可用网关）。

如果 *GlobalProtect* 应用程序使用缓存的门户配置，则无法回退到门户。

如果您对辅助门户使用基于 SAML 的身份验证，请在集成时输入以下值：

- ***Single sign on URL***（单点登录 ***URL***）：输入 ***https://Portal-FQDN:443/SAML20/SP/ACS***

  Portal-FQDN 是 *Prisma Access* 门户的 *FQDN*

  即使您已配置辅助门户 *(8443)*，也请使用门户 ***443***。
- ***Audience URI (SP Entity ID)***（受众 ***URI***（***SP*** 实体 ***ID***））：输入 ***https://Portal-FQDN:443/SAML20/SP***

在 Prisma Access 中配置多个门户 (Panorama)

STEP 1 | 请联系您的 Palo Alto Networks 客户代表以激活此功能。

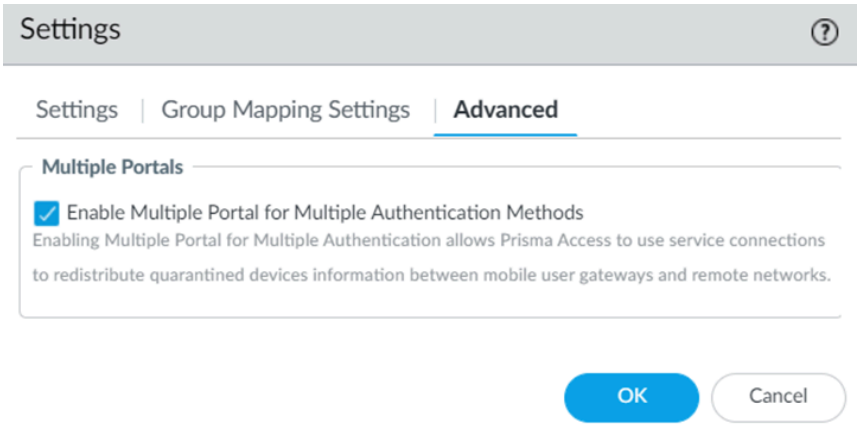
通过流量导向配置多个 *GlobalProtect* 门户时，请勿配置 ***Accept Default Routes over Service Connections***（通过服务连接接受默认路由）（***Panorama*** > ***Cloud Services***（云服务）> ***Configuration***（配置）> ***Traffic Steering***（流量导向）> ***Settings***（设置）> ***Accept Default Route over Service Connection***（通过服务连接接受默认路由））；否则，移动用户将无法连接到辅助门户。

STEP 2 | 配置移动用户及其身份验证方法。

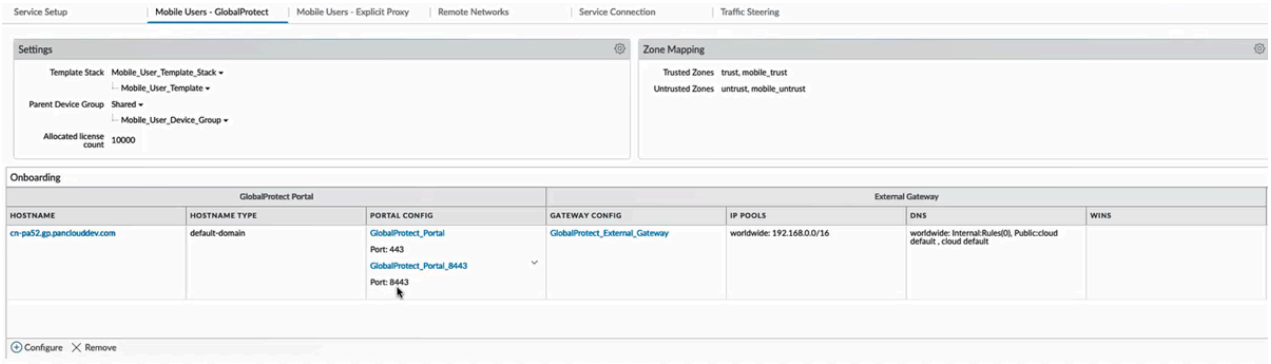
©2025 Palo Alto Networks, Inc.

STEP 3 | 选择 **Cloud Services**（云服务） > **Configuration**（配置） > **Mobile Users—GlobalProtect**（移动用户—**GlobalProtect**） > **Settings**（设置） > **Advanced**（高级）。

STEP 4 | **Enable Multiple Portal for Multiple Authentication Methods**（为多种身份验证方法启用多个门户）。



同一租户的 8443 端口上会出现新门户。此门户从原始端口（即端口 443）继承配置设置。



 ©2025 Palo Alto Networks, Inc.

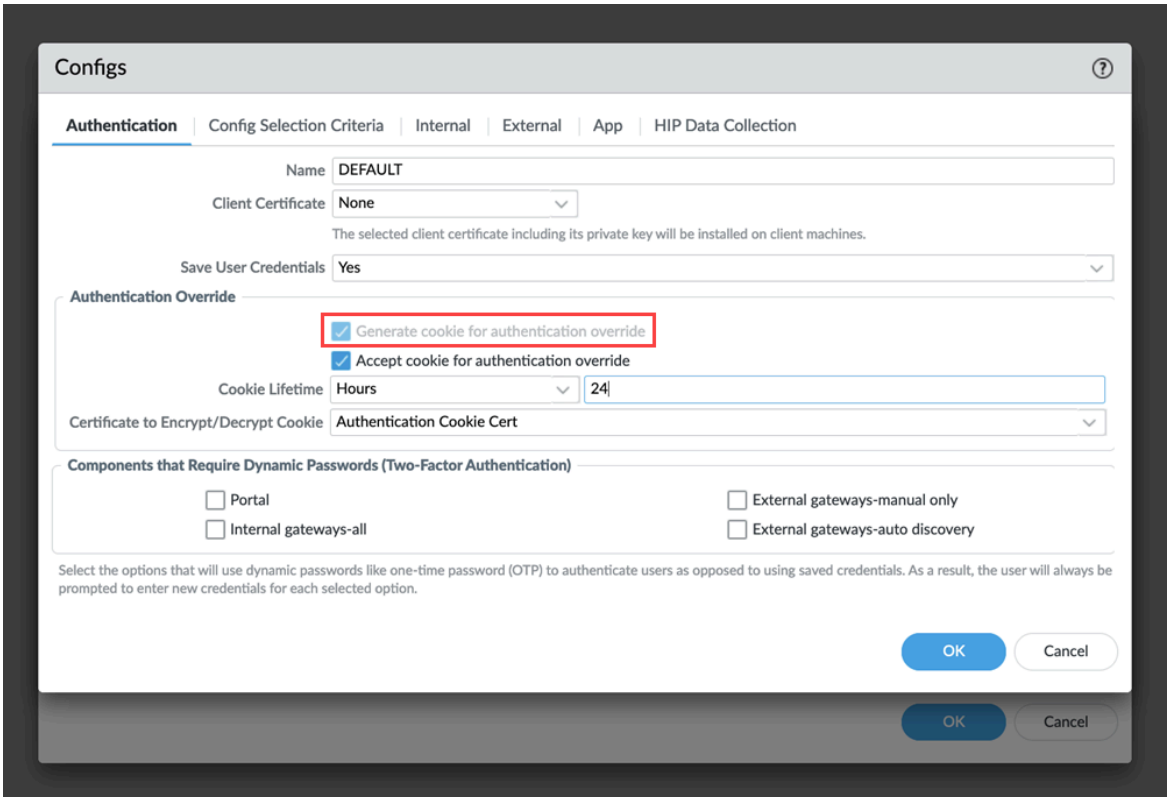
STEP 5 | 编辑门户配置以更新身份验证设置。

1. 单击门户超链接，或选择 **Panorama** > **Templates**（模板） > **Network**（网络） > **GlobalProtect** > **Portals**（门户），然后单击门户超链接。
2. 在 **Authentication**（身份验证）部分中，使用不同的 **Authentication Profile**（身份验证配置文件）**Add**（添加）**Client Authentication**（客户端身份验证）。

您只能编辑 **Client Authentication**（客户端身份验证）和 **Certificate Profile**（证书配置文件）身份验证设置。

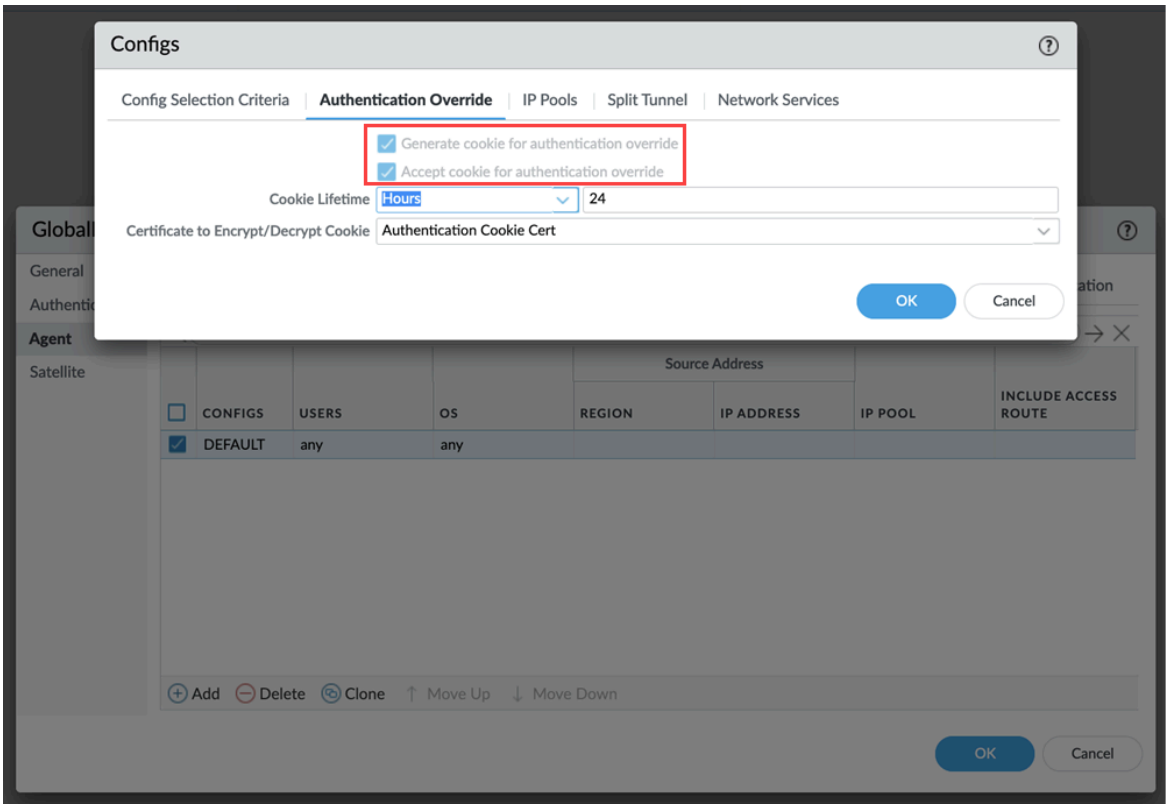
如果您在两个门户中均使用基于证书的身份验证，请确保网关没有基于证书的身份验证。

此功能启用身份验证覆盖设置，以便在 GlobalProtect 应用程序设置中为两个门户生成 Cookie。



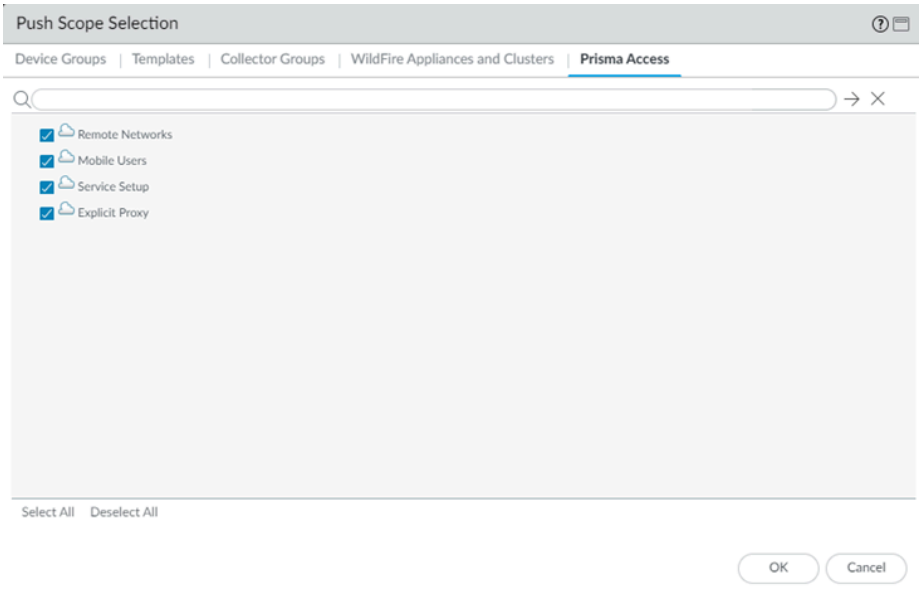
此功能启用身份验证覆盖设置，以便在隧道设置中为两个门户生成并接受 Cookie。

 ©2025 Palo Alto Networks, Inc.



STEP 6 | 将所有更改提交到 Panorama 并将配置更改推送到 Prisma Access。

1. 单击 **Commit**（提交） > **Commit and Push**（提交并推送）。
2. **Edit Selections**（编辑选择），在 **Prisma Access** 选项卡中，确保在 **Push Scope**（推送范围）中选择 **Mobile Users**（移动用户），然后单击 **OK**（确定）。



3. 单击 **Commit and Push**（提交并推送）。

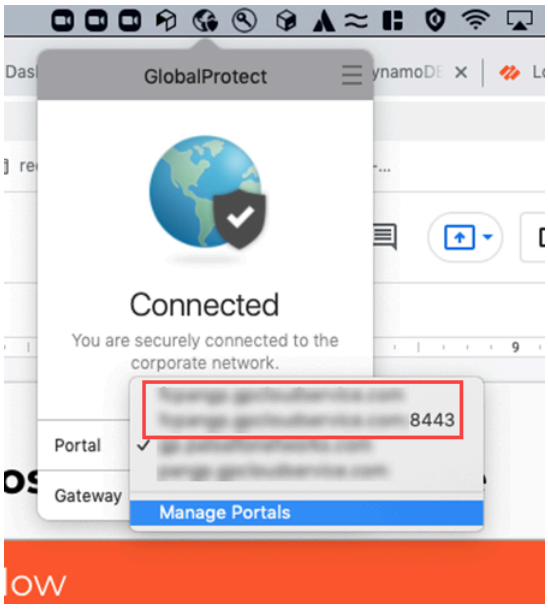
STEP 7 | 手动添加门户或使用 GlobalProtect 应用程序中的端点管理软件添加门户。

©2025 Palo Alto Networks, Inc.

STEP 8 | 验证您是否可以连接到该网关使用不同的身份验证配置文件的两个门户。

1. 登录到 Windows 计算机。
2. 连接到 GlobalProtect 应用程序中的门户。

   当您更改使用不同的身份验证方法的门户之间的连接时，请对用户登录进行身份验证。



   如果在连接到 *8443* 门户并切换到手动网关时身份验证 *Cookie* 过期，*GlobalProtect* 将连接到 ***Best Available Gateway***（最佳可用网关）。

   如果 *GlobalProtect* 应用程序使用缓存的门户配置，则无法回退到门户。
3. 在 **Monitor**（监控） > **Logs**（日志） > **GlobalProtect**中查看两个门户的日志，以查看门户和身份验证信息。

如果您对辅助门户使用基于 SAML 的身份验证，请在集成时输入以下值：

- ***Single sign on URL***（单点登录 ***URL***）：输入 ***https://Portal-FQDN:443/SAML20/SP/ACS***

  Portal-FQDN 是 *Prisma Access* 门户的 *FQDN*

  即使您已配置辅助门户 *(8443)*，也请使用门户 ***443***。
- ***Audience URI (SP Entity ID)***（受众 ***URI***（***SP*** 实体 ***ID***））：输入 ***https://Portal-FQDN:443/SAML20/SP***

支持动态 DNS 注册，实现远程故障排查与更新

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager)	☐ Prisma Access 许可证，包括移动用户 — GlobalProtect

©2025 Palo Alto Networks, Inc.

在何处可以使用？	需要提供什么？
	❑ 要求的最低 Prisma Access 版本：5.1 Innovation（至少需要 PAN-OS 数据平面版本 11.2）

当移动用户使用 GlobalProtect 代理远程连接到 Prisma Access 时，GlobalProtect 网关将为用户分配 IP 地址和端点 FQDN。但 Prisma Access 并不会使用此信息更新企业中的 DNS 服务器。由于 DNS 服务器没有为移动用户分配的 IP 地址和 FQDN 信息，因此您的 IT 管理员和网络中的应用程序无法使用 FQDN 识别和更新远程端点。

使用动态 DNS 注册，您可以将 Prisma Access 与 IP 地址管理（IPAM）供应商集成，以使用 nsupdate 在 DNS 服务器中动态创建 A 记录和 PTR 记录，这样做有以下好处：

- 与领先的 IPAM 供应商（如 InfoBlox、BlueCat 和 Windows）直接集成。
- 将使用事务签名 (TSIG) 或 Kerberos 作为身份验证协议来执行 DDNS 更新，确保 DNS 数据库更新安全。
- 从 Prisma Access 到 DNS 服务器完成实时 DDNS 更新，并且使用的是基于 GlobalProtect 连接和断开事件的批处理 nsupdate 调用。这些更新使用移动用户安全处理节点 (MU-SPN) 上的 DDNS 服务。

设置此解决方案后，可以执行以下操作：

- 可以使用 Microsoft Endpoint Configuration Manager (MECM) 等软件工具将软件更新推送到 GlobalProtect 端点。
- IT 和服务台工作人员可以使用设备的 FQDN 连接和管理 GlobalProtect 端点。
- 可以实施依赖 DNS 反向查找的客户应用程序（例如银行应用程序），从而允许从批准的 GlobalProtect 端点进行访问。

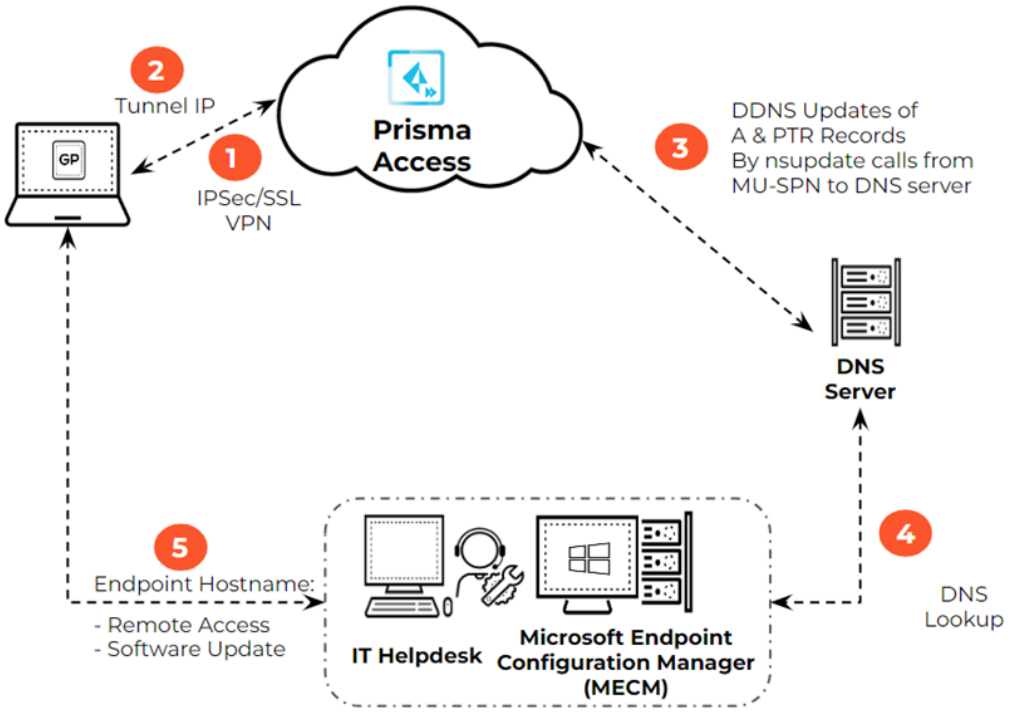
此 *DDNS* 解决方案与对移动用户的动态 DNS 注册支持 — GlobalProtect解决方案不兼容，后者使用 *Strata Logging Service* 将 *DDNS* 更新推送到服务器。如果您现有的解决方案是使用 *Strata Logging Service* 实现的，然后又部署了此解决方案，则 *Prisma Access* 将使用此解决方案并禁用使用 *Strata Logging Service* 的现有解决方案。

动态 DNS 注册支持用例

下图说明了 Prisma Access DDNS 解决方案的典型用例。在此示例中，您希望使用 MECM 更新 GlobalProtect 端点，或者希望 IT 帮助台能够远程登录 GlobalProtect 端点以进行故障排除。

1. GlobalProtect 在 GlobalProtect 端点和 Prisma Access 网关之间建立 SSL 隧道。
2. GlobalProtect 通过隧道将移动用户设备的主机名、域名和隧道 IP 地址信息发送到本地或 Prisma Access 网关。
3. Prisma Access 使用 DNS 服务器的 nsupdate 提供 A 记录和 PTR 记录的 DDNS 更新。Prisma Access 在处理登录和注销事件时实时提供这些安全更新。
4. IT 管理员或企业软件通过 DNS 或 RDNS 查找使用这些记录，并解析端点名称或 IP 地址。
5. IT 管理员或端点管理软件使用此信息来管理端点或推送软件更新。

 ©2025 Palo Alto Networks, Inc.



网络连接要求

在实施此解决方案之前，请确保您的网络满足以下要求：

- 已添加路由，以确保从 MU-SPN 和 Prisma Access 服务连接到 DNS 服务器的连接。

  为此，请从 Prisma Access 基础设施子网中添加路由，可 **Workflows**（工作流） > > **Prisma Access Setup**（**Prisma Access** 设置） > **Prisma Access** > **Infrastructure Subnet**（基础设施子网）中找到，对于移动用户 - GlobalProtect IP 地址池，则可在 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **GlobalProtect** > **Client IP Pool**（客户端 **IP** 池）中找到。
- 您建立连接（在 Prisma Access 与连接到 DNS 服务器的 IPSec 终端设备（例如，下一代防火墙或路由器）之间创建服务连接）。
- 您已确保可以通过服务连接 IPSec 隧道访问 DNS 服务器。
- 已确认从 Prisma Access 移动用户 -GlobalProtect 安全处理节点 (SPN) 发送的 nsupdate 命令已获准执行并可以访问 DNS 服务器。

  要实现此连接而执行的步骤会因所使用的 DNS 服务器的位置和类型而异。例如：
  - 如果 DNS 服务器位于数据中心，则可以使用 IPSec 隧道建立从移动用户—GlobalProtect SPN 到服务连接的连接，然后建立从服务连接到 DNS 服务器所在的网关路由器（例如，配置为 VM 的下一代防火墙）的连接。
  - 如果 DNS 服务器位于云中，您可以使用适当的安全策略规则实现从移动用户 - GlobalProtect SPN 到 DNS 服务器的连接。
- 已在 DNS 服务器上配置了正向和反向查找区域。
- 已经实现了支持 nsupdate 的 Infoblox、BlueCat 或 Windows DNS 服务器。

 ©2025 Palo Alto Networks, Inc.

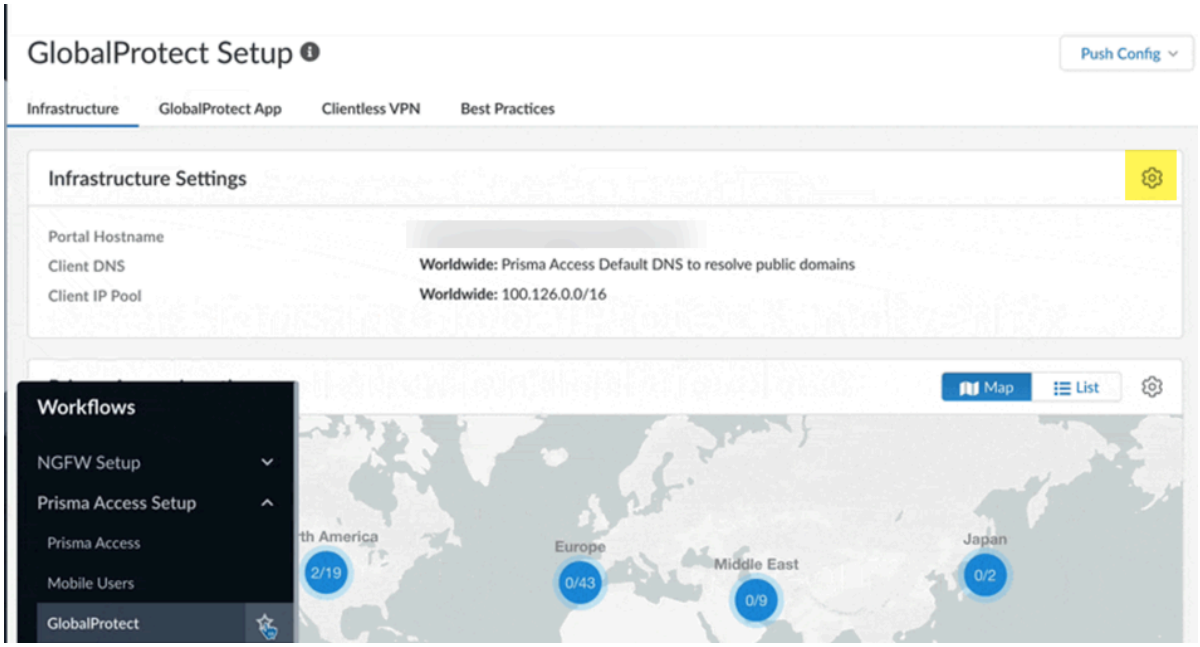
- 如果您单独维护区域的权限，请确保已创建安全策略规则，以允许持有正确 TSIG 或 Kerberos 密钥的设备进行 nsupdates。

要配置此解决方案，请根据您的部署类型使用以下步骤之一。

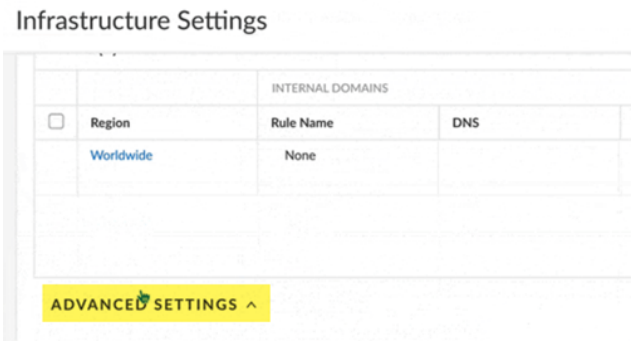
- 云端管理
- Panorama

为 Prisma Access (Managed by Strata Cloud Manager) 配置动态 DNS 更新

STEP 1 | 在 Strata Cloud Manager 中，转到 **Workflows**（工作流） > **GlobalProtect**，单击齿轮图标以编辑 **Infrastructure Settings**（基础架构设置）。



STEP 2 | 选择 **Advanced Settings**（高级设置）。



STEP 3 | 配置 **Dynamic DNS Support**（动态 **DNS** 支持）设置。

1. 选择 **Dynamic DNS Support for GlobalProtect**（**GlobalProtect** 的动态 **DNS** 支持）。
2. 选择 **Domain Type**（域类型）。
   - **Fallback Domain**（备用域）— 用于 nsupdate 事件的域将回退到您在 **Fallback Domain**（备用域）区域中指定的域。如果 GlobalProtect 客户端未加入任何域，或

©2025 Palo Alto Networks, Inc.

者它们加入的域与 DDNS 服务用于更新 DNS 服务器上的记录的域相同，请使用此选项。

如果您选择 **Fallback Domain**（备用域），并且未连接到域的用户登录 GlobalProtect，则他们的信息将会添加到在 DNS 服务器上创建的备用域服务区下。

如果登录到 GlobalProtect 的 GlobalProtect 客户端属于 DNS 服务器上未配置的意外域，nsupdate 可能会失败；在这种情况下，选择 **Override Domain**（覆盖域）以使用 DNS 服务器已知的域覆盖未知域。

- **Override Domain**（覆盖域）— Prisma Access 仅使用您指定的域来更新 DNS 服务器，并覆盖所有其他域。如果 GlobalProtect 客户端登录到另一个域，DDNS 服务将使用您在此处指定的域来更新 DNS A 和 PTR 记录。

3. 在 **Fallback Domain**（备用域）字段中选择用于更新备用域或覆盖域的 PTR 记录的域。
4. 选择 **DNS Server IP**（**DNS** 服务器 **IP**）地址。
5. 选择 **Server Type**（服务器类型）（**TSIG** 或 **Kerberos**）。
6. （仅限 TSIG 部署）选择要用于 TSIG 的 **TSIG Key**（**TSIG** 密钥）。

   确保 TSIG 文件格式正确且文件类型为 .key。

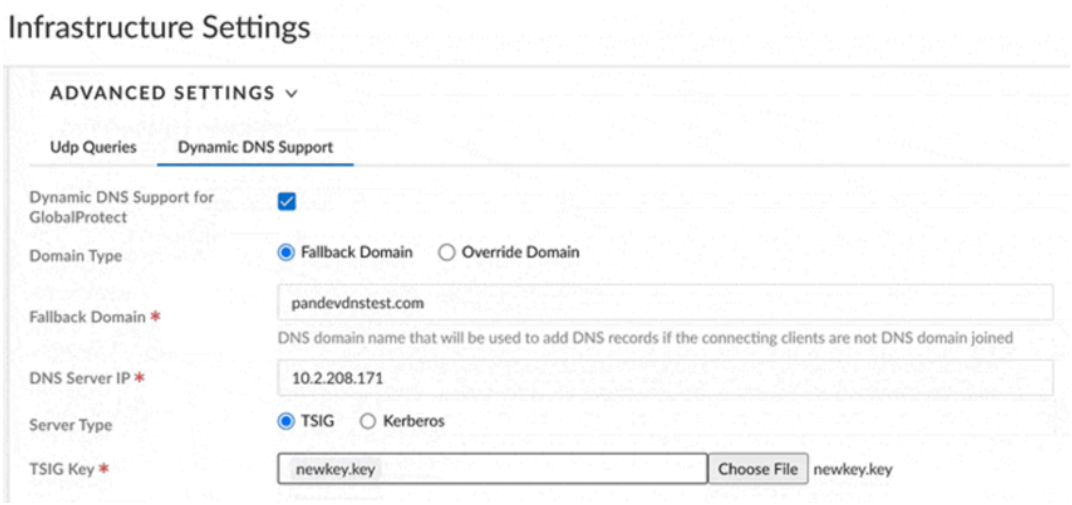
   如果选择 Kerberos 身份验证类型，请通过 .key 文件上传身份验证密钥，该文件包含从 DNS 服务器检索到的未编码 Kerberos 密钥表文件。

   TSIG 文件应采用以下格式：

   ```
   key "ddns-gp" { algorithm hmac-sha256; secret
    "aBCDEFGhiJklMNO89PQR+8stUVWX+YZAbcdeFgHI5J="; };
   ```

7. （仅限 Kerberos 部署）指定要使用的 Kerberos 选项。
   - 输入 **Kerberos Domain Controller**（**Kerberos** 域控制器）的 IP 地址。
   - 输入 **Kerberos Admin Server**（**Kerberos** 管理服务器）的 IP 地址。
   - 输入 **Kerberos User Name**（**Kerberos** 用户名）。
   - 输入要使用的 **Kerberos Key**（**Kerberos** 密钥）（密钥表）。

     确保 Kerberos 密钥的格式是正确的。



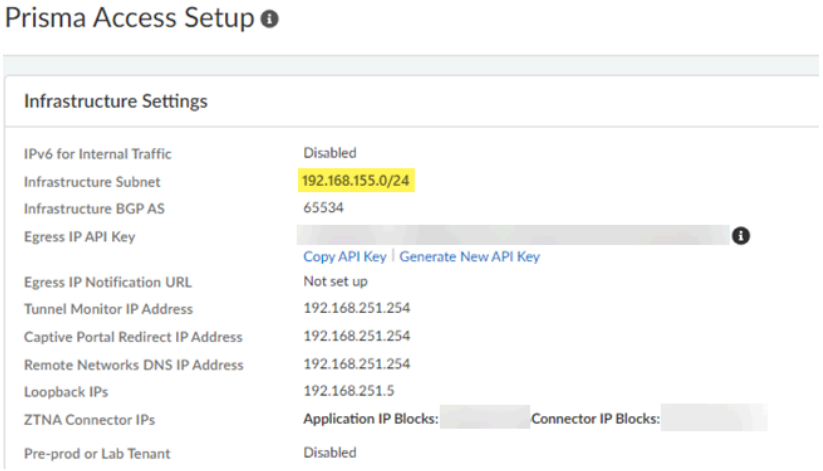
 ©2025 Palo Alto Networks, Inc.

STEP 4 | **Save**（保存）更改。

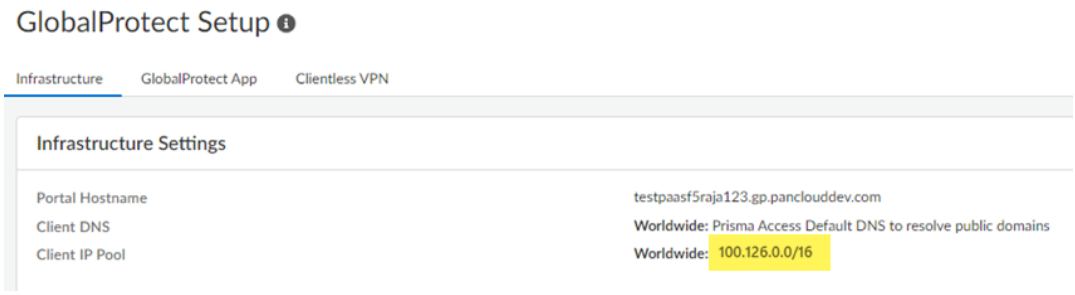
STEP 5 | 在 DNS 服务器上设置正向查找和反向查找服务区。

请参阅 IPAM 供应商的文档来设置这些服务区。在此步骤中，您需要在 Prisma Access 中输入 **Infrastructure Subnet**（基础架构子网）和 **Client IP Pool**（客户端 **IP** 池）。

- 要查找基础架构子网，请转到 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **Prisma Access**，并记下 **Infrastructure Subnet**（基础架构子网）。



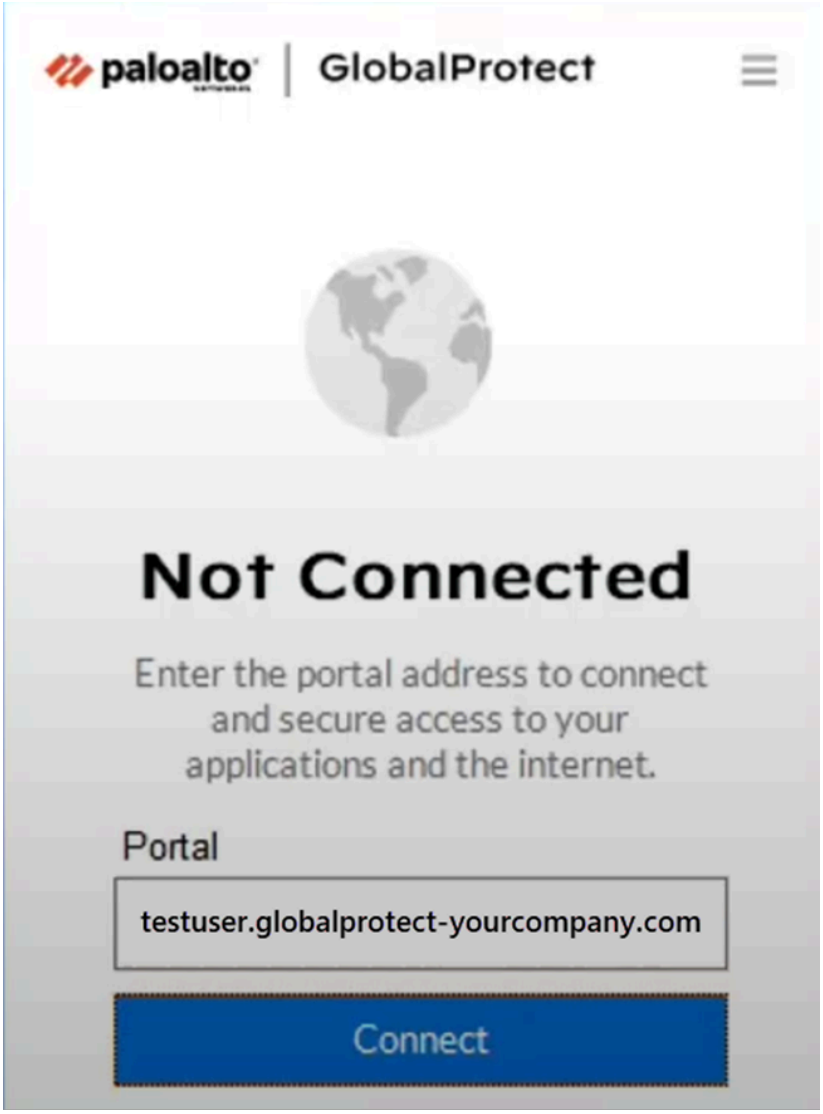
- 要查找 GlobalProtect 移动用户 IP 地址池，请转到 **Workflows**（工作流） > **Prisma Access Setup**（**Prisma Access** 设置） > **GlobalProtect**，并记下 **Client IP Pool**（客户端 **IP** 池）。



 ©2025 Palo Alto Networks, Inc.

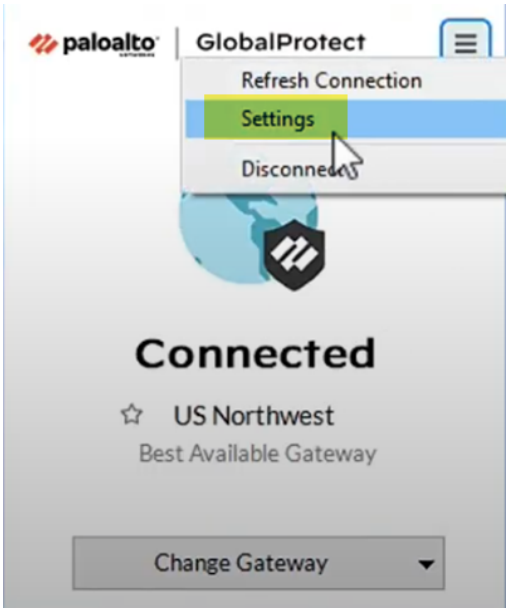
STEP 6 | 验证 IPAM DNS 服务器上的 DNS 记录是否正在更新。

1. 打开客户端计算机并连接到 Prisma Access GlobalProtect 网关。

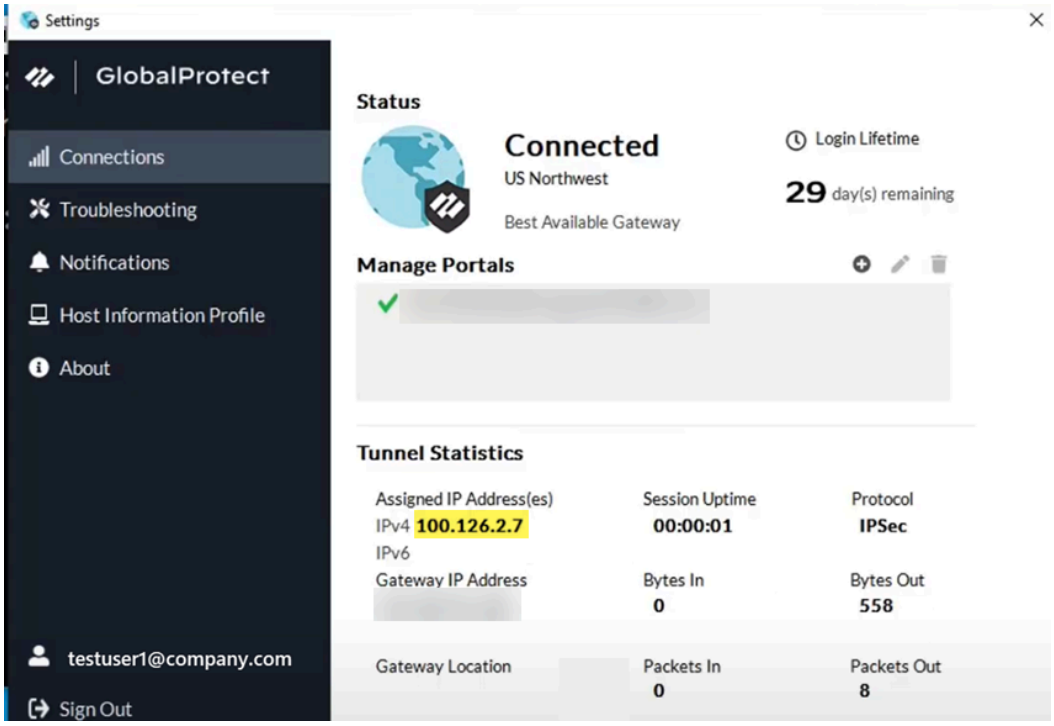


2. 选择 GlobalProtect **Settings**（设置），验证 Prisma Access 分配给用户的 GlobalProtect IP 地址。

 ©2025 Palo Alto Networks, Inc.

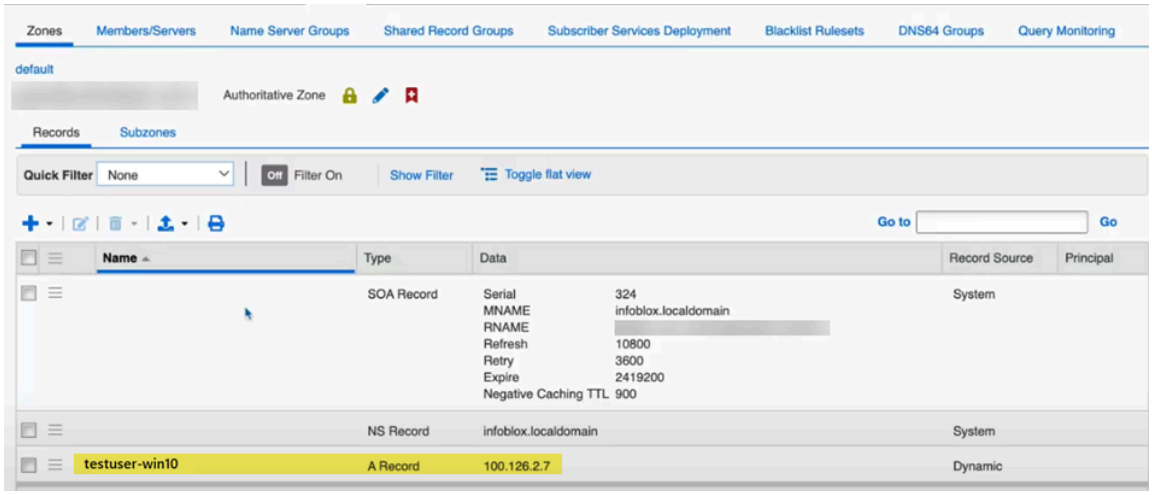


Assigned IP Address(es)（分配的 **IP** 地址） (100.126.2.7) 表明该 IP 地址来自 GlobalProtect IP 地址池 (100.126.0.0/16)。

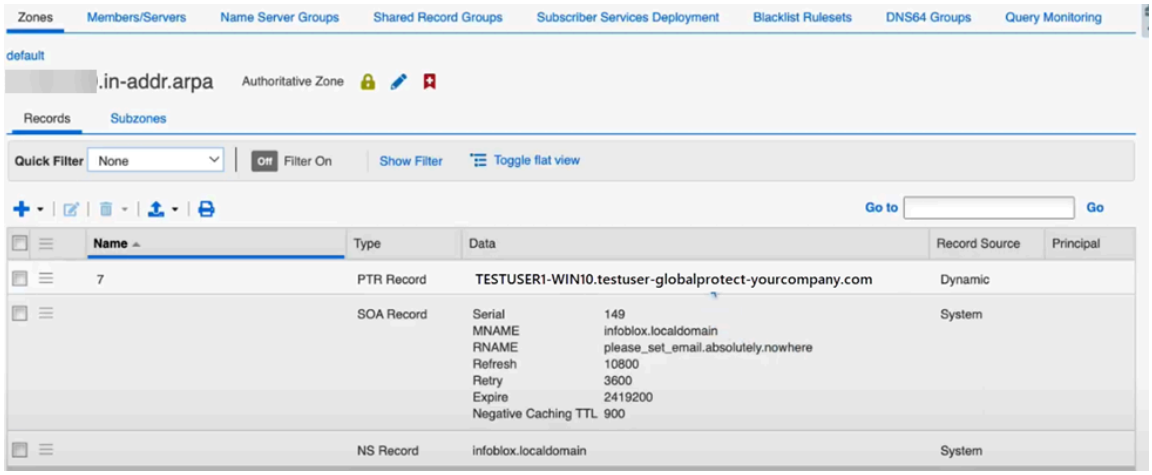


3. 从 IPAM DNS 服务器查看用户的记录。
   在此示例中，用户名为 `testuser1-win10`。

 ©2025 Palo Alto Networks, Inc.



DNS 反向查找还会在 PTR 记录中显示用户名。



4. 从 GlobalProtect 注销用户并检查记录，以确保 DNS 服务器已删除该用户的记录。

为 Prisma Access (Managed by Panorama) 配置动态 DNS 更新

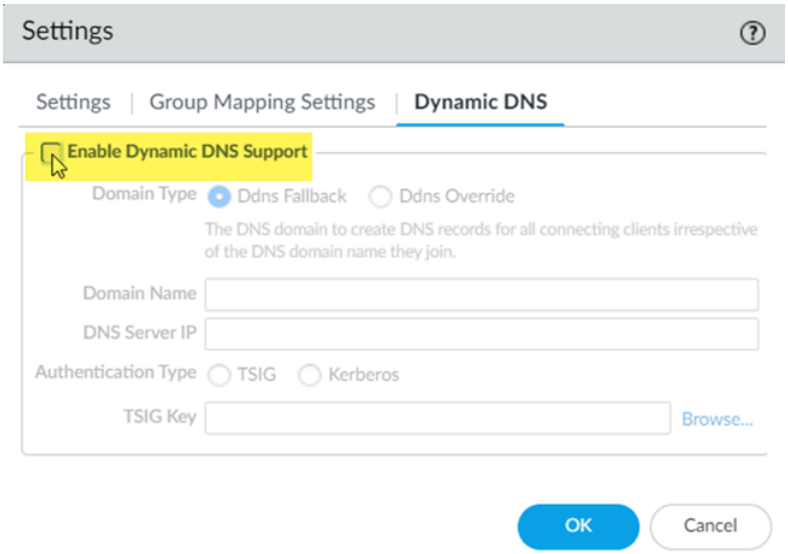
要为 Prisma Access (Managed by Panorama) 配置动态 DNS 更新，请完成以下步骤。

STEP 1 | 在 Panorama 中，转到 **Cloud Services**（云服务） > **Configuration**（配置） > **Mobile Users—GlobalProtect**（移动用户—**GlobalProtect**），然后单击齿轮来编辑 **Settings**（设置）。

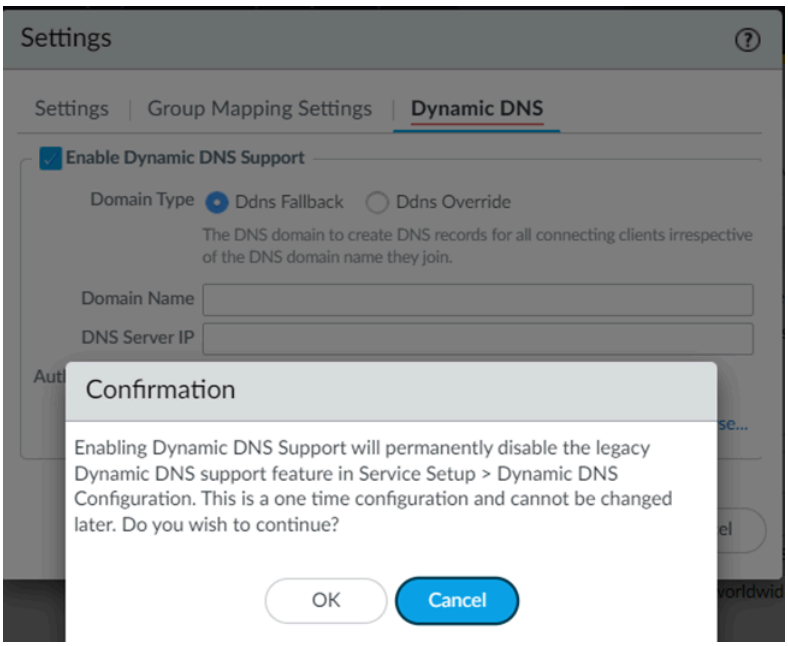
STEP 2 | 选择 **Dynamic DNS**（动态 **DNS**）。

©2025 Palo Alto Networks, Inc.

STEP 3 | **Enable Dynamic DNS Support**（启用动态 **DNS** 支持）。



STEP 4 | 系统提示您，如果您启用的是旧版动态 **DNS** 支持，则启用更新后的支持将永久禁用旧版支持。单击 **OK**（确定）继续。



©2025 Palo Alto Networks, Inc.

STEP 5 | 配置 **Dynamic DNS**（动态 **DNS**）设置。

1. 选择 **Enable Dynamic DNS Support**（启用动态 **DNS** 支持）。
2. 选择 **Domain Type**（域类型）。
   - **Ddns Fallback**（**Ddns** 回退）— 用于 nsupdate 事件的域将回退到您在 **Domain Name**（域名）区域中指定的域。如果 GlobalProtect 客户端未加入任何域，或者它们加入的域与 DDNS 服务用于更新 DNS 服务器上的记录的域相同，请使用此选项。

     如果您选择 **Ddns Fallback**（**Ddns** 回退），并且未连接到域的用户登录 GlobalProtect，则他们的信息将会添加到在 DNS 服务器上创建的 Ddns 回退服务区下。

     如果登录到 GlobalProtect 的 GlobalProtect 客户端属于未在 DNS 服务器上配置的意外域，则 nsupdate 可能会失败；在这种情况下，请选择 **Ddns Override**（**Ddns** 覆盖）以使用 DNS 服务器已知的域覆盖未知域。
   - **Ddns Override**（**Ddns** 覆盖）— Prisma Access 仅使用您指定的域来更新 DNS 服务器，并覆盖所有其他域。如果 GlobalProtect 客户端登录到另一个域，DDNS 服务将使用您在此处指定的域来更新 DNS A 和 PTR 记录。
3. 在 **Domain Name**（域名）字段中选择用于更新回退或域名的 PTR 记录的域。
4. 选择 **DNS Server IP**（**DNS** 服务器 **IP**）地址。
5. 选择 **Authentication Type**（身份验证类型）（**TSIG** 或 **Kerberos**）。
6. （仅限 TSIG 部署）选择要用于 TSIG 的 **TSIG Key**（**TSIG** 密钥）。

   确保 TSIG 文件格式正确且文件类型为 .key。
   - 如果运行 Panorama 托管部署时使用 5.2.0 版本或更高版本的插件，并且选择了 Kerberos 身份验证类型，请通过 .key 文件上传身份验证密钥，该文件

 ©2025 Palo Alto Networks, Inc.

包含从 DNS 服务器检索到的 Kerberos 密钥的 base64 编码字符串，例如：
"ABCDEFGHIJKLMNOPQRSTUV5WXYZOUy5DT00ADUFabcDluaXN0cmF0b3IAAAABAAAAAAEAE

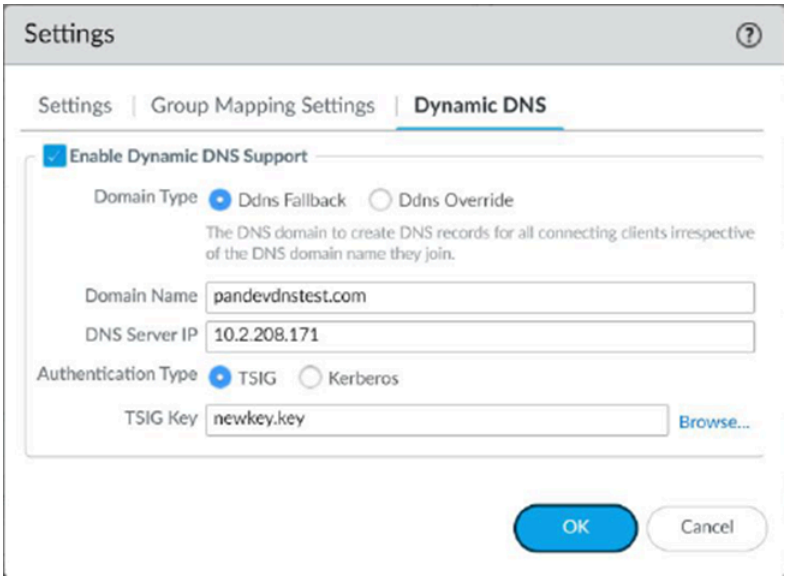
- 如果运行 Panorama 托管部署时使用的插件版本低于 5.1.0，并且您选择了 Kerberos 身份验证类型，请通过 .key 文件上传身份验证密钥，该文件包含从 DNS 服务器检索到的未编码 Kerberos 密钥表文件。

TSIG 文件应采用以下格式：

```
key "ddns-gp" { algorithm hmac-sha256; secret
 "aBCDEFGhiJklMNO89PQR+8stUVWX+YZAbcdeFgHI5J="; };
```

7. （仅限 Kerberos 部署）指定要使用的 Kerberos 选项。
   - 输入 **Kerberos Domain Controller**（**Kerberos** 域控制器）的 IP 地址。
   - 输入 **Kerberos Admin Server**（**Kerberos** 管理服务器）的 IP 地址。
   - 输入 **Kerberos User Name**（**Kerberos** 用户名）。
   - 输入要使用的 **Kerberos Key**（**Kerberos** 密钥）（密钥表）。

     请对 Kerberos 密钥使用 base64 编码，然后再上传该密钥。



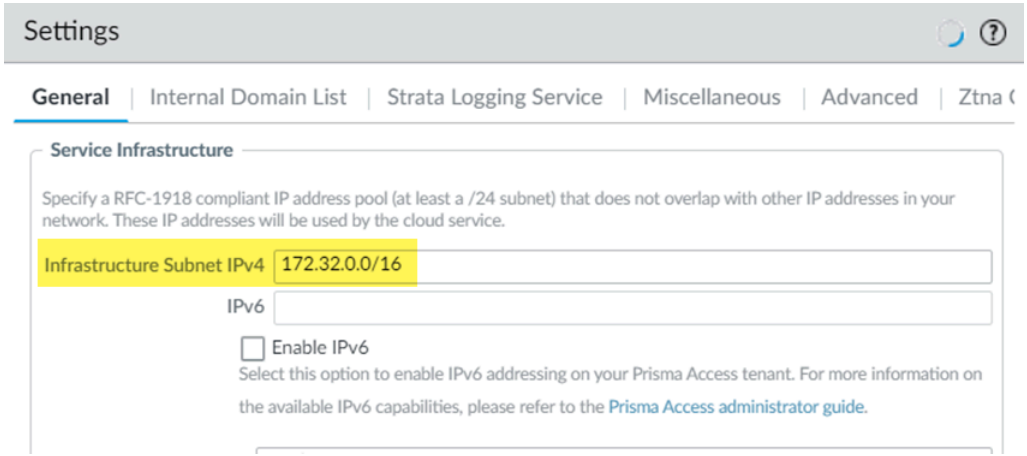
STEP 6 | **Save**（保存）更改。

©2025 Palo Alto Networks, Inc.

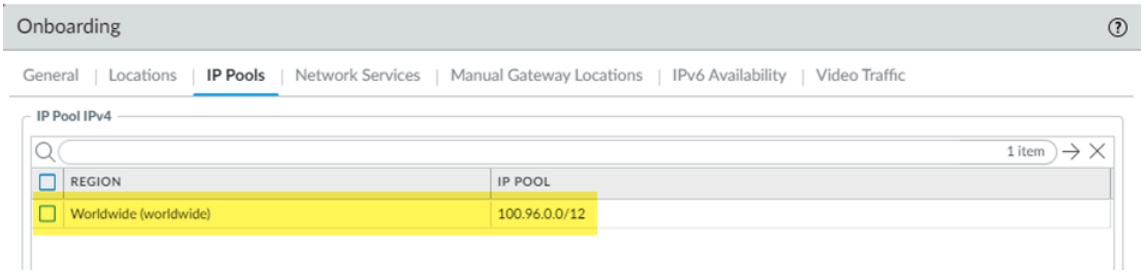
STEP 7 | 在 DNS 服务器上设置正向查找和反向查找服务区。

请参阅 IPAM 供应商的文档来设置这些服务区。在此步骤中，您需要在 Prisma Access 中输入 **Infrastructure Subnet**（基础架构子网）和 **Client IP Pool**（客户端 **IP** 池）。

- 要查找基础架构子网，请转到 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Service Setup**（服务设置），单击齿轮图标以编辑 **Settings**（设置），并记下 **Infrastructure Subnet IPv4**（基础架构子网 **IPv4**）。



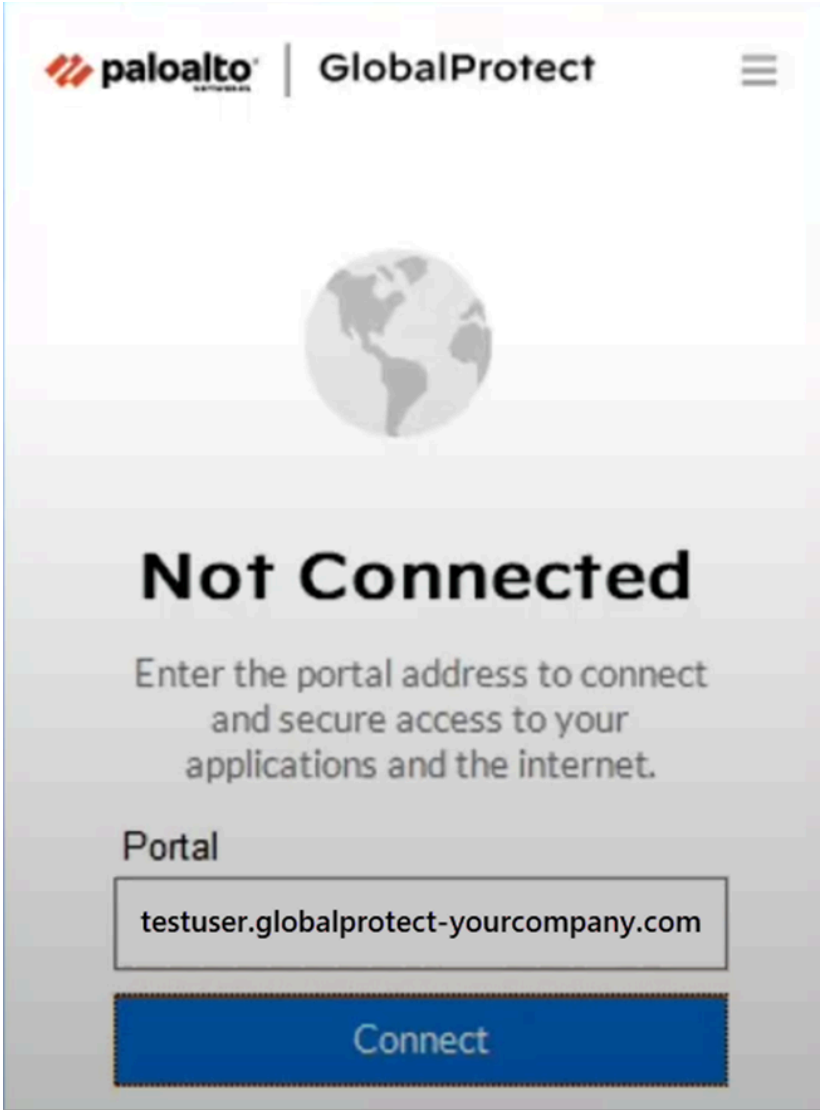
- 要查找 GlobalProtect 移动用户 IP 地址池，请转到 **Panorama** > **Cloud Services**（云服务） > **Mobile Users—GlobalProtect**（移动用户—**GlobalProtect**），选择 **Hostname**（主机名），选择 **IP Pools**（**IP** 池）并记下 **IP Pool IPv4**（**IP** 池 **IPv4**）。



 ©2025 Palo Alto Networks, Inc.

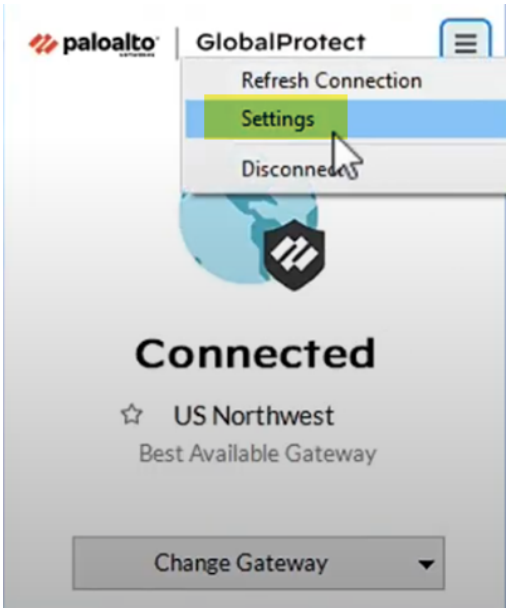
STEP 8 | 验证 IPAM DNS 服务器上的 DNS 记录是否正在更新。

1. 打开客户端计算机并连接到 Prisma Access GlobalProtect 网关。

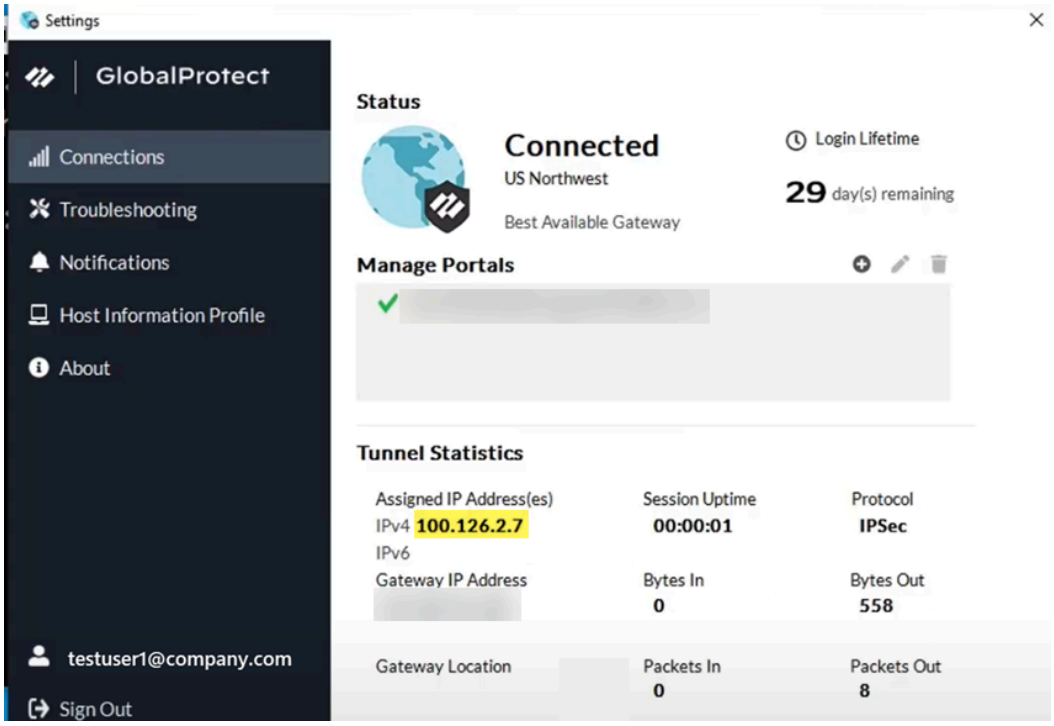


2. 选择 GlobalProtect **Settings**（设置），验证 Prisma Access 分配给用户的 GlobalProtect IP 地址。

 ©2025 Palo Alto Networks, Inc.

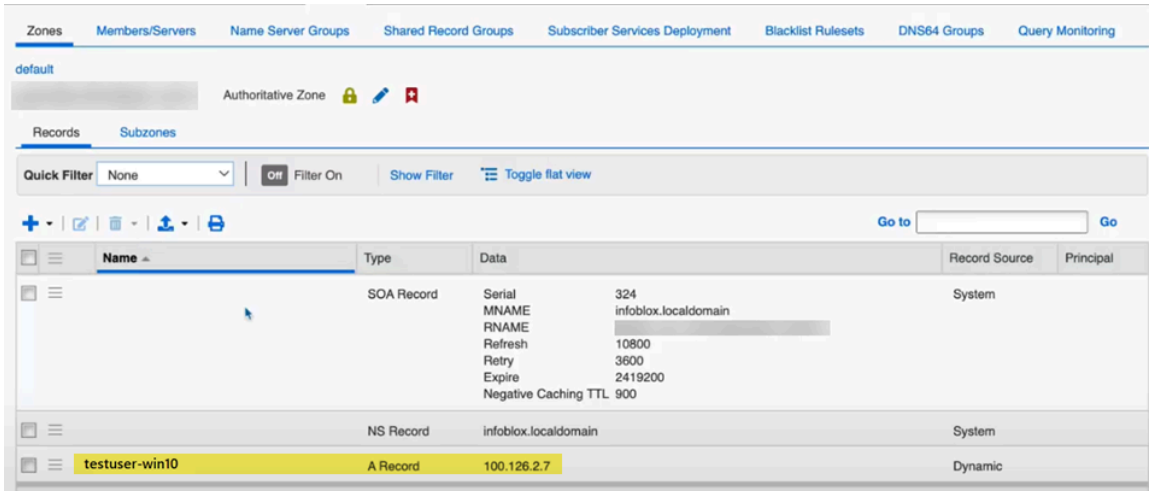


Assigned IP Address(es)（分配的 **IP** 地址） (100.126.2.7) 表明该 IP 地址来自 GlobalProtect IP 地址池 (100.126.0.0/16)。

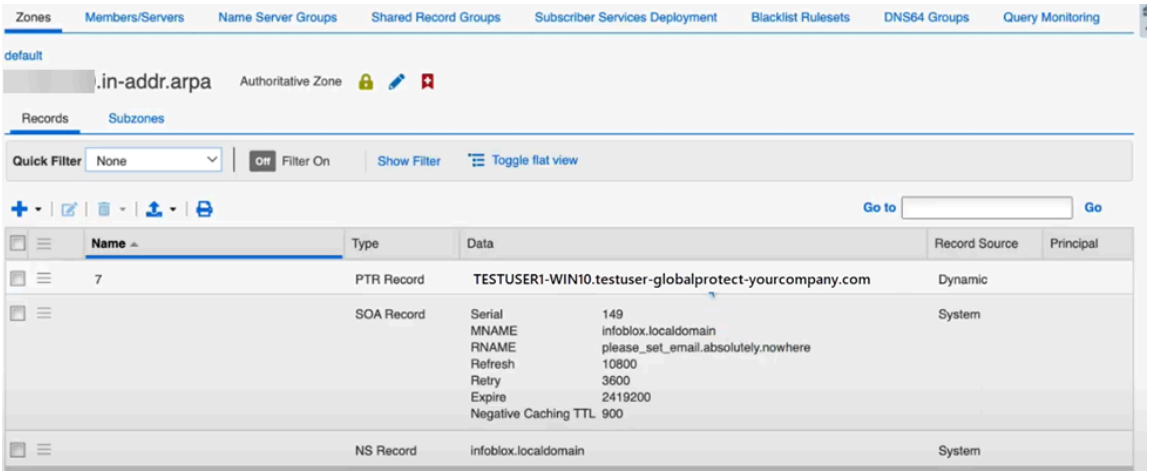


3. 从 IPAM DNS 服务器查看用户的记录。
   在此示例中，用户名为 `testuser1-win10`。

 ©2025 Palo Alto Networks, Inc.



DNS 反向查找还会在 PTR 记录中显示用户名。



4. 从 GlobalProtect 注销用户并检查记录，以确保 DNS 服务器已删除该用户的记录。

对“移动用户—GlobalProtect”的动态 DNS 注册支持

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama) • 由 Panorama 管理的新一代防火墙，且具备有效的 Strata Logging Service 许可证和云服务插件	❑ Prisma Access 许可证 ❑ Minimum Required Prisma Access Version：3.1.1 Preferred 或 Innovation ❑ 在运行 10.2 及更高版本的 Panoramas 上受支持（在运行 10.1 的 Panoramas 上不受支持） ❑ 您的客户端端点必须已加入域。

从 *Prisma Access (Managed by Panorama) 3.1.1* 开始的 *Prisma Access* 部署支持此功能。

Prisma Access (Managed by Strata Cloud Manager) 部署不支持此功能。

©2025 Palo Alto Networks, Inc.

当移动用户使用 GlobalProtect 远程连接到 Prisma Access 时，您企业中的 DNS 服务器不会使用 GlobalProtect 网关分配的 IP 地址进行更新。在启用动态域名系统 (DDNS) 之前，隧道 IP 地址与端点名称之间不存在映射关系，这种映射会被记录为地址和指针（A 和 PTR）记录。因此，您的 IT 管理员或用户管理软件无法将远程端点名称映射到 IP 地址。

在 Prisma Access 上启用 DDNS 功能后，Prisma Access 云服务插件每15分钟检查一次 Strata Logging Service 中的 GlobalProtect 事件，以捕获端点主机名、域名和隧道 IP 地址。该插件使用 NSUPDATE 在 DNS 服务器中动态创建 A 和 PTR 记录。

“移动用户—**GlobalProtect**”的动态 **DNS** 工作流

启用 DDNS 后，当移动用户使用 GlobalProtect 应用程序登录时：

阅读以下几节，了解 DDNS 的工作原理、准则和要求，以及如何启用。

1. GlobalProtect 在 GlobalProtect 端点和本地或 Prisma Access 网关之间建立 SSL 隧道。
2. GlobalProtect 通过隧道将移动用户设备的主机名、域名和隧道 IP 地址信息发送到本地或 Prisma Access 网关。
3. 本地网关或 Prisma Access 将此信息作为 GlobalProtect 事件转发到 Strata Logging Service。
4. Prisma Access 云服务插件每 15 分钟探测一次 Strata Logging Service 以更新 DNS 服务器。

   如果插件未收到来自 Strata Logging Service 的 GlobalProtect 事件，则最多重试请求五次。如果重试请求不成功，插件会每 15 分钟重试一次，最多重试 4 次。因此，插件可以在一小时的时间间隔内接收更新。

   如果需要提高更新的频率，可以输入 `debug plugins cloud_services set-gp-ddns-interval` 命令将更新间隔更改为五分钟。A 不需要更新时间间隔。如果将时间间隔更改为 5 分钟，则云服务插件最多可以更新 15000 条记录，网络延迟为 50 毫秒，并且可以在 20 分钟的时间间隔内接收更新。

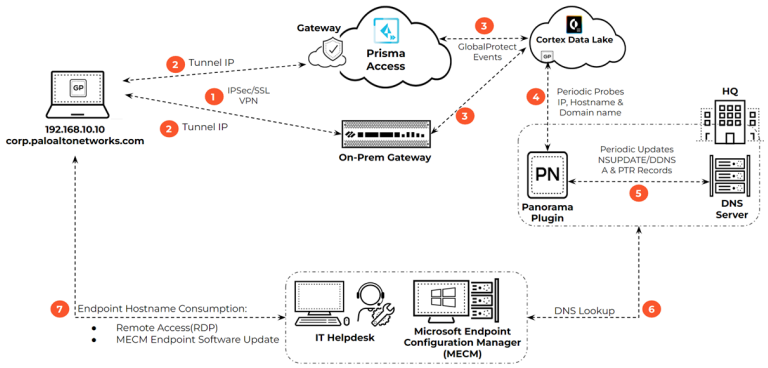
   - 使用以上命令更改时间间隔后，不需要进行提交。
   - 这些数值来自受控环境，实际操作条件可能会影响这些数值。
5. 云服务插件收到 Strata Logging Service 的更新后，便会将 A 和 PTR 记录打包为 NSUPDATE，并每 15 分钟更新一次主 DNS 服务器。

   如果使用 `debug plugins cloud_services set-gp-ddns-interval` 命令将时间间隔更改为五分钟，则该插件将每五分钟更新一次 DNS 服务器。

   如果插件无法通过 NSUPDATE 更新 DNS 服务器，则插件最多重试更新操作五次。如果更新不成功，插件将每 15 分钟重试一次更新操作，如果您将时间间隔更改为五分钟，则每五分钟重试一次，最多重试四次。因此，插件会尝试更新最多记录一小时（如果您使用 15 分钟的时间间隔）或 20 分钟（如果您使用 5 分钟的时间间隔）的事件，然后重新启动。
6. GlobalProtect 移动用户的 A 和 PTR 记录在 DNS 服务器中可用后，IT 管理员或企业软件通过 DNS 或 RDNS 查找使用这些记录，并解析端点名称或 IP 地址。
7. IT 管理员或端点管理软件使用此信息来管理端点或推送软件更新。

下图说明了此工作流。

 ©2025 Palo Alto Networks, Inc.



要查看连接故障日志，请针对 ***Mobile_User_Device_Group*** 选择 ***Dashboard***（指示板）> ***System Logs***（系统日志），或者选择 ***Monitor***（监视）> ***Logs***（日志）> ***System***（系统）。

动态 **DNS** 指南和要求

在启用 DDNS 之前，请确保您的部署和 DNS 服务器符合以下准则和要求：

- 您的客户端端点必须已加入域。
- 根据您的操作系统，将您的 GlobalProtect 客户端更新为以下 GlobalProtect 应用程序版本：
  - Windows：5.2.11 或更高版本
  - Mac：5.2.11 或更高版本
  - Linux：5.3.3 或更高版本
- 如果使用除 Prisma Access 之外的本地网关，请启用 Strata Logging Service。
- 需要最低版本为 8.6.1 且支持通过 NSUPDATE 进行 DDNS 更新的 Infoblox DNS 服务器。
- 多租户 Prisma Access 部署不支持 DDNS。
- 将 DNS 服务器中的身份验证密钥保存为 BASE64 格式，文件扩展名为 .key。您只能在 Prisma Access 中以此格式上载密钥。
- 在 DNS 服务器上启用 NTP，并确保它与 Prisma Access 的 NTP 相同。
- 在 Infoblox 中为反向 PTR 和转发 A 地址创建区。

可以使用新一代防火墙和 *Prisma Access* 在独立部署中部署动态 *DNS*。对于防火墙，本节中的所有先决条件都适用，您还必须拥有有效的 *Strata Logging Service* 许可证并且必须使用 Panorama 中的云服务插件进行日志记录。

为“移动用户 — GlobalProtect”启用 DDNS

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

要使用 GlobalProtect 移动用户的 A 和 PTR 记录更新 DNS 服务器，请完成以下步骤。

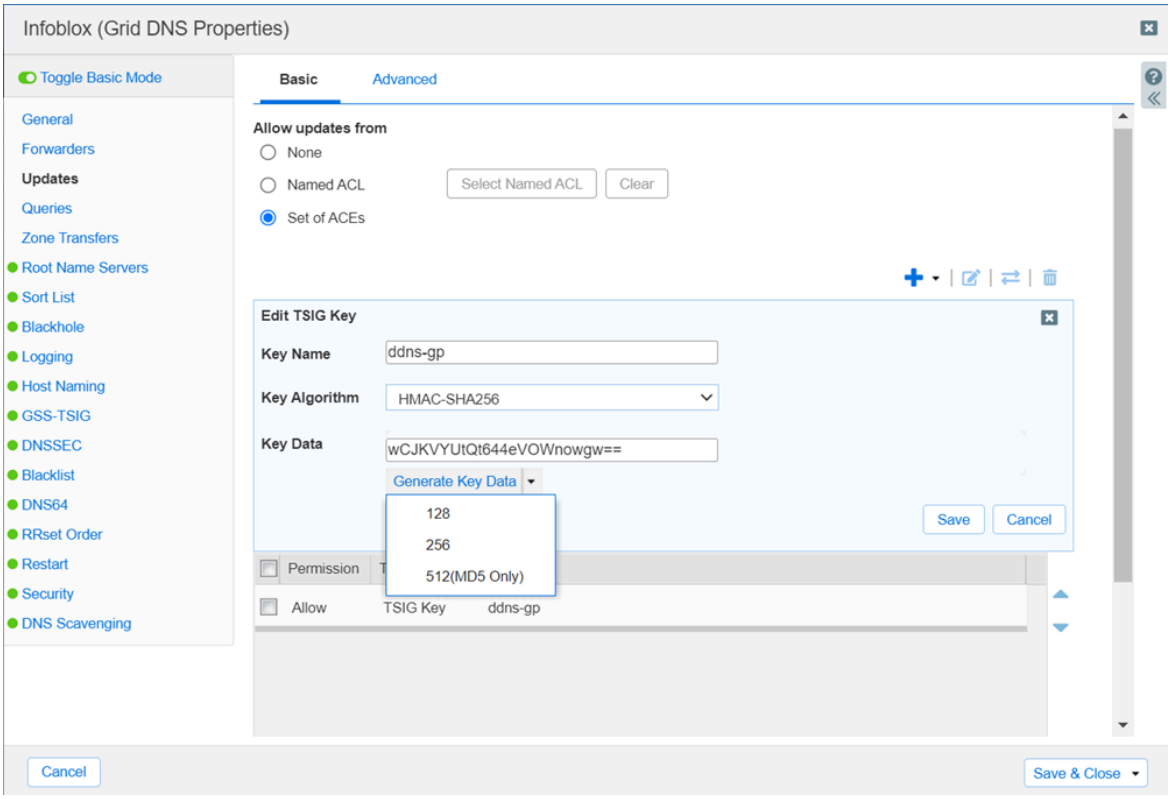
 ©2025 Palo Alto Networks, Inc.

STEP 1 | 在您的 DNS 服务器中创建一个身份验证密钥。

此示例使用 Infoblox 作为 *DNS* 服务器。

1. 登录到您的 DNS 服务器。
2. 选择 **Data Management**（数据管理） > **DNS** > **Grid DNS Properties**（网格 **DNS** 属性） > **Updates**（更新）。
3. 允许从 **Set of ACEs**（**ACE** 集）进行更新。
4. 填写详细信息后添加 **TSIG Key**（**TSIG** 密钥）。

   - 选择 ***256*** 位密钥算法。
   - 选择 ***Generate Key Data***（生成密钥数据）以创建新密钥。选择 ***256*** 位密钥数据。



5. 将密钥数据复制到以下格式的文件中，并以 .key 扩展名保存文件。

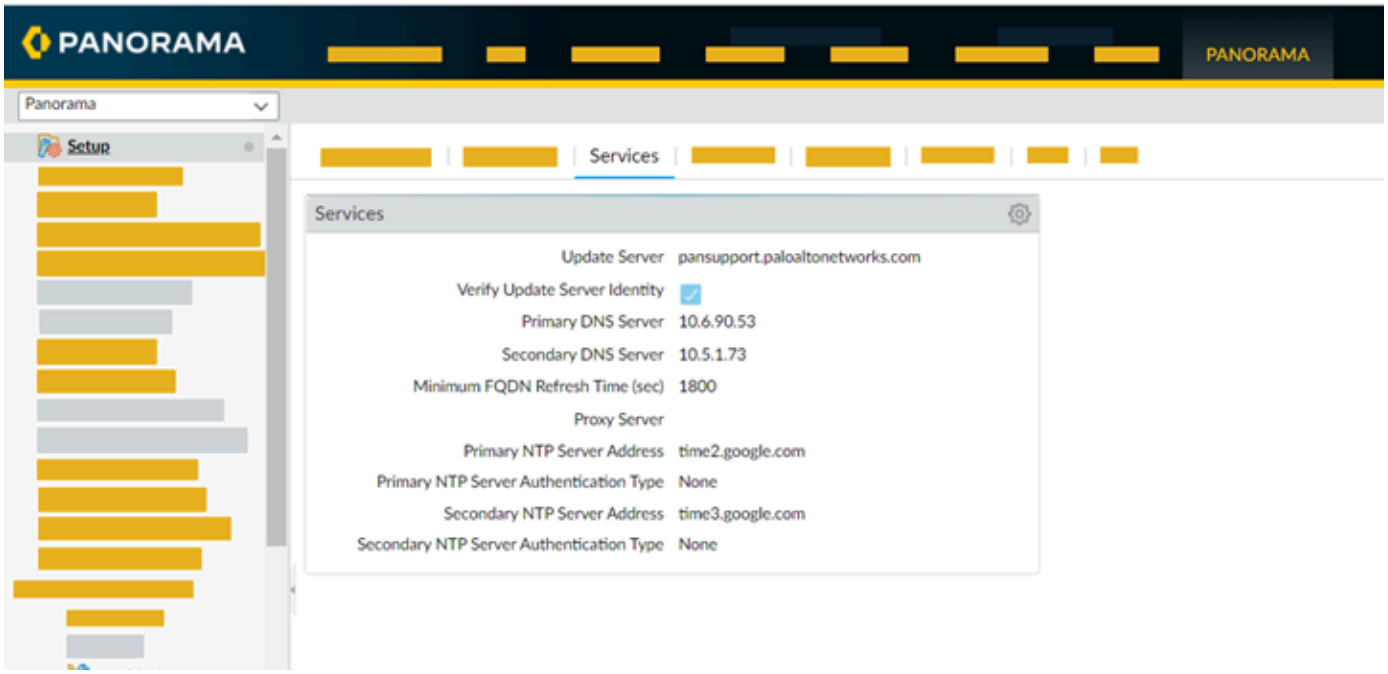
```
key "ddns-gp" { algorithm hmac-sha256; secret
 "wCJKVYUtQt644eVOWnowgw=="; };
```

您将此密钥上传至 Prisma Access 云服务插件（后面的步骤将会使用）。

©2025 Palo Alto Networks, Inc.

STEP 2 | 在您的 Prisma Access 部署时，指定您的 DNS 服务器作为主 DNS 服务器。

1. 选择 **Panorama** > **Setup**（设置） > **Services**（服务）。
2. 选择 **Edit**（编辑）以编辑设置并更新主 DNS 服务器详细信息。

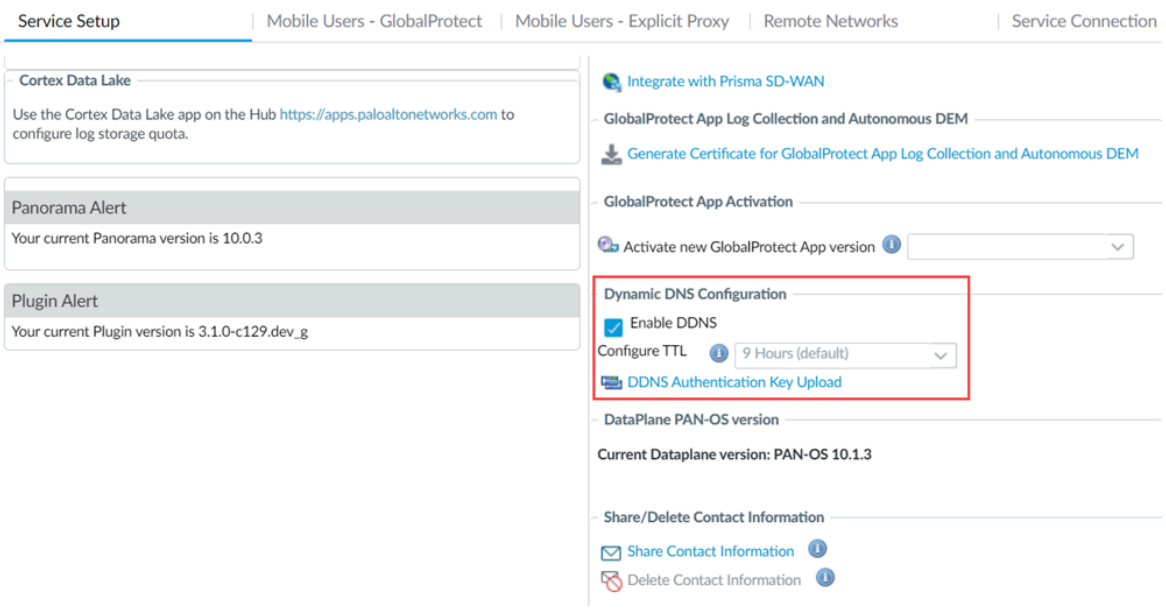


 ©2025 Palo Alto Networks, Inc.

STEP 3 | 配置 DDNS 设置。

1. 在 Panorama 中，选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Service Setup**（服务设置）。
2. 选择 **Service Operations**（服务操作） > **Dynamic DNS Configuration**（动态 **DNS** 配置），然后选择 **Enable DDNS**（启用 **DDNS**）。
3. （可选）选择 **Configure TTL**（配置 **TTL**）（也就是生存时间 (TTL) 值），将其配置为您希望 Prisma Access 刷新其缓存中的 FDQN 的频率。

   默认值设置为 9 小时。



4. 从 DNS 服务器上载您在步骤 1 中创建的 DDNS 身份验证密钥。

STEP 4 | **Commit to Panorama**（提交到 **Panorama**）。

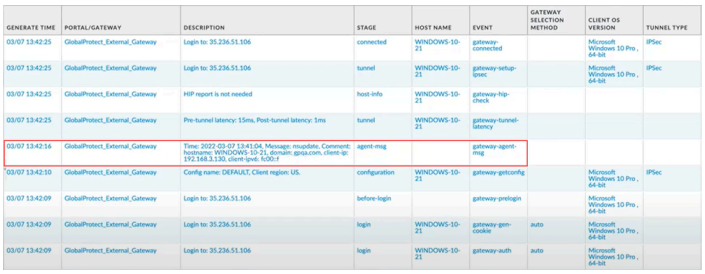
验证动态 DNS 配置

在何处可以使用？	需要提供什么？
• Panorama	• Prisma Access 许可证

启用 DDNS 后，请检查以下 Prisma Access 组件来监视日志并排除问题。

选择 **Monitor**（监视） > **Logs**（日志） > **GlobalProtect**。网关客户端消息包含主机名、域名和隧道 IP 地址信息。仅当端点是域或 AD 的一部分时，GlobalProtect 才会发送客户端消息。

©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	

在 Panorama CLI 中检查 `gp_ddns_support.log` 命令以查看其他 DDNS 日志。

在 Prisma Access GlobalProtect 部署中识别和隔离感染设备

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 许可证

Prisma Access 可以识别和隔离与 GlobalProtect 应用程序连接的感染设备。可以通过手动或自动将设备添加到隔离列表来完成此操作。隔离设备后，可以阻止隔离设备访问网络，以确保策略的一致性。

每个 Prisma Access 移动用户位置会在管理 Prisma Access 的 Panorama 与其最近的服务连接之间收发隔离信息。如果您有新一代防火墙或网关，则应让服务连接在 Panorama 和本地防火墙或网关之间重新分发隔离列表信息。还应该将隔离列表信息从 Panorama 重新分发到服务连接，以确保始终如一对 Prisma Access 中所有移动用户位置（网关）执行策略。

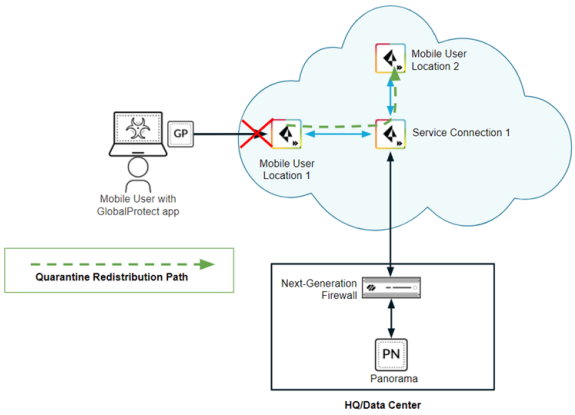
隔离名单重新分配的用例

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 许可证

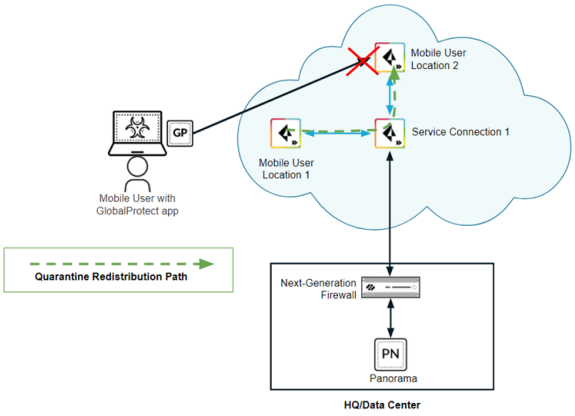
以下部分描述了一些常见 Prisma Access 部署场景，在这些场景中，隔离列表的重新分配对于对受损设备的一致政策执行非常有用。

 ©2025 Palo Alto Networks, Inc.

- 移动用户位置之间的隔离列表重新分配 — 在以下示例中，连接到移动用户位置 1 的 GlobalProtect 移动用户被攻陷并自动隔离。Prisma Access 根据策略阻止或限制隔离设备。

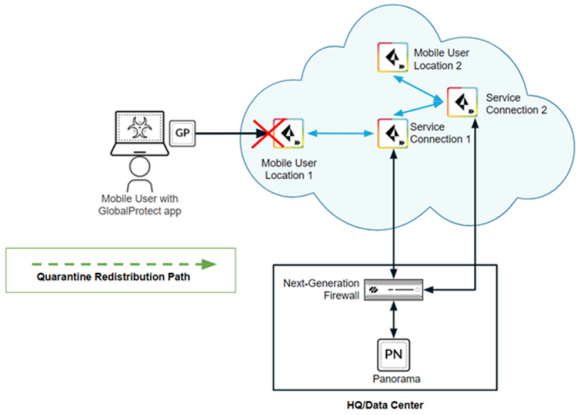


服务连接（本例中的服务连接 1）在其连接的所有移动用户位置之间重新分配隔离列表信息。由于移动用户位置2通过服务连接1接收重新分配的隔离列表信息，因此全球保护移动用户尝试连接到移动用户位置2也被阻止。



 ©2025 Palo Alto Networks, Inc.

- 移动用户位置之间的隔离列表重新分配，连接到不同的服务连接 — 在以下示例中，有两个移动用户位置，但它们连接到两个不同的服务连接。一名 GlobalProtect 用户尝试连接到移动用户位置1。移动用户位置 1 检测到 GlobalProtect 用户端点被破坏并将其隔离。

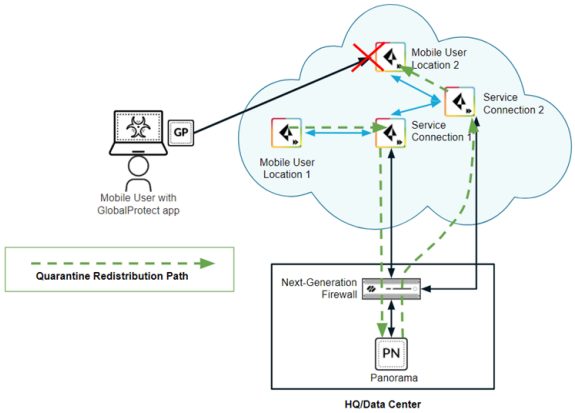


要将移动用户位置1的隔离列表信息重新分配到移动用户位置 2，请执行以下操作：

- 将服务连接 1 的隔离列表信息重新分配到 Panorama。
- 将隔离列表信息从Panorama重新分配到服务连接 2。

在此配置下，当 GlobalProtect 用户连接到移动用户位置 1 并被隔离时，隔离列表信息将从移动用户位置 1 重新分配到移动用户位置 2，任何对移动用户位置 2 的连接尝试都将被阻止。

如果 *GlobalProtect* 用户连接到移动用户位置*2*并被隔离，则此配置也是有效的；隔离列表信息从移动用户位置 *2* 重新分配到移动用户位置 *1*。



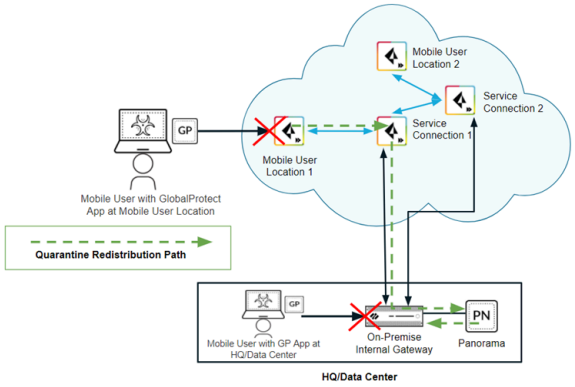
- 隔离列表在 **Prisma Access** 和新一代防火墙或网关之间的重新分发 — 在以下示例中，GlobalProtect 用户尝试连接到移动用户位置 1。移动用户位置 1 检测到 GlobalProtect 用

 ©2025 Palo Alto Networks, Inc.

户端点被破坏并将其隔离。移动用户随后前往公司的总部，并尝试再次登录。总部配备了新一代防火墙，配置为使用内部主机检测的 GlobalProtect 网关。

移动用户位置 1 通过服务连接 1 将隔离列表信息重新分配给 Panorama，Panorama 再将隔离列表信息重新分配给本地内部网关。当用户尝试从总部位置登录时，GlobalProtect 检测到本地网关被配置为内部网关，并在没有隧道的情况下连接到该网关。

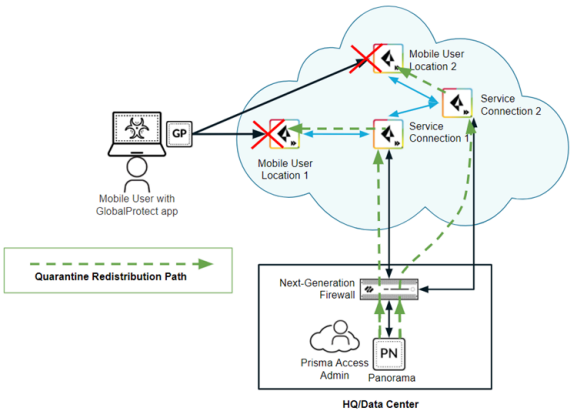
由于隔离名单信息已重新分配到本地网关，用户根据配置的用户策略在网关处被阻止。



如果将 Prisma Access 与新一代防火墙或网关配合使用，则应该配置 Panorama 将隔离列表信息重新分发到防火墙或网关、所有服务连接和 Panorama。

- 管理员在 **Panorama** 手动隔离移动用户 — 在此示例中，Prisma Access 管理员已手动将移动用户添加到管理 Prisma Access 设备的隔离列表中。管理员已在 Panorama、新一代防火墙和服务连接之间设置了重新分配。Panorama 将更新的隔离名单信息重新分配给防火墙和服务连接。服务连接随后将隔离列表信息重新分配到移动用户位置。

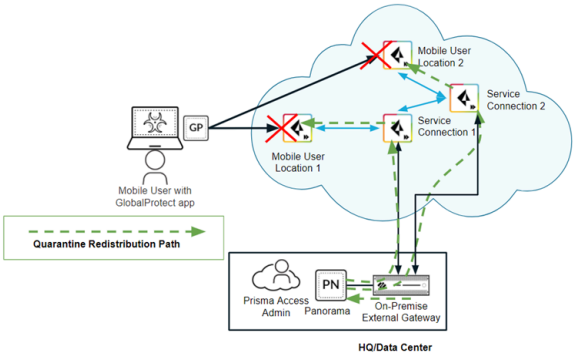
  移动用户已连接到移动用户位置 1。在移动用户位置1接收到更新的隔离名单信息后，用户被断开连接。如果用户尝试连接到移动用户位置 2，则连接会被阻止，移动用户会收到隔离通知。



 ©2025 Palo Alto Networks, Inc.

- 移动用户在本地网关处被自动或手动隔离 — 在这个例子中，有一个新一代防火墙被配置为总部或数据中心位置的外部网关。管理员已在外部网关手动隔离了一名移动用户。外部网关将隔离列表信息从外部网关重新分配到 Panorama。

  在 Panorama 接收到来自外部网关的更新隔离列表信息后，它将该信息重新分发给服务连接 1 和 2，然后再将其重新分发给移动用户位置 1 和 2。如果移动用户尝试连接到移动用户位置 1 或 2，则 Prisma Access 会阻止连接，并且用户会收到隔离通知。



在 Prisma Access 中配置隔离列表重新分发

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama) • Prisma Access (Managed by Strata Cloud Manager)	❑ Prisma Access 许可证

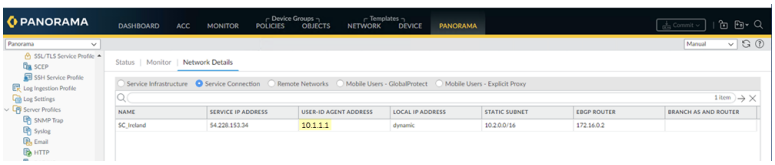
要在服务连接、管理 Prisma Access 的 Panorama 和新一代防火墙之间重新分发隔离信息，请完成以下步骤。

©2025 Palo Alto Networks, Inc.

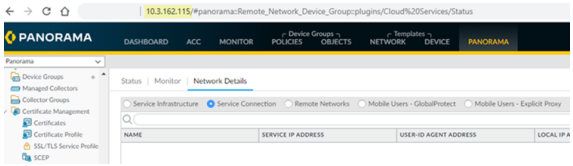
STEP 1 | 确保 Panorama 管理 IP 地址能够与要重新分发隔离列表信息的所有服务连接的 User-ID 代理地址进行通信。

为了使 Prisma Access 能够在 Panorama 和服务连接之间发送和接收隔离列表信息，需要在服务连接的 User-ID 代理地址和 Panorama 的管理 IP 地址之间进行通信。

- 要查找 **User-ID Agent Address**（**User-ID** 代理地址），请选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息） > **Service Connection**（服务连接） > **User-ID Agent Address**（**User-ID** 代理地址）。



- 要查找管理 Prisma Access 的 Panorama 的 IP 地址，请记下访问 Panorama 时 Web 浏览器中显示的 IP 地址。



STEP 2 | 允许 Prisma Access 重新分发隔离列表信息。

1. 在 Panorama 中，选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Service Setup**（服务设置）。
2. 单击齿轮图标以编辑设置。
3. 在 **Advanced**（高级）选项卡中，选择 **Enable Quarantine List Redistribution**（启用隔离列表重新分发）。

   启用隔离列表重新分发后，Prisma Access 可将从一个或多个移动用户位置（网关）收到的隔离列表信息重新分发到服务连接。

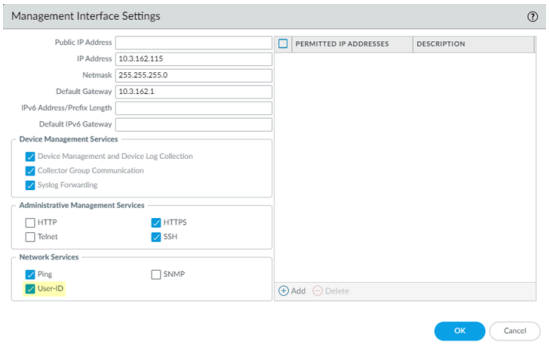


STEP 3 | **Commit**（提交）并 **Push**（推送）更改。

 ©2025 Palo Alto Networks, Inc.

STEP 4 | 通过配置管理接口设置，将 Panorama 配置为从 Prisma Access 接收隔离列表信息。

1. 在管理 Prisma Access 的 Panorama 中，选择 **Panorama** > **Setup**（设置） > **Interfaces**（接口）。
2. 选择 **Management**（管理）接口。
3. 选择 **User-ID**。



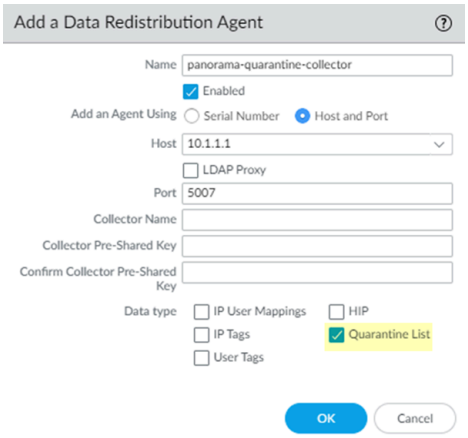
 ©2025 Palo Alto Networks, Inc.

STEP 5 | 配置数据重新分发代理，将隔离列表信息从服务连接重新分发到 Panorama。

1. 在管理 Prisma Access 的 Panorama 中，选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息） > **Service Connection**（服务连接）。
2. 记下每个服务连接的 **User-ID Agent Address**（**User-ID** 代理地址）（**Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息） > **Service Connection**（服务连接） > **User-ID Agent Address**（**User-ID** 代理地址））。
3. 选择 **Panorama** > **Data Redistribution**（数据重新分发） > **Agents**（代理）。
4. **Add**（添加）数据重新分发代理，为其提供 **Name**（名称）并选择 **Enabled**（已启用）。
5. 输入服务连接的 **User-ID Agent Address**（**User-ID** 代理地址）作为 **Host**（主机），输入 5007 作为 **Port**（端口）。

   确保您的网络不会阻止 *Panorama* 和 *Prisma Access* 之间对此端口的访问。

6. （可选）如果您已将此服务连接配置为收集器（**Device**（设备） > **Data Redistribution**（数据重新分发） > **Collector Settings**（收集器名称）），请输入 **Collector Name**（收集器名称）和 **Collector Pre-Shared Key**（收集器预共享密钥）
7. 选择 **Quarantine List**（隔离列表）；然后单击 **OK**（确定）。



8. 对 Prisma Access 部署中的所有服务连接重复步骤 5。

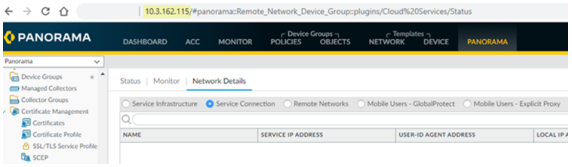
STEP 6 | 选择 **Commit**（提交） > **Commit to Panorama**（提交到 **Panorama**），以在管理 Prisma Access 的 Panorama 上本地保存更改。

 ©2025 Palo Alto Networks, Inc.

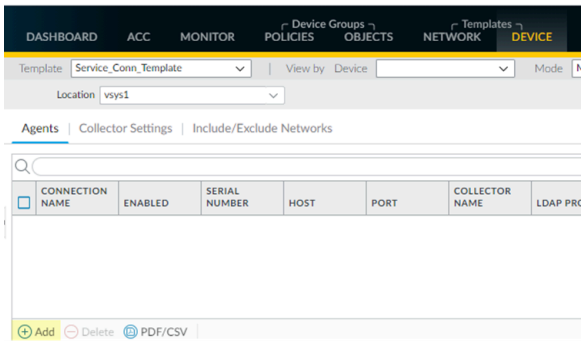
STEP 7 | 配置数据重新分发代理，将隔离列表信息从 Panorama 重新分发到服务连接。

1. 查找管理 Prisma Access 的 Panorama 的管理 IP 地址。

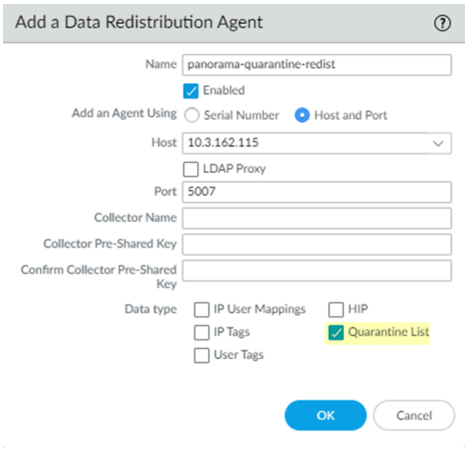
   当您访问 Panorama 时，此地址将显示在 Web 浏览器地址栏中。



2. 确保您位于 **Service_Conn_Template** 模板中，然后选择 **Device**（设备） > **Data Redistribution**（数据重新分发） > **Agents**（代理）。



3. **Add**（添加）数据重新分发代理，为其提供 **Name**（名称）并选择 **Enabled**（已启用）。
4. 输入 Panorama 设备的管理 IP 地址作为 **Host**（主机），输入 5007 作为 **Port**（端口）。



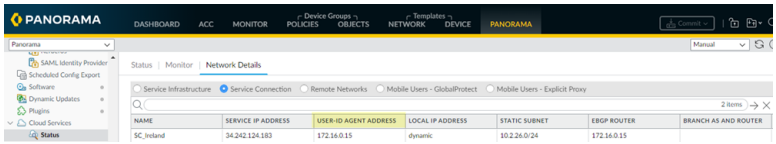
5. 选择 **Quarantine List**（隔离列表）；然后单击 **OK**（确定）。

 ©2025 Palo Alto Networks, Inc.

STEP 8 | 配置数据重新分发代理，将隔离列表信息从服务连接重新分发到移动用户网关。

1. 在管理 Prisma Access 的 Panorama 中，选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息） > **Service Connection**（服务连接）。
2. 记下要重新分发隔离列表信息的服务连接的 **User-ID Agent Address**（**User-ID** 代理地址）。

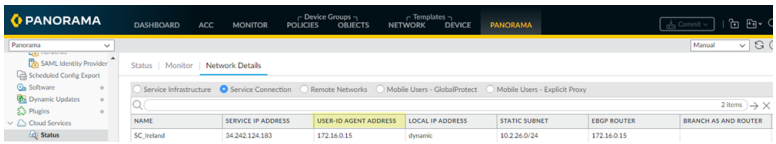
   由于所有服务连接都具有相同的重新分发隔离列表信息，因此请选择任意服务连接。您还可以配置多个服务连接。



3. 确保您位于 **Mobile_User_Template** 中，然后选择 **Device**（设备） > **Data Redistribution**（数据重新分发） > **Agents**（代理）。
4. **Add**（添加）数据重新分发代理，为其提供 **Name**（名称）并选择 **Enabled**（已启用）。
5. 输入服务连接的 **User-ID Agent Address**（**User-ID** 代理地址）作为“主机”，输入 **5007** 作为“端口”。

   确保您的网络不会阻止 *Panorama* 和 *Prisma Access* 之间对此端口的访问。

6. （可选）如果您已将此服务连接配置为收集器（**Device**（设备） > **Data Redistribution**（数据重新分发） > **Collector Settings**（收集器名称）），请输入 **Collector Name**（收集器名称）和 **Collector Pre-Shared Key**（收集器预共享密钥）。
7. 选择 **Quarantine List**（隔离列表）；然后单击 **OK**（确定）。



8. **Commit and Push**（提交并推送）更改。

STEP 9 | 通过选择 **Panorama** > **Device Quarantine**（设备隔离）查看隔离列表信息。

有关详细信息，请参阅 GlobalProtect 管理员指南中的查看隔离设备信息。

移动用户中的 IPv6 流量陷坑 — GlobalProtect 部署

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

在可以同时处理 IPv4 和 IPv6 流量的双栈端点中，GlobalProtect 应用程序通过 GlobalProtect VPN 隧道将需要保护的移动用户 IPv4 流量发送到 Prisma Access。然而，移动用户的 IPv6 流量不会发

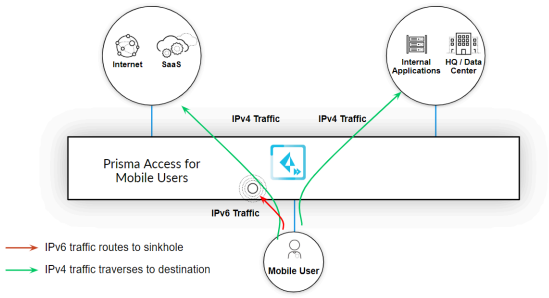
 ©2025 Palo Alto Networks, Inc.

送到 Prisma Access 默认情况下，而是发送到端点上的本地网络适配器。为了减少基于 IPv6 的威胁的攻击面，Palo Alto Networks 建议您配置 Prisma Access 导致 IPv6 流量瘫痪。由于端点可以自动回退到 IPv4 地址，因此您可以为移动用户的互联网流量提供安全、不间断的用户体验。

默认 *IPv6* 路由优先于其他路由。但是，如果通过物理网络接口存在更具体的 *IPv6* 路由，或者您指定了物理接口的 *IPv6* 源地址，则此类流量将被发送到本地网络适配器。

此外，Palo Alto Networks 建议您配置 GlobalProtect 以完全 禁用本地网络适配器上的网络流量。如果您拥有混合 Prisma Access 部署，其中本地下一代防火墙配置为 GlobalProtect 网关，则可以 在本地 GlobalProtect 网关上配置 IPv6 sinkhole 功能。

您可以配置 Prisma Access 这样它就会阻塞所有移动用户的 IPv6 流量。启用此功能时，除 IPv4 地址外，Prisma Access 还会为连接端点分配一个 IPv6 地址。然后，它将 IPv6 流量路由到 Prisma Access，并使用内置的安全策略将其丢弃，如下图中所示。



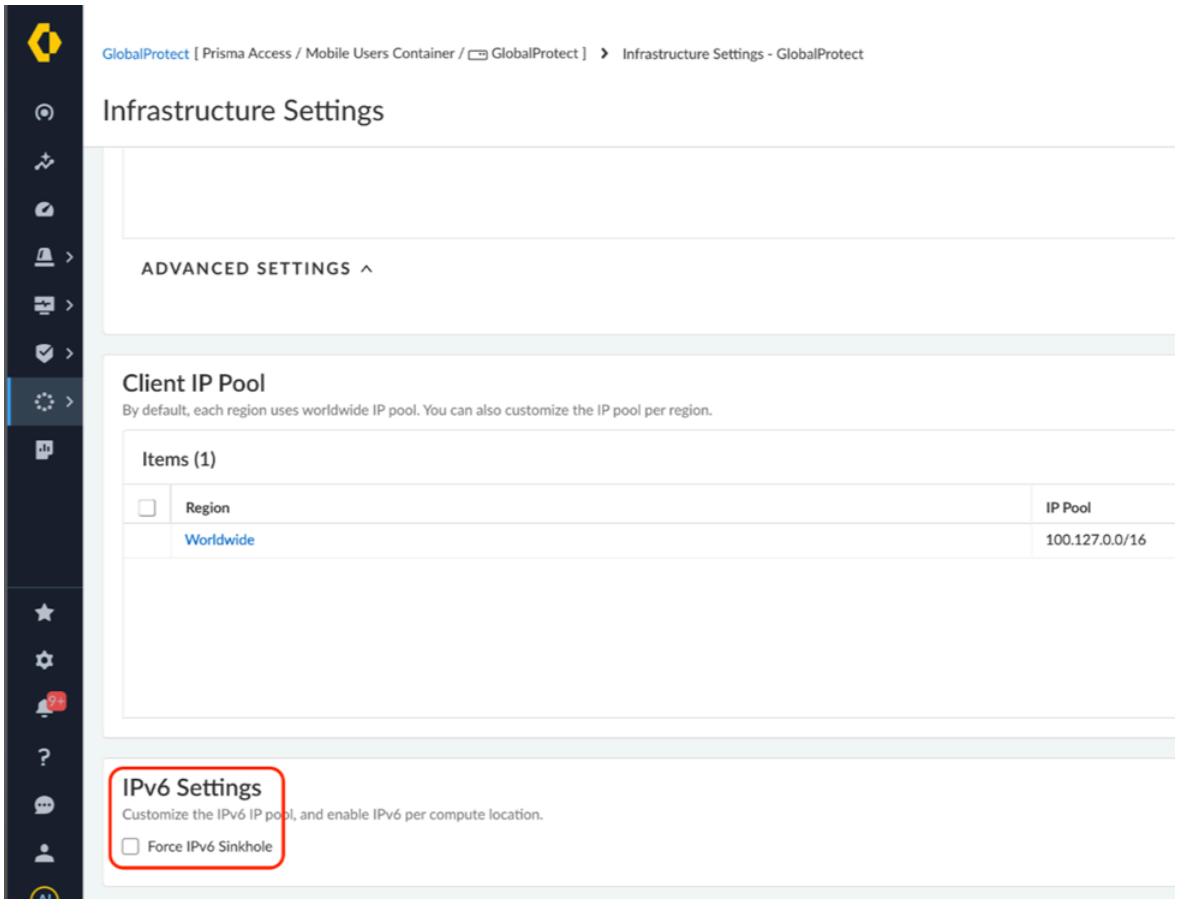
配置 Prisma Access 为了使它吸收所有移动用户 IPv6 流量，请完成以下步骤。

©2025 Palo Alto Networks, Inc.

- Prisma Access (Managed by Strata Cloud Manager) 部署：

  转到 工作流程 > **Prisma Access** 设置 > 移动用户 > **GlobalProtect** 设置 > 高级设置 并选择 强制 **IPv6 Sinkhole**。

  Prisma Access 使用 fc00:0:0:0:0:0:0:0/64 作为 sinkhole 地址。



- Prisma Access (Managed by Panorama) 部署：

  1. 使用与登录到用于管理 Prisma Access 的 Panorama 相同的 IP 地址，以管理员级权限打开 CLI 会话。
  2. 输入 `configure` 进入配置模式。
  3. 输入 **`set plugins cloud_services mobile-users ipv6 yes`** 命令。

     如果您以后需要禁用此命令，请输入 **`set plugins cloud_services mobile-users ipv6 no`**。
  4. 输入 **`Commit`** 以在本地保存更改。
  5. 输入 **`exit`** 退出配置模式。
  6. 输入 **`commit-all shared-policy include-template yes device-group Mobile_User_Device_Group`** 提交并推送您的更改，并使其在 Prisma Access。

 ©2025 Palo Alto Networks, Inc.

配置 GlobalProtect 以禁用对本地网络的直接访问

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证 ❑ 在所有 macOS 和 Windows GlobalProtect 端点上均受支持。从 GlobalProtect 应用程序 6.0.0 版本开始，在 Linux 端点上受支持。

为了确保所有移动用户流量都发送到 Prisma Access，您可以完全禁用发送到本地适配器的传出连接（包括本地子网流量）。您可以对 GlobalProtect 网关进行配置更改，以停用发送到本地适配器的所有传出连接。

您可以在 Panorama 上或已配置为 GlobalProtect 网关的本地防火墙上执行以下步骤。

启用 ***No direct access to local network***（禁止直接访问本地网络）设置，以降低不可信网络（例如恶意 *Wi-Fi* 访问点）中的风险。

STEP 1 | 选择 **Network**（网络） > **GlobalProtect** > **Gateways**（网关）。

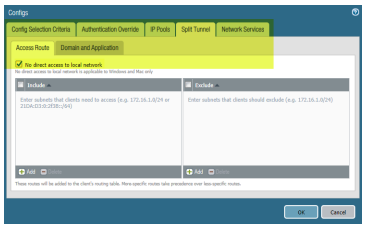
STEP 2 | 选择现有 GlobalProtect 网关或 **Add**（添加）新网关。

STEP 3 | 选择 **Agent**（代理） > **Client Settings**（客户端设置）。

STEP 4 | 选择 **DEFAULT**（默认）配置，或选择 **Add**（添加）以添加新配置。

STEP 5 | 选择 **Split Tunnel**（拆分隧道）；然后选择 **No direct access to local network**（无法直接访问本地网络）。

禁用本地网络访问后，所有流量（包括 *IPv4* 和 *IPv6* 流量）将会发送到本地适配器。此外，您将无法访问本地子网上的资源，例如打印机。根据访问路由、目标域和应用程序拆分隧道流量仍然按预期工作。



STEP 6 | （仅限 Panorama 和 Prisma Access 部署）在本地提交您的更改，使其在 Panorama 中生效。

1. 选择 **Commit**（提交） > **Commit to Panorama**（提交到 **Panorama**）。
2. 确保您的更改属于 **Commit Scope**（提交范围）的一部分。
3. 单击 **OK**（确定）保存对推送范围进行的更改。
4. **Commit**（提交）更改。

 ©2025 Palo Alto Networks, Inc.

STEP 7 | **Commit**（提交）并 **Push**（推送）更改，使其在 Prisma Access 中生效。

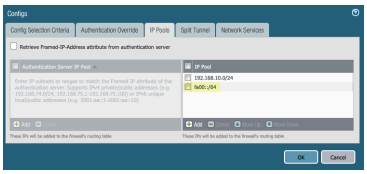
在本地网关上设置 IPv6 Sinkhole

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

如果您有一个混合部署，使用配置为 Prisma Access 网关的新一代防火墙，请在本地网关上执行以下任务以丢弃IPv6流量。

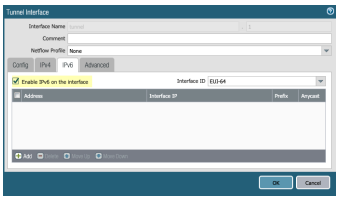
STEP 1 | 将IPv6 IP池添加到您的GlobalProtect代理配置中。

1. 选择 **Network**（网络） > **GlobalProtect** > **Gateways**（网关）。
2. 选择一个现有的 GlobalProtect 网关或 **Add**（添加）一个新的。
3. 选择 **Agent**（代理） > **Client Settings**（客户端设置）。
4. 选择要修改的代理配置或 **Add**（添加）一个新的代理配置。
5. 选择 **IP Pools**（**IP** 池），然后 **Add**（添加）一个 IPv6 池以分配给连接到 GlobalProtect 网关用于移动网络流量的端点上的虚拟网络适配器，然后单击 **OK**（确定）。



STEP 2 | 在接口上启用 IPv6。

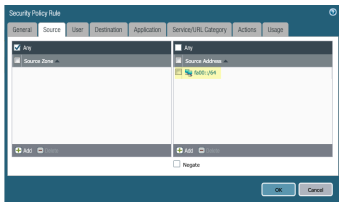
1. > > 选择设备接口隧道，并选择您用于移动用户流量的隧道接口。
2. 选择 **IPv6**，然后选择 **Enable IPv6 on the interface**（在接口上启用 **IPv6**）。



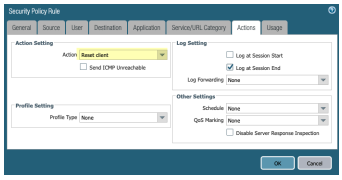
 ©2025 Palo Alto Networks, Inc.

STEP 3 | 1添加安全策略以设置 TCP 重置操作，该操作将终止与您在步骤中配置的 IP 池匹配的 IPv6 源流量的会话。

1. 选择 **Policies**（策略） > **Security**（安全），并 **Add**（添加）新的安全策略。
2. 1在规则中设置源地址，以匹配您在步骤中配置的IP池。



3. 选择操作；然后，选择重置客户端的操作设置并点击确定。



STEP 4 | **Commit**（提交）更改。

STEP 5 | （可选）在您部署的所有网关防火墙上执行此任务。

使用 Prisma Access 重新分发 HIP 信息

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

为了确保一致地执行主机信息配置文件 (HIP) 策略并简化策略管理，您可以将从使用 Prisma Access 的 GlobalProtect 应用程序的移动用户和远程网络用户接收到的 HIP 信息重新分发到企业中的其他网关、防火墙和 Panorama 设备，包括管理的 Panorama。Prisma Access

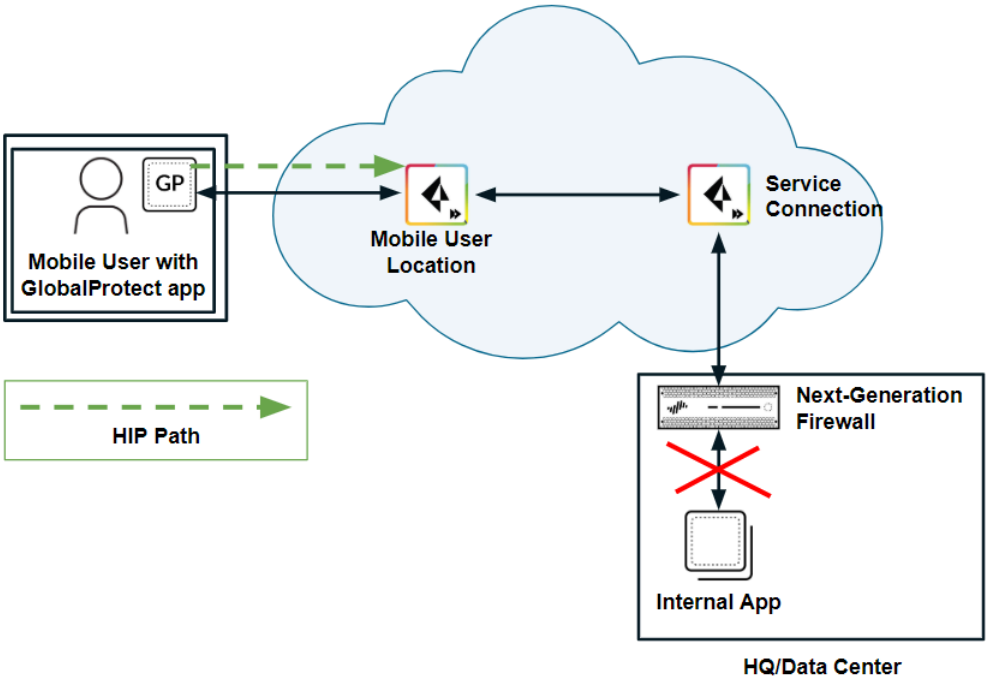
以下部分描述了一些常见的 Prisma Access 部署场景，其中 HIP 重新分发对于一致地执行策略和查看 HIP 报告非常有用：

- 从 **Prisma Access** 重新分发 **HIP** 到新一代防火墙 — 如果您的组织在数据中心或总部位置有新一代防火墙，并且已使用基于 HIP 的安全策略配置了该防火墙，则在将 HIP 从 Prisma Access 重新分发到防火墙之前，您无法对 Prisma Access 移动用户强制执行这些策略。

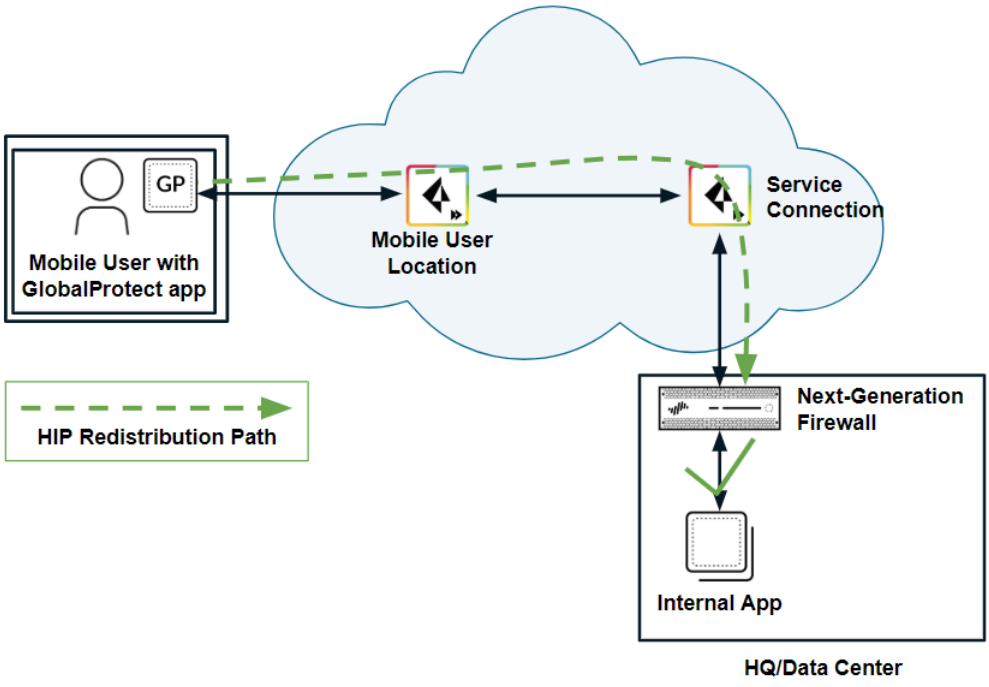
  下图显示了一位移动用户，其终端受到 GlobalProtect 应用程序的保护。用户尝试访问一个位于总部/数据中心的内部应用，该应用的访问由采用基于 HIP 的安全策略的新一代防火墙控制。当用户登录到 GlobalProtect 应用程序时，该应用程序收集 HIP 信息并将其发送到 Prisma

 ©2025 Palo Alto Networks, Inc.

Access；但是，Prisma Access 不会将此信息重新分发到本地防火墙。由于防火墙没有用户的 HIP 信息，因而阻止用户访问该应用程序。



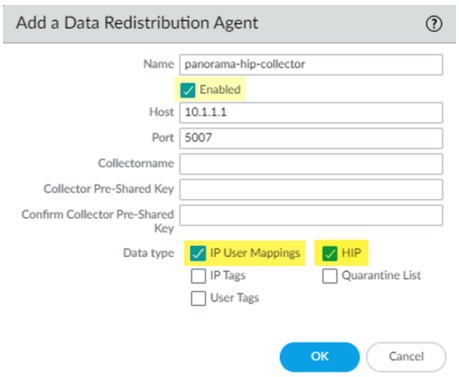
通过 HIP 重新分发，您可以移动用户的 HIP 信息分发到本地防火墙。防火墙可以根据配置的安全策略检查用户的 HIP 信息，并授予用户访问应用程序的权限。



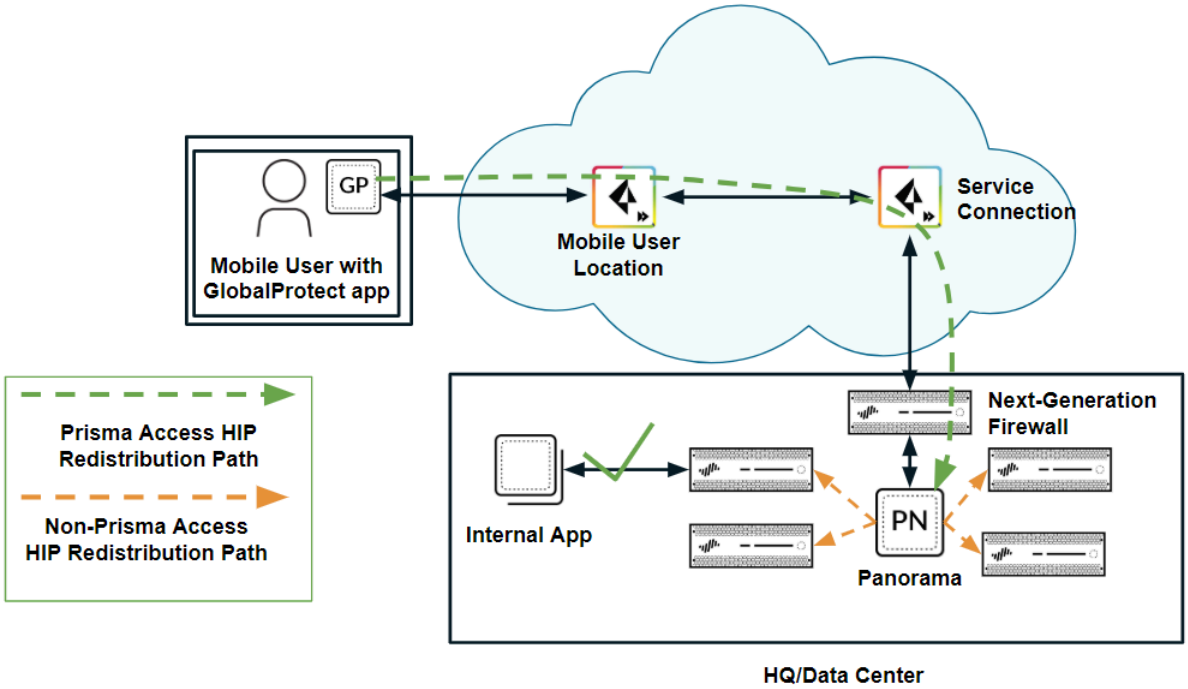
要将 HIP 信息从 Prisma Access 重新分发到防火墙，您要允许 Prisma Access 重新分发 HIP 信息，然后，对于 Panorama 9.1.*x* 设备，在防火墙上 **Add**（添加） **User-ID Agent**（**User-ID** 代理）（**Panorama** > **User Identification**（用户标识） > **User-ID Agents**（**User-ID** 代理），

 ©2025 Palo Alto Networks, Inc.

对于 Panorama 10.*x* 设备，在防火墙上添加 **Panorama** > **Data Redistribution**（数据重新分发），同时指定 Prisma Access **User-ID Agent Address**（**User-ID** 代理地址）（**Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息） > **Service Connection**（服务连接） > **User-ID Agent Address**（**User-ID** 代理地址））作为 **Host**（主机）（以下示例中为 10.1.1.1），并指定 **5007** 作为 **Port**（端口）。



- **HIP** 从 **Prisma Access** 重新分发到 **Panorama** — 如果您的组织有多个防火墙或网关，并且使用基于 HIP 的安全策略，则可以通过在 Panorama 中创建一个 User-ID 代理并指定 Prisma Access **User-ID Agent Address**（**User-ID** 代理地址）作为 User-ID **Host**（主机），将 HIP 信息从 Prisma Access 重新分发到管理 Prisma Access 的 Panorama。然后，使用与您用于将 User-ID 信息重新分发到受管理防火墙并为内部应用程序和资源执行一致策略的相同工作流程，您可以将 HIP报告从该 Panorama 设备重新分发到您企业中的其他受管理 Panorama 设备、网关、防火墙和虚拟系统，如下图所示。



或者，通过在每个设备上创建 User-ID 代理，您可以在企业中配置每个内部防火墙或网关，以直接从 Prisma Access 收集 HIP 信息，而无需使用 Panorama 作为中心位置。请注意，Prisma

 ©2025 Palo Alto Networks, Inc.

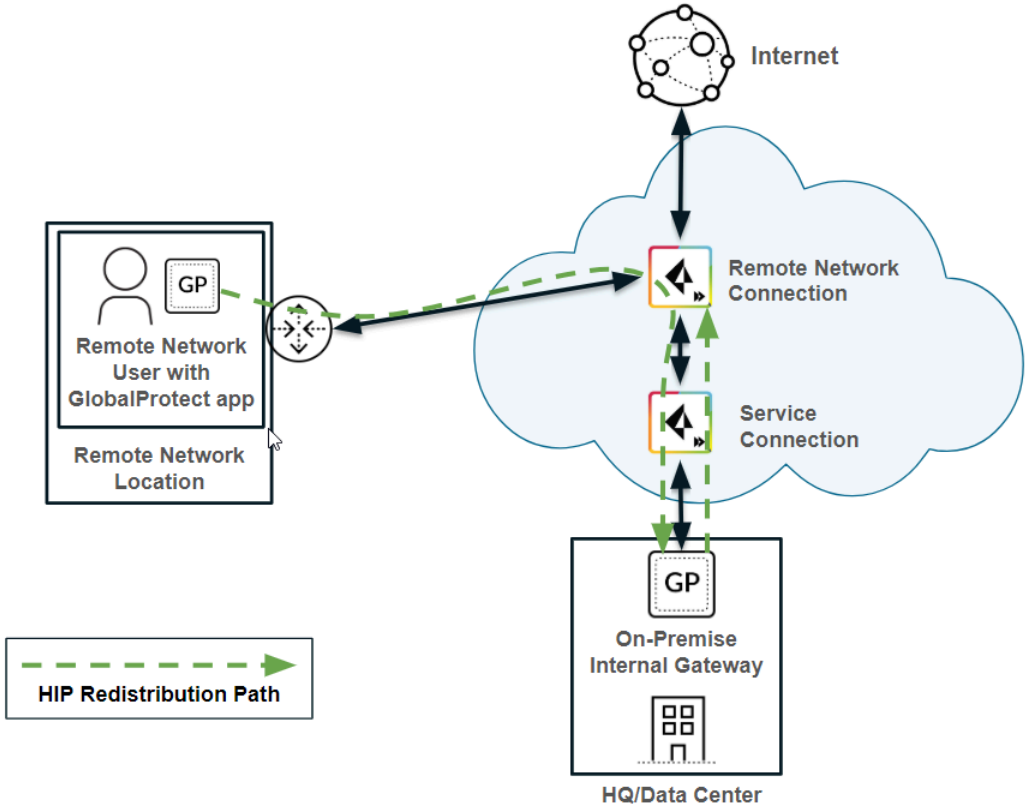
Access 使用服务连接发送 HIP 信息，并且，如果 Prisma Access 发送大量 HIP 报告，服务连接的带宽消耗可能会增加。

- **HIP 从远程网络的用户重新分发到 Prisma Access** — 之前的用例展示了 Prisma Access 从移动用户收集 HIP 信息。如果您想在 Prisma Access 中为远程网络位置的用户应用基于 HIP 的策略，则需要一种方法将远程网络用户的 GlobalProtect 应用程序中的 HIP 信息分发到 Prisma Access。

  以下示例显示了一位位于远程网络位置的用户，其互联网访问位于远程网络连接上。在 Prisma Access 中，您可以通过在 **Remote_Network_Device_Group** 或共享设备组中创建的安全策略控制用户在远程网络位置的互联网访问。要在远程网络位置为用户正确执行政策，您需要配置 Prisma Access 以从内部网关检索用户的 HIP 信息。

  在该示例中，位于总部/数据中心的 GlobalProtect 网关被配置为使用内部主机检测（用于检查用户 GlobalProtect 应用程序中的 HIP 信息）的内部网关。内部网关检测到用户在远程网络位置内，并收集用户的 User-ID 和 HIP 信息。

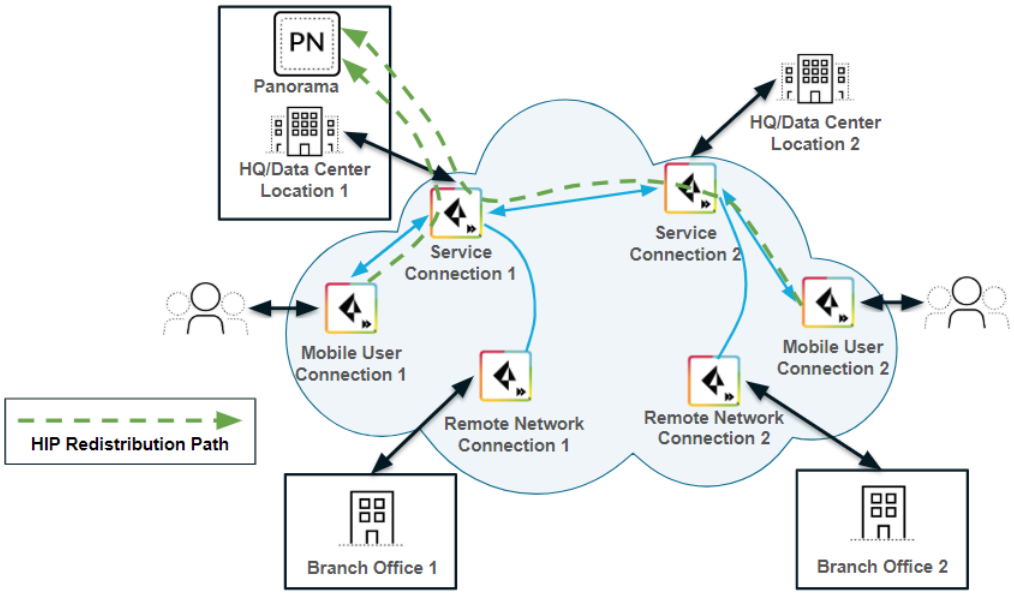
  要将此 HIP 信息从内部网关分发到 Prisma Access，请在 Panorama 中创建一个 User-ID 代理，并指定内部网关的 IP 地址作为主机。



- 查看来自 **Panorama** 的详细 **HIP** 日志 — 当移动用户使用 GlobalProtect 应用程序登录时，该应用程序会将 HIP 信息发送到 Prisma Access。Panorama 从 Strata Logging Service 中检索日志结果，以查看 HIP 匹配日志的结果（**Monitor**（监控） > **Logs**（日志） > **HIP Match**（**HIP** 匹

©2025 Palo Alto Networks, Inc.

配）；但是，在配置 Panorama 以从 Prisma Access 重新分发 HIP 报告详细信息到 Panorama 之前，您无法查看详细的 HIP 报告。

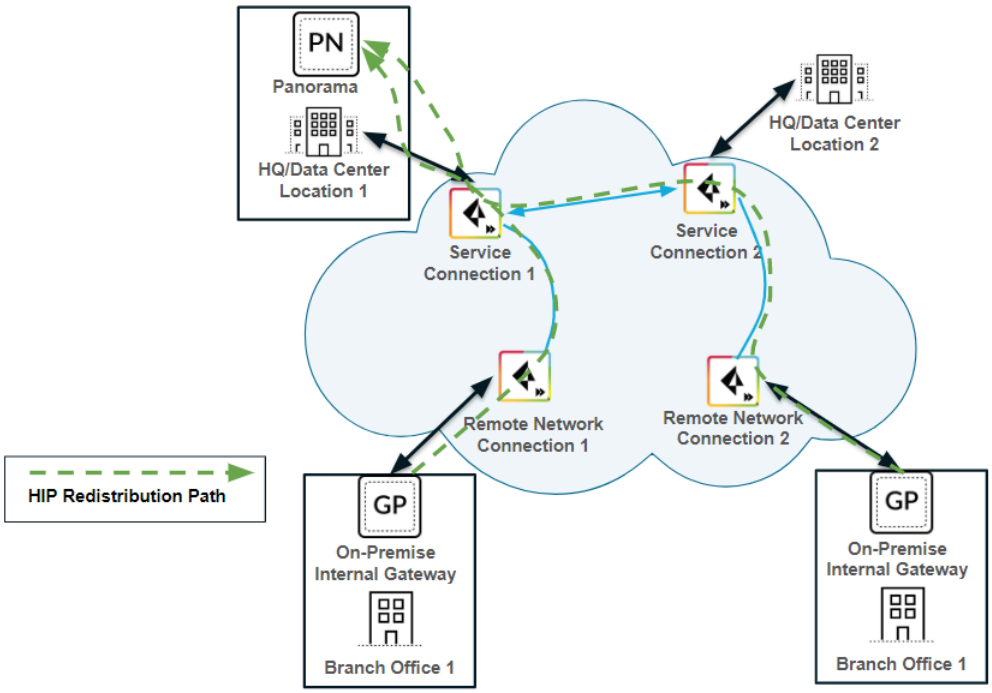


要将移动用户的 HIP 详细信息重新分发到 Panorama，请在 Panorama 中创建一个 User-ID 代理，并将 **User-ID Agent Address**（**User-ID** 代理地址）（**Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息） > **Service Connection**（服务连接） > **User-ID Agent Address**（**User-ID** 代理地址））指定为 User-ID 主机。

如果已将本地网关配置为远程用户位置的内部网关，您还可以通过在 Panorama 中创建 User-ID 代理并指定远程网络 **EBGP Router**（**EBGP** 路由器）地址（**Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息） > **Remote Networks**（远程网

 ©2025 Palo Alto Networks, Inc.

络） > **EBGP Router**（**EBGP** 路由器））作为 User-ID 主机，将远程网络用户的 HIP 信息发送到 Panorama。



在 Prisma Access 中启用和配置重新分发 HIP：

- 在 Prisma Access 中配置 HIP 重新分发

在 Prisma Access 中配置 HIP 重新分发

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证

当安装了 GlobalProtect 应用程序的端点的移动用户连接到 Prisma Access 时，Prisma Access 会从端点的 GlobalProtect 应用程序收集用户的 HIP 信息，使 HIP 报告在 Prisma Access 中可供使用。

要使用 *HIP* 重新分发，用户必须在其端点上安装 *GlobalProtect* 应用程序。尽管 *Prisma Access* 支持无客户端 VPN，但您无法为无客户端 *VPN* 用户重新分发 *HIP* 信息。

HIP 重新分发适用于移动用户和远程网络的用户。但是，对于远程网络的用户，本地网关必须使用内部主机检测功能检测到用户位于组织网络的内部，然后本地网关才能将 HIP 信息发送到 Prisma Access。

在 *Prisma Access* 中，您可以在配置移动用户部署时配置内部主机检测。

©2025 Palo Alto Networks, Inc.

为了确保策略实施的一致性，您可以使用 HIP 重新分发允许 Prisma Access 将用户的 HIP 信息分发到部署中的其他 Panorama 设备、网关、防火墙和虚拟系统，以及在某些情况下将这些设备的 HIP 信息分发到 Prisma Access。此功能允许您对用户流量一致地应用基于 HIP 的策略实施，包括针对互联网绑定流量或访问组织总部或数据中心内部应用程序或资源的流量的策略。通过将 HIP 信息重新分发到 Panorama 设备，您还可以从该设备查看 Prisma Access 用户的详细 HIP 信息。

请记住，GlobalProtect 内部和外部网关不支持双向 HIP 重新分发。因此，最佳实践是使用 Panorama 设备作为重新分发点。在此部署中，您需要配置内部和外部网关以将 HIP 报告发送到 Panorama，并让 Panorama 将这些报告转发到您的防火墙，以便在您的环境中实施一致的策略。

- Strata Cloud Manager
- Panorama

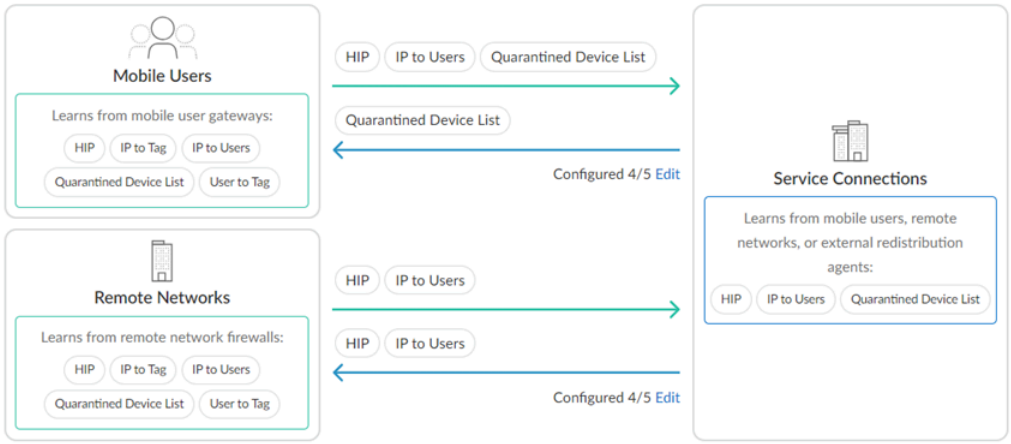
在 Prisma Access 中配置 HIP 重新分发 (Strata Cloud Manager)

默认情况下，在 **Strata Cloud Manager** 中启用 HIP 报告重新分发。要查看重新分发详细信息或禁用重新分发，请按照以下步骤操作。

STEP 1 | 在 **Strata Cloud Manager** 中，选择 **Manage**（管理） > **Configuration**（配置） > **NGFW** 和 **Prisma Access** > **Identify Services**（识别服务） > **Identify Redistribution**（识别重新分发）。

Prisma Access 标识重新分发图显示了移动用户和服务连接之间以及远程网络和服务连接之间的默认 HIP 报告重新分发设置。

Prisma Access Identity Redistribution Diagram



STEP 2 | 要禁用分段之间的重新分发，请单击 **Edit**（编辑），然后单击相关的源远程网络旁边的 **Edit**（编辑）。

STEP 3 | 禁用 **HIP**。

在 Prisma Access 中配置 HIP 重新分发 (Panorama)

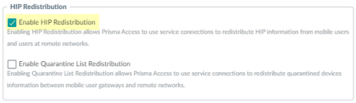
要允许 Prisma Access 收集和重新分发 HIP 信息，请完成以下任务。

©2025 Palo Alto Networks, Inc.

STEP 1 | 允许 Prisma Access 重新分发 HIP 信息。

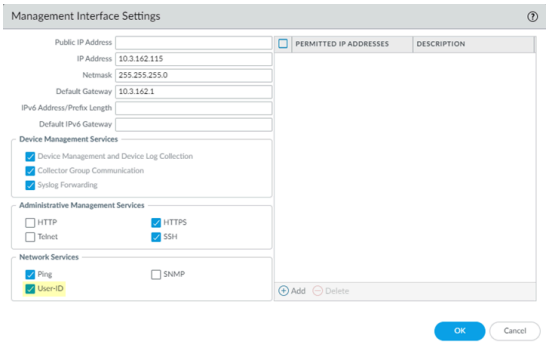
1. 在 Panorama 中，选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Service Setup**（服务设置）。
2. 单击齿轮图标以编辑设置。
3. 在 **Advanced**（高级） 选项卡中，选择 **Enable HIP Redistribution**（启用 **HIP** 重新分发）。

   启用 HIP 重新分发后，Prisma Access 可以将从 GlobalProtect 应用程序收到的 HIP 报告重新分发到内部防火墙和 Panorama。



STEP 2 | 配置 Panorama 以接收来自 Prisma Access 的 HIP 报告。

1. 选择 **Panorama** > **Setup**（设置） > **Interfaces**（接口）。
2. 选择 **Management**（管理）接口。
3. 选择 **User-ID**。



STEP 3 | 配置 Panorama 以从 Prisma Access 收集 User-ID 映射。

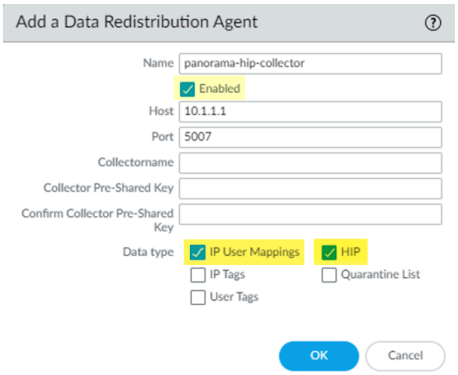
1. 从管理 Prisma Access 的 Panorama 中，选择 **Panorama** > **Data Redistribution**（数据重新分发） > 代理（适用于 Panorama 10.*x* 设备），或选择 **Panorama** > **User Identification**（用户标识） > **User-ID Agents**（**User-ID** 代理）（适用于 9.1.*x* Panorama 设备）。
2. **Add**（添加） User-ID 代理并为其提供 **Name**（名称）。
3. 根据要收集的 HIP 信息的类型，在 **Host**（主机）字段中输入以下值之一。
   - 要收集移动用户的 HIP 信息，请输入 **User-ID Agent Address**（**User-ID** 代理地址）（**Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息） > **Service Connection**（服务连接） > **User-ID Agent Address**（**User-ID** 代理地址））。
   - 要从具有内部网关的远程网络位置的用户收集 HIP 信息，请输入内部网关的 IP 地址。
   - 要从远程网络连接的用户收集 HIP 信息，请输入 **EBGP Router**（**EBGP** 路由器）地址（**Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息） > **Remote Networks**（远程网络） > **EBGP Router**（**EBGP** 路由器））作为 User-ID 主机。

 ©2025 Palo Alto Networks, Inc.

4. 在端口字段中输入 **5007**。

   默认情况下，User-ID 代理使用端口 5007 来侦听 HIP 信息请求。

   确保您的网络不会阻止 *Prisma Access* 与 *Active Directory* 服务器或 *User-ID* 代理之间对此端口的访问。
5. 选择 **Enabled**（已启用），以使 Panorama 能够与 User-ID 代理进行通信。
6. 选择 **IP User Mappings**（**IP** 用户映射）和 **HIP**，以使 Panorama 能够从所有移动用户位置接收 IP 地址到用户名的映射和 GlobalProtect HIP 数据。
7. 单击 **OK**（确定）。



STEP 4 | 对您想要配置 HIP 报告收集的每个服务连接重复步骤 3。

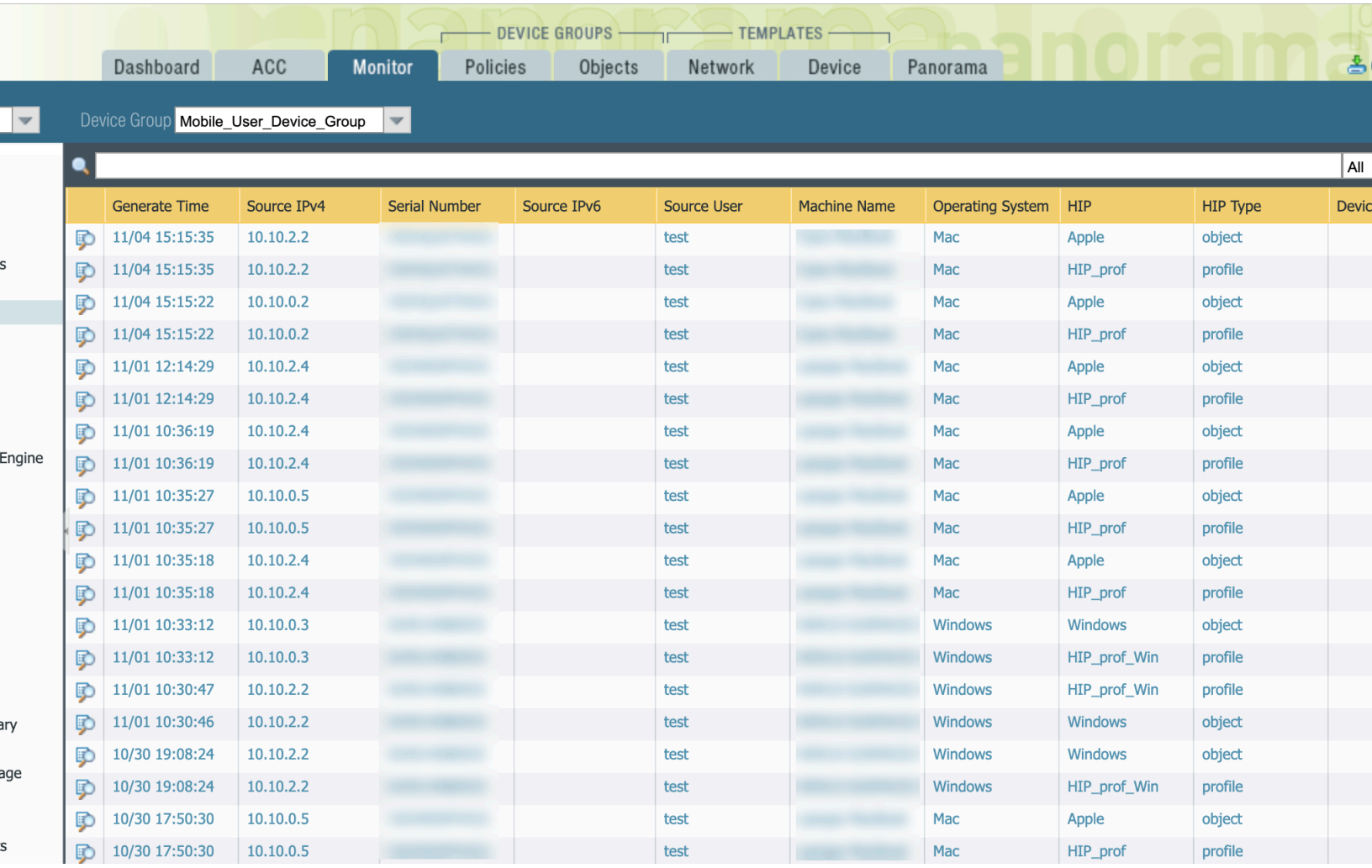
查看 HIP 报告

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

将 Prisma Access 配置为收集并重新分发 HIP 信息到 Panorama 后，请按照以下工作流程来查看 Panorama 中的 HIP 信息。

©2025 Palo Alto Networks, Inc.

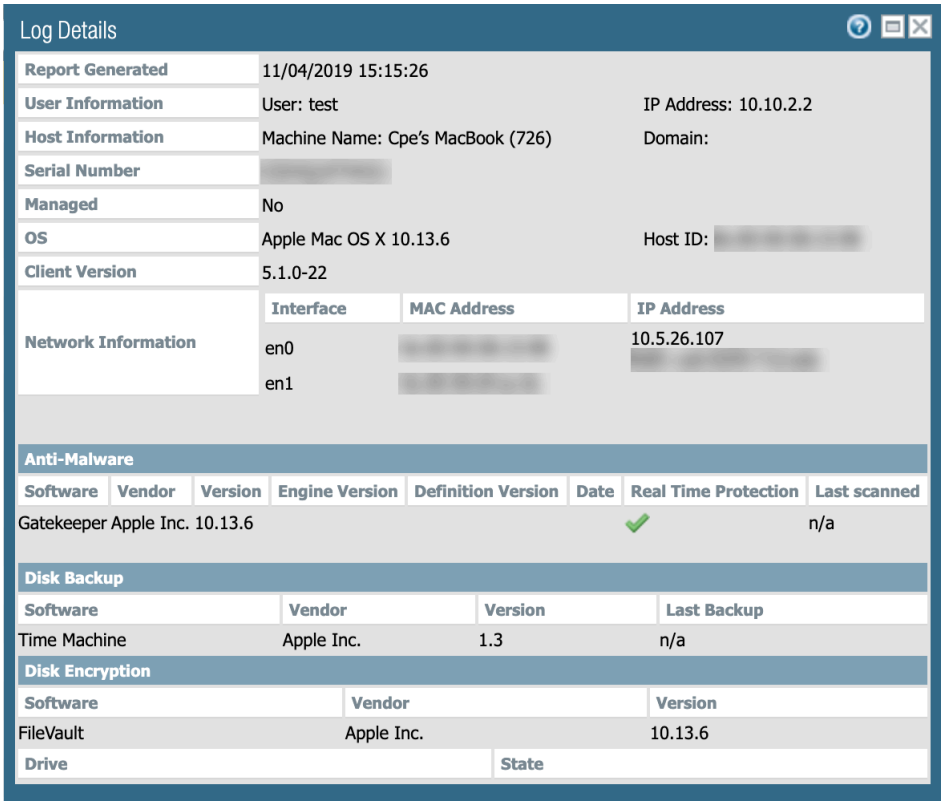
STEP 1 | 选择 **Monitor**（监视） > **Logs**（日志） > **HIP Match**（**HIP** 匹配），以查看 HIP 信息。



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 | 单击记录左侧的图标以查看 HIP 详细信息。



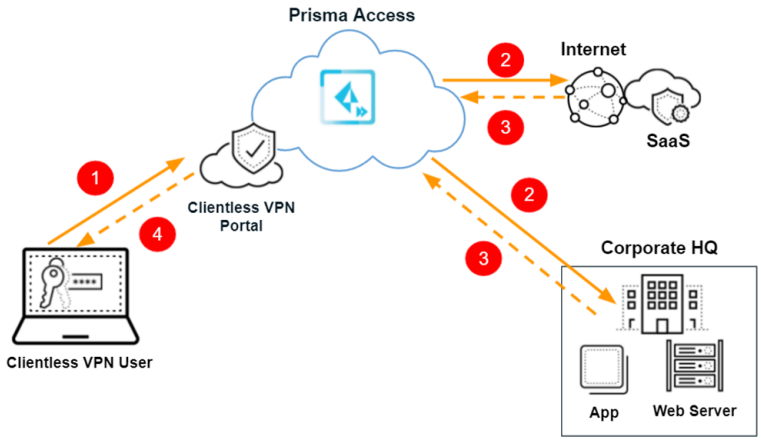
无客户端 VPN 中支持 Gzip 编码

在何处可以使用？	需要提供什么？
• Panorama	• Prisma Access 许可证

GlobalProtect 无客户端 VPN 提供对一般企业 Web 应用程序的远程访问。Prisma Access 无客户端 VPN 允许移动用户访问 Gzip 压缩的网站以使用内部和 SaaS 应用程序。对 Gzip 编码的支持可确保 HTTP 标头内的 Gzip 编码请求被无客户端 VPN 门户接受。这可确保通过无客户端 VPN 门户访问时正确呈现 Gzip 压缩网页的内容。

下图说明了扩展支持，以允许用户通过无客户端 VPN 访问内部和 SaaS 应用程序 Prisma Access。

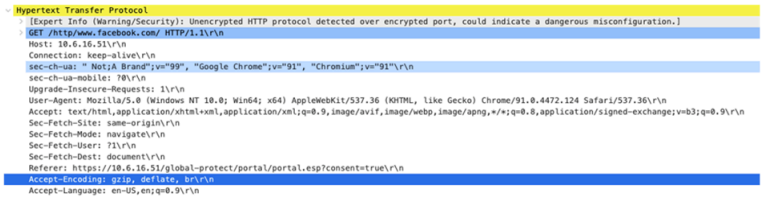
©2025 Palo Alto Networks, Inc.



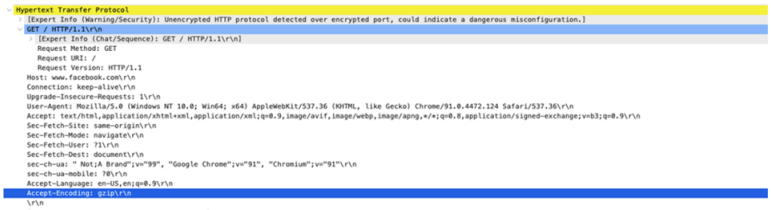
无客户端 VPN 可以根据来自客户端的 HTTP 请求和来自应用程序的相应响应来确定是否使用 Gzip 编码。**gzip** 值必须作为 Accept-Encoding 标头值之一包含在内，以便无客户端 VPN 可以接受它。

例如，当无客户端 VPN 使用 Gzip 编码时，请考虑以下场景：

1. 浏览器向网站发送 HTTP 请求，并将 Accept-Encoding 标头值设置为 **gzip**、**deflate**和 **br**，如以下示例所示。



2. 无客户端 VPN 门户 Prisma Access 解析来自浏览器的传入 HTTP 请求，并将 Accept-Encoding 标头值设置为 **gzip**，表示支持 Gzip 编码，如下例所示。

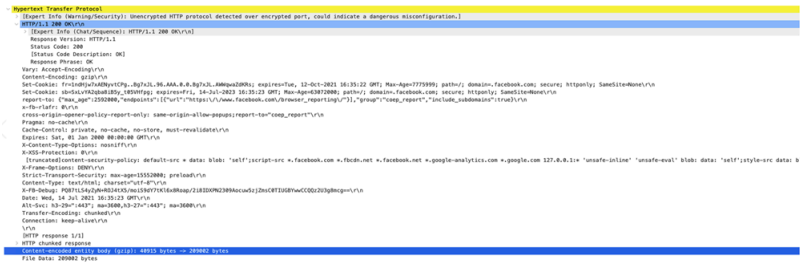


3. 如果网站在 HTTP 响应中支持 Gzip 编码，则网站会将 Content-Encoding 标头发送为 **gzip**，以指示内容采用 Gzip 格式，如下例所示。



 ©2025 Palo Alto Networks, Inc.

4. 无客户端 VPN 以相同的格式将从网站收到的响应转发到 Web 浏览器，如下例所示。



如果无客户端 VPN 收到的 HTTP 请求不包含 **gzip** 作为编码方法之一，则无客户端 VPN 也不接受 Gzip 编码。

Prisma Access 中的流量复制

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证 ❑ 流量复制附加许可证 ❑ 流量复制需要最低 4.1Prisma Access 释放移动用户流量。 ❑ 流量复制需要最低 5.0 Prisma Access 针对移动用户和远程网络流量发布。 ❑ TLS 1.3 对远程网络的支持至少需要 Prisma Access 5.2 发布。 ❑ PubSub 要求最低 Prisma Access 5.2.1 发布。

内部网络记录器已成为组织执行取证和违规分析的有力工具。在本地拓扑中，通常会实现分路端口、跨度端口或数据包代理的并行基础设施，这些基础设施将提供用于此类带外分析的流量副本。

然而，随着混合工作和云的加速采用，组织正在迁移到 SASE 架构来应对这些挑战。遵守 SASE 云安全解决方案为这些取证分析工具创造了盲点，其中从远程用户到 SaaS 应用程序的流量副本不再可用。

Prisma Access 流量复制通过提供正在传输的流量副本，为涉及 SASE 架构的取证和事后分析增加了全面的可视性 Prisma Access。流量复制发挥作用的一些常见用例包括：

- 取证和威胁搜寻分析，其中数据包捕获提供了攻击和所用方法的确凿证据
- 满足特定的法规要求，即数据包捕获需要保存一定时间
- 继续使用贵组织投资的任何首选第三方工具
- 数据包级网络和应用程序性能调试

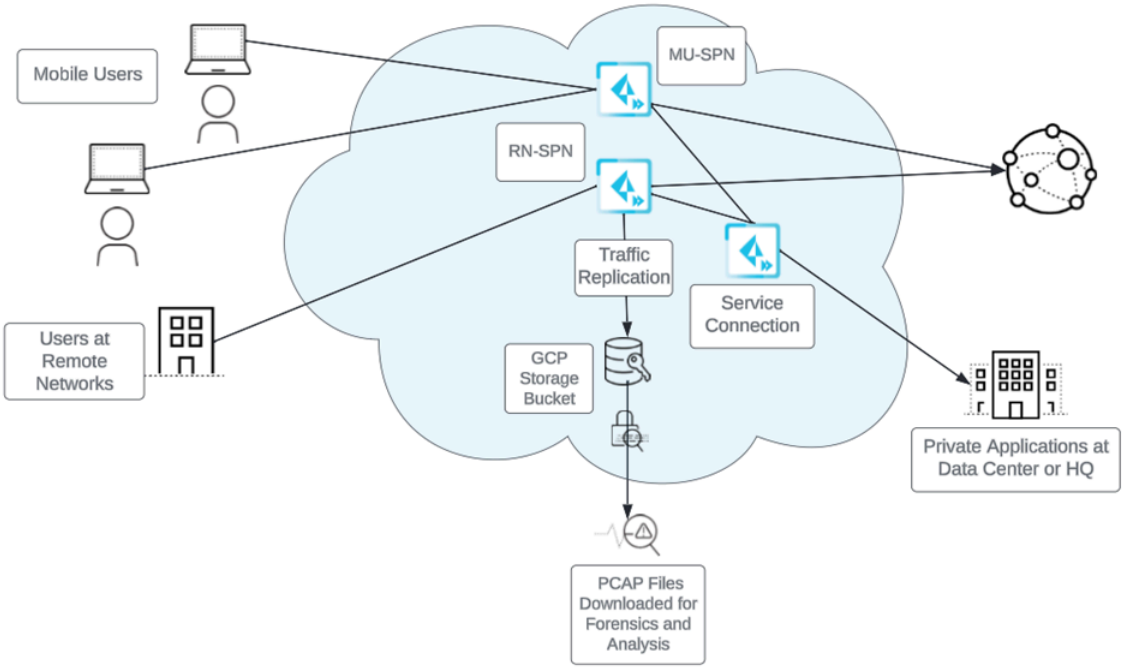
流量复制提供对用户真实世界流量的数据包捕获 (pcap) 的访问，从而可以检测和补救可能跨越多个会话的威胁，或者识别和应对异常行为以降低风险并确保企业安全。

 ©2025 Palo Alto Networks, Inc.

启用流量复制时， Prisma Access 在每个云存储桶中创建专用的云存储桶 Prisma Access 计算启用此功能的位置，并连续保存包含正在传输的流量副本的 pcap 文件 Prisma Access。

要在新的 pcap 文件上传到存储桶时收到通知，您可以订阅 Pub/Sub 通知。使用新的 pcap 文件的 Pub/Sub 通知后，在有新文件夹或新文件添加到存储桶中时，无需开发工具来通知您。

您需要提供一个 Google 云服务帐户，该帐户将用于共享这些存储桶的只读权限，从而实现对 pcap 文件的安全访问。对静态 pcap 文件进行了额外的加密，涉及通过证书共享的公钥 Prisma Access。只有您才拥有解密和恢复原始 pcap 文件的私钥。



流量复制的先决条件

在开始配置流量复制之前，请注意以下先决条件。

- 确保您已在 Google Cloud Platform (GCP) 中创建 服务帐户 。
- 确保您已在 对象 > 证书管理 > 证书 > 自定义证书 > 生成 页面中创建了通过证书共享的公钥，以用于 SSL 解密。
- 推荐的架构要求从每个存储桶读取 pcap 文件的计算或服务位于存储桶正在读取的同一 GCP 区域中。虽然从不同 GCP 区域甚至 GCP 云外部的存储桶读取 pcap 文件可能会有效，但这些不是受支持的部署模型。

流量复制指南

请遵循以下准则来进行流量复制：

- **TLS** 支持— 移动用户部署中使用的流量复制支持 TLS 1.2；远程网络部署中使用的流量复制支持 TLS 1.2 和 1.3。
- **IPSec** 隧道算法— 支持移动用户和远程网络部署的所有 IPSec 隧道算法也均支持流量复制。

了解如何设置流量复制：

- Strata Cloud Manager

 ©2025 Palo Alto Networks, Inc.

- Panorama

Prisma Access 中的流量复制 (Strata Cloud Manager)

要配置流量复制并访问数据包捕获 (pcap) 文件，请完成以下步骤。

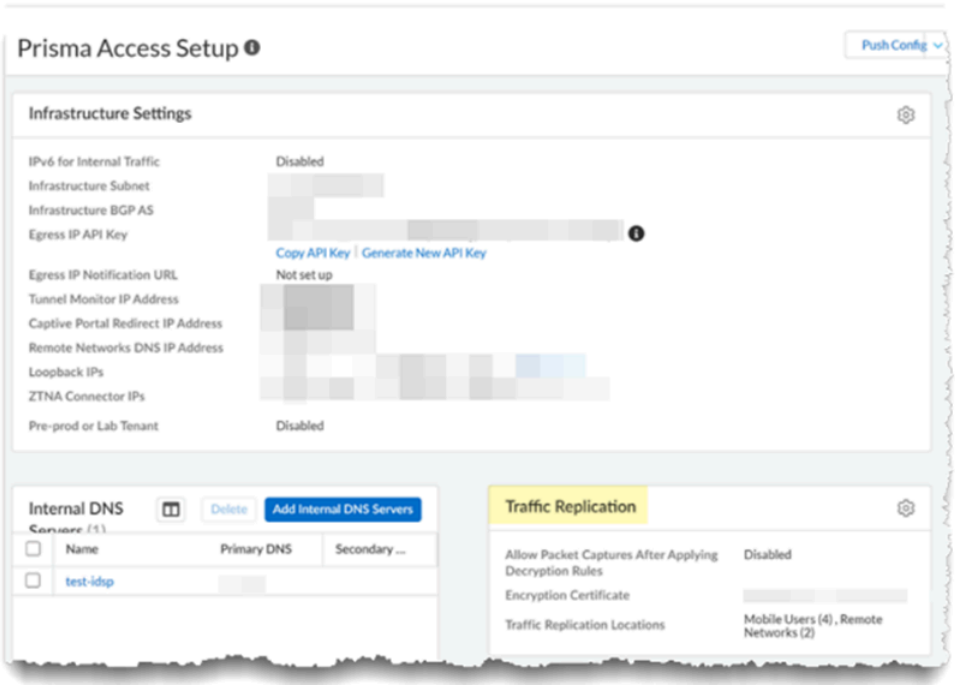
STEP 1 | 加入并配置移动用户 — GlobalProtect，适用于您想要启用流量复制并 提交和推送 更改的位置。

您必须启用移动用户—全局保护位置，然后才能对这些位置启用流量复制。

©2025 Palo Alto Networks, Inc.

STEP 2 | （可选）对数据包捕获应用 SSL 解密。

1. 转至 Prisma Access (Managed by Strata Cloud Manager) 并选择 **Prisma Access** 设置 > **Prisma Access** > 流量复制 并单击齿轮来编辑 设置。

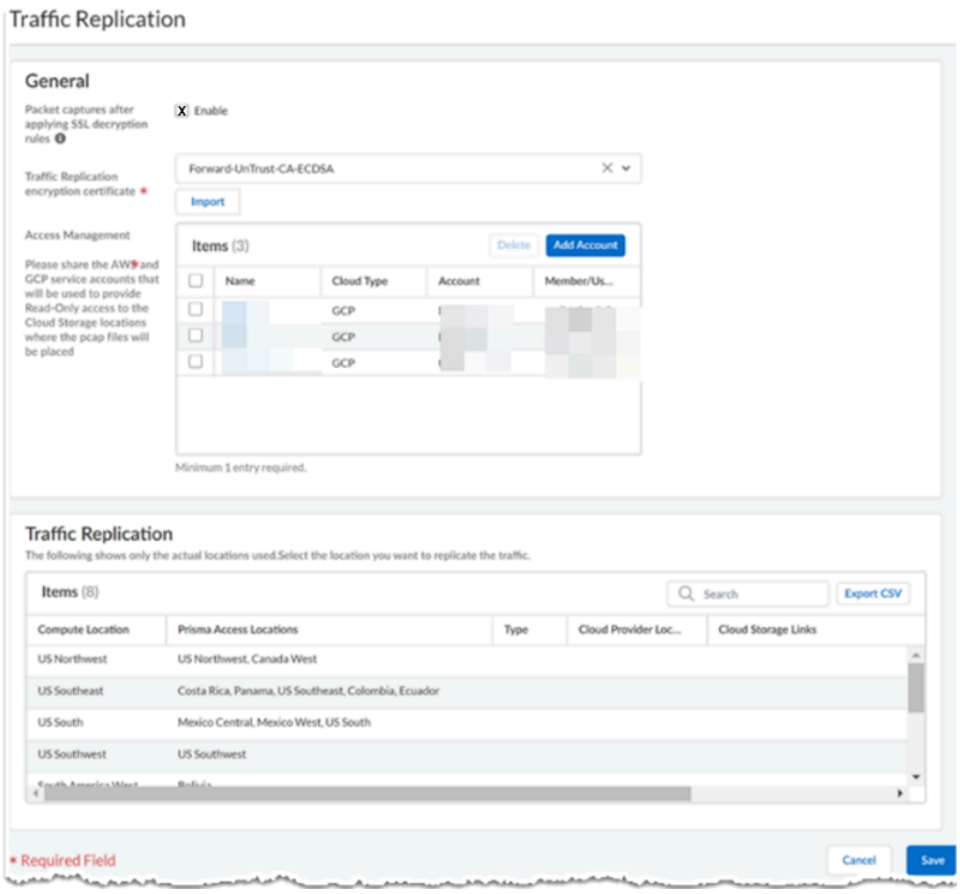


2. 应用 **SSL** 解密规则后启用数据包捕获， 以便在 pcap 文件上应用已配置的 SSL 解密策略。

   只有与内联 SSL 解密策略匹配的流量才会被解密。

   如果选择此选项，pcap 文件将使用您在部署中指定的相同 解密规则 。如果取消选择此选项，则无论您配置了什么解密规则，都不会对 pcap 文件执行解密。

©2025 Palo Alto Networks, Inc.



STEP 3 | 对于 流量复制加密证书，选择您在 对象 > 证书管理 > 证书 > 自定义证书 > 生成 页面中添加的任何证书或 导入 要用于 SSL 解密的证书。

证书由公钥和私钥组成。上传公钥 Prisma Access；您保留私钥并在从存储桶下载压缩的 pcap 文件时使用它进行解密。这样，您就保证只有您的组织可以访问存储 pcap 文件的存储桶。

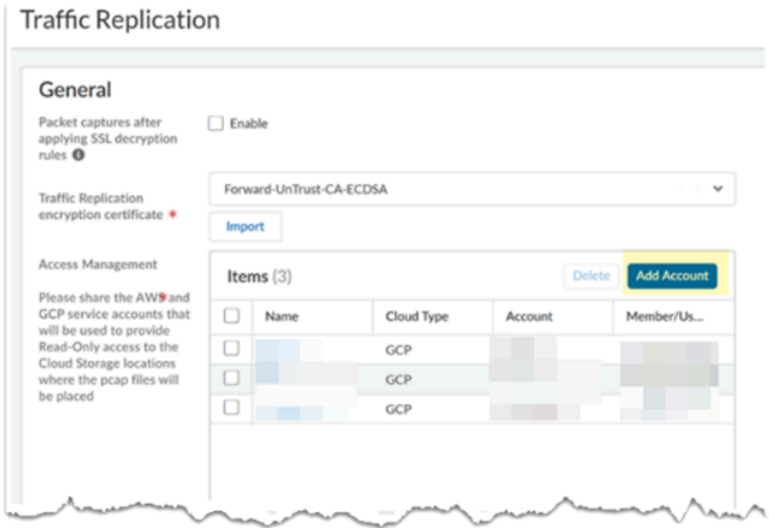
STEP 4 | 配置您在 步骤 1中创建的 GCP 服务帐户。

只有 GCP 帐户支持流量复制。此服务账户用于共享对存储桶的只读访问权限，其中 pcap 文件存储在您已启用流量复制的位置。您可以使用常规 GCP 服务帐户创建程序在您的 GCP 帐户中

©2025 Palo Alto Networks, Inc.

创建这些服务帐户。您有责任控制哪些用户可以访问这些服务帐户。任何同时具有 pcap 文件访问权限和私钥访问权限的用户都可以访问 pcap 文件。

1. 在 访问管理 区域， 添加帐户 详细信息以共享对存储 pcap 文件的存储桶的只读访问权限。



2. 输入以下参数：
   - 给帐户一个唯一的帐户名。
   - 指定 **GCP** 作为帐户的 类型 。
   - 从您创建的 GCP 服务帐户中指定帐户信息。
   - 输入 GCP 服务帐户的成员/用户名称。

 ©2025 Palo Alto Networks, Inc.

STEP 5 | (可选)如果要添加在将新文件夹或新文件添加到存储区时通知您的 Pub/Sub 通知，请在 Google Cloud Service 帐户中设置 Pub/Sub 通知。

Prisma Access 为每个租户为该租户中的所有位置创建一个 Pub/Sub 通道。从Prisma Access 5.2 开始支持

发布/订阅通知。如果您已有帐户，并希望添加发布/订阅通知，请升级到 *Prisma Access 5.2*,然后选择以下选项之一添加发布/订阅通知：

- 修改已在 *Prisma Access* 中配置的现有 *Google* 云服务帐户。
- 添加新帐户，并在*Prisma Access*配置中指定该帐户。

  如果添加新帐户，则需要在现有帐户上禁用流量复制，并在新帐户上启用流量复制。
- 上禁用和启用流量复制。

Prisma Access 发送 Pub/Sub 消息的标题为 `panw-traffic-replication-file-Notification-<tenantid>`，其中 *<tenantid>* 是发送通知的租户的 ID。消息的格式如下：

```
Message { 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-xxxxxxx/12345678_190000_xxxxx.zip",
 "payloadFormat":"NONE" } }
```

其中：

- `objectGeneration` 是更改对象的生成编号。
- `objectID` 是已更改对象的名称。

STEP 6 | 为一个或多个移动用户位置配置流量复制。

1. 在 流量复制 区域中，选择要启用流量复制的位置，然后选择 移动用户。

   您选择与以下项关联的 计算位置**Prisma Access** 位置。为连接到选定位置的所有移动用户客户端启用流量复制。

STEP 7 | **Save**（保存）配置。

STEP 8 | 提交并推送更改。

1. 选择 **Manage**（管理） > **Operation**（操作） > **Push Config**（推送配置）。
2. 在 推送范围中选择 移动用户容器，然后 推送配置 并 推送 您的更改。
3. 查看推送目标并 **Push**（推送）。

STEP 9 | 检查流量复制的状态，请访问 **Prisma Access** 设置 > **Prisma Access** > 流量复制。

 ©2025 Palo Alto Networks, Inc.

STEP 10 | 下载 pcap 文件。

使用 云存储链接 访问 GCP 存储桶中的 pcap 文件。

- 这些存储桶支持与任何其他 GCP 存储桶相同的常规操作、命令和查询。
- 您最多可以下载 72 小时的 pcap 数据。72小时后，文件将被永久删除。
- 文件使用您的公钥加密。
- 最大文件大小为 200 MB 或 5 分钟的数据包捕获，以较小者为准。

1. 通过输入 enter `gsutil ls gs://<storage_bucket_link>/` 列出服务中的文件，其中 *<storage_bucket_link>* 是 GCP 服务帐户中存储文件的存储链接。
2. 通过输入 enter `gsutil cp gs://<storage_bucket_link>/<file_name> <destination folder>`从服务帐户下载文件，其中：
   - *<storage_bucket_link>* 是 GCP 服务帐户中存储文件的存储链接。
   - *<file_name>* 是 pcap 文件的名称。
   - *<destination folder>* 是您想要下载 pcap 文件的文件夹。
3. 解压缩下载的文件。
4. 解密下载的文件。

Prisma Access 中的流量复制 (Panorama)

要配置流量复制并访问 PCAP 文件，请完成以下步骤。

STEP 1 | 板载并配置移动用户—GlobalProtect(如果为移动用户配置流量复制)、远程网络(如果为远程网络配置流量复制)或两者兼有(如果同时为移动用户和远程网络配置流量复制)。

STEP 2 | （可选）对数据包捕获应用 SSL 解密。

1. 转到全景 > 云服务 > 配置 > 流量复制并单击齿轮以编辑设置。
2. 在应用解密规则后选择允许数据包捕获，对 PCAP 文件应用已配置的 SSL 解密策略。

   如果选择此选项，PCAP 文件将使用您在部署中指定的相同解密规则。如果取消选择此选项，则不会对 PCAP 文件执行解密，不管您配置了何种解密规则。

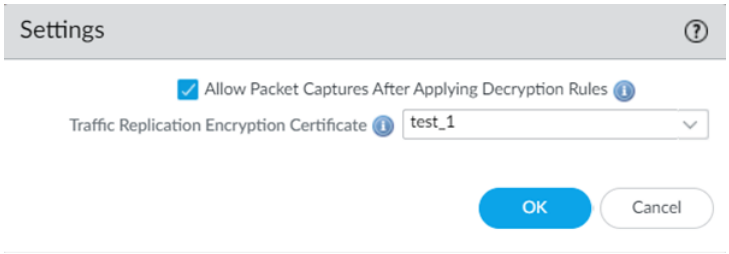
STEP 3 | 在 **Mobile_User_Template** 用于移动用户部署）或 **Remote_Network_Template**（用于远程网络部署）中选择要用于 SSL 解密的先前步骤中创建的 **Traffic Replication Encryption Certificate**（流量复制加密证书）（公钥）。

此步骤是必需的。您可以在 **Mobile_User_Template** 或 **Remote_Network_Template** 中的 **Device** > **Certificate Management** > **Certifificates** > **Device Certificates** 区域中选

 ©2025 Palo Alto Networks, Inc.

择您添加的任何证书。如果同时为移动用户和远程网络启用流量复制，请将证书放入 **Mobile_User_Template** 和 **Remote_Network_Template** 中。

证书由公钥和私钥组成。Prisma Access 中上传公钥；您保留私钥，并在从存储桶下载压缩的 PCAP 文件时用于解密。通过这种方式，您可以保证只有您的组织才能访问存储 PCAP 文件的存储桶。



STEP 4 | 为一个或多个移动用户配置流量复制 — GlobalProtect 位置、远程网络位置或两者，方法是在配置区域中选择位置并选择要启用流量复制的位置，然后选择 **MU-GP**、**RN** 或两者。

选择与**Prisma Access**位置关联的计算位置。对所有连接到选定位置的移动用户 — GlobalProtect 客户端、远程网络用户或两者均启用流量复制。

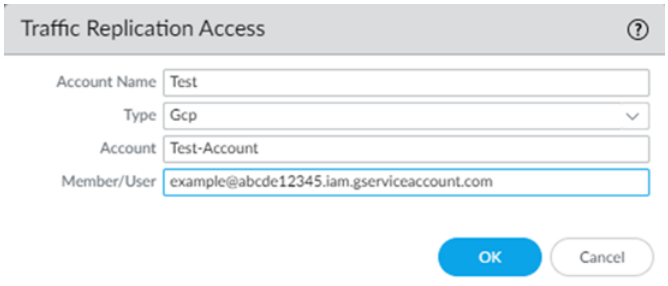


STEP 5 | 添加一个帐户，允许您访问流量复制数据包捕获 (PCAP) 数据。

此服务帐户用于共享对存储存储存储桶的只读访问，其中PCAP文件存储在已启用流量复制的位置。您在 GCP 帐户中使用正常的 GCP 服务帐户创建过程创建这些服务帐户。您有责任控制哪些用户有权访问这些服务帐户。任何同时拥有PCAP文件和私钥访问权限的用户都可以访问PCAP文件。

1. 在流量复制访问区域中，添加帐户。
2. 输入以下参数：
   - 给帐户一个唯一的帐户名。
   - 指定 **Gcp** 作为帐户的类型。

     只有 GCP 帐户支持流量复制。
   - 从您创建的 GCP 服务帐户中指定帐户信息。
   - 输入 GCP 服务帐户的成员/用户名称。



 ©2025 Palo Alto Networks, Inc.

STEP 6 | (可选)如果要添加在将新文件夹或新文件添加到存储区时通知您的 Pub/Sub 通知，请在 Google Cloud Service 帐户中设置 Pub/Sub 通知。

Prisma Access 为每个租户为该租户中的所有位置创建一个 Pub/Sub 通道。从Prisma Access 5.2 开始支持

发布/订阅通知。如果您已有帐户，并希望添加发布/订阅通知，请升级到 *Prisma Access 5.2*,然后选择以下选项之一添加发布/订阅通知：

- 修改已在 *Prisma Access* 中配置的现有 *Google* 云服务帐户。
- 添加新帐户，并在*Prisma Access*配置中指定该帐户。

  如果添加新帐户，则需要在现有帐户上禁用流量复制，并在新帐户上启用流量复制。
- 上禁用和启用流量复制。

Prisma Access 发送 Pub/Sub 消息的标题为 `panw-traffic-replication-file-Notification-<tenantid>`，其中 *<tenantid>* 是发送通知的租户的 ID。消息的格式如下：

```
Message { 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-xxxxxxx/12345678_190000_xxxxx.zip",
 "payloadFormat":"NONE" } }
```

其中：

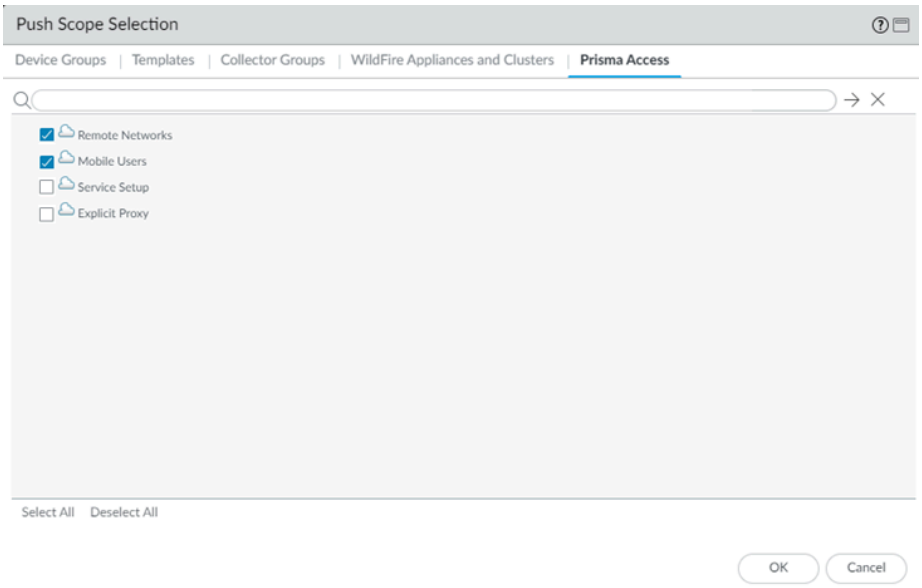
- `objectGeneration` 是更改对象的生成编号。
- `objectID` 是已更改对象的名称。

 ©2025 Palo Alto Networks, Inc.

STEP 7 | 提交并推送您的更改，确保移动用户(用于移动用户部署)、远程网络(用于远程网络部署)或同时在推送范围中选中。

1. 单击 **Commit**（提交） > **Commit and Push**（提交并推送）。
2. 编辑选择，并在**Prisma Access**选项卡中，确保推送范围中选择了移动用户和远程网络，然后单击确定。

   可能无法自动选择推送范围。



3. 单击 **Commit and Push**（提交并推送）。

STEP 8 | 通过转到全景 > 云服务 > 状态 > 流量复制检查流量复制状态。



存储链接是您可以访问 PCAP 文件的 GCP 存储桶的名称，云提供商位置是装载 GCP 实例的位置。

©2025 Palo Alto Networks, Inc.

STEP 9 | 使用只有您拥有的私钥下载 PCAP 文件。

使用存储链接访问 GCP 存储桶中的 PCAP 文件。

- 这些存储桶支持与任何其他 GCP 存储桶相同的常规操作、命令和查询。
- 您可以下载长达72小时的PCAP数据。72小时后，文件将被永久删除。
- 文件使用您的公钥加密。
- 最大文件大小为 200 MB 或 5 分钟的数据包捕获，以较小者为准。

1. 通过输入 enter `gsutil ls gs://<storage_bucket_link>/` 列出服务中的文件，其中 *<storage_bucket_link>* 是 GCP 服务帐户中存储文件的存储链接。
2. 通过输入 enter `gsutil cp gs://<storage_bucket_link>/<file_name> <destination folder>`从服务帐户下载文件，其中：
   - *<storage_bucket_link>* 是 GCP 服务帐户中存储文件的存储链接。
   - *<file_name>*是PCAP文件的名称。
   - *<destination folder>* 是您希望下载 PCAP 文件的文件夹。
3. 解压缩下载的文件。
4. 使用只有您拥有的私钥解密下载的文件。

 ©2025 Palo Alto Networks, Inc.

Prisma Access 远程网络高级部署

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

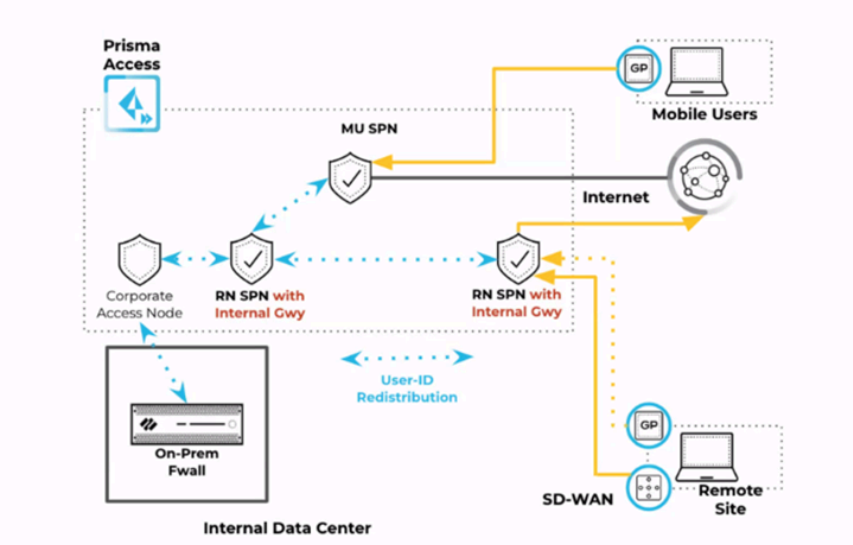
以下部分介绍了可用于 Prisma Access 远程网络的高级部署：

- 提供对远程网络地点的安全入站访问
- 为远程站点创建高带宽网络

Prisma Access 内部网关

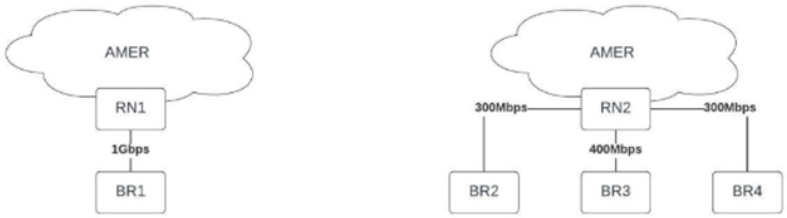
在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	❑ Prisma Access 和移动用户许可证 ❑ Minimum Required Prisma Access Version：5.1 ❑ Prisma Access (Managed by Panorama) 要求的数据平面最低版本：10.2.4 ❑ 最低要求的 GlobalProtect 客户端版本：6.0

以前，要为 Prisma Access 远程网络中运行 GlobalProtect 客户端软件的主机生成 IP 用户映射和 HIP，您必须部署本地 NGFW 作为内部网关。这种解决方案不是云原生的。使用 Prisma Access 云原生内部网关，您可以避免使用本地内部网关，Prisma Access 内部网关在远程网络中以本地方式生成 IP 用户映射和 HIP。远程网络使用本地数据库中的 IP 用户映射和 HIP 进行态势检查，而不是从其他防火墙学习。

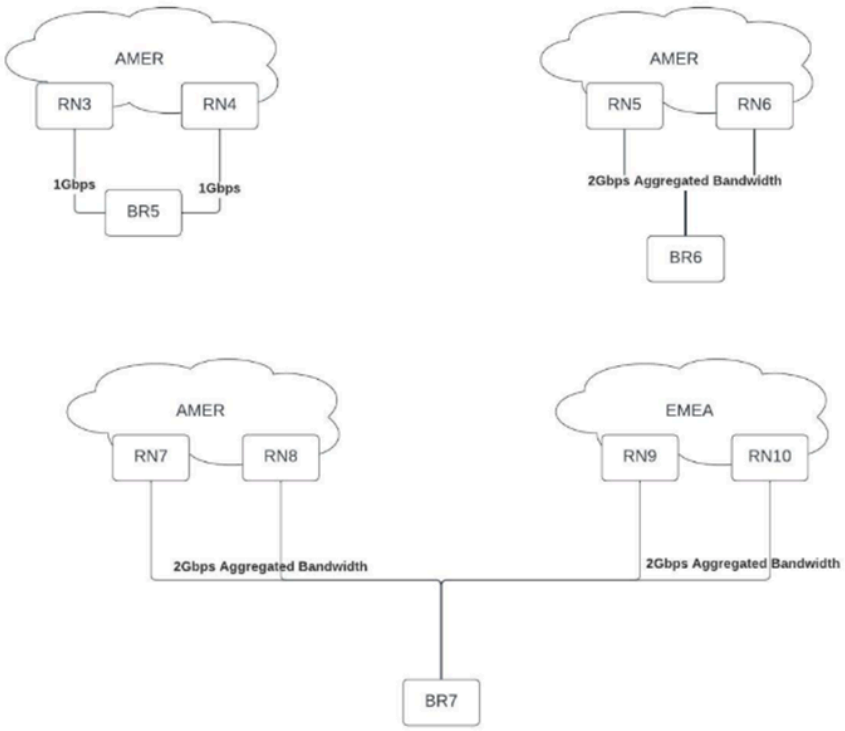


 ©2025 Palo Alto Networks, Inc.

请注意，当远程站点与不同的远程网络站点存在多条 IPsec 隧道（例如，活动/活动隧道），或者该站点为高带宽站点时，您无法部署内部网关。下图显示了内部网关部署的支持环境的示例。



下图提供了不支持内部网关的部署示例。



设置 Prisma Access 内部网关之前，请先接入您的移动用户。

- Strata Cloud Manager
- Panorama

Prisma Access 内部网关 (Strata Cloud Manager)

完成以下步骤来设置 Prisma Access 内部网关。

STEP 1 | 在 Strata Cloud Manager 中，设置 GlobalProtect，添加应用程序设置，并接入远程网络。
请注意，目前没有内部主机检测和内部网关配置。

©2025 Palo Alto Networks, Inc.

STEP 2 | 从 **Workflows**（工作流） > **Prisma Access** 设置 > **Prisma Access**中，记下 **Remote Networks DNS IP Address**（远程网络**DNS IP**地址）中显示的值。

STEP 3 | 从 **Workflows**（工作流） > **Prisma Access** 设置 > **GlobalProtect** > **Infrastructure**（基础设施） > **Infrastructure Settings**（基础设施设置） > **Gateway FQDNs**（网关 **FQDN**）中，记下 **Gateway FQDNs**（网关 **FQDN**）中显示的值。

STEP 4 | 选择 **Workflows**（工作流） > **Prisma Access** 设置 > **Remote Networks**（远程网络） > **Advanced Settings**（高级设置）。

STEP 5 | 编辑 **Prisma Access** 内部网关的设置以启用内部网关，然后选择 **Save**（保存）以保存更改。

（可选）如果您不想使用自己的 DNS 服务器，请针对 IPv4 选择 **Enable Internal Host Detection**（启用内部主机检测）。只有在选择 **Enable Internal Gateway**（启用内部网关）之后才能启用内部主机检测。

Prisma Access 仅对 ***Always On***（始终开启）连接方法支持内部主机检测。



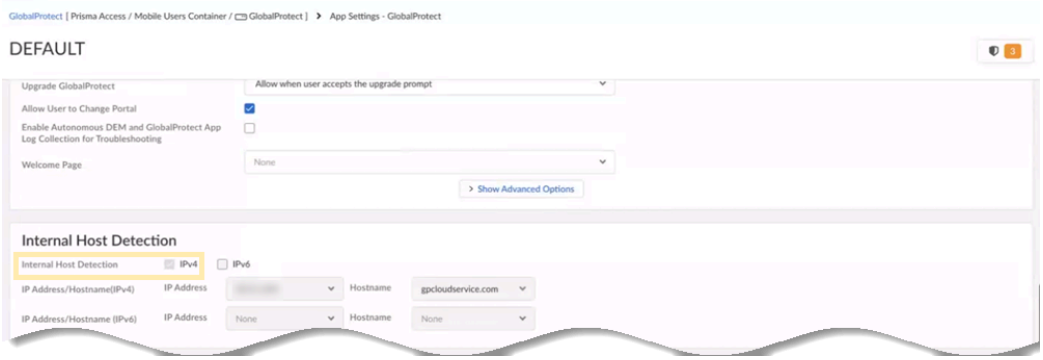
启用内部网关时，远程网络实例将充当内部网关。启用内部主机检测时，Prisma Access 会在远程网络 DNS 代理服务器上创建 PTR 记录，用于内部主机检测过程。

STEP 6 | 选择 **Workflows**（工作流） > **Prisma Access** 设置 > **GlobalProtect** > **GlobalProtect App**（**GlobalProtect** 应用）。

 ©2025 Palo Alto Networks, Inc.

STEP 7 | 选择应用程序设置并查看内部主机检测详细信息和内部网关详细信息。

当您在步骤 5 中启用内部网关和内部主机检测时，Prisma Access 也会在此处启用 IPv4 内部主机检测和内部网关。Prisma Access 将步骤2中的 **Remote Networks DNS IP Address**（远程网络 **DNS IP** 地址）值填充为 IP 地址。



请注意，不支持在 Prisma Access DNS 代理上进行 IPv6 内部主机检测。

不能移除这个 **Prisma Access** 内部网关条目。但是，您可以添加自己部署的内部网关。您可以在内部网络中部署自己的 DNS 服务器以进行内部主机检测，但请确保添加 PTR 记录，以便可以进行内部主机检测。Prisma Access 将步骤3中的 **Gateway FQDNs**（网关 **FQDN**）值附加到地址。



可以通过选择 **Workflows**（工作流） > **Prisma Access** 设置 > **Prisma Access**来查看 DNS 代理服务器 IP 地址详细信息。

如果启用 **Internal Host Detection**（内部主机检测），请验证 DNS 解析是否正常工作，执行从内部网络到 DNS 代理服务器 IP 的反向 DNS 查找，并确保它返回以 **`any-igw`** 开头的 FQDN。

STEP 8 | 选择 **Push**（推送）以同时将更改推送到移动用户和远程网络。

STEP 9 | 登录端点。

当您连接到 GlobalProtect 时，首先要通过 GlobalProtect 门户进行身份验证。内部主机检测触发 GlobalProtect 以连接到内部网关。然后，随着 GlobalProtect 代理继续在非隧道模式下运行，第二次身份验证出现，并将主机信息提交给远程网络上的内部网关。

Prisma Access 内部网关 (Panorama)

STEP 1 | 在 Panorama 中，设置 GlobalProtect，添加应用程序设置，并接入远程网络。

请注意，目前没有内部主机检测和内部网关配置。

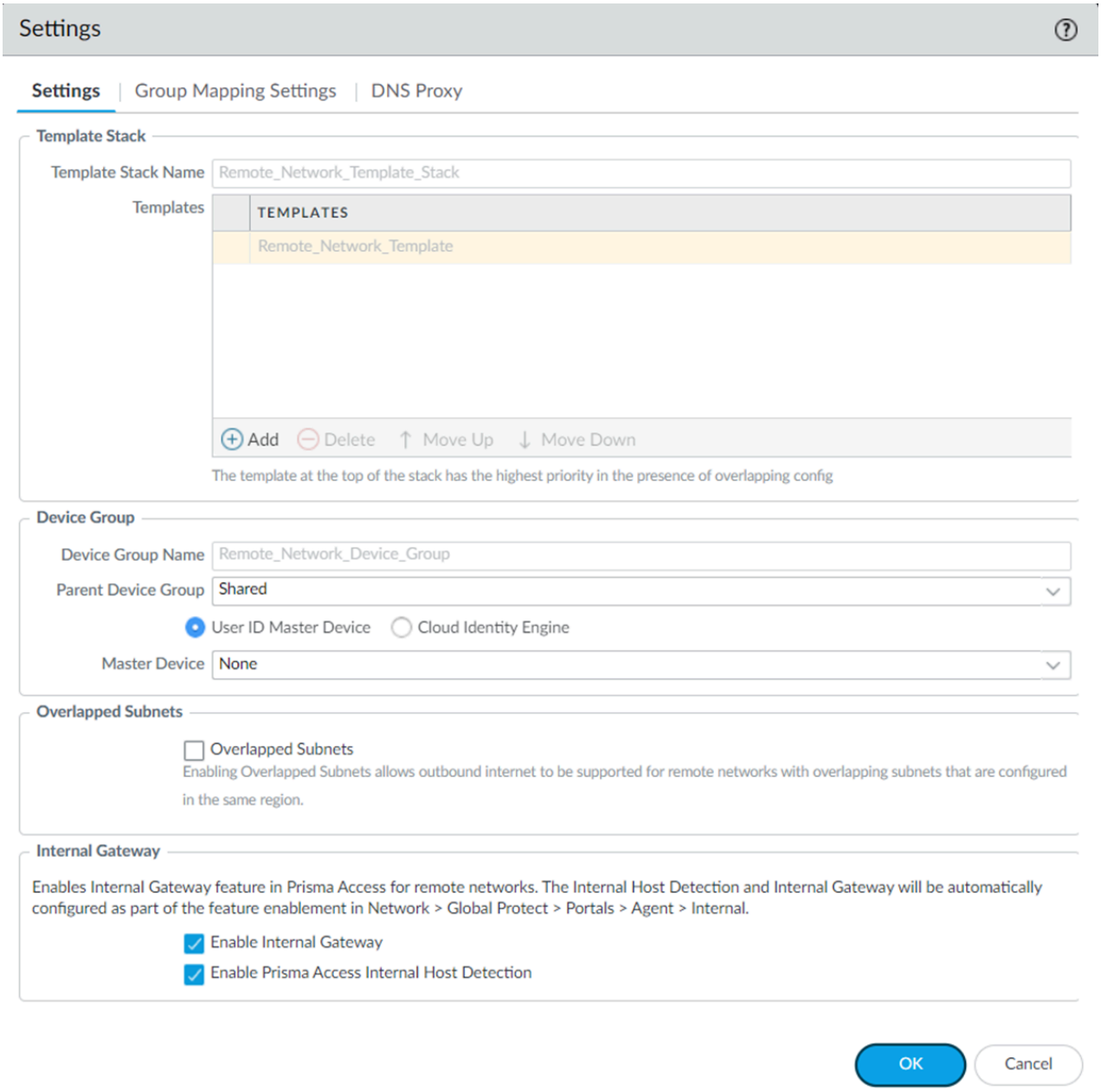
STEP 2 | 转到 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Remote Networks**（远程网络） > **Settings**（设置）。

 ©2025 Palo Alto Networks, Inc.

STEP 3 | 选择 **Enable Internal Gateway**（启用内部网关）并保存更改。

（可选）如果您不想使用自己的 DNS 服务器，请针对 IPv4 选择 **Enable Prisma Access Internal Host Detection**（启用 **Prisma Access** 内部主机检测）。只有在选择 **Enable Internal Gateway**（启用内部网关）之后才能启用内部主机检测。

Prisma Access 仅对 ***Always On***（始终开启）连接方法支持内部主机检测。



启用内部网关时，远程网络实例将充当内部网关。启用内部主机检测时，Prisma Access 将在远程网络 DNS 代理服务器上为内部主机检测进程创建 PTR 记录。

启用内部网关时，Prisma Access 将在远程网络模板中创建内部网关配置。

©2025 Palo Alto Networks, Inc.

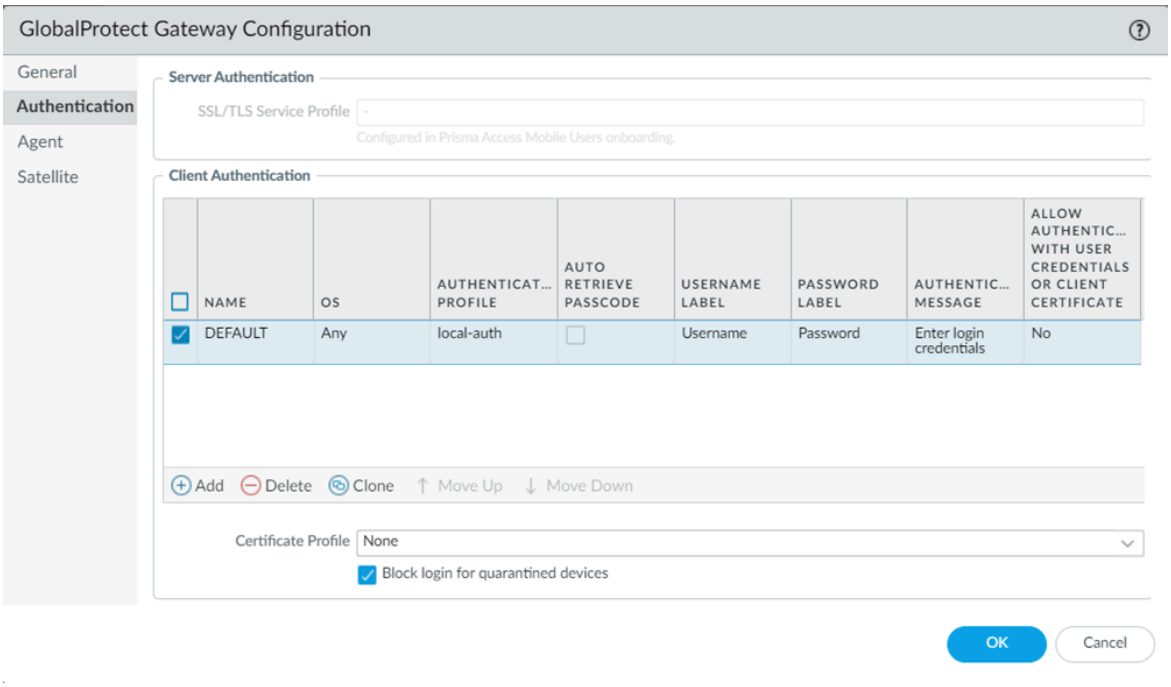
STEP 4 | 转到 **Templates**（模板） > **Network**（网络） > **GlobalProtect** > **Gateways**（网关），然后选择 **Remote_Network_Template**。

您将找到为内部网关创建的 **GlobalProtect_Internal_Gateway** 模板。

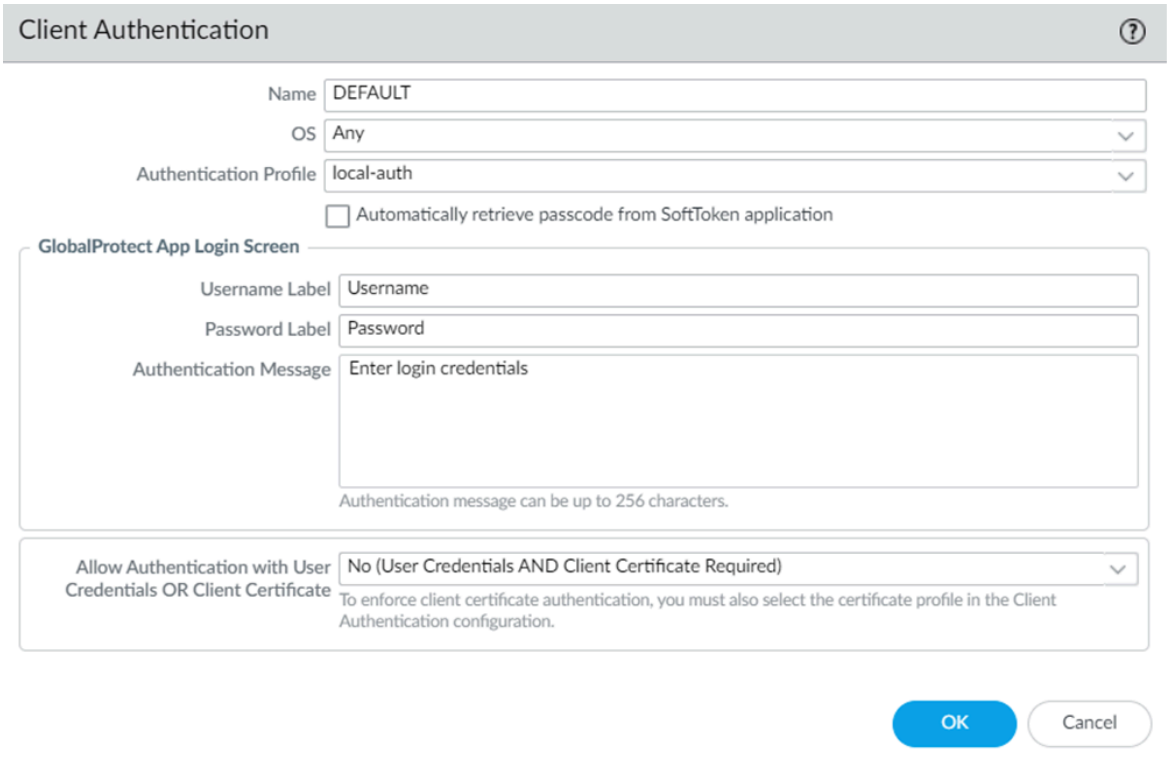
©2025 Palo Alto Networks, Inc.

STEP 5 | 为此远程网络模板创建一个身份验证配置文件，类似于移动用户模板中的身份验证配置文件。

1. 选择远程网络模板（即 **GlobalProtect_Internal_Gateway** 模板）超链接。
2. 转到 **Authentication**（身份验证） > **Client Authentication**（客户端身份验证）。

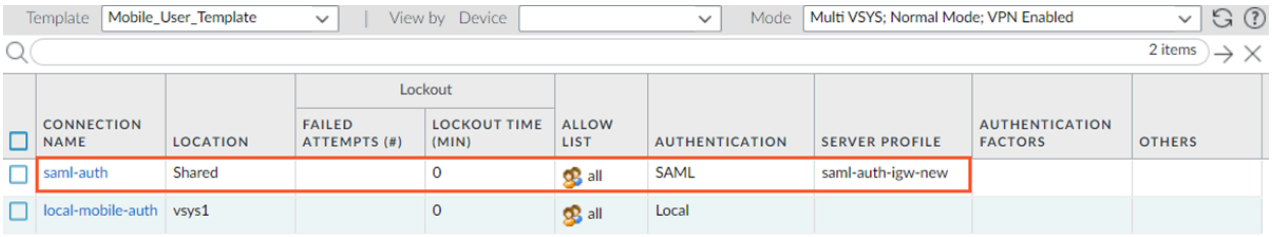


3. 编辑 **DEFAULT**（默认）客户端身份验证的身份验证配置文件详细信息。

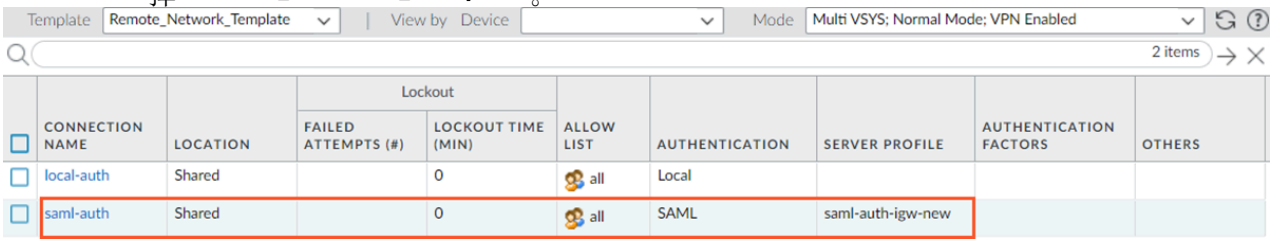


 ©2025 Palo Alto Networks, Inc.

创建一个与移动用户模板中的身份验证配置文件相同的配置文件。您可以在 **Template**（模板） > **Device**（设备） > **Authentication Profile**（身份验证配置文件）下找到移动用户模板中使用的身份验证配置文件。确保选择 **Mobile_User_Template**。



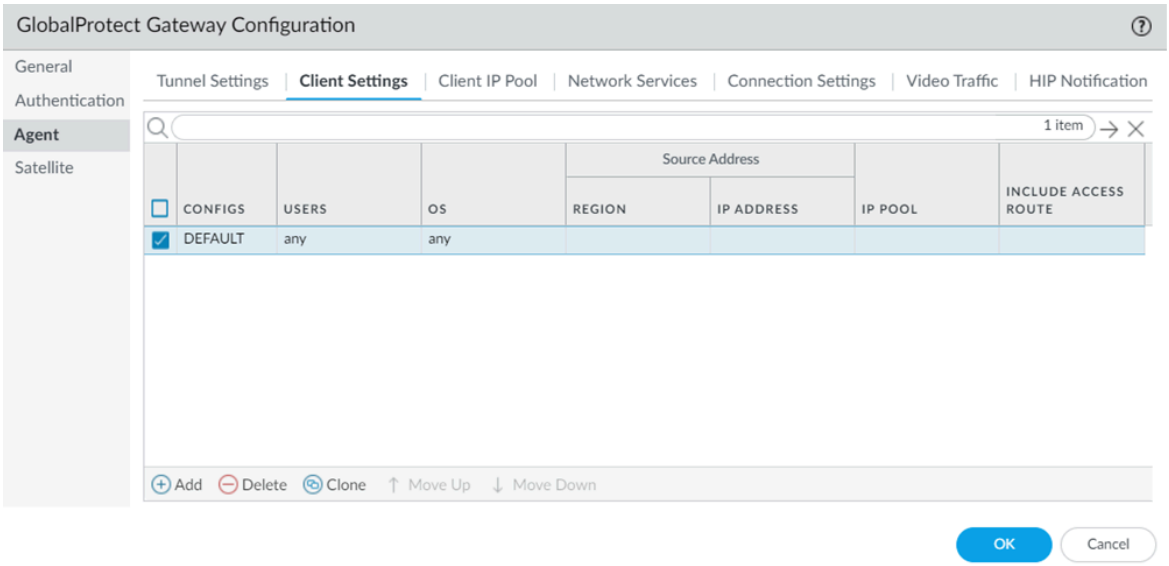
您还可以通过选择 ***Templates***（模板） > ***Device***（设备） > ***Authentication Profile***（身份验证配置文件）来查看远程网络模板的身份验证配置文件。选择 ***Remote_Network_Template***。



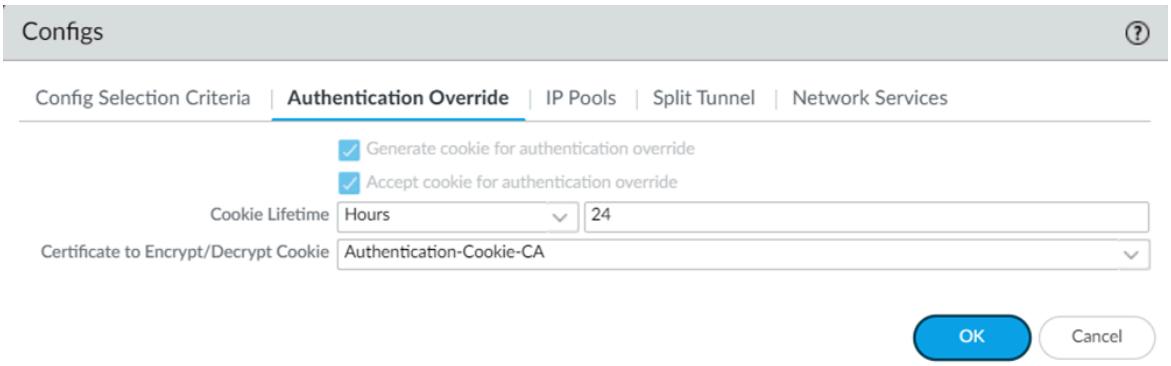
©2025 Palo Alto Networks, Inc.

STEP 6 | 为远程网络模板创建一个设备证书，类似于移动用户模板中的设备证书。

1. 选择远程网络模板（即 **GlobalProtect_Internal_Gateway**）超链接。
2. 转到 **Agent**（代理） > **Client Settings**（客户端设置）。



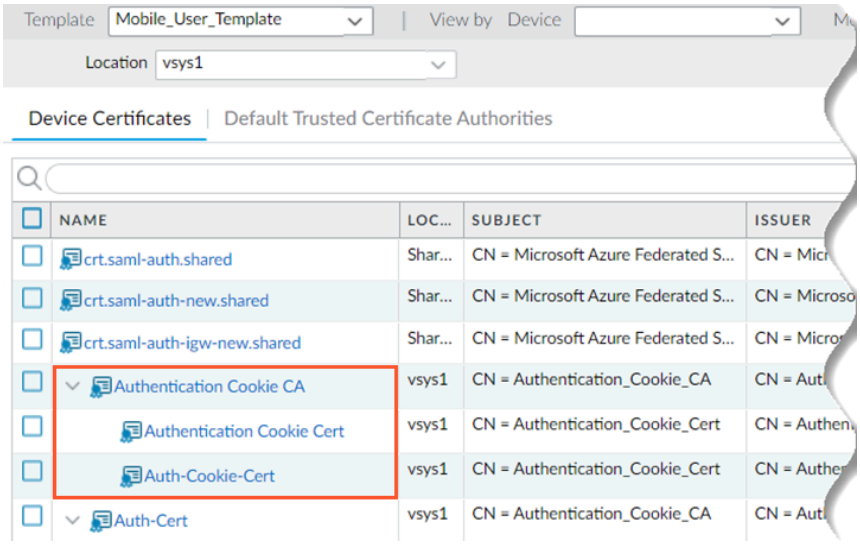
3. 选择 **DEFAULT**（默认）配置，然后转到 **Authentication Override**（身份验证覆盖）设置。
4. 编辑 **Certificate to Encrypt/Decrypt Cookie**（用于加密/解密 **Cookie** 的证书）设置，并创建新的设备证书。



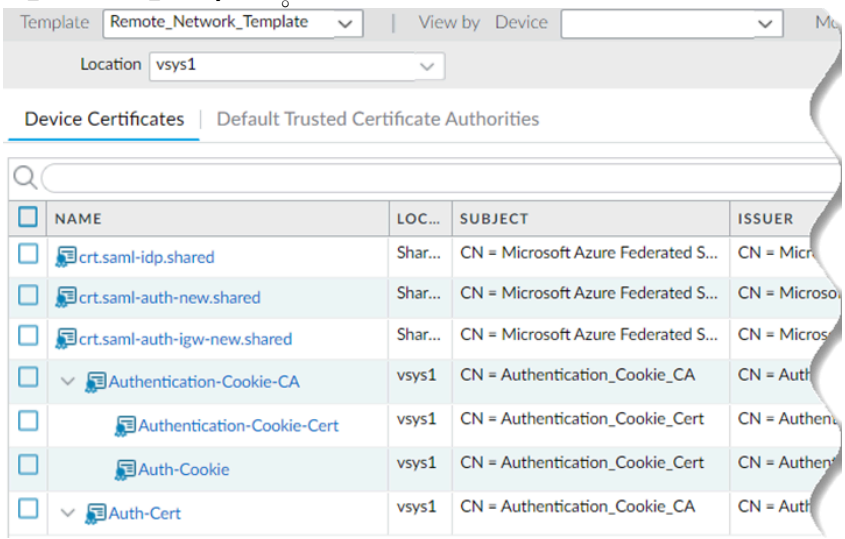
创建一个与移动用户模板中的设备证书相同的证书。您可以在 **Templates**（模板） > **Device**（设备） > **Certificate Management**（证书管理） > **Certificates**（证书） > **Device Certificates**（设备证书）下找到移动用户模板中使用的设备证书。确保选择 **Mobile_User_Template**。**DEFAULT**（默认）配置引用 **Authentication Cookie CA**（身份

 ©2025 Palo Alto Networks, Inc.

验证 **Cookie CA**）证书。要确保身份验证成功，请遵循与 **Mobile_User_Template** 中相同的层次结构。



还可以通过选择 ***Templates***（模板） ***> Device***（设备） ***> Certificate Management***（证书管理） ***> Certificates***（证书） ***> Device Certificates***（设备证书）来查看远程网络模板的设备证书。选择 ***Remote_Network_Template***。



STEP 7 | 选择 **Push**（推送）以同时将更改推送到移动用户和远程网络。

提供对远程网络地点的安全入站访问

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证，包括用于站点到站点访问和用户到站点访问的 Net Interconnect

©2025 Palo Alto Networks, Inc.

如果您的组织在远程网络站点托管可通过互联网访问的应用程序，则提供对这些应用程序的访问权限会使您的网络面临由开放互联网带来的所有威胁。本节介绍 Prisma Access 如何提供对这些应用程序进行安全访问的方法、应在什么情况下实施以及如何对其进行配置。

- 确保远程网络站点的入站访问安全
- 确保入站访问安全的示例
- 安全入站访问使用指南
- 为远程网络站点配置安全入站访问

确保远程网络站点的入站访问安全

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证，包括用于站点到站点和用户到站点访问的网络互连

适用于远程网络的 Prisma Access 允许对连接互联网的应用程序进行出站访问。在某些情况下，您的组织可能需要提供对远程站点上应用程序或网站的入站访问，并为任何连接互联网的用户（而不仅仅是受 Prisma Access 保护的用户）提供对该应用程序的安全访问。例如：

- 您在远程网络站点上托管面向公众的自定义应用程序或门户。
- 您有一个实验室或暂存环境，想要为其提供安全访问。
- 您需要向非组织域成员的用户提供对应用程序或网站的访问权限。
- 您拥有需要访问内部资产管理、跟踪或状态应用程序的 IoT 设备。

为此，请创建一个允许安全入站访问的远程网络。如果需要对远程网络站点进行出站访问和入站访问，请在同一位置创建两个远程网络 — 一个用于入站访问，一个用于出站访问。

虽然该解决方案可以为每个远程网络提供最多 *50,000* 个并发入站会话的访问权限，但 *Palo Alto Networks* 不建议使用此解决方案来提供对大容量应用程序或网站的访问。

确保入站访问安全的示例

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证，包括用于站点到站点和用户到站点访问的网络互连

本节提供了入站访问示例，以及 Prisma Access 在各种部署中分配的 IP 地址。

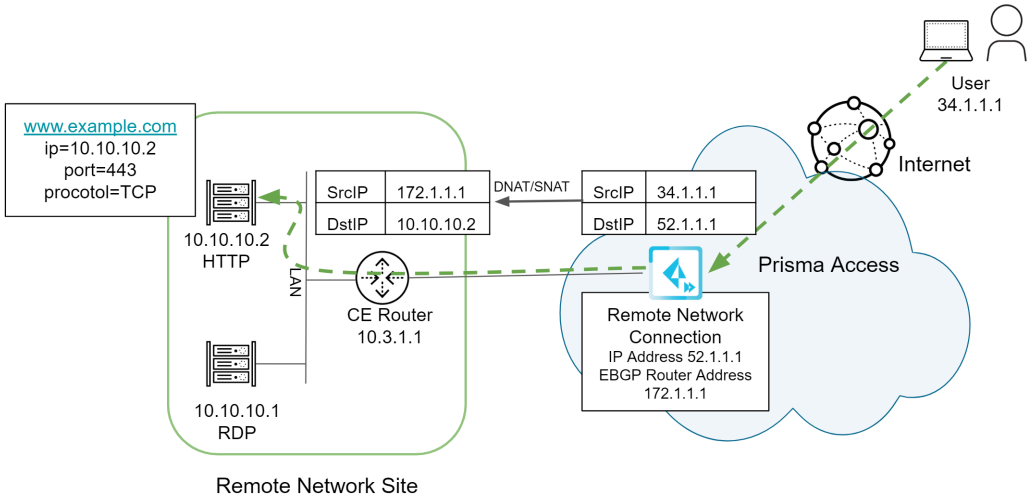
以下示例显示了为远程网络站点的应用程序 (www.example.com) 启用入站访问的示例配置。您为该应用程序分配 IP 地址 10.10.10.2、端口 443 和 TCP 协议。然后，在配置入站访问时，您在

 ©2025 Palo Alto Networks, Inc.

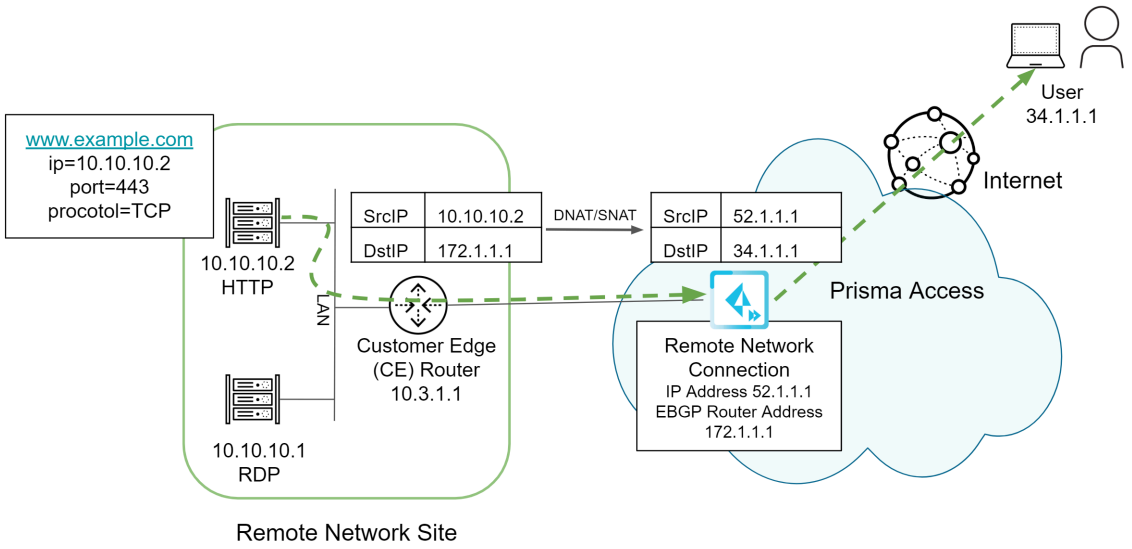
Prisma Access 中输入这些值。保存并提交更改后， Prisma Access 为您定义的应用程序分配一个公共 IP 地址，在本例中为 52.1.1.1。

Prisma Access 默认对数据包执行源网络地址转换（源 NAT）。如果远程网络站点上支持 IPSec 的设备能够执行对称返回（例如 Palo Alto Networks 新一代防火墙），则可以禁用源 NAT。

下图显示了从用户到应用程序的流量流向。由于启用了源 NAT，路由表中的源 IP 地址从用户设备的 IP (34.1.1.1) 更改为远程网络的 **EBGP Router**（**EBGP** 路由器）地址（**Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息） > **Remote Networks**（远程网络） > **EBGP Router**（**EBGP** 路由器））。(172.1.1.1)。

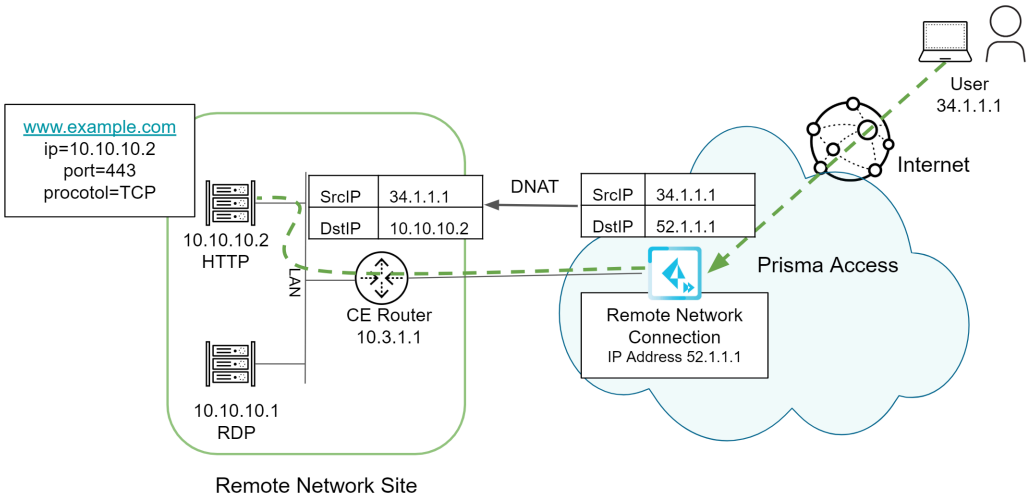


下图显示了启用源 NAT 后的流量返回路径。

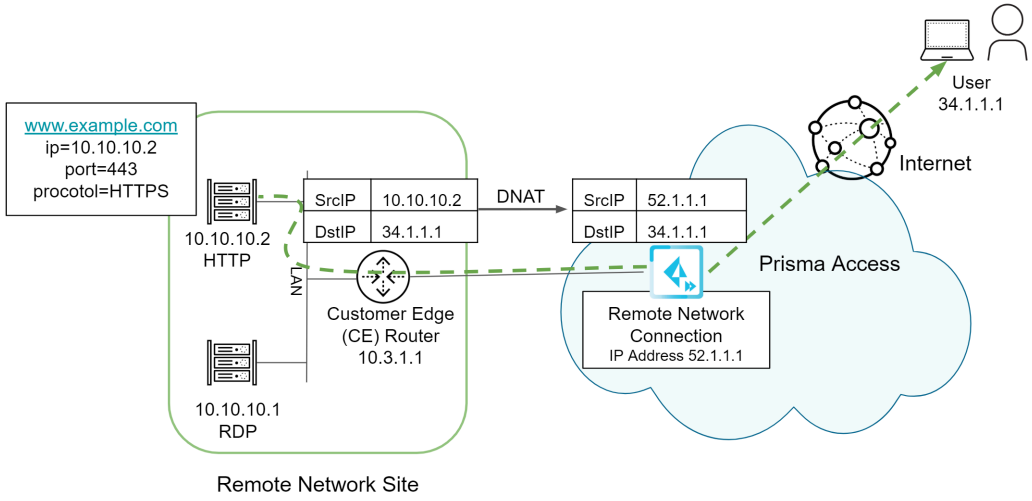


如果禁用源 NAT， Prisma Access 仍会执行目标 NAT，但是请求的源 IP 地址不变。

 ©2025 Palo Alto Networks, Inc.



对于返回流量，SNAT 将被禁用，并且所有路由表的目标地址都是用户的 IP 地址 (34.1.1.1)。



如果您的资源位于已启用入站访问的远程网络站点中，并且您希望非入站访问站点的用户可以访问该资源，则在配置非入站访问远程网络时，可以 **Allow inbound flows to other Remote Networks over the Prisma Access backbone**（允许入站流量通过 **Prisma Access** 主干网流向其他远程网络）。

如果允许来自其他远程网络的入站流量，则必须启用源 *NAT*。



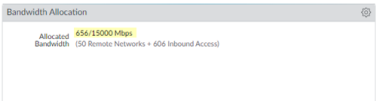
 ©2025 Palo Alto Networks, Inc.

安全入站访问使用指南

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证，且包含“站点到站点”和“用户到站点”访问权的网络互联

将远程网络配置为使用安全入站访问时，请遵循以下准则和限制：

- 配置远程网络以实现入站访问时，需要根据分配的 IP 地址，从许可证中分配相应的带宽单位 (Mbps)（分配 5 个 IP 地址需配置 150 Mbps，分配 10 个 IP 地址需配置 300 Mbps）。因此在开始之前，请确保您有足够的剩余许可带宽来接入入站访问远程网络。要查看可用带宽，请选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Remote Networks**（远程网络），然后查看获得许可的 **Bandwidth Allocation**（带宽分配）。该区域显示您已分配的带宽以及总许可带宽。



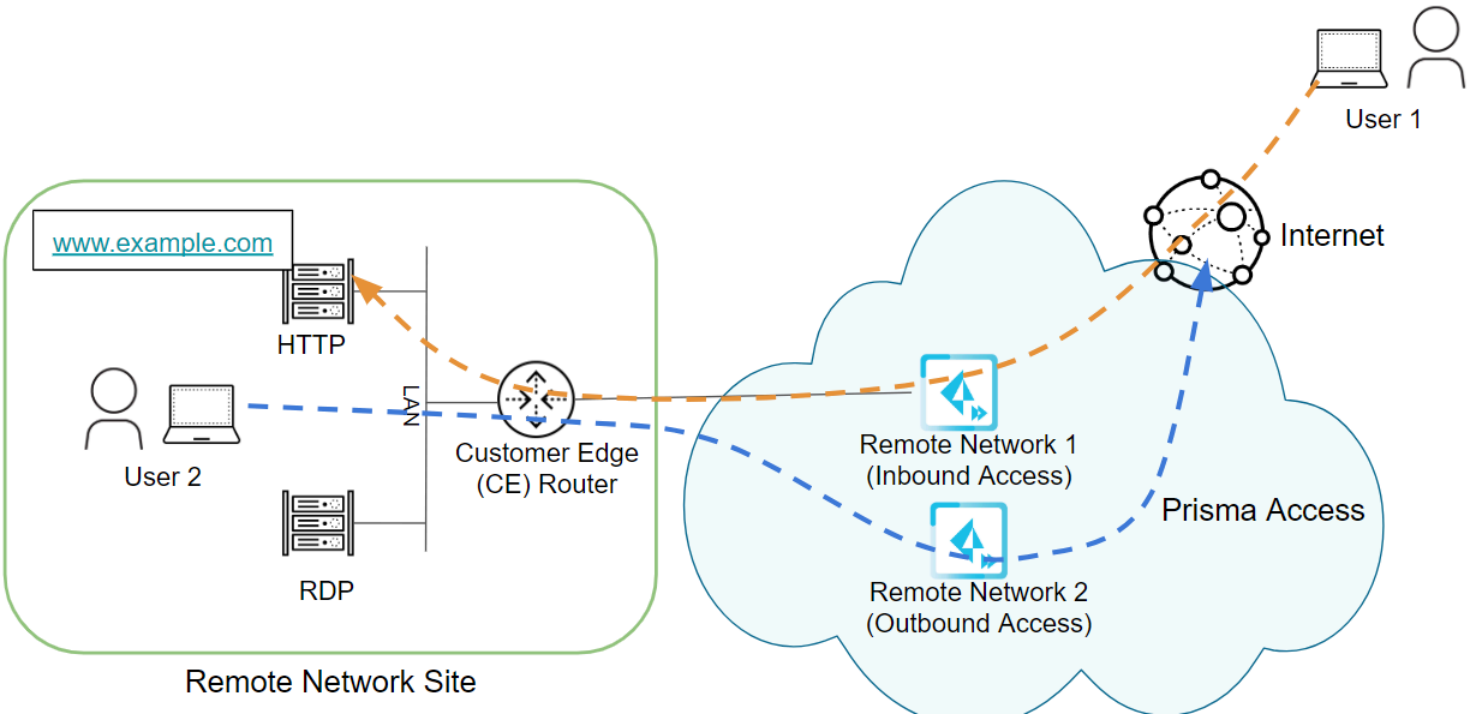
- 安全入站访问使用 Prisma Access 位置的某个子集。
- 无法通过对现有的远程网络进行修改来提供安全的入站访问；而是需要创建一个新的远程网络。
- 入站访问功能在使用 ECMP 负载平衡的远程网络上不可用。
- 不支持应用程序端口转换。
- 用于接入远程网络的批量导入功能不支持入站访问。使用 Panorama 来接入新的入站访问远程网络。
- 请勿将远程网络入站访问与带有服务连接的流量转发规则一起使用。
- 入站远程网络上不允许来自分支的出站流量。
- 不支持 User-ID 和应用程序身份验证。
- Prisma Access 强制实施以下速率限制阈值以提供洪泛攻击保护，并以每秒连接数（简称 CPS）来衡量速率：

洪泛攻击保护类型	警报率（以 **CPS** 为单位）	激活率（以 **CPS** 为单位）
SYN 洪泛攻击	10000	15000
ICMP 洪泛攻击	20	20

  如果您需要针对新会话提供更强的泛洪攻击手段，请联系您的 Palo Alto Networks 团队。
- 配置为用于安全入站访问的远程网络只能用于该目的。如果您需要为某个远程网络站点同时提供入站访问和出站访问，请在同一位置创建两个远程网络站点，一个用于入站访问，另一个用

©2025 Palo Alto Networks, Inc.

于出站访问，如下图所示。在这个例子中，用户 1 使用远程网络 1 访问www.example.com，用户 2 则使用远程网络 2 从远程网络位置进行出站互联网访问。



- 如果您有一个自定义 Prisma Access 部署，其中一个云提供商被排除，则可能不支持入站访问；在这种情况下，您无法在远程网络接入时选择位置。
- 不支持使用评估许可证进行安全入站访问。

为远程网络站点配置安全入站访问

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证，包括用于站点到站点访问和用户到站点访问的 Net Interconnect

您的部署可能按计算地点载入带宽或按地点载入带宽；这两种方法均支持配置远程网络入站访问。当您为按计算地点分配带宽的远程网络配置入站访问时，可以根据每个地点指定带宽。要创建允许安全入站访问的远程网络站点，请完成以下工作流之一：

- 要为按计算地点分配带宽的远程网络部署配置安全入站访问，请完成此工作流。
- 要为按地点分配带宽的远程网络部署配置安全入站访问，请完成此工作流。

©2025 Palo Alto Networks, Inc.

为远程网络配置安全入站访问

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	• Prisma Access 许可证，包括用于站点到站点访问和用户到站点访问的 Net Interconnect

为了使应用程序可从远程网络站点访问互联网，请先列出您要提供访问权限的应用程序，并为每个应用程序分配专用 IP、端口号和协议组合。如果将同一个 IP 地址用于多个应用程序，则每个应用程序的端口/协议组合必须是唯一的；如果将相同的端口/协议组合用于多个应用程序，则每个 IP 地址必须是唯一的。

要开始配置，请选择要为该应用程序关联的公共 IP 地址的数量。您可以为每个远程网络站点指定 5 个或 10 个公共 IP 地址。除了您为与远程网络关联的计算地点分配的带宽之外，所分配的每个公共 IP 都会从远程网络许可证中占用带宽（单位）。若分配 5 个 IP 地址，则占用远程网络许可证中 150 Mbps 的带宽，10 个 IP 地址则占用 300 Mbps 的带宽。

选择公共 IP 地址的数量后，输入要为其提供安全入站访问的应用程序及其关联的专用 IP/端口号/协议组合。

您可以决定将应用程序映射到公共 IP 地址的方式。默认情况下，Prisma Access 将公共 IP 地址分配给您指定的应用程序，并且可以向多个应用程序分配单个 IP 地址。如果您需要将单个应用程序映射到单个公共 IP 地址，则可以在系统配置期间选择 **Dedicated IP**（专用 IP）。您可以为每组预配置的公共 IP 地址（5 个或 10 个）配置最多 100 个入站应用程序。

- Strata Cloud Manager
- Panorama

为远程网络配置安全入站访问 *(Strata Cloud Manager)*

下面介绍如何使连接互联网的所有用户（而不仅仅是 Prisma Access 个用户）能够从远程网络站点访问应用程序。

STEP 1 | 如果您尚未进行过此配置，请查看入站访问远程网络指南。

STEP 2 | 收集开始使用该应用程序所需的详细信息。

列出您要提供访问权限的应用程序，并为每个应用程序分配专用 IP、端口号和协议组合。如果将同一个 IP 地址用于多个应用程序，则每个应用程序的端口/协议组合必须是唯一的；如果将相同的端口/协议组合用于多个应用程序，则每个 IP 地址必须是唯一的。

STEP 3 | 在 Strata Cloud Manager 中，转到 **Workflows**（工作流） > **Prisma Access** 设置 > **Remote Networks**（远程网络） > **Inbound Access**（入站访问） > **Add Inbound Access**（添加入站访问权限）。

 ©2025 Palo Alto Networks, Inc.

STEP 4 | 输入所需的详细信息。

选择要用于这些应用程序的 **Number of Public IPs**（公共 **IP** 的数量），可以是 5 或 10 个。

除了远程网络的许可证费用外，分配的每个公共 IP 都会占用您的远程网络许可证中的带宽。若分配 5 个 IP 地址，则占用远程网络许可证中 150 MB 的带宽，10 个 IP 地址则占用 300 MB 的带宽。

从 Prisma Access 4.1 版本开始，如果您的资源位于已启用入站访问的远程网络站点中，并且您希望非入站访问站点的用户可以访问该资源，则在配置非入站访问远程网络时，您可以 **Allow inbound flows to other Remote Networks over the Prisma Access backbone**（允许入站流量通过 **Prisma Access** 骨干网络流向其他远程网络）。

从 Prisma Access 版本 5.0 开始，当配置非入站访问远程网络时，您可以允许入站流量通过服务提供商 (SP) 骨干网络流向其他远程网络。

SP 互连仅支持：

- *GCP* 区域
- 新的 *Prisma Access* 部署
- 显式代理出口流量

STEP 5 | 添加您要保护其访问的 **Inbound Access Applications**（入站访问应用程序）。

为该应用程序添加关联的专用 IP/端口号/协议组合。

STEP 6 | 确定您希望如何将应用程序映射到公共 IP 地址。

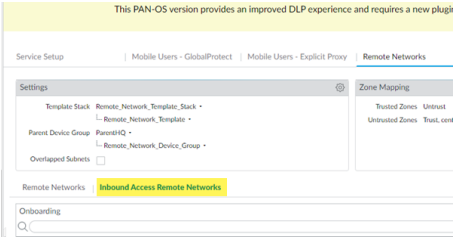
默认情况下，Prisma Access 将公共 IP 地址分配给您指定的应用程序，并且可以向多个应用程序分配单个 IP 地址。如果您需要将单个应用程序映射到单个公共 IP 地址，则可以在系统配置期间 **Assign Dedicated IP**（分配专用 **IP**）。您可以为每组预配置的公共 IP 地址（5 个或 10 个）配置最多 100 个入站应用程序。

STEP 7 | 像设置常规远程网络站点一样完成入站访问远程网络的设置。

为远程网络配置安全入站访问 *(Panorama)*

如果您的 Prisma Access 部署按计算地点分配远程网络带宽，请通过完成以下步骤来配置入站访问。

STEP 1 | 选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Remote Networks**（远程网络），然后选择 **Inbound Access Remote Networks**（入站访问远程网络）。



STEP 2 | **Add**（添加）入站访问的远程网络。

 ©2025 Palo Alto Networks, Inc.

STEP 3 | 指定入站访问远程网络连接的设置。

1. 输入入站访问连接的 **Name**（名称）。
2. 输入 **Location**（位置）。

   入站访问支持位置子集。
3. 指定用于入站访问连接的 **Bandwidth**（带宽）。

   您可以根据每个位置为入站访问连接分配带宽。
4. 指定用于入站访问连接的 **Number of Public IPs**（公共 **IP** 的数量）。

   指定 5 个或 10 个公共 IP 地址。除了您为与远程网络关联的计算地点分配的带宽之外，所分配的每个公共 IP 都会从远程网络许可证中占用带宽（单位）。
5. 选择用于入站访问连接的 IPSec 隧道。
6. 选择是否允许入站流量通过 **Prisma Access** 骨干网络流向其他远程网络。

   如果您的资源位于已启用入站访问的远程网络站点中，并且您希望非入站访问站点的用户可以访问该资源，则在配置非入站访问远程网络时，可以允许入站流量通过 **Prisma Access** 骨干网络流向其他远程网络。如果允许来自其他远程网络的入站流量，则必须启用源 NAT。
7. （可选）如果此位置有辅助 WAN 链路，请选择 **Enable Secondary WAN**（启用辅助 **WAN**），并提供与主 IPSec 隧道不同的 **IPSec Tunnel**（**IPSec** 隧道）。

STEP 4 | 为您的部署配置 **Static Routes**（静态路由）、**BGP** 和 **QoS**。

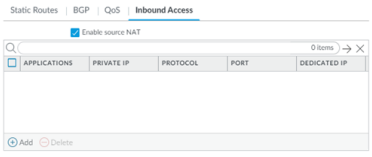
此配置与非入站访问远程网络连接相同。

STEP 5 | 单击 **Inbound Access**（入站访问）选项卡以配置入站访问选项。

1. （可选）要禁用源 NAT，请取消选择 **Enable Source NAT**（启用源 **NAT**）。

   默认情况下，源 NAT 处于已启用状态。如果远程网络站点上支持 IPSec 的设备能够执行对称返回（例如 Palo Alto Networks 新一代防火墙），或者如果您未选择允许入站流量通过 **Prisma Access** 骨干网络流向其他远程网络，请取消选择 **Enable source NAT**（启用源 **NAT**）。

   如果选中此复选框，则必须在 ***Inbound Access***（入站访问）选项卡中选择 ***Enable source NAT***（启用源 ***NAT***）。源 *NAT* 是允许入站流量流向其他远程网络的必要条件。

2. **Add**（添加）应用程序以提供安全的入站访问。

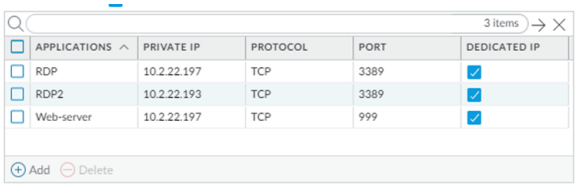
   您可以为每组预配置的公共 IP 地址（5 个或 10 个）配置最多 100 个入站应用程序。为每个应用程序输入唯一的 **Private IP**（专用 **IP**）地址、**Protocol**（协议）和 **Port**（端

 ©2025 Palo Alto Networks, Inc.

口）组合。可以将重复的专用 IP 地址和端口用于两个应用程序，只要您为一个应用程序选择 **TCP**，为另一个应用程序选择 **UDP** 即可。

提供以下值：

- 指定 **Application**（应用程序）的名称。
- 指定要用于此应用程序的 **Private IP**（专用 **IP**）地址。
- 指定要用于该应用程序的 **Protocol**（协议）（**TCP** 或 **UDP**）。
- 指定要用于该应用程序的 **Port**（端口）。
- 选择是否要将单个公共 IP 地址专用于单个应用程序；为此，请选择 **Dedicated IP**（专用 **IP**）。

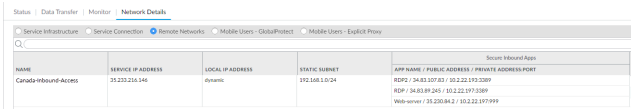


STEP 6 | 单击 **OK**（确定）保存更改。

STEP 7 | **Save**（保存）并 **Commit**（提交）更改。

STEP 8 | 等待约 30 分钟，以便 Prisma Access 生成公共 IP 地址；然后选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息） > **Remote Networks**（远程网络），并记下与您创建的应用程序的 **App Name**（应用程序名称）关联的 **Public Address**（公共地址）。

如果您选择了 **Dedicated IP**（专用 **IP**），请找到与 **Public Address**（公共地址）关联的单个应用程序。



 ©2025 Palo Alto Networks, Inc.

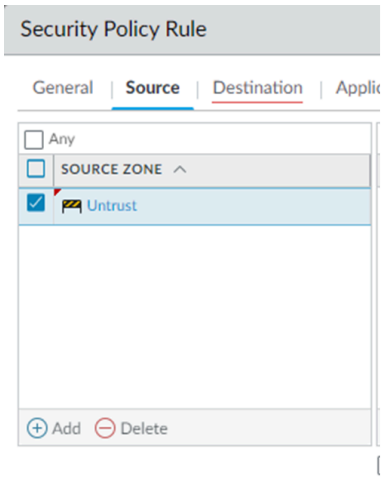
STEP 9 | 创建安全策略以允许来自入站互联网用户的流量。

由于 Prisma Access 的默认安全策略仅允许 untrust-to-untrust 流量，因此您需要配置安全策略以允许入站访问应用程序的 untrust-to-trust 流量。Palo Alto Networks 建议您限制允许入站应用程序访问的类型。以下示例提供对 SSH 服务器、Web 门户和 RDP 服务器的访问权限。

1. 选择 **Policies**（策略） > **Security**（安全），然后 **Add**（添加）策略。

   请确保在 **Remote_Network_Device_Group** 设备组下创建此策略。

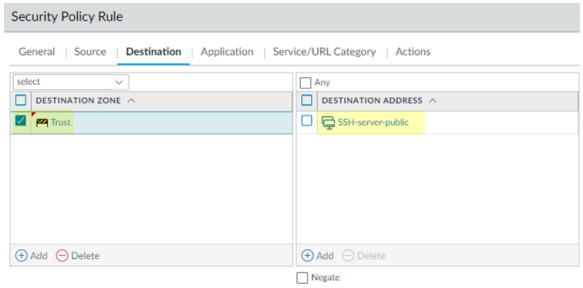
2. 为 **Source**（源）流量选择 **Untrust**（不可信）。



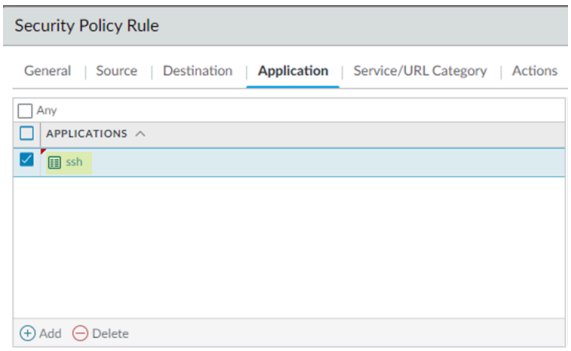
3. 创建策略以允许 SSH 服务器流量，方法是为目标流量的 **Destination Zone**（目标服务区）选择 **Trust**（信任），并将 **Destination Address**（目标地址）指定为 **SSH-server-**

 ©2025 Palo Alto Networks, Inc.

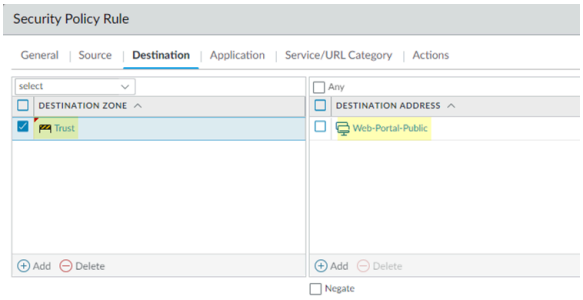
public。这是您创建的地址或地址组对象，其中包含用于 SSH 登录的所有公共 IP 地址的列表。



4. 为 **Application**（应用程序）选择 **ssh**。

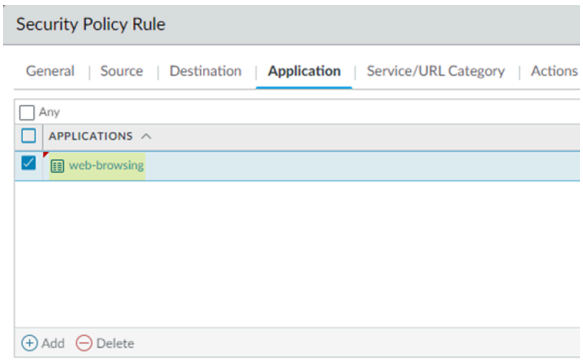


5. 选择 **application-default** 作为 **Service/URL Category**（服务/**URL** 类别），以便仅根据 Palo Alto Networks 定义的默认端口允许或拒绝应用程序。
6. 在 **Actions**（操作）中，选择 **Allow**（允许）。
7. 单击 **OK**（确定）以保存策略。
8. 创建策略以允许 Web 门户访问，方法是在前面的步骤中创建策略，但在 **Destination**（目标）和 **Application**（应用程序）选项卡中替换以下设置：
   - 选择 **Web-Portal-Public** 作为某个地址或地址组的 **Destination Address**（目标地址），其中包含 Web 门户的所有公共 IP 地址。



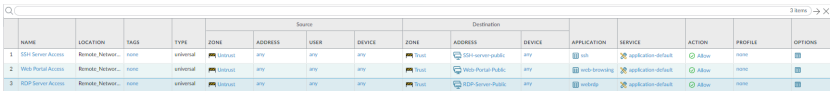
   - 在 **Application**（应用程序）中选择 **web-browsing**。

©2025 Palo Alto Networks, Inc.



9. 为 RDP 服务器访问创建安全策略，使用与其他策略相同的设置，但需要创建一个名为 **RDP-Server-Public** 的地址或地址组对象，其中包含 RDP 服务器的公共 IP 地址（作为 **Destination Address**（目标地址））和 **webrdp**（作为 **Application**（应用程序））。

   完成后，您将拥有三个不同的策略来允许 SSH 服务器访问、Web 门户访问和 RDP 服务器访问。

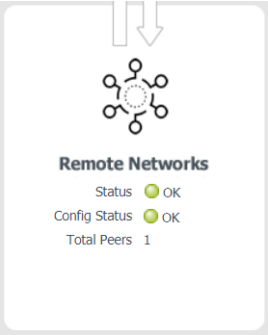


STEP 10 | **Save**（保存）并 **Commit**（提交）更改。

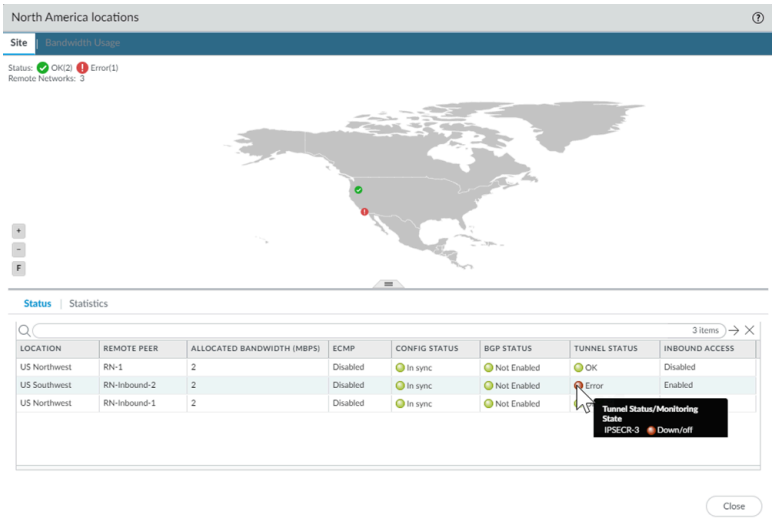
 ©2025 Palo Alto Networks, Inc.

STEP 11 | 检查远程网络连接是否正常运行并正确处理入站流量。

1. 选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > > **Status**（状态） > **Remote Networks**（远程网络），将鼠标悬停在 **Status**（状态）和 **Config Status**（配置状态）区域上以查看隧道的状态。



2. 如果发现问题，请选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > > **Monitor**（监控） > **Remote Networks**（远程网络），选择该远程网络隧道在地图中的位置，然后将鼠标悬停在 **Tunnel Status**（隧道状态）区域上以确定错误的原因。



为按地点分配带宽的地点配置远程网络站点的安全入站访问

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	• Prisma Access 许可证，包括用于站点到站点访问和用户到站点访问的 Net Interconnect

如果您的 Prisma Access 部署按地点分配远程网络带宽，请通过完成以下步骤来配置入站访问。

 ©2025 Palo Alto Networks, Inc.

STEP 1 | 选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Remote Networks**（远程网络），**Add**（添加）连接，然后配置远程网络，包括路由和 IPSec 隧道选项。

有关详细信息，请参阅Prisma Access 远程网络。您的部署可能按计算地点或按地点加入带宽；这两种方法均支持入站访问。

确保您选择了入站访问支持的地点之一。

STEP 2 | 单击 **Inbound Access**（入站访问）选项卡以配置入站访问选项。

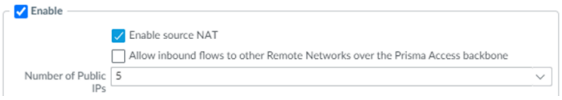
1. 选择 **Enable**（启用）以启用远程网络的入站访问。

   如果您选择的地点不支持入站访问，Prisma Access 会提示您选择支持的地点。

2. （可选）要禁用源 NAT，请取消选择 **Enable Source NAT**（启用源 **NAT**）。

   默认情况下，源 NAT 处于已启用状态。如果远程网络站点上支持 IPSec 的设备能够执行对称返回（例如 Palo Alto Networks 新一代防火墙），或者如果您未选择 **Allow inbound flows to other Remote Networks over the Prisma Access backbone**（允许入站流量通过 **Prisma Access** 骨干网络流向其他远程网络），请取消选择 **Enable source NAT**（启用源 **NAT**）。

   如果选中此复选框，则必须在 ***Inbound Access***（入站访问）选项卡中选择 ***Enable source NAT***（启用源 ***NAT***）。源 *NAT* 是允许入站流量流向其他远程网络的必要条件。



STEP 3 | **Add**（添加）应用程序以提供安全的入站访问。

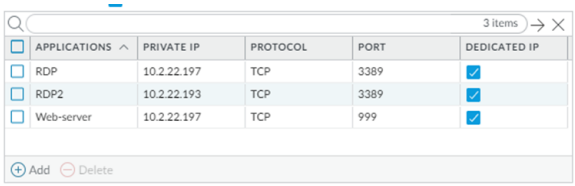
您可以为每组预配置的公共 IP 地址（5 个或 10 个）配置最多 100 个入站应用程序。为每个应用程序输入唯一的 **Private IP**（专用 **IP**）地址、**Protocol**（协议）和 **Port**（端口）组合。可以

 ©2025 Palo Alto Networks, Inc.

将重复的专用 IP 地址和端口用于两个应用程序，只要您为一个应用程序选择 **TCP**，为另一个应用程序选择 **UDP** 即可。

提供以下值：

- 指定 **Application**（应用程序）的名称。
- 指定要用于此应用程序的 **Private IP**（专用 **IP**）地址。
- 指定要用于该应用程序的 **Protocol**（协议）（**TCP** 或 **UDP**）。
- 指定要用于该应用程序的 **Port**（端口）。
- 选择是否要将单个公共 IP 地址专用于单个应用程序；为此，请选择 **Dedicated IP**（专用 **IP**）。

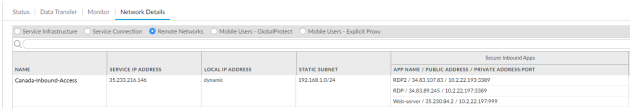


STEP 4 | 单击 **OK**（确定）保存更改。

STEP 5 | **Save**（保存）并 **Commit**（提交）更改。

STEP 6 | 等待约 30 分钟，以便 Prisma Access 生成公共 IP 地址；然后选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息） > **Remote Networks**（远程网络），并记下与您创建的应用程序的 **App Name**（应用程序名称）关联的 **Public Address**（公共地址）。

如果您选择了 **Dedicated IP**（专用 **IP**），请找到与 **Public Address**（公共地址）关联的单个应用程序。



 ©2025 Palo Alto Networks, Inc.

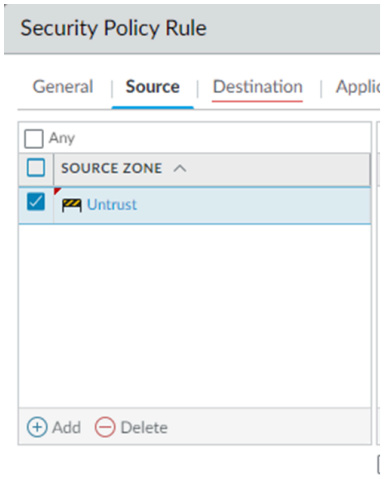
STEP 7 | 创建安全策略以允许来自入站互联网用户的流量。

由于 Prisma Access 的默认安全策略仅允许 untrust-to-untrust 流量，因此您需要配置安全策略以允许入站访问应用程序的 untrust-to-trust 流量。Palo Alto Networks 建议您限制允许入站应用程序访问的类型。以下示例提供对 SSH 服务器、Web 门户和 RDP 服务器的访问权限。

1. 选择 **Policies**（策略） > **Security**（安全），然后 **Add**（添加）策略。

   请确保在 **Remote_Network_Device_Group** 设备组下创建此策略。

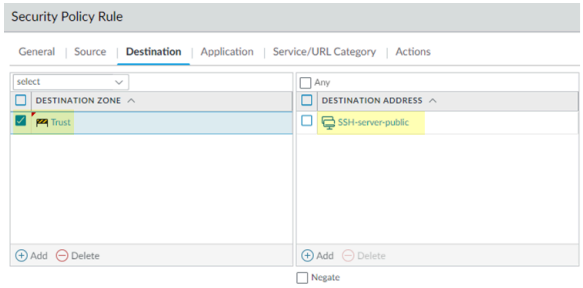
2. 为 **Source**（源）流量选择 **Untrust**（不可信）。



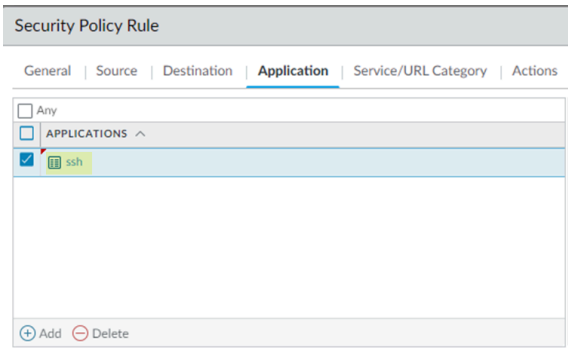
3. 创建策略以允许 SSH 服务器流量，方法是为目标流量的 **Destination Zone**（目标服务区）选择 **Trust**（信任），并将 **Destination Address**（目标地址）指定为 **SSH-server-**

 ©2025 Palo Alto Networks, Inc.

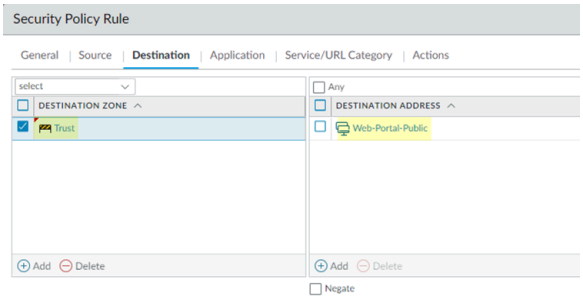
public。这是您创建的地址或地址组对象，其中包含用于 SSH 登录的所有公共 IP 地址的列表。



4. 为 **Application**（应用程序）选择 **ssh**。

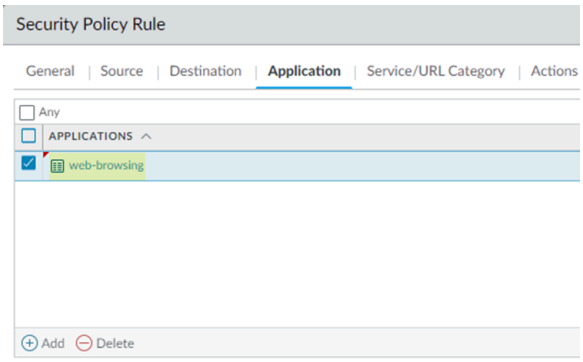


5. 选择 **application-default** 作为 **Service/URL Category**（服务/**URL** 类别），以便仅根据 Palo Alto Networks 定义的默认端口允许或拒绝应用程序。
6. 在 **Actions**（操作）中，选择 **Allow**（允许）。
7. 单击 **OK**（确定）以保存策略。
8. 创建策略以允许 Web 门户访问，方法是在前面的步骤中创建策略，但在 **Destination**（目标）和 **Application**（应用程序）选项卡中替换以下设置：
   - 选择 **Web-Portal-Public** 作为某个地址或地址组的 **Destination Address**（目标地址），其中包含 Web 门户的所有公共 IP 地址。



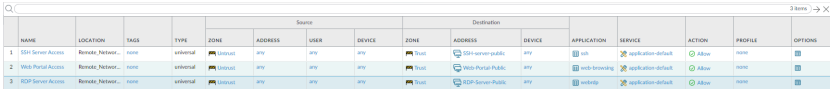
   - 在 **Application**（应用程序）中选择 **web-browsing**。

©2025 Palo Alto Networks, Inc.



9. 为 RDP 服务器访问创建安全策略，使用与其他策略相同的设置，但需要创建一个名为 **RDP-Server-Public** 的地址或地址组对象，其中包含 RDP 服务器的公共 IP 地址（作为 **Destination Address**（目标地址））和 **webrdp**（作为 **Application**（应用程序））。

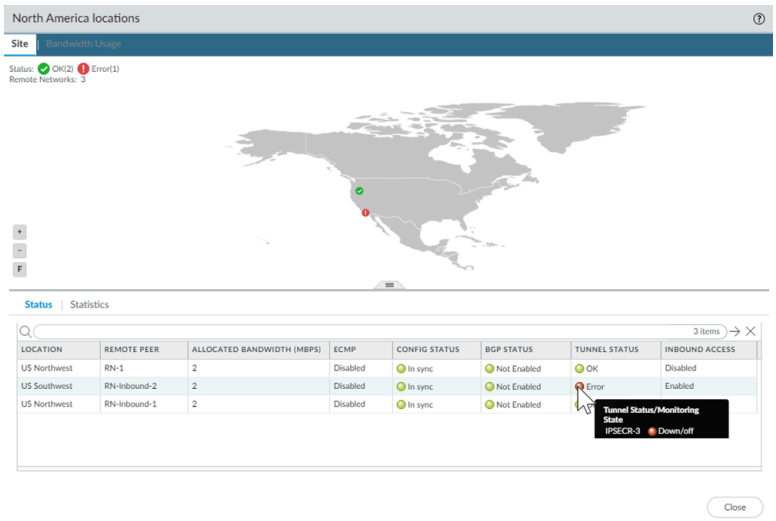
   完成后，您将拥有三个不同的策略来允许 SSH 服务器访问、Web 门户访问和 RDP 服务器访问。



STEP 8 | **Save**（保存）并 **Commit**（提交）更改。

STEP 9 | 检查远程网络连接是否正常运行并正确处理入站流量。

1. 选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > > **Status**（状态） > **Remote Networks**（远程网络），将鼠标悬停在 **Status**（状态）和 **Config Status**（配置状态）区域上以查看隧道的状态。
2. 如果发现问题，请选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > > **Monitor**（监控） > **Remote Networks**（远程网络），选择该远程网络隧道在地图中的位置，然后将鼠标悬停在 **Tunnel Status**（隧道状态）区域上以确定错误的原因。



 ©2025 Palo Alto Networks, Inc.

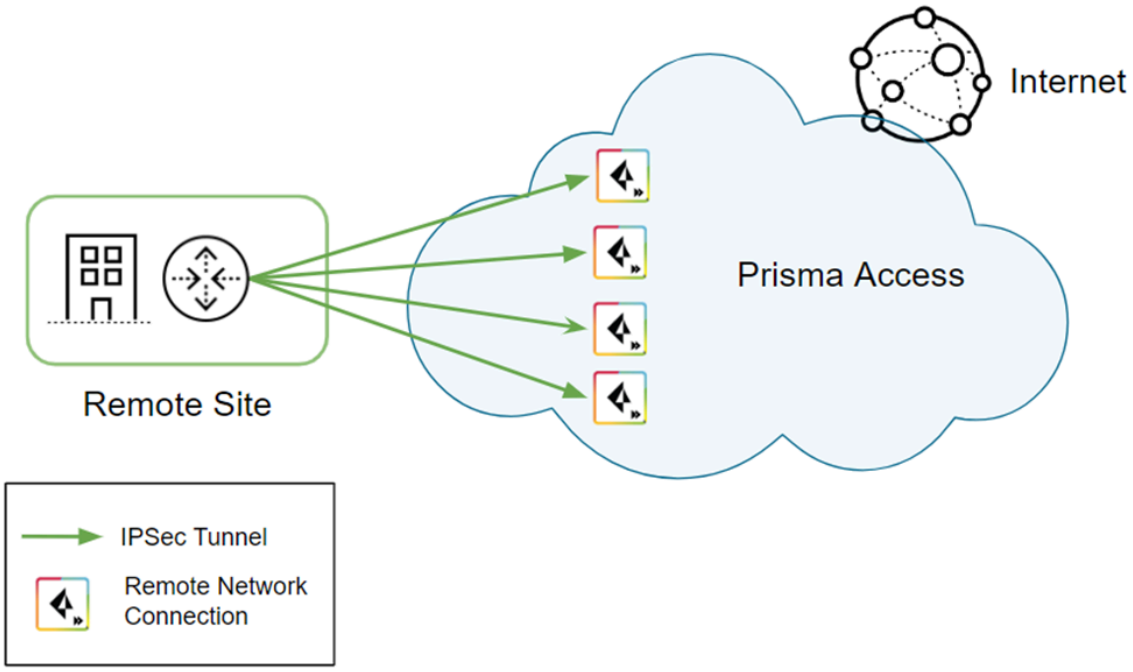
为远程站点创建高带宽网络

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

如果要通过与 Prisma Access 的高带宽连接来保护分支机构或站点的出站互联网访问，则可以通过完成本节中的步骤，使用多个 IPSec 隧道对来自分支机构或站点的流量进行负载均衡。

下图显示了使用同一远程站点的四个远程网络连接。在加入之前，为计算地点分配 4 Gbps (4000 Mbps)，在本例中为韩国，对应于远程站点。4000 Mbps 提供四个 IPSec 终止节点，每个 IPSec 终止节点提供最大 1000 Mbps 的带宽。在加入过程中为每个远程网络连接分配其自己的 IPSec 终止节点，以利用完整的带宽。

此示例显示了四个隧道。*Prisma Access* 中可用于高带宽连接的最大隧道数取决于客户终端设备 *(CPE)* 支持的 *IPSec* 隧道的最大数量以及您使用的负载均衡协议。



在部署此配置之前，请考虑以下限制和建议：

- 对 IPSec 隧道使用 BGP 路由；不支持静态路由。
- 仅将此配置用于出站互联网访问。
- 请勿在 Prisma Access 或 CPE 上使用隧道监控。通过 CPE 和 Prisma Access 远程网络之间的 BGP 对等体关系确定 IPSec 隧道的可用性。如果 IPSec 隧道关闭且 BGP 连接中断，则通过该隧道上的 BGP 学习到的路由将自动从 ECMP 中删除。
- 由于您使用 BGP 来确定隧道是何时关闭的，因此请考虑您在 CPE 上配置的 HoldTime 值。保持计时器确定在删除路由之前隧道关闭的时间。Prisma Access 使用 RFC 4271 定义的默认 BGP HoldTime 值 90 秒。如果在远程网络站点中为 BGP CPE 配置了较低的保持时间，则 BGP 将使

©2025 Palo Alto Networks, Inc.

用较低的保持时间值。Palo Alto Networks 建议在此部署中为 CPE 设置 10 秒的 KeepAlive 值和 30 秒的 HoldTime 值。

要创建高带宽远程网络连接，请完成以下任务。

©2025 Palo Alto Networks, Inc.

STEP 1 | 在 Panorama 中，配置 Prisma Access 远程网络隧道。

1. （可选）如果尚未设置 IKE 网关、IKE 加密和 IPSec 加密配置文件，以及您创建的远程网络连接的 IPSec 隧道，请进行设置。

   记下 IKE 和 IPSec 加密配置文件；在用于终止远程网络位置中的远程网络连接的 CPE 上指定相同的设置。

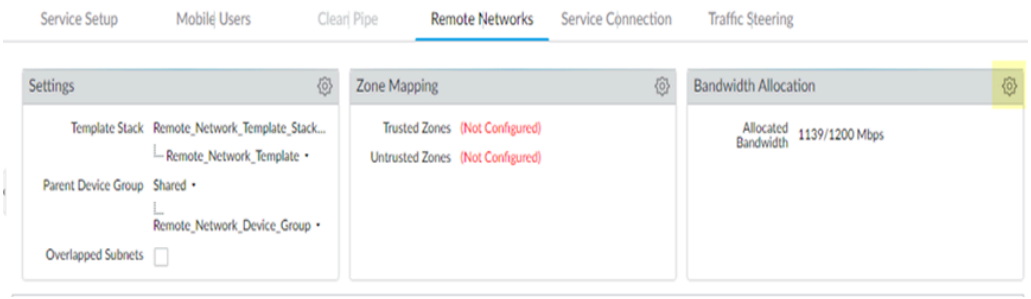
2. 确定您拥有的远程网络部署的类型。

   Prisma Access 部署按计算地点分配带宽或按地点分配带宽。

3. 加入远程网络。

   - 要加入按计算地点分配带宽的远程网络，请执行以下操作：

     1. 单击 **Bandwidth Allocation**（带宽分配）区域中的齿轮图标，为您要加入的地点分配带宽。

     2. 输入与您要加入的 **Prisma Access** 地点相关联的每个 **Compute Location**（计算地点）所需的 **Bandwidth Allocation**（带宽分配）。
     3. 等待带宽反映在页面顶部的 **Allocated Total**（分配的总带宽量）字段中；然后单击 **OK**（确定）。

   - 要加入按地点分配带宽的远程网络，请继续执行下一步；在远程网络加入期间分配带宽。

4. 选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Remote Networks**（远程网络），创建四个远程网络连接，指定以下设置：

   - 为每个连接选择相同的 **Location**（地点）。
   - 选择 **IPSec Termination Node**（IPSec 终止节点）。

     为每个远程网络连接选择单独的 IPSec 终止节点。

     如果您的部署按地点分配带宽，请选择 ***500 Mbps*** 的 ***Bandwidth***（带宽）。

     您选择的带宽不能超过您已获得许可的总带宽量。使用此设置定义要分配给此地点的总许可带宽量。

   - **Enable**（启用）BGP，选择 **Advertise Default Route**（通告默认路由）和 **Don't Advertise Prisma Access Routes**（不通告 **Prisma Access** 路由）。
   - 为所有远程网络连接指定相同的 **Peer AS**（对等 **AS**）。

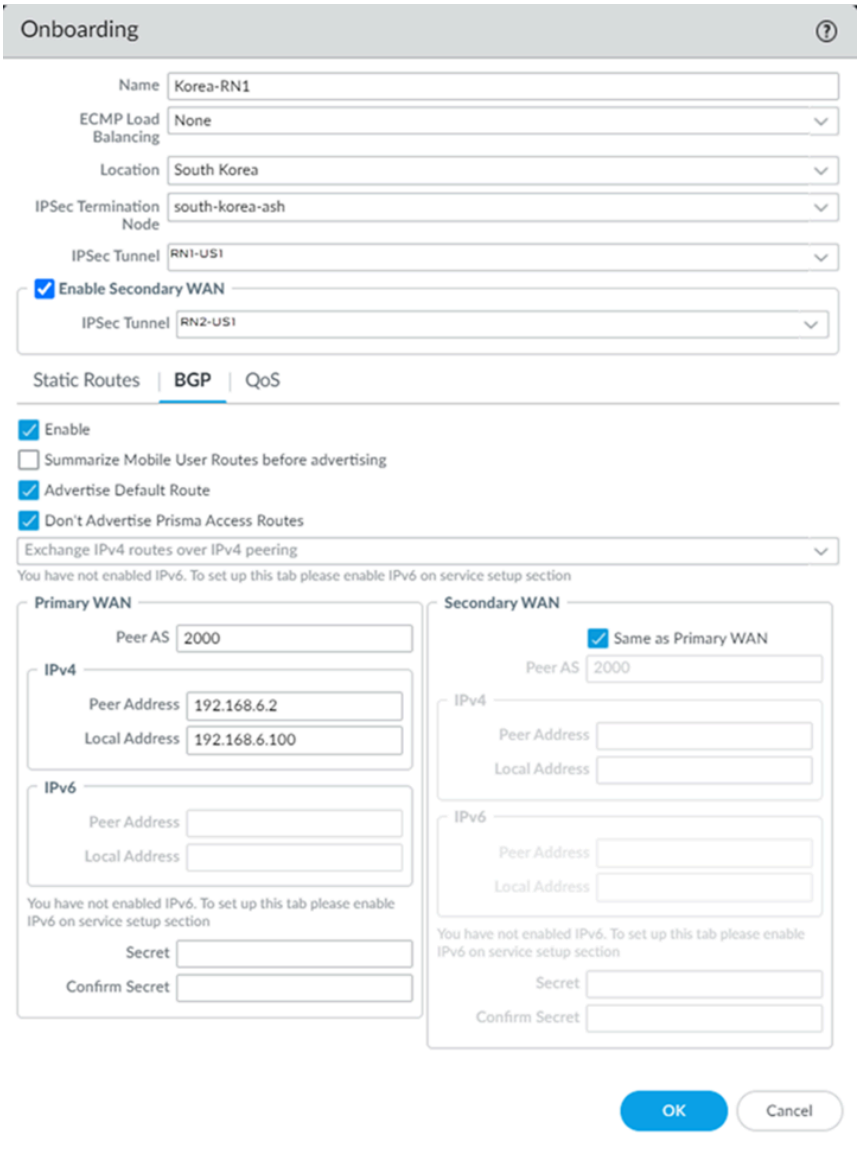
©2025 Palo Alto Networks, Inc.

此示例显示 **Peer AS**（对等 **AS**）为 2000；在此示例中，您为所有四个连接选择的 **Peer AS**（对等 **AS**）为 2000。

- （可选）如果您想要创建备份远程网络，请选择 **Enable Secondary WAN**（启用辅助广域网）来创建一个；然后选择您为备份隧道创建的 **IPSec Tunnel**（**IPSec** 隧道）。

以下部署不支持配置辅助 WAN：

- 如果您的辅助 WAN 的主 IPSec 隧道设置为主动-主动模式。
- 如果您的客户端设备 (CPE) 的主 IPSec 隧道和辅助 IPSec 隧道设置为等价多路径 (ECMP) 配置。

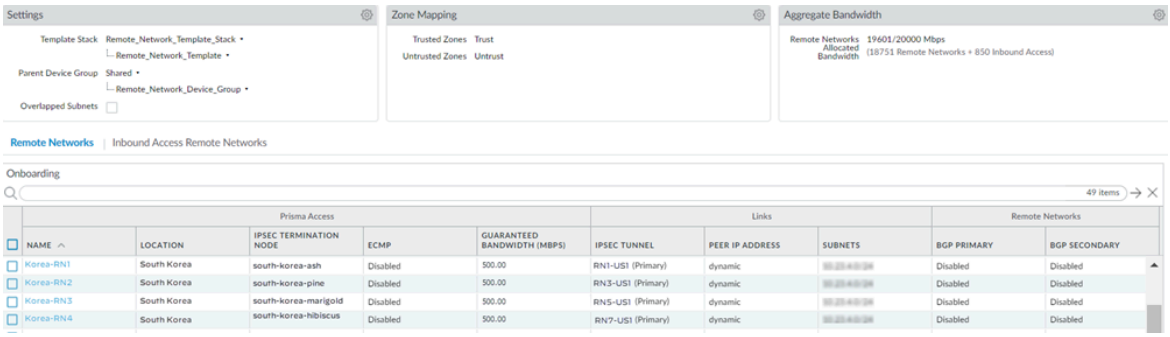


完成后，同一地点将拥有四个带宽为 1000 Mbps 的远程网络连接。

由于按地点分配带宽的部署的最大带宽为 500 Mbps，因此，此配置将为每个地点提供 500 Mbps 的带宽。

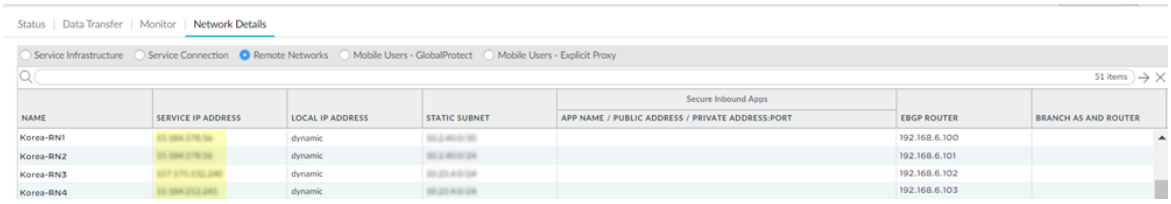
如果配置了备份隧道，则还有四个辅助隧道可用于故障转移。

 ©2025 Palo Alto Networks, Inc.



5. 选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息） > **Remote Networks**（远程网络），记下 **Service IP Address**（服务 **IP** 地址）和 **EBGP Router**（**EBGP** 路由器）地址。

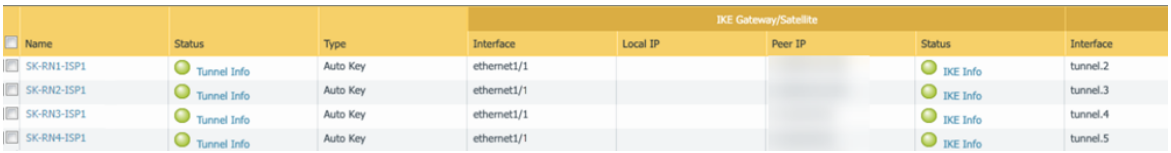
   当您在远程网络站点的 CPE 上配置 IPSec 隧道时，使用 **Service IP Address**（服务 **IP** 地址）作为对等体 IP 地址；当您在 CPE 上创建静态路由时，使用这些地址和 **EBGP Router**（**EBGP** 路由器）地址。



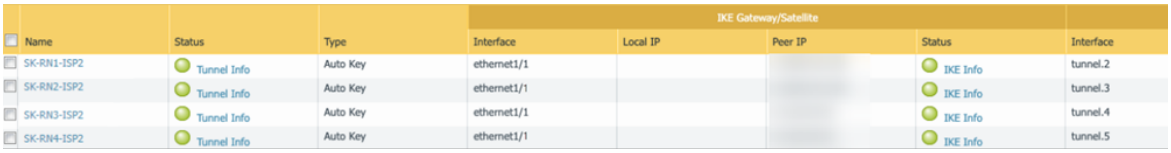
STEP 2 | 在远程网络站点的 CPE 上，配置远程网络隧道。

- 这些步骤中的配置使用 *Palo Alto Networks* 新一代防火墙；您可以使用支持 *IPSec* 隧道和 *ECMP* 的任何 *CPE* 设备进行此部署。
- 带宽是否平衡取决于 *ECMP* 的 *CPE* 哈希。但是，*Prisma Access* 可确保流量的对称返回。

1. 创建从活动 CPE 到四个网络连接的四个活动隧道。对于 **Peer IP**（对等体 **IP**）地址，请输入您在上一步中从 Prisma Access 收到的远程网络的 **Service IP Address**（服务 **IP** 地址）。



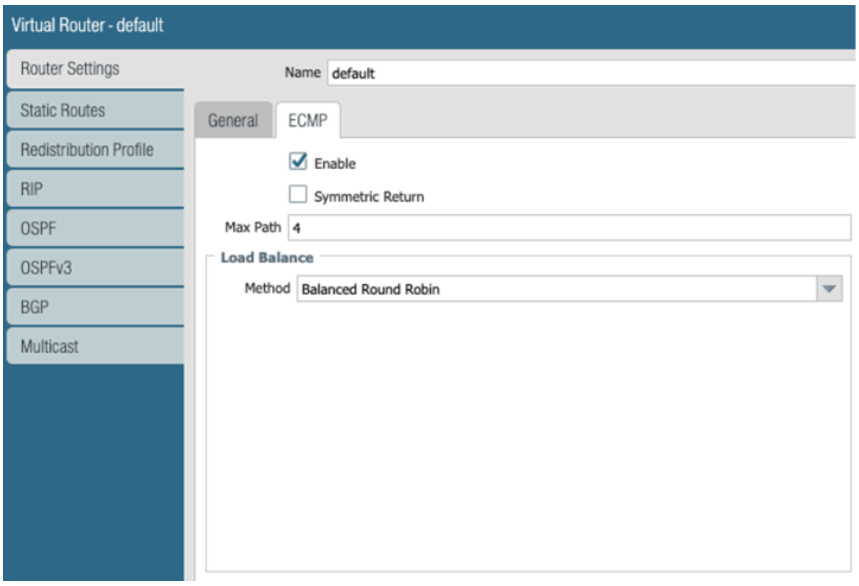
2. （可选）如果创建备份隧道，请创建从活动 CPE 到四个网络连接的四个备份隧道。对于 **Peer IP**（对等体 **IP**）地址，请输入您在上一步中从 Prisma Access 收到的远程网络的 **Service IP Address**（服务 **IP** 地址）。



 ©2025 Palo Alto Networks, Inc.

STEP 3 | 在远程网络站点的 CPE 上配置 ECMP。

1. 选择 **Network**（网络） > **Virtual Routers**（虚拟路由器）。
2. 选择 **default**（默认）虚拟路由器或 **Add**（添加）新的虚拟路由器。
3. 选择 **Router Settings**（路由器设置） > **Enable**（启用） > **ECMP**，然后 **Enable**（启用）ECMP，将 **Max Path**（最大路径）设置为 **4**，在负载均衡 **Method**（方法）中选择 **Balanced Round Robin**（平衡轮询调度）。

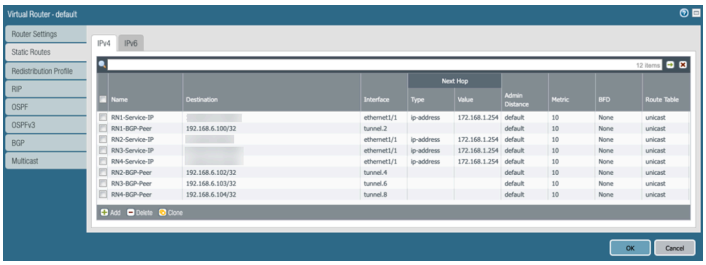


STEP 4 | 在远程网络站点的 CPE 上，创建指向您在上一步中检索到的 Prisma Access **Service IP Address**（服务 **IP** 地址）和 **EBGP Router**（**EBGP** 路由器）IP 地址的静态路由。

如前所述，此配置需要使用 BGP 的动态路由。为了方便在 CPE 和 Prisma Access 的 eBGP 路由器之间建立 BGP 连接，您需要为 CPE 上的 eBGP 路由器 IP 地址添加静态路由，并且下一跳必须是 CPE 上的隧道接口。您必须对其余隧道上的所有其他远程网络 eBGP 路由器 IP 地址重复此步骤。

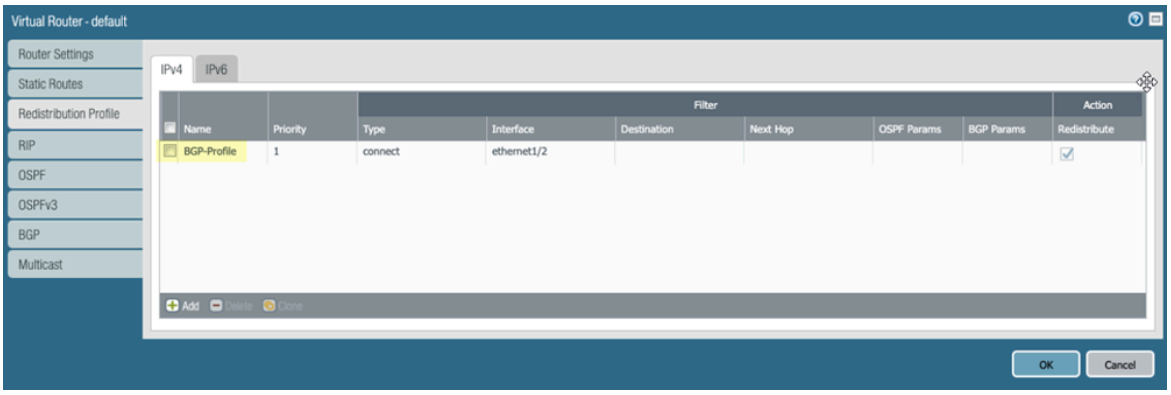
以下示例显示了活动 CPE 上的路由。如果您在备用 CPE 上创建了备份隧道，请在备用 CPE 上创建相同的路由。

如果要配置 Palo Alto Networks 新一代防火墙，请选择 **Static Routes**（静态路由） > **IPv4** 以添加静态路由。

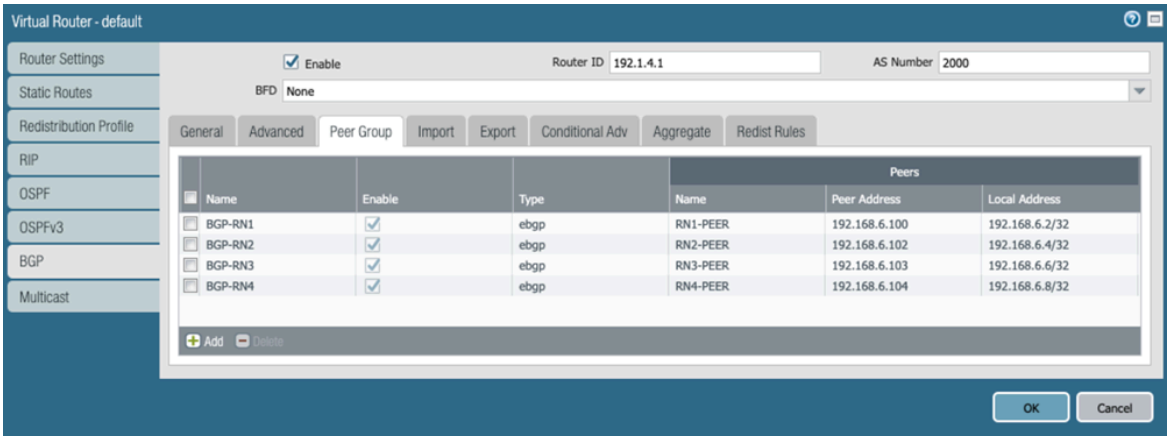


 ©2025 Palo Alto Networks, Inc.

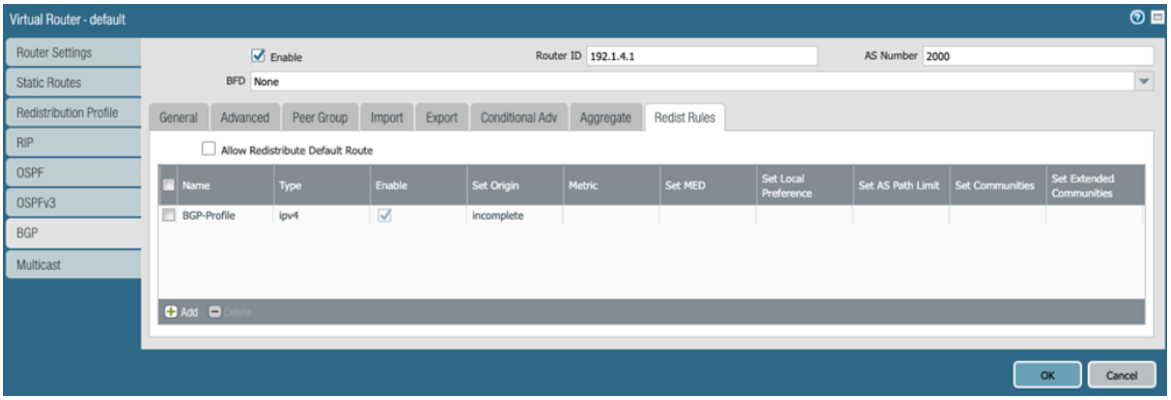
STEP 5 | 通过选择 **Redistribution Profile**（重新分发配置文件） > **IPv4**，在 CPE 上启用路由重新分发，然后 **Add**（添加）IPv4 路由重新分发配置文件。



STEP 6 | 选择 **BGP** > **Peer Group**（对等体组），在虚拟路由器实例上 **Enable**（启用）BGP，然后 **Add**（添加）远程网络 BGP 对等体。



STEP 7 | 选择 **BGP** > **Redist Rules**（重新分发规则），然后附加您在上一步中创建的路由重新分发配置文件。



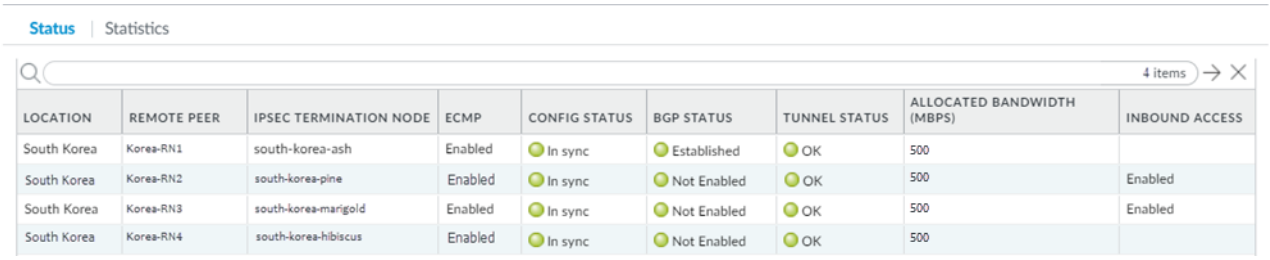
STEP 8 | 验证 CPE 是否在其所有四个隧道上传输流量。

 ©2025 Palo Alto Networks, Inc.

STEP 9 | 在 Prisma Access 中检查启用 ECMP 的连接的状态。

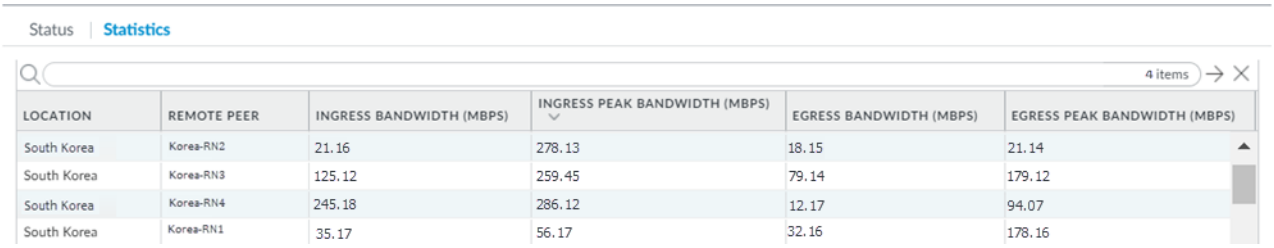
- 选择 **Panorama** > **Cloud Services**（云服务） > **Monitor**（监控） > **Remote Networks**（远程网络），选择部署 ECMP 连接的区域，然后选择 **Status**（状态）。

  - 在此区域中，***ECMP*** 显示为 ***No***（否）。这是意料之中的情况，因为您没有配置 *Prisma Access* ECMP 负载均衡功能。
  - *ECMP* 将流量从 *CPE* 定向传输到 *Prisma Access*，并且 *Prisma Access* 确保从 *CPE* 对称返回流量。



LOCATION	REMOTE PEER	IPSEC TERMINATION NODE	ECMP	CONFIG STATUS	BGP STATUS	TUNNEL STATUS	ALLOCATED BANDWIDTH (MBPS)	INBOUND ACCESS
South Korea	Korea-RN1	south-korea-ash	Enabled	In sync	Established	OK	500	
South Korea	Korea-RN2	south-korea-pine	Enabled	In sync	Not Enabled	OK	500	Enabled
South Korea	Korea-RN3	south-korea-marigold	Enabled	In sync	Not Enabled	OK	500	Enabled
South Korea	Korea-RN4	south-korea-hibiscus	Enabled	In sync	Not Enabled	OK	500	

- 选择 **Statistics**（统计信息），查看流量是否通过每个远程网络隧道。



LOCATION	REMOTE PEER	INGRESS BANDWIDTH (MBPS)	INGRESS PEAK BANDWIDTH (MBPS)	EGRESS BANDWIDTH (MBPS)	EGRESS PEAK BANDWIDTH (MBPS)
South Korea	Korea-RN2	21.16	278.13	18.15	21.14
South Korea	Korea-RN3	125.12	259.45	79.14	179.12
South Korea	Korea-RN4	245.18	286.12	12.17	94.07
South Korea	Korea-RN1	35.17	56.17	32.16	178.16

完成此工作流程后，即为远程网络创建了高带宽配置。请谨记，此解决方案仅支持出站流量。

©2025 Palo Alto Networks, Inc.

©2025 Palo Alto Networks, Inc.

Prisma Access for Clean Pipe

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

使用 *Prisma Access for Clean Pipe*，快速轻松地配置多个干净的出站互联网连接实例。

不支持用于 *Prisma Access (Managed by Strata Cloud Manager)*。

Prisma Access for Clean Pipe 概述

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

为了让管理其他组织的 IT 基础架构的组织（例如服务提供商、MSSP 或电信公司）能够快速轻松地保护其租户的出站互联网流量，Palo Alto Networks 提供 Prisma Access for Clean Pipe。服务提供商、MSSP 或电信公司可以使用合作伙伴互连将其客户（配置为租户）路由到 Prisma Access for Clean Pipe。流量通过合作伙伴互连后，将发送到租户专用的 Clean Pipe 实例以确保安全，然后再路由到互联网。

Prisma Access for Clean Pipe 还提供一个 API，您可以使用它快速轻松地为租户创建 Clean Pipe。

Clean Pipe 用例

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

如果您满足以下所有用例，请使用 Prisma Access for Clean Pipe：

- 您管理着拥有大量租户的网络部署。

  例如，假设您是服务提供商、电信公司或 MSSP，负责管理和维护许多不同组织（多达数万个）的网络。
- 您希望为部署中的每个租户提供一种方法，以保护其出站互联网流量。
- 您需要一种快速且可扩展的方式来为您管理其网络的组织加入 Clean Pipe。
- 除了出站互联网安全之外，您在保护您所管理网络的移动用户、总部或分支机构位置方面没有额外的要求。

  如果您有额外的安全要求，我们建议您在 Prisma Access 中创建多个租户，而不是实施 Clean Pipe，以便您为单独的远程网络和移动用户组创建和强制执行安全配置文件。

Clean Pipe 示例

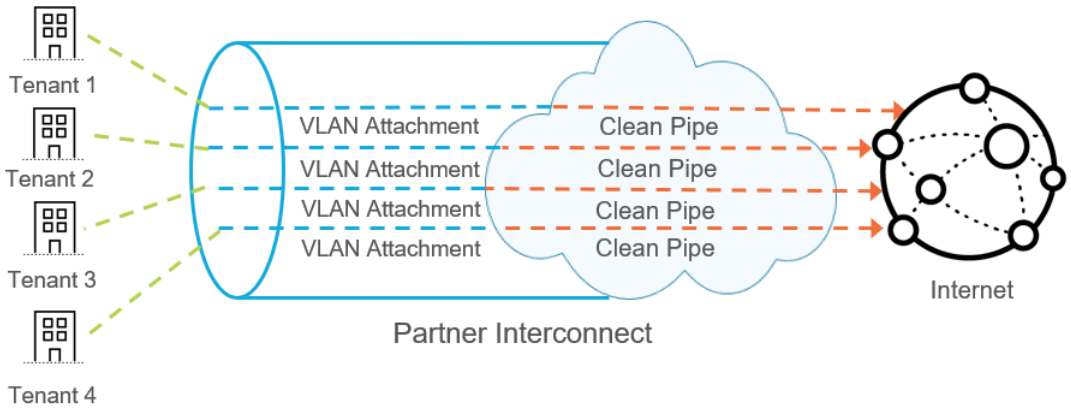
在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

下图提供了为单个租户配置的 Clean Pipes 示例，在该示例中为该租户配置了多个 Clean Pipe。

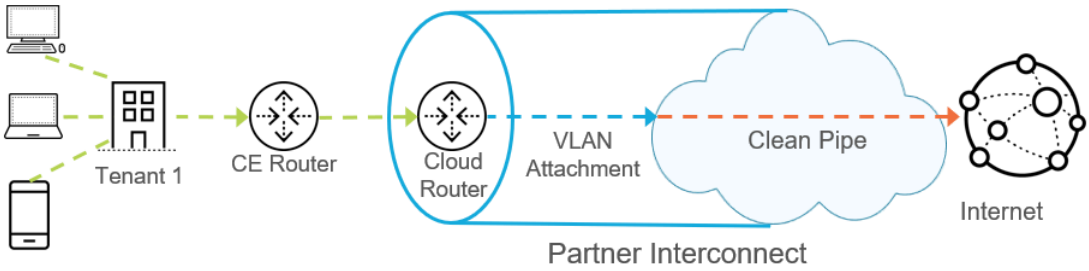
在此示例中，服务提供商管理四个组织的互联网连接，并希望保护这些组织的出站互联网接入。服务提供商创建 Google Cloud Platform (GCP) 合作伙伴互连，并为每个租户创建 VLAN 连接。服务提供商使用 Panorama 配置 Prisma Access for Clean Pipe，以实现 VLAN 连接的安全。

©2025 Palo Alto Networks, Inc.

在此示例中，为每个租户配置一个 Clean Pipe。您还可以在单个租户中创建多个 Clean Pipe。确保您为租户指定的每个 Clean Pipe 使用不同的位置。



下图更详细地展示了需要干净的互联网连接的租户的单个 Clean Pipe。客户边缘 (CE) 路由器为租户提供 WAN 连接。CE 路由器连接到云路由器，云路由器为合作伙伴互连提供连接。服务提供商为租户创建 VLAN 连接，并在 Panorama 中配置 Prisma Access for Clean Pipe 以实现 VLAN 连接的安全，从而保护租户的基于互联网的流量。



Clean Pipe 和合作伙伴互连要求

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	❑ Prisma Access 许可证

开始之前，请注意以下 Clean Pipe 部署要求，并注意 Prisma Access for Clean Pipe 与其他 Prisma Access 部署之间的以下差异：

- 您必须拥有 Prisma Access for Clean Pipe 许可证。

  Prisma Access for Clean Pipe 许可证是独立于其他 Prisma Access 产品的许可证。但是，购买和安装 Panorama 和 Strata Logging Service 许可证的要求也同样适用于 Clean Pipe。

©2025 Palo Alto Networks, Inc.

- Prisma Access for Clean Pipe 具有以下 GCP 合作伙伴互连要求：
  - 您必须能够在 GCP 中创建合作伙伴互连。
  - 您必须能够在 GCP 中创建 VLAN 连接。
  - 对于第 2 层 (L2) 合作伙伴互连，您必须能够访问 MSSP 端的客户边缘 (CE) 路由器，并能够对其进行配置更改。

  有关 GCP 配置的更多信息，请参阅 GCP 文档。
- 请注意 Clean Pipe 部署的最低带宽要求。

  您可以购买的最小许可证为 1000 Mbps。为每个 Clean Pipe 租户分配的最低带宽为 100 Mbps。

  创建租户后，您可以在该租户中创建 Clean Pipe。每个 Clean Pipe 的最低带宽必须为 100 Mbps。每个 Clean Pipe 共享该租户的访问域、模板和模板堆栈以及设备组。
- 如果为单个租户配置多个 Clean Pipe，则每个 Clean Pipe 都必须位于唯一位置。如果要在主用/备用配置中为单个 Clean Pipe 位置配置两个 VLAN 连接以实现服务区内冗余，请在添加新的 Clean Pipe 实例时指定 **REDUNDANT**（冗余）选项。
- 在 Clean Pipe 租户内创建连接时，带宽分配需与 VLAN 连接的带宽分配相一致。请勿创建带宽高于或低于连接带宽的 VLAN 连接。
- 启用多租户后，请勿使用配置区域中的任何其他选项卡配置 Clean Pipe 部署，**Service Setup**（服务设置）选项卡中的 **Generate API key**（生成 **API** 密钥）链接除外，使用该链接可生成 API 密钥以检索 Clean Pipe IP 地址。所有配置都是 Prisma Access for Clean Pipe 独有的，独立于其他 Prisma Access 部署（例如 Prisma Access for Networks 或 Prisma Access for Users）。
- 提交 Clean Pipe 配置后，请勿对其进行更改。如果在提交 Clean Pipe 后对其进行更改，则在重新提交时您会收到提交错误。相反，请删除现有的 Clean Pipe 并添加新的 Clean Pipe。请将此更改安排在系统停机时段进行。如果您已进行更改但尚未提交，则可以通过将 Clean Pipe 配置编辑回以前的值来恢复更改。

©2025 Palo Alto Networks, Inc.

- 请注意，Clean Pipe 使用的位置与其他 Prisma Access 部署有所不同。 Prisma Access for Clean Pipe 支持以下位置：
  - 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
- 请注意 Clean Pipe 的以下网络限制：
  - 仅在入口（从互联网到 Clean Pipe 方向）支持 Clean Pipe 的 QoS。
  - 不支持 User-ID。
  - Clean Pipe 支持基于源和目标 IP 地址的会话保持，并且不可配置。
  - Trust-to-Trust 策略对 Clean Pipe 无效，因为流量始终绑定到互联网。仅可使用 Trust-to-Untrust 策略。

 ©2025 Palo Alto Networks, Inc.

完成 Clean Pipe 配置

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	• Prisma Access 许可证

要完成 Prisma Access for Clean Pipe 的配置，您需要在合作伙伴互连和 Panorama 中执行配置。

确保您可以访问和配置合作伙伴互连（非 *Prisma Access*）端的 *CE* 和云路由器。

STEP 1 | 在配置的合作伙伴互连端，使用从 Panorama 检索的 **Pairing Key**（配对密钥）创建 VLAN 连接。

有关通过合作伙伴互连创建 VLAN 连接以及配置客户边缘 (CE) 路由器以与云路由器通信的更多信息，请参阅 Google Cloud 文档：https://cloud.google.com/interconnect/docs/

确保所选择的位置和带宽与您在 Panorama 中指定的 **Location**（位置）相匹配。您用于合作伙伴互连的服务提供商使用配对密钥以及您请求的连接位置和容量来完成 VLAN 连接的配置。

STEP 2 | 连接建立后，返回 Panorama，选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Network Details**（网络详细信息） > **Clean Pipe**，并记下 **MSSP CE** 和 **Cloud Router IP**（云路由器 **IP**）地址。

在 VLAN 连接的另一端输入 **Pairing Key**（配对密钥）后，系统将会填充这些值。



STEP 3 | 登录到 CE 路由器并执行以下配置。

1. 输入 **MSSP CE** 地址作为本地 IP 地址。
2. 输入 **Cloud Router IP**（云路由器 **IP**）地址作为对等体 IP 地址。
3. 输入与您在 Panorama 中配置 Clean Pipe 时输入的 **BGP Peer ASN**（**BGP** 对等体 **ASN**）匹配的 BGP ASN。

   确保您正确输入这些值；这些值无法更改。

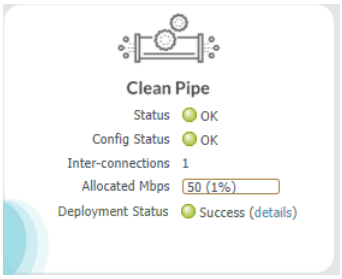
 ©2025 Palo Alto Networks, Inc.

STEP 4 | 检查 Clean Pipe 状态。

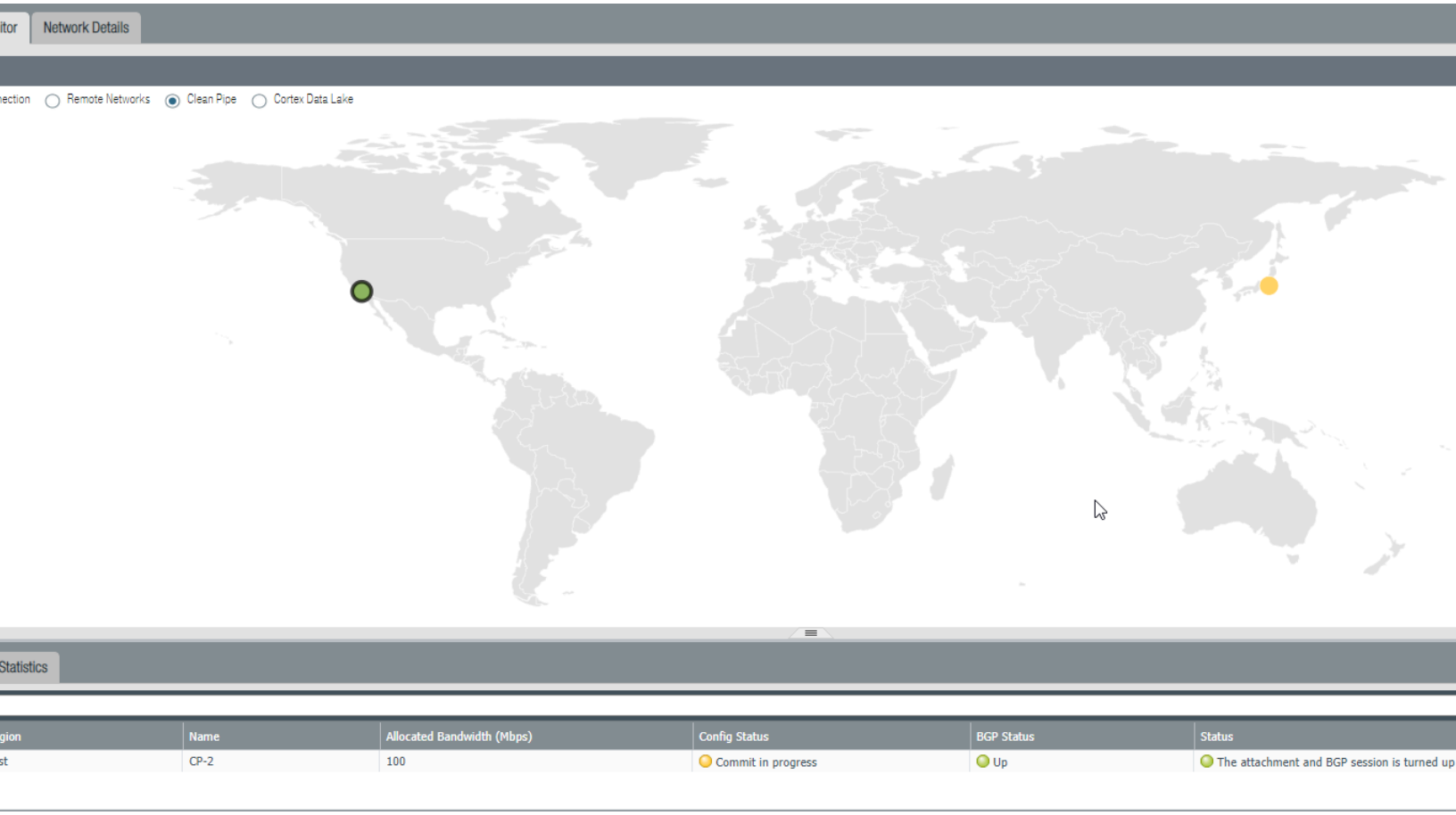
1. 在 Panorama 中，选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态），从下拉列表中选择 **Tenant**（租户），并检查 Clean Pipe 的 **Status**（状态）。

   查看 Prisma Access 地点列表，了解可接受的值。

   在 **Deployment Status**（部署状态）区域中，您可以在载入和部署作业完成前查看其进度，以及查看有关已完成作业的状态的更多信息。有关详细信息，请参阅部署进度和状态。



2. 选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态） > **Clean Pipe**，然后单击 **Monitor**（监控）选项卡，查看包含已部署 Clean Pipe 的状态的地图。



单击地图下方的选项卡，查看 Clean Pipe 的其他统计信息。

Status（状态）选项卡：

 ©2025 Palo Alto Networks, Inc.

- **Compute Region**（计算区域）— 为 Clean Pipe 实例部署云服务基础架构的计算区域。
- **Name**（名称）— Clean Pipe 实例的名称。
- **Allocated Bandwidth (Mbps)**（分配的带宽 **(Mbps)**）— 您为 Clean Pipe 实例分配的带宽量。
- **Config Status**（配置状态）— 您上次推送到服务的配置的状态。如果您在本地进行了更改，但尚未将配置推送到云端，则状态显示 **Out of sync**（不同步）。将鼠标悬停在状态指示器上，以获取更多详细信息。提交配置并将其推送到 Prisma Access 后，配置状态更改为 **In sync**（同步）。
- **BGP Status**（**BGP** 状态）— 显示有关 Clean Pipe 实例的防火墙或路由器与 Prisma Access 之间的 BGP 状态的信息。虽然您可能会暂时看到状态经历各种 BGP 状态（**idle**（空闲）、**active**（活跃）、**open send**（**Open** 消息发送）、**open pend**（**Open** 消息待处理）、**open confirm**（**Open** 消息确认）），但最常见的情况是，BGP 状态显示：
  - **Connect**（连接）— Clean Pipe 实例的路由器正在尝试与云防火墙建立 BGP 对等体关系。
  - **Established**（已建立）— BGP 对等体关系已建立。

    如果 BGP 连接处于错误状态，此字段还会显示：
  - 警告 — 超过八分钟没有 BGP 状态更新。这可能表示防火墙中断。

 ©2025 Palo Alto Networks, Inc.

  - **Error**（错误）— BGP 状态未知。
- **Status**（状态）— Prisma Access 和 Clean Pipe 实例之间的连接的运行状态。

Statistics（统计信息）选项卡：

- **Region**（区域）— 为 Clean Pipe 实例部署云服务基础架构的区域。
- **Name**（名称）— Clean Pipe 实例的名称。
- **Allocated Bandwidth (Mbps)**（分配的带宽 **(Mbps)**）— 您为远程网络位置分配的带宽量。
- **QoS** — 选择 **QoS** 以显示包含图形 QoS 统计信息的页面。
- **Avg Egress Bandwidth 5 Min (Mbps)**（**5** 分钟内的平均出口带宽 **(Mbps)**）— 5 分钟内 Clean Pipe 的平均出口带宽量。
- **Avg Egress Bandwidth 60 Min (Mbps)**（**60** 分钟内的平均出口带宽 **(Mbps)**）— 60 分钟内 Clean Pipe 的平均出口带宽量。
- **Avg Ingress Bandwidth 5 Min (Mbps)**（**5** 分钟内的平均入口带宽 **(Mbps)**）— 5 分钟内 Clean Pipe 的平均入口带宽量。
- **Avg Ingress Bandwidth 60 Min (Mbps)**（**60** 分钟内的平均入口带宽 **(Mbps)**）— 60 分钟内 Clean Pipe 的平均入口带宽量。
- **Egress Peak Bandwidth 1 Hour (Mbps)**（**1** 小时内的出口峰值带宽 **(Mbps)**）— 过去 1 小时内 Clean Pipe 实例的峰值出口带宽量。
- **Egress Peak Bandwidth 24 Hour (Mbps)**（**24** 小时内的出口峰值带宽 **(Mbps)**）— 过去 24 小时内 Clean Pipe 实例的峰值出口带宽量。
- **Egress Peak Bandwidth 7 Days (Mbps)**（**7** 天内的出口峰值带宽 **(Mbps)**）— 过去 7 天内 Clean Pipe 实例的峰值出口带宽量。
- **Egress Peak Bandwidth 30 Days (Mbps)**（**30** 天内的出口峰值带宽 **(Mbps)**）— 过去 30 天内 Clean Pipe 实例的峰值出口带宽量。
- **Ingress Peak Bandwidth 1 Hour (Mbps)**（**1** 小时内的入口峰值带宽 **(Mbps)**）— 过去 1 小时内 Clean Pipe 实例的峰值入口带宽量。
- **Ingress Peak Bandwidth 24 Hour (Mbps)**（**24** 小时内的入口峰值带宽 **(Mbps)**）— 过去 24 小时内 Clean Pipe 实例的峰值入口带宽量。
- **Ingress Peak Bandwidth 7 Days (Mbps)**（**7** 天内的入口峰值带宽 **(Mbps)**）— 过去 7 天内 Clean Pipe 实例的峰值入口带宽量。
- **Ingress Peak Bandwidth 30 Days (Mbps)**（**30** 天内的入口峰值带宽 **(Mbps)**）— 过去 30 天内 Clean Pipe 实例的峰值入口带宽量。

启用多租户并创建一个租户

在何处可以使用？	需要提供什么？
• Prisma Access (Managed by Panorama)	• Prisma Access 许可证

要开始 Clean Pipe 配置，请在 Panorama 中创建多租户部署并创建一个或多个租户。

 ©2025 Palo Alto Networks, Inc.

STEP 1 | 安装并激活 Prisma Access for Clean Pipe。

Prisma Access for Clean Pipe 需要单独的许可证，激活它会在云服务插件中创建特定于 Clean Pipe 的选项卡。安装 Prisma Access for Clean Pipe 的步骤与集合和安装 Prisma Access 许可证的步骤相同，包括安装云服务插件。

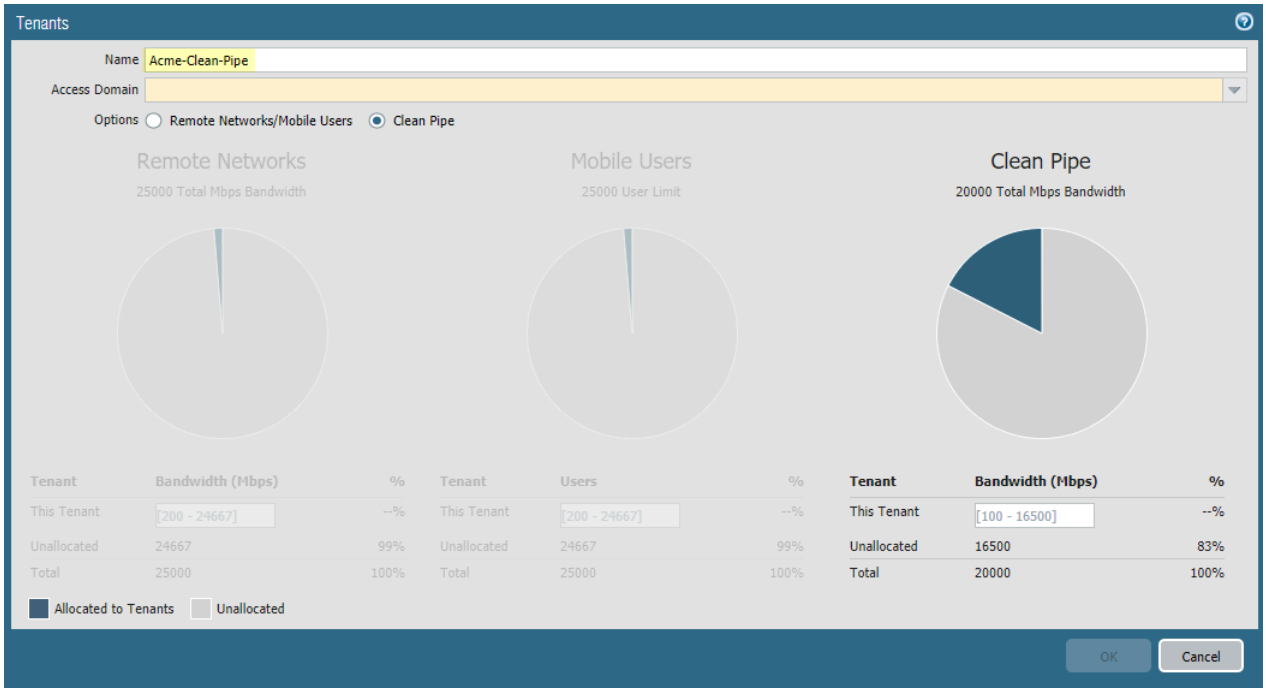
 ©2025 Palo Alto Networks, Inc.

STEP 2 | 启用多租户（如果尚未启用）。

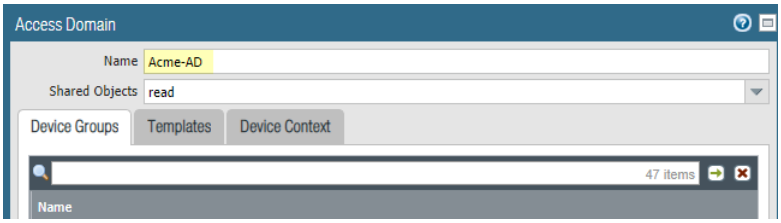
1. 选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置）。
2. 选择 **Enable Multitenancy**（启用多租户）（位于页面右上角）。
3. 单击 **OK**（确定）。

   此时将显示 **Tenants**（租户）页面。
4. 在 **Options**（选项）区域中，选择 **Clean Pipe**。

   要为远程网络和/或移动用户配置租户，请参阅 Prisma Access 中的“管理多个租户”。



5. 在 **Name**（名称）中输入第一个租户的名称。
6. 单击 **Access Domain**（访问域）为第一个租户创建并配置新的访问域，然后单击 **OK**（确定）。



7. 在 **Clean Pipe** 区域中 **Bandwidth (Mbps)**（带宽 **(Mbps)**）下面的 **This Tenant**（此租户）中，输入带宽。

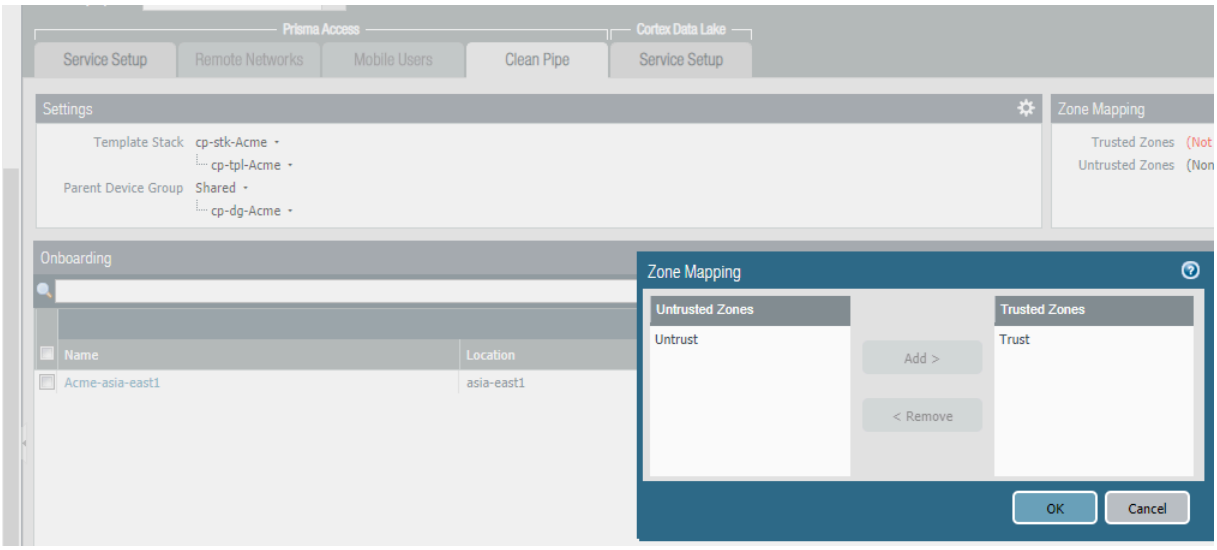
   为创建的每个租户输入至少 100 Mbps。
8. 单击 **OK**（确定）。

©2025 Palo Alto Networks, Inc.

STEP 3 | 为租户创建区域，并为租户映射这些区域。

1. 选择 **Network**（网络） > **Zones**（区域）。

   确保已为您创建的租户 **(cp-tpl-*tenant*)** 选择了 Clean Pipe 模板。
2. 为租户创建区域（例如，**Trust**（信任）和 **Untrust**（不信任））。
3. 选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置），然后从下拉列表中选择 **Tenant**（租户）。
4. 选择 **Clean Pipe** 选项卡。
5. 单击 **Zone Mapping**（区域映射）旁边的齿轮图标以编辑设置。
6. 单击 **Add**（添加）和 **Remove**（移除）以将您创建的区域映射到可信区域和不可信区域。



STEP 4 | 接入新的 Clean Pipe。

1. 在 Panorama 中，选择 **Panorama** > **Cloud Services**（云服务） > **Configuration**（配置） > **Clean Pipe**。
2. 单击 **Add**（添加）为租户添加新的 Clean Pipe 实例，输入以下信息：
   - **Name**（名称） — 指定 Clean Pipe 的名称。
   - **Bandwidth**（带宽） — 选择要为 Clean Pipe 分配的带宽。

     您可以以 100 Mbps、200 Mbps、300 Mbps、400 Mbps、500 Mbps、1000 Mbps、2000 Mbps、5000 Mbps 和 10000 Mbps 的增量接入 Clean Pipe 实例。您指

 ©2025 Palo Alto Networks, Inc.

定的带宽量必须在许可的带宽分配范围内，并且必须与您在伙伴互连中创建的 VLAN 附件的带宽相匹配。

- **Edge Availability Domain**（边缘可用性域） — 选择要用于 Clean Pipe 的可用性域。可以选择 **1**、**2**、**ANY**（任意）或 **REDUNDANT**（冗余）。
  - 对于非冗余 Clean Pipe 部署，请指定 **ANY**（任意）选项。

    确保您的云提供商支持此选择；您还必须在合作伙伴互连的云提供商一端选择 **ANY**（任意）。如果该选项不适用于您的云提供商，请选择其他选项。
  - 要在同一位置的活跃/备用配置中指定位于同一位置的两个 VLAN 连接，请选择 **REDUNDANT**（冗余）。

    Prisma Access 为 **REDUNDANT**（冗余）配置创建两个配对密钥（每个可用性区域一个），并在 Clean Pipe 名称后附加 `zone1`（对应第一个可用性区域）和 `zone2`（对应第二个可用性区域）。例如，如果将 **Name**（名称）指定为 **San Francisco**（旧金山），则 Prisma Access 会创建两个区域，分别名为 **San Francisco-zone1** 和 **San Francisco-zone2**。

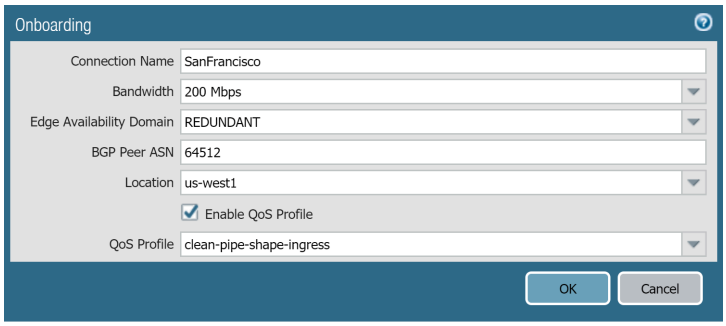
    请确保将第一个可用性区域 *(zone1)* 配置为 *CPE* 上的主要区域。

  您还可以为不同位置的单个租户冗余构建一对 Clean Pipe；为此，请为一个位置的第一个 Clean Pipe 指定 **1**，为不同位置的第二个 Clean Pipe 指定 **2**。
- **BGP Peer ASN**（**BGP** 对等 **ASN**） — 输入 BGP 自治系统编号 (ASN)。

  可以指定专用或公用 BGP ASN。

  记下此值；完成 Clean Pipe 配置后，在客户边缘 (CE) 路由器上配置此值。
- **Location**（位置） — 选择位置。

  我们建议您使用为伙伴互连创建 VLAN 连接时所使用的相同位置。
- 要启用 QoS，请选择 **QoS**，然后选择用于 Clean Pipe 的 QoS 配置文件。Clean Pipe QoS 在入口处进行调整。



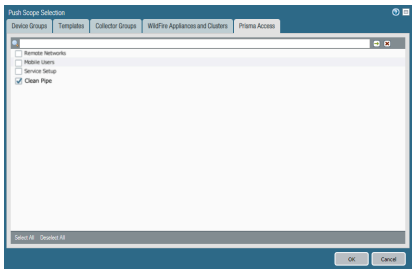
STEP 5 | 重复步骤 4，根据需要添加更多 Clean Pipe 实例。

确保每个额外的 Clean Pipe 使用不同的位置。

©2025 Palo Alto Networks, Inc.

STEP 6 | 提交并推送您的更改，使其在 Prisma Access 中处于活动状态。

1. 选择 **Commit**（提交） > **Commit and Push**（提交并推送）和推送范围中的 **Edit Selections**（编辑选择）。
2. 选择 **Prisma Access**，选择 **Clean Pipe**。



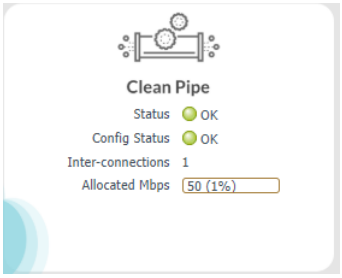
3. 单击 **OK**（确定）保存对推送范围所作的更改。
4. **Commit**（提交）并 **Push**（推送）您的更改。

STEP 7 | 检查您的 Clean Pipe 是否已配置。

1. 选择 **Panorama** > **Cloud Services**（云服务） > **Status**（状态）。
2. 从页面顶部的下拉列表中选择 **Tenant**（租户）。
3. 单击 **Status**（状态）。

   此时将显示 Clean Pipe 的状态。
4. 将鼠标悬停在 Clean Pipe 的 **Config Status**（配置状态）上，等待状态从 **Provisioning in Progress**（正在进行配置）变为 **Provisioned**（已配置）。

   配置最多可能需要 30 分钟。



STEP 8 | 单击 **Network Details**（网络详细信息）选项卡，单击 **Clean Pipe** 单选按钮，并记下 **Pairing Key**（配对密钥）中显示的值。

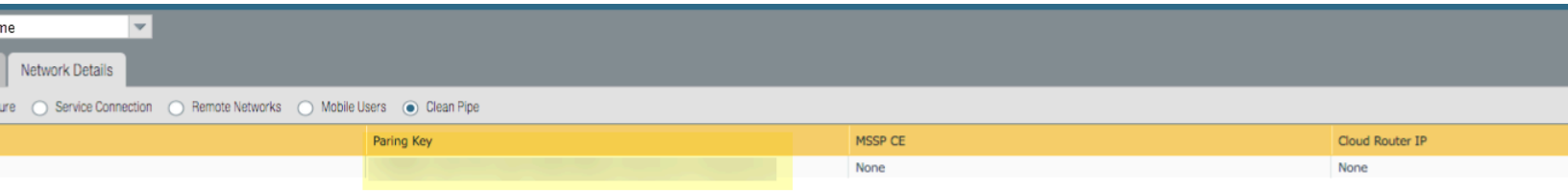
开始配置 Clean Pipe 时，**MSSP CE** 和 **Cloud Router IP**（云路由器 **IP**）字段为空。完成 \Clean Pipe 配置并创建了 VLAN 连接后，将会填充这些字段。

如果您指定了 **REDUNDANT**（冗余）连接，Prisma Access 将创建两个配对密钥，每个可用性区域一个，并在 Clean Pipe 名称后附加 zone1（对应第一个可用性区域）和 zone2（对应第二个可用性区域）。下面的屏幕截图显示了具有冗余配置的 **SanFrancisco** Clean Pipe。Prisma

©2025 Palo Alto Networks, Inc.

Access 已创建两个配对密钥，一个用于 **SanFrancisco-zone1**，另一个用于 **SanFrancisco-zone2**。

请确保将第一个可用性区域 *(zone1)* 配置为 *CPE* 上的主要区域。



STEP 9 | 完成 Clean Pipe 配置。

©2025 Palo Alto Networks, Inc.

 ©2025 Palo Alto Networks, Inc.